aws

デベロッパーガイド

Amazon Elastic Container Service

Amazon Elastic Container Service: デベロッパーガイド

Table of Contents

Amazon Elastic Container Service とは

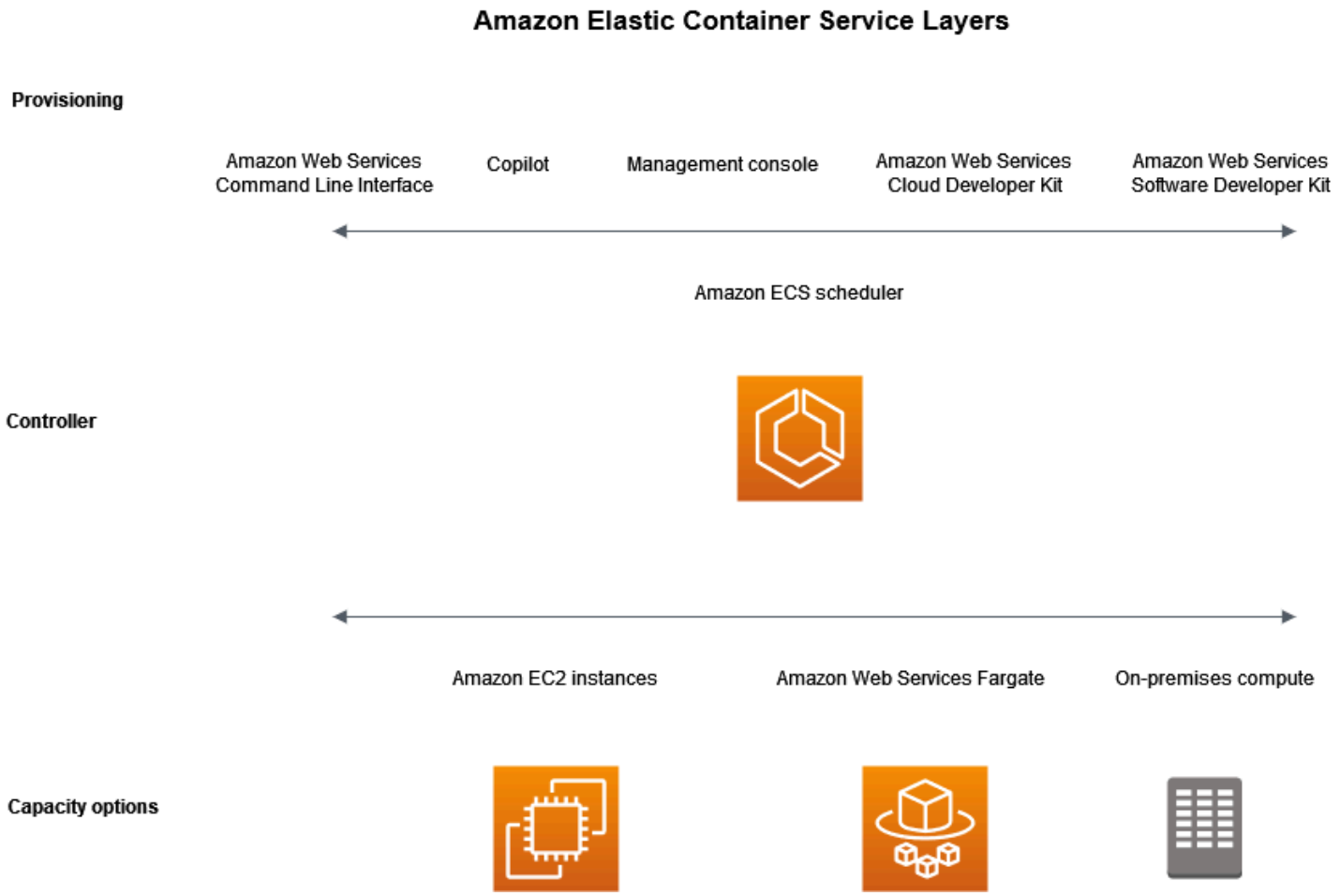
Amazon Elastic Container Service (Amazon ECS) は、コンテナ化されたアプリケーションを簡単にデプロイ、管理、スケーリングできる、完全マネージド型のコンテナオーケストレーションサービスです。フルマネージドサービスである Amazon ECS には、AWS の設定と運用に関するベストプラクティスが組み込まれています。Amazon Elastic Container Registry などの AWS ツールと Docker などのサードパーティーツールの両方に統合されています。この統合により、チームは環境ではなくアプリケーションの構築に集中しやすくなります。コントロールプレーンの複雑な管理は必要なく、クラウドの AWS リージョン 間またはオンプレミスで、コンテナワークロードを実行およびスケーリングできます。

Amazon ECS の用語とコンポーネント

Amazon ECS には次の 3 つのレイヤーがあります。

- キャパシティ - コンテナが稼働するインフラストラクチャ
- コントローラー - コンテナ上で実行されるアプリケーションをデプロイして管理します
- プロビジョニング - スケジューラーと連携してアプリケーションやコンテナをデプロイおよび管理するために使用できるツール

Amazon のレイヤーは以下の図のようになります。



Amazon ECS キャパシティ

Amazon ECS キャパシティは、コンテナが稼働するインフラストラクチャです。以下は、キャパシティオプションの概要です。

- クラウド内 AWS の Amazon EC2 instances

  インスタンスタイプ、インスタンス数を選択し、キャパシティを管理します。
- AWS クラウドでの (AWS Fargate) サーバーレス

  Fargate はサーバーレスの従量制料金計算エンジンです。Fargate を使用すると、サーバーを管理したり、キャパシティ計画に対処したり、セキュリティのためにコンテナワークロードを分離したりする必要がなくなります。
- オンプレミス仮想マシン (VM) またはサーバー

  Amazon ECS Anywhere は、オンプレミスサーバーや仮想マシン (VM) などの外部インスタンスを Amazon ECS クラスターに登録するためのサポートを提供します。

キャパシティは次の AWS リソースのいずれかに配置できます。

- アベイラビリティーゾーン
- ローカルゾーン
- Wavelength Zone
- AWS リージョン
- AWS Outposts

Amazon ECS コントローラ

Amazon ECS スケジューラは、アプリケーションを管理するソフトウェアです。

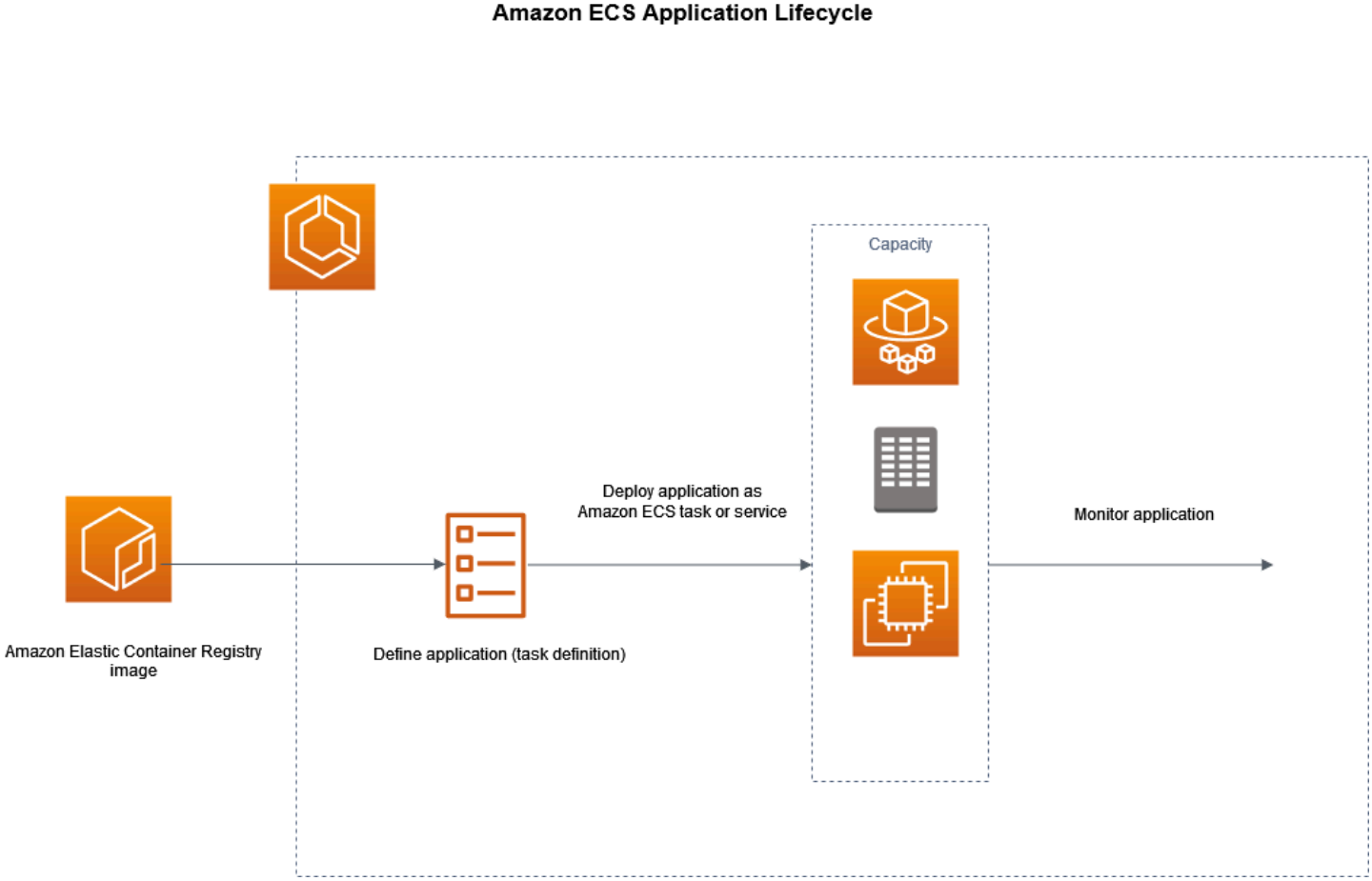
Amazon のプロビジョニング

Amazon ECS のプロビジョニングには複数のオプションがあります。

- AWS Management Console — Amazon ECSリソースへのアクセスに使用するウェブインターフェイスを提供します。
- AWS Command Line Interface (AWS CLI) — Amazon ECSを含む一連のさまざまな AWS サービス用のコマンドを提供します。Windows、Mac、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 SDK — 言語固有の API を提供し、接続の詳細の多くを処理します。これらには、署名の計算、リクエストの再試行処理、エラー処理などを含みます。詳細については、AWS SDK を参照してください。
- Copilot — Amazon ECS で本番稼働可能なコンテナ化されたアプリケーションを構築、リリース、運用するためのオープンソースツールをデベロッパーに提供します。この詳細については、GitHub ウェブサイトの Copilot を参照してください。
- AWS CDK - 使い慣れたプログラミング言語を使用して、クラウドアプリケーションリソースをモデル化およびプロビジョニングするために使用できるオープンソースのソフトウェア開発フレームワークを提供します。AWS CDK は、AWS CloudFormation を通じて安全かつ繰り返し可能な方法でリソースをプロビジョニングします。

アプリケーションのライフサイクル

次の図は、アプリケーションのライフサイクルと Amazon ECS コンポーネントとの連携を示しています。



アプリケーションをコンテナ上で実行できるように設計する必要があります。コンテナとは、ソフトウェアアプリケーションの実行に必要なものをすべて保持する、標準化されたソフトウェア開発の単位です。これには、関連するコード、ランタイム、システムツール、およびシステムライブラリが含まれます。コンテナは、イメージと呼ばれる読み取り専用テンプレートから作成されます。イメージは通常 Dockerfile から構築されます。Dockerfile は、コンテナを構築するための手順を含むプレーンテキストファイルです。これらのイメージは、Amazon ECR など、構築された後にダウンロード可能な場所であるレジストリに保存されます。

イメージを作成して保存した後、Amazon ECS のタスク定義を作成します。タスク定義はアプリケーションのブループリントです。これは、アプリケーションを形成するパラメータと 1 つ以上のコンテナを記述する JSON 形式のテキストファイルです。例えば、オペレーティングシステムのパラメータ、使用するコンテナ、アプリケーションで開くポート、タスクのコンテナで使用するデータボリュームなどの指定に使用できます。タスク定義で使用できる特定のパラメータは、お客様の特定のアプリケーションのニーズによって異なります。

タスク定義を定義したら、それをサービスまたはタスクとしてクラスターにデプロイします。クラスターは、クラスターに登録されているキャパシティインフラストラクチャ上で実行されるタスクまたはサービスを論理的にグループ化したものです。

タスクはクラスター内のタスク定義のインスタンス化です。スタンドアロンタスクを実行することもできますし、サービスの一部としてタスクを実行することもできます。Amazon ECS サービスを使用すると、Amazon ECS クラスターで必要な数のタスクを同時に実行して維持できます。仕組みとしては、タスクがいずれかの理由で失敗または停止した場合に、Amazon ECS サービススケジューラがタスク定義に基づいて別のインスタンスを起動することによって動作します。これは、それを置き換え、サービス内の必要な数のタスクを維持するために行われます。

コンテナエージェントは Amazon ECS クラスター内の各コンテナインスタンス上で実行されます。エージェントは、現在実行中のタスクとリソースのコンテナの使用率に関する情報を Amazon ECS に送信します。Amazon ECS からのリクエストを受信するたびに、タスクを開始および停止します。

タスクまたはサービスをデプロイしたら、次のいずれかのツールを使用してデプロイとアプリケーションを監視できます。

- CloudWatch
- Runtime Monitoring

Amazon ECS の関連情報

このサービスを利用する際に役立つ関連リソースは次のとおりです。

- AWS Fargate– Fargate 機能の概要。
- Windows on AWS - Windows on AWS のワークロードとサービスの概要です。
- AWS からの Linux — AWS の提供する最新の Linux ベースオペレーティングシステムポートフォリオ。

デベロッパーツール

- AWS App2Container – .NET および Java アプリケーションをコンテナ化されたアプリケーションにモダナイズするためのコマンドラインツール。
- Amazon Web Services のツール – AWS SDK を使用して、さまざまなプログラミング言語の Amazon ECS リソースと操作を管理できます。

- AWS CloudFormation – 自動デプロイで環境内のすべての AWS リソースを定義および管理します。
- AWS Copilot コマンドラインインターフェイスを使用した Amazon ECS リソースの作成 – インフラストラクチャの AWS ベストプラクティスに準拠したコンテナアプリケーションを作成、リリース、運用するエンドツーエンドのデベロッパーワークフロー。
- AWS Cloud Development Kit (AWS CDK) – 任意のプログラミング言語を使用して、AWS クラウドインフラストラクチャの定義に使用できる Infrastructure as Code (IAC) フレームワーク。

開発者向けチュートリアル

- AWS コンピューティングブログ– 新機能、機能の詳細、コードサンプル、ベストプラクティスに関する情報。

AWS re:Post

- AWS re:Post — AWS が運営する質疑応答 (Q & A)。技術的な質問に対して、専門家がレビューしたクラウドソーシングによる回答を提供します。

料金

- Amazon ECS の料金 - Amazon ECS の料金情報です。
- AWS Fargate の料金 – Fargate の料金に関する情報。

一般的な AWS リソース

AWS を利用する際に役立つ一般的なリソースは以下の通りです。

- クラスとワークショップ – AWS のスキルを磨き、実践的な経験を得るために役立つセルフペースラボに加えて、ロールベースのコースと特別コースへのリンクです。
- AWS デベロッパーセンター – チュートリアルの検索、ツールのダウンロード、AWS デベロッパーイベントの確認を行います。
- AWS デベロッパーツール - AWS アプリケーションを開発および管理するためのデベロッパーツール、SDK、IDE ツールキット、およびコマンドラインツールへのリンクです。
- ご利用開始のためのリソースセンター — AWS アカウント をセットアップする方法、AWS コミュニティに参加する方法、最初のアプリケーションを起動する方法を説明します。

- ハンズオンチュートリアル - ステップ バイ ステップのチュートリアルに従って、最初のアプリケーションを AWS で起動します。
- AWS ホワイトペーパー – アーキテクチャ、セキュリティ、エコノミクスなどのトピックについて、AWS のソリューションアーキテクトや他の技術エキスパートが記述した AWS の技術ホワイトペーパーの包括的なリストへのリンクです。
- AWS サポート センター – AWS サポート のケースを作成して管理するためのハブです。フォーラム、技術上のよくある質問、サービスヘルスステータス、AWS Trusted Advisor など、他の役立つリソースへのリンクも含まれています。
- サポート – サポート に関する情報のメインウェブページです。クラウド内でのアプリケーションの構築および実行を支援するために 1 対 1 での迅速な対応を行うサポートチャネルとして機能します。
- お問い合わせ - AWS の請求、アカウント、イベント、不正使用、その他の問題などに関するお問い合わせの受付窓口です。
- AWS サイトの利用規約 – 当社の著作権、商標、お客様のアカウント、ライセンス、サイトへのアクセス、その他のトピックに関する詳細情報。

Amazon ECS のリソースの作成および使用方法について説明します。

以下のガイドでは、Amazon ECS にアクセスするために利用できるツールの概要と、コンテナを実行するための初歩的な手順について説明します。Docker の基本では、Docker コンテナイメージを作成し、Amazon ECR プライベート リポジトリにアップロードする基本的な手順を説明します。入門ガイドでは、AWS Copilotのコマンドラインインターフェースと AWS Management Consoleを使用して、Amazon ECS と AWS Fargate でコンテナを実行するための一般的なタスクを完了する手順について説明します。

内容

Amazon ECS を使用するようにセットアップする

すでに Amazon Web Services (AWS) にサインアップしていて、Amazon Elastic Compute Cloud (Amazon EC2) を使用している場合は、すぐに Amazon ECS を使用し始めることができます。2 つのサービスのセットアッププロセスは似ています。次のガイドでは、最初の Amazon ECS のクラスターを起動する準備をします。

Amazon ECS のセットアップを行うには、以下のタスクを完了します。

AWS Management Console

AWS Management Consoleは、Amazon ECS リソースを管理するためのブラウザベースのインターフェイスです。コンソールには、サービスの概要が視覚的に表示されるため、追加のツールを使用

しなくても、Amazon ECS の特徴と機能を簡単に探索できます。コンソールの使用について説明した、関連するチュートリアルが多数用意されています。

コンソールに関するチュートリアルについては、「Amazon ECS のリソースの作成および使用方法について説明します。」を参照してください。

アクションが成功するかどうかについてすぐに視覚的なフィードバックがもたらされるため、多くのお客様はコンソールを使用することを好みます。AWS Management Consoleに慣れているAWSお客様は、ロードバランサーや Amazon EC2 インスタンスなどの関連リソースを簡単に管理できます。

AWS Management Console から始めます。

AWS アカウントへのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

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

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

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

サインアップ処理が完了すると、AWS からユーザーに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

AWS アカウント にサインアップしたら、AWS アカウントのルートユーザー をセキュリティで保護し、AWS IAM Identity Center を有効にして、管理ユーザーを作成します。これにより、日常的なタスクにルートユーザーを使用しないようにします。

AWS アカウントのルートユーザーをセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console 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」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

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。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「 Configure user access with the default 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 アイデンティティセンター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 User Guide」の「Signing in to the AWS access portal」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。

仮想プライベートクラウドを作成する

Amazon Virtual Private Cloud (Amazon VPC) を使用すると、定義した仮想ネットワーク内で AWS リソースを起動できます。コンテナインスタンスは、VPC で起動することを強くお勧めします。

デフォルトの VPC がある場合は、このセクションをスキップして次のタスク「セキュリティグループの作成」に移動できます。デフォルトの VPC があるかどうかを確認するには、「Amazon VPC ユーザーガイド」の「デフォルトの VPC とデフォルトのサブネットを使って作業する」を参照してください。また、次の手順を使用して、アカウントにデフォルト以外の VPC を作成することもできます。

VPC の作成方法の詳細については、「Amazon VPC ユーザーガイド」の「VPC を作成する」を参照し、次の表を使用して、選択するオプションを決定します。

オプション	値
作成するためのリソース	VPC 専用
名前	オプションで、VPC の名前を指定します。
IPv4 CIDR ブロック	IPv4 CIDR 手動入力 CIDR ブロックサイズは /16 から /28 の間である必要があります。
IPv6 CIDR ブロック	IPv6 CIDR ブロックなし
テナンシー	デフォルト値

Amazon VPC の詳細については、Amazon VPC ユーザーガイドのAmazon VPC とはを参照してください。

セキュリティグループの作成

セキュリティグループは、関連付けられたコンテナインスタンスのファイアウォールとして動作し、インバウンドトラフィックとアウトバウンドトラフィックの両方をコンテナインスタンスレベルで制御します。SSH を使用して IP アドレスからコンテナインスタンスに接続するためのルールをセキュリティグループに追加できます。さらに、任意の場所からのインバウンドおよびアウトバウンドの HTTP アクセスおよび HTTPS アクセスを可能にするルールを追加できます。タスクで使用するポートを開くためのルールを追加します。コンテナインスタンスには、Amazon ECS サービスエンドポイントと通信するために外部ネットワークアクセスが必要です。

複数のリージョンでコンテナインスタンスを起動する予定がある場合は、各リージョンでセキュリティグループを作成する必要があります。詳細については、Amazon EC2 ユーザーガイドの「リージョンとアベイラビリティゾーン」を参照してください。

> **Tip**
>
> ローカルコンピュータのパブリック IP アドレスが必要になります。このアドレスはサービスを使って取得できます。例えば、次のサービスが提供されています。http://checkip.amazonaws.com/ または https://checkip.amazonaws.com/。IP アドレスを提供する別のサービスを検索するには、検索フレーズwhat is my IP addressを使用します。インターネットサービスプロバイダー (ISP) 経由で、またはファイアウォールの内側から静的 IP アドレスなしで接続する場合は、クライアントコンピュータで使用されている IP アドレスの範囲を見つける必要があります。

セキュリティグループの作成方法の詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンスのセキュリティ グループの作成」を参照し、次の表を使用して選択するオプションを決定してください。

オプション	値	
リージョン	キーペアを作成したリージョンと同じリージョン。	

オプション	値
名前	「ecs-instances-default-cluster」など、覚えやすい名前。
VPC	デフォルトの VPC (「(デフォルト)」となっています)。 **Note** アカウントが Amazon EC2 Classic をサポートしている場合は、前のタスクで作成した VPC を選択します。

ユースケースに追加するアウトバウンドルールの詳細については、「Amazon EC2 ユーザーガイド」の「さまざまなユースケースのセキュリティグループのルール」を参照してください。

Amazon ECS コンテナインスタンスでは、インバウンドポートが開いている必要はありません。ただし、コンテナインスタンスにログインして Docker コマンドでタスクを確認できるように、SSH ルールを追加できます。また、ウェブサーバーを実行するタスクをコンテナインスタンスでホストする場合は、HTTP と HTTPS のルールを追加できます。コンテナインスタンスには、Amazon ECS サービスエンドポイントとの通信に外部ネットワークアクセスが必要です。これらのオプションのセキュリティグループルールを追加するには、以下のステップを実行します。

セキュリティグループに次の 3 つのインバウンドルールを追加します。セキュリティグループの作成方法の詳細については、「Amazon EC2 ユーザーガイド」の「セキュリティグループのルールを設定する」を参照してください。

オプション	値
HTTP ルール	Type: HTTP ソース: 任意の場所 (`0.0.0.0/0`)

オプション	値	
	このオプションでは、送信元として IPv4 の CIDR ブロック 0.0.0.0/0 が自動的に追加されます。この設定は、テスト環境での短時間の使用であれば許容できますが、実稼働環境においては安全ではありません。実稼働環境では、特定の IP アドレスまたは特定のアドレス範囲にのみ、インスタンスへのアクセスを限定します。	
HTTPS ルール	タイプ: HTTPS ソース: 任意の場所 (`0.0.0.0/0`) この設定は、テスト環境での短時間の使用であれば許容できますが、実稼働環境においては安全ではありません。実稼働環境では、特定の IP アドレスまたは特定のアドレス範囲にのみ、インスタンスへのアクセスを限定します。	

オプション	値
SSH ルール	タイプ: SSH ソース: [Custom] で、コンピュータまたはネットワークのパブリック IP アドレスを CIDR 表記で指定します。CIDR 表記で個々の IP アドレスを指定するには、ルーティングプレフィックスを追加します。/32例えば、IP アドレスが 203.0.113.25 の場合は、203.0.113.25/32 を指定します。会社が特定の範囲からアドレスを割り当てている場合、 203.0.113.0/24 などの範囲全体を指定します。 **Important** セキュリティ上の理由で、すべての IP アドレス (0.0.0.0/0) からインスタンスへの SSH アクセスを許可することはお勧めしません。ただし、それがテスト目的で短期間の場合は例外です。

EC2 インスタンスに接続するための認証情報を作成します。

Amazon ECS では、EC2 起動タイプを使用する場合にのみキーペアが必要です。

AWS では公開キー暗号化を使用して、お客様のインスタンスのログイン情報の安全性を保護します。Amazon ECS コンテナインスタンスなどの Linux インスタンスでは、SSH アクセスにパスワードを使いません。キーペアを使用してインスタンスに安全にログインします。コンテナインスタンスを起動するときにキーペアの名前を指定し、プライベートキーを指定して、SSH でログインします。

キーペアをまだ作成していない場合は、Amazon EC2 コンソールを使用して作成できます。複数のリージョンでインスタンスを起動する予定がある場合は、各リージョンでキーペアを作成する必要があります。リージョンの詳細については、「Amazon EC2 ユーザーガイド」の「Regions and Availability Zones」を参照してください。

キーペアを作成するには

- Amazon EC2 コンソールを使用して、キーペアを作成します。キーペアの作成の詳細については、「Amazon EC2 ユーザーガイド」の「Create a key pair」を参照してください。

Linux インスタンスに接続する方法については、「Amazon EC2 ユーザーガイド」の「Linux インスタンスへの接続」を参照してください。

AWS CLI のインストール

Amazon ECS を使用すると、AWS Management Console でのすべてのオペレーションを手動で管理できます。ただし、ローカルのデスクトップまたはデベロッパーボックスに AWS CLI をインストールすることは可能です。この場合は、Amazon ECS 内の共通の管理タスクを自動化するための、スクリプトを作成できます。

Amazon ECS で AWS CLI を使用するには、最新バージョンの AWS CLI をインストールします。AWS CLI のインストールまたは最新バージョンへのアップグレードについては、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

AWS Command Line Interface (AWS CLI) は、AWS サービスを管理するために使用できる統合ツールです。この 1 つのツールだけでは、複数の AWS サービスを制御し、スクリプトを使用してこれらのサービスを自動化することができます。AWS CLIのAmazon ECS コマンドは、Amazon ECS API を反映しています。

AWS CLI は、スクリプト作成やコマンドラインツールとのインターフェイスを好みかつ使い慣れており、Amazon ECS リソースに対して実行するアクションを正確に把握しているお客様に適しています。AWS CLI は、Amazon ECS API に詳しくなりたいお客様にも役立ちます。お客様は、AWS

CLI を使用して、Amazon ECS リソースでコマンドラインインターフェイスから直接作成、読み取り、更新、削除などの多数の操作を実行できます。

Amazon ECS API および対応する CLI コマンドに詳しくなり、自動スクリプトを作成し、Amazon ECS リソースに対して特定のアクションを実行したい場合は、AWS CLI を使用します。

AWS では、AWS Tools for Windows PowerShell コマンドラインツールも提供されています。詳細については、AWS Tools for Windows PowerShell ユーザーガイドを参照してください。

Amazon ECS を使用するための次のステップ

AWS CLI をインストールした後は、さまざまなツールを利用して Amazon ECS を引き続き使用できます。以下のリンクでは、これらのツールのいくつかについて説明し、Amazon ECS で使用する方法の例を示します。

- Docker で最初のコンテナイメージを作成し、Amazon ECS タスク定義で使用するために Amazon ECR にプッシュします。
- Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する方法について説明します。.
- Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。.
- EC2 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。.
- 希望するプログラミング言語を使用して、AWS CDK を使用した Amazon ECS リソースの作成 でインフラストラクチャまたはアーキテクチャをコードとして定義します。
- AWS CloudFormation を使用した Amazon ECS リソースの作成 を使用して、自動デプロイにより、環境内のすべての AWS リソースを定義および管理します。
- 包括的な AWS Copilot コマンドラインインターフェイスを使用した Amazon ECS リソースの作成 エンドツーエンドのデベロッパーワークフローを使用して、インフラストラクチャの AWS ベストプラクティスに準拠したコンテナアプリケーションを作成、リリース、運用します。

Amazon ECS で使用するコンテナイメージの作成

Amazon ECS は、タスク定義で Docker イメージを使用して、コンテナを起動します。Docker は、コンテナ内の分散アプリケーションの構築、実行、テスト、デプロイするためのツールを提供するテクノロジーです。

ここでは、最初の Docker イメージを作成し、そのイメージを Amazon ECS タスク定義で使用するために、コンテナレジストリである Amazon ECR にプッシュするステップを説明します。この

チュートリアルは、Docker の概念と機能を基本的に理解していることを前提としています。Docker の詳細については、「Docker とは」および「Docker ドキュメント」を参照してください。

前提条件

開始する前に、以下の前提条件を満たしていることを確認します。

- Amazon ECR のセットアップステップを完了したことを確認します。詳細については、「Amazon Elastic Container Registry ユーザーガイド」の「Amazon でのライフサイクルを通じたイメージの移動 ECR」を参照してください。
- ユーザーは、Amazon ECR サービスにアクセスし、使用するために必要な IAM 権限を持ちます。詳細については、「Amazon ECRマネージドポリシー」を参照してください。
- Docker をインストールします。Amazon Linux 2 の Docker インストールステップについては、「AL2023 に Docker をインストールする」を参照してください。他のすべてのオペレーティングシステムについては、[Docker Desktop overview] (Docker デスクトップの概要) の Docker ドキュメントを参照してください。
- AWS CLI がインストールされ、設定されている。詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

ローカル開発環境がない、または不要で、Amazon EC2 インスタンスを使って Docker を使用したい場合は、Amazon Linux 2 を使用してAmazon EC2 インスタンスを起動し、Docker Engine と Docker CLI をインストールするためのステップを以下に示します。

AL2023 に Docker をインストールする

Docker は、Ubuntu のような最新の Linux ディストリビューションから macOS や Windows まで、さまざまなオペレーティングシステムで使用できます。特定のオペレーティングシステムに Docker をインストールする方法の詳細については、Docker インストールガイド を参照してください。

Docker を使用するには、ローカルの開発システムは必要ありません。Amazon EC2 をすでに使用している場合は、Amazon Linux 2023 インスタンスを起動し、Docker をインストールして開始できます。

Docker をインストール済みの場合は、この手順をスキップして「「Docker イメージの作成」」に進んでください。

Amazon Linux 2023 AMI を使用して Amazon EC2 インスタンスに Docker をインストールするには

1. 最新の Amazon Linux 2023 AMI を使用してインスタンスを起動します。詳細については、「Amazon EC2 ユーザーガイド」の「コンソールのインスタンス起動ウィザードを使用して EC2 インスタンスを起動する」を参照してください。
2. インスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「EC2 インスタンスへの接続」を参照してください。
3. インスタンスでインストールされているパッケージとパッケージキャッシュを更新します。

```
sudo yum update -y
```

4. 最新の Docker Community Edition パッケージをインストールします。

```
sudo yum install docker
```

5. Docker サービスを開始します。

```
sudo service docker start
```

6. ec2-user を docker グループに追加すると、sudo を使用せずに Docker コマンドを実行できます。

```
sudo usermod -a -G docker ec2-user
```

7. ログアウトし、再びログインして、新しい docker グループアクセス権限を取得します。これは、現在の SSH ターミナルウィンドウを閉じて、新しいウィンドウでインスタンスに再接続することで達成できます。新しい SSH セッションには適切な docker グループ権限があります。
8. ec2-user が sudo を使用せずに Docker コマンドを実行できることを確認します。

```
docker info
```

> **Note**
>
> 場合によっては、Docker デーモンにアクセスするための ec2-user に対するアクセス権限を提供するため、インスタンスを再起動する必要があります。次のエラーが表示された場合は、インスタンスを再起動してください。

```
Cannot connect to the Docker daemon. Is the docker daemon running on this
 host?
```

「Docker イメージの作成」

Amazon ECS のタスク定義では、Docker イメージを使用してクラスター内のコンテナインスタンスでコンテナを起動します。このセクションでは、シンプルなウェブアプリケーションの Docker イメージを作成し、ローカルシステムまたは Amazon EC2 インスタンスでテストしてから、そのイメージを Amazon ECR コンテナレジストリにプッシュして、Amazon ECS タスク定義で使用できるようにします。

シンプルなウェブアプリケーションの Docker イメージを作成するには

1. `Dockerfile` という名前のファイルを作成します。Dockerfile は、Docker イメージに使用する基本イメージと、そのイメージにインストールして実行するものを記述するマニフェストです。Dockerfile の詳細については、「Dockerfile リファレンス」を参照してください。

   ```
   touch Dockerfile
   ```

2. 前の手順で作成した `Dockerfile` を編集し、以下のコンテンツを追加します。

   ```
   FROM public.ecr.aws/amazonlinux/amazonlinux:latest

   # Update installed packages and install Apache
   RUN yum update -y && \
    yum install -y httpd

   # Write hello world message
   RUN echo 'Hello World!' > /var/www/html/index.html

   # Configure Apache
   RUN echo 'mkdir -p /var/run/httpd' >> /root/run_apache.sh && \
    echo 'mkdir -p /var/lock/httpd' >> /root/run_apache.sh && \
    echo '/usr/sbin/httpd -D FOREGROUND' >> /root/run_apache.sh && \
    chmod 755 /root/run_apache.sh

   EXPOSE 80
   ```

```
CMD /root/run_apache.sh
```

この Dockerfile は、Amazon ECR パブリックでホストされているパブリック Amazon Linux 2 イメージを使用します。RUN の手順により、パッケージキャッシュが更新され、ウェブ サーバー用のいくつかのソフトウェアがインストールされてから、「Hello World!」 のコンテンツがウェブサーバーのドキュメントルートに書き込みされます。EXPOSE の命令でコンテナ上のポート 80 がリッスン中のものになり、CMD の命令でウェブサーバーが起動します。

3. Dockerfile から Docker イメージを作成します。

> **Note**
>
> Docker の一部のバージョンでは、下に示す相対パスの代わりに、次のコマンドで Dockerfile への完全パスが必要になる場合があります。
> MacOS M1/Mx-chip で コマンドを実行する場合は、--platform オプション 「--platform linux/amd64」を使用します。

```
docker build -t hello-world .
```

4. コンテナイメージを一覧表示します。

```
docker images --filter reference=hello-world
```

出力:

```
REPOSITORY          TAG                 IMAGE ID            CREATED
 SIZE
hello-world         latest              e9ffedc8c286        4 minutes ago
 194MB
```

5. 新しく構築されたイメージを実行します。-p 80:80 オプションは、コンテナ上の公開されたポート 80 をホストシステム上のポート 80 にマッピングします。

```
docker run -t -i -p 80:80 hello-world
```

> **Note**
>
> Apache ウェブサーバーからの出力はターミナルウィンドウに表示されます。"Could not reliably determine the fully qualified domain name" メッセージは無視できます。

6. ブラウザーを開き、Docker を実行している、コンテナのホストサーバーを参照します。

   - EC2 インスタンスを使用している場合、これはサーバーの [Public DNS] 値であり、SSH でインスタンスに接続するときに使用するアドレスと同じです。インスタンスのセキュリティグループでポート 80 上の受信トラフィックを許可していることを確認します。
   - Docker をローカルに実行している場合は、ブラウザで http://localhost/ を参照します。
   - Windows または Mac コンピューターで docker-machine を使用している場合は、docker-machine ip コマンドを使用して Docker のホスト VirtualBox VM の IP アドレスを見つけ、*machine-name* を、使用中の Docker マシンの名前に置き換えます。

     ```
     docker-machine ip machine-name
     ```

   ウェブページに「Hello, World!」が確認できます。表示されます。

7. [Ctrl + C] キーを押して、Docker コンテナを停止します。

Amazon Elastic Container Registry にイメージをプッシュします

Amazon ECR はマネージド型 AWS Docker レジストリサービスです。Docker CLI を使用して、Amazon ECR リポジトリ内のイメージをプッシュ、プル、および管理できます。Amazon ECR 製品の詳細、主なお客様導入事例、FAQ については、Amazon Elastic コンテナレジストリ 製品の詳細ページを参照してください。

イメージにタグを付け、Amazon ECR にプッシュするには

1. `hello-world` イメージを保存する Amazon ECR リポジトリを作成します。出力の `repositoryUri` に注目してください。

   `region` を、AWS リージョン に置き換えます (例えば `us-east-1`)。

```
aws ecr create-repository --repository-name hello-repository --region region
```

出力:

```
{
    "repository": {
        "registryId": "aws_account_id",
        "repositoryName": "hello-repository",
        "repositoryArn": "arn:aws:ecr:region:aws_account_id:repository/hello-
repository",
        "createdAt": 1505337806.0,
        "repositoryUri": "aws_account_id.dkr.ecr.region.amazonaws.com/hello-
repository"
    }
}
```

2. 前のステップの repositoryUri の値で hello-world イメージにタグを付けます。

```
docker tag hello-world aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository
```

3. aws ecr get-login-password コマンドを実行します。認証先のレジストリ URI を指定します。詳細については、Amazon Elastic Container Registry ユーザーガイドの「レジストリの認証」を参照してください。

```
aws ecr get-login-password --region region | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.region.amazonaws.com
```

出力:

```
Login Succeeded
```

> **Important**
>
> エラーが発生した場合は、AWS CLI の最新バージョンをインストールまたはアップグレードします。詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

4. repositoryUri前のステップの値 を使用して、Amazon ECR にイメージをプッシュします。

```
docker push aws_account_id.dkr.ecr.region.amazonaws.com/hello-repository
```

クリーンアップ

Amazon ECS タスク定義の作成、およびコンテナイメージを使用したタスク起動を続行するには、次のステップ に進んでください。Amazon ECR イメージの試用を終了したら、レポジトリを削除し、イメージストレージに対して課金されないようにします。

```
aws ecr delete-repository --repository-name hello-repository --region region --force
```

次のステップ

タスク定義にはタスク実行ロールが必要です。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

コンテナイメージを作成して Amazon ECR にプッシュしたら、そのイメージをタスク定義で使用できます。詳細については、以下のいずれかを参照してください。

- the section called “Fargate 起動タイプ用のタスクを作成する方法について説明します。”
- the section called “Fargate 起動タイプ用の Windows タスクを作成する方法について説明します。”
- AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する

Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する方法について説明します。

Amazon Elastic Container Service (Amazon ECS) は、非常にスケーラブルで高速なコンテナ管理サービスで、クラスターでコンテナの実行、停止、管理を簡単に行うことができます。AWS Fargate でサービスやタスクを起動して、Amazon ECS 管理のサーバーレスインフラストラクチャにあるコンテナをホストすることができます。Fargate の詳細については、Amazon ECS の AWS Fargate を参照してください。

Amazon ECS で AWS Fargate がサポートされているリージョンで、タスクに Fargate 起動タイプを使用し、Amazon ECS on AWS Fargate の使用を開始します。

AWS Fargateで Amazon ECSの使用を開始するには、以下のステップを完了します。

前提条件

開始する前に、Amazon ECS を使用するようにセットアップする のステップを完了し、AWS ユーザーに `AdministratorAccess` IAM ポリシー例で指定されているアクセス許可があることを確認します。

コンソールは、Fargate タスクに必要なタスク実行 IAM ロールを自動で作成しようとします。コンソールがこの IAM ロールを作成できるようにするには、次のいずれかがtrueである必要があります。

- ユーザーが管理者権限を持っていることが必要です。詳細については、「Amazon ECS を使用するようにセットアップする」を参照してください。
- ユーザーがサービスロールを作成するための IAM 権限を持っていることが必要です。詳細については、「AWS サービスにアクセス許可を委任するロールの作成」を参照してください。
- 管理者権限を持つユーザーは、タスク実行ロールを手動で作成することにより、使用するアカウントで有効にできます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

> **Important**
>
> タスク定義を使用してサービスを作成するときに選択するセキュリティグループには、インバウンドトラフィック用にポート 80 が開いている必要があります。セキュリティグループに次のインバウンドルールを追加します。セキュリティグループの作成方法については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンス用のセキュリティグループの作成」を参照してください。
>
> - [Type]: HTTP
> - [Protocol]: TCP
> - ポート範囲: 80
> - ソース: 任意の場所 (`0.0.0.0/0`)

ステップ 1: クラスターを作成する

デフォルトの VPC を使用するクラスターを作成します。

開始する前に、適切な IAM アクセス許可を割り当ててください。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [Cluster configuration] (クラスター設定) で、[Cluster name] (クラスター名) に一意の名前を入力します。

   名前には、最大 255 文字 (大文字と小文字)、数字、およびハイフンを含めることができます。
6. (オプション) Container Insights を有効にするには、[Monitoring] (モニタリング) を展開し、[Use Container Insights] (Container Insights を使用する) をオンにします。
7. (オプション) クラスターを識別しやすくするには、[Tags] (タグ) を展開し、タグを設定します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。
8. [Create] (作成) を選択します。

ステップ 2: タスク定義を作成する

タスク定義はアプリケーションの設計図のようなものです。Amazon ECS でタスクを起動するたびに、タスク定義を指定します。サービスは、コンテナに使用する Docker イメージ、タスクで使用するコンテナの数、各コンテナのリソース割り当てを認識します。

1. ナビゲーションペインで、[タスク定義] を選択します。
2. [Create new Task Definition] (新しいタスク定義の作成)、[Create new revision with JSON] (JSON で新しいリビジョンを作成) の順に選択します。
3. 以下のタスク定義の例をコピーしてボックスに貼り付け、[Save (保存)] を選択します。

```
{
    "family": "sample-fargate",
```

```
    "networkMode": "awsvpc",
    "containerDefinitions": [
        {
            "name": "fargate-app",
            "image": "public.ecr.aws/docker/library/httpd:latest",
            "portMappings": [
                {
                    "containerPort": 80,
                    "hostPort": 80,
                    "protocol": "tcp"
                }
            ],
            "essential": true,
            "entryPoint": [
                "sh",
  "-c"
            ],
            "command": [
                "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample
 App</title> <style>body {margin-top: 40px; background-color: #333;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</
h1> <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html &&
 httpd-foreground\""
            ]
        }
    ],
    "requiresCompatibilities": [
        "FARGATE"
    ],
    "cpu": "256",
    "memory": "512"
}
```

4. [Create] (作成) を選択します。

ステップ 3: サービスを作成する

タスク定義を使用してサービスを作成します。

1. ナビゲーションペインで、[Clusters] (クラスター) を選択してから、ステップ 1: クラスターを作成する で作成したクラスターを選択します。

2. [Services] (サービス) タブから、[Create] (作成) を選択します。
3. [Deployment configure] (デプロイ設定) で、アプリケーションのデプロイ方法を指定します。
   a. [Task definition] (タスク定義) で、ステップ 2: タスク定義を作成する で作成したタスク定義を選択します。
   b. [Service name] (サービス名) でサービスの名前を入力します。
   c. [Desired tasks] (必要なタスク) に、1と入力します。
4. [ネットワーク] で、タスク用に新しいセキュリティグループを作成するか、既存のセキュリティグループを選択できます。使用するセキュリティグループに、前提条件 に一覧表示されているインバウンドルールがあることを確認してください。
5. [Create] (作成) を選択します。

ステップ 4: サービスを表示する

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. サービスを実行したクラスターを選択します。
4. [サービス] タブの [サービス名] で、ステップ 3: サービスを作成する に作成したサービスを選択します。
5. [タスク] タブ > サービス内のタスクの順に選択します。
6. [タスク] ページの [設定] セクションの [パブリック IP] で、[オープンアドレス] を選択します。

ステップ 5 : クリーンアップ

Amazon ECS クラスターの使用が終了したら、使用していないリソースに対する料金が発生しないよう、それに関連付けられたリソースをクリーンアップする必要があります。

タスク、サービス、クラスター、コンテナインスタンスなど、一部の Amazon ECS リソースは、Amazon ECS コンソールを使用してクリーンアップします。Amazon EC2 インスタンス、Elastic Load Balancing ロードバランサー、Auto Scaling グループなど他のリソースは、Amazon EC2 コンソールで手動でクリーンアップするか、それを作成した AWS CloudFormation スタックを削除することでクリーンアップする必要があります。

1. ナビゲーションペインで [Clusters] (クラスター) を選択します。
2. [クラスター] ページで、このチュートリアル用に作成したクラスターを選択します。

3. [サービス] タブを選択します。
4. サービス > [削除] の順に選択します。
5. 確認プロンプトで、delete (削除) と入力し、[Delete] (削除) を選択します。または、サービスを削除する前に、ユーザーに代わって Amazon ECS がサービスをスケールダウンする `Force delete` オプションを使用することもできます。

   サービスが削除されるまでお待ちください。
6. [Delete Cluster] を選択します。確認プロンプトで、delete ***`cluster-name`***と入力し、[Delete] (削除) を選択します。クラスターを削除すると、Auto Scaling グループ、VPC、ロードバランサーなどを含むクラスターで作成された関連リソースがクリーンアップされます。

Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。

Amazon ECS で AWS Fargate がサポートされているリージョンで、タスクに Fargate 起動タイプを使用し、Amazon ECS on AWS Fargate の使用を開始します。

AWS Fargateで Amazon ECSの使用を開始するには、以下のステップを完了します。

前提条件

開始する前に、Amazon ECS を使用するようにセットアップする のステップを完了し、AWS ユーザーに `AdministratorAccess` IAM ポリシー例で指定されているアクセス許可があることを確認します。

コンソールは、Fargate タスクに必要なタスク実行 IAM ロールを自動で作成しようとします。コンソールがこの IAM ロールを作成できるようにするには、次のいずれかがtrueである必要があります。

- ユーザーが管理者権限を持っていることが必要です。詳細については、「Amazon ECS を使用するようにセットアップする」を参照してください。
- ユーザーがサービスロールを作成するための IAM 権限を持っていることが必要です。詳細については、「AWS サービスにアクセス許可を委任するロールの作成」を参照してください。
- 管理者権限を持つユーザーは、タスク実行ロールを手動で作成することにより、使用するアカウントで有効にできます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

Important

タスク定義を使用してサービスを作成するときに選択するセキュリティグループには、インバウンドトラフィック用にポート 80 が開いている必要があります。セキュリティグループに次のインバウンドルールを追加します。セキュリティグループの作成方法については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンス用のセキュリティグループの作成」を参照してください。

- [Type]: HTTP
- [Protocol]: TCP
- ポート範囲: 80
- ソース: 任意の場所 (`0.0.0.0/0`)

ステップ 1: クラスターを作成する

デフォルトの VPCを使用する [ウィンドウズ] という名前の新しいクラスターを作成できます。

AWS Management Console を使用してクラスターを作成するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [Cluster configuration] (クラスター設定) の [Cluster name] (クラスター名) に「windows」と入力します。
6. (オプション) Container Insights を有効にするには、[Monitoring] (モニタリング) を展開し、[Use Container Insights] (Container Insights を使用する) をオンにします。
7. (オプション) クラスターを識別しやすくするには、[Tags] (タグ) を展開し、タグを設定します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。

8. [Create] (作成) を選択します。

ステップ 2: Windows タスク定義を登録する

Amazon ECS クラスターで Windows コンテナを実行する前に、タスク定義を登録する必要があります。次のタスク定義の例では、mcr.microsoft.com/windows/servercore/iis コンテナイメージを使用してコンテナインスタンスのポート 8080 でシンプルなウェブページを表示します。

AWS Management Console を使用してサンプルタスク定義を登録するには

1. ナビゲーションペインで、タスクの定義 を選択します。
2. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
3. 以下のタスク定義の例をコピーしてボックスに貼り付け、[Save (保存)] を選択します。

```
{
    "containerDefinitions": [
        {
            "command": ["New-Item -Path C:\\inetpub\\wwwroot\\index.html
 -Type file -Value '<html> <head> <title>Amazon ECS Sample App</title>
 <style>body {margin-top: 40px; background-color: #333;} </style> </head><body>
 <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
 <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p>'; C:\\ServiceMonitor.exe w3svc"],
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "essential": true,
            "cpu": 2048,
            "memory": 4096,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "name": "sample_windows_app",
            "portMappings": [
                {
                    "hostPort": 80,
                    "containerPort": 80,
                    "protocol": "tcp"
                }
            ]
```

```
        }
    ],
    "memory": "4096",
    "cpu": "2048",
    "networkMode": "awsvpc",
    "family": "windows-simple-iis-2019-core",
    "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
    "runtimePlatform": {"operatingSystemFamily": "WINDOWS_SERVER_2019_CORE"},
    "requiresCompatibilities": ["FARGATE"]
}
```

4. 情報を確認し、[Create] (作成) を選択します。

ステップ 3: タスク定義を使用してサービスを作成する

タスク定義を登録したら、それを使用してクラスターにタスクを配置できます。次の手順では、タスク定義を使用してサービスを作成し、クラスターに 1 つのタスクを配置します。

コンソールを使用してタスク定義からサービスを作成するには

1. ナビゲーションペインで、[Clusters] (クラスター) を選択してから、ステップ 1: クラスターを作成する で作成したクラスターを選択します。
2. [Services] (サービス) タブから、[Create] (作成) を選択します。
3. [Deployment configure] (デプロイ設定) で、アプリケーションのデプロイ方法を指定します。
   a. [Task definition] (タスク定義) で、ステップ 2: Windows タスク定義を登録する で作成したタスク定義を選択します。
   b. [Service name] (サービス名) でサービスの名前を入力します。
   c. [Desired tasks] (必要なタスク) に、1と入力します。
4. [ネットワーク] で、セキュリティグループを作成するか、既存のグループを選択できます。使用するセキュリティグループに、前提条件 に一覧表示されているインバウンドルールがあることを確認してください。
5. [Create] (作成) を選択します。

ステップ 4: サービスを表示する

サービスによってクラスターでタスクが起動されたら、サービスを表示し、ブラウザで IIS テストページを開いてコンテナが実行中であることを確認できます。

> **Note**
>
> コンテナインスタンスで Windows コンテナベースレイヤーをダウンロードして抽出するまでに最大 15 分かかる場合があります。

サービスを表示するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. サービスを実行したクラスターを選択します。
4. [サービス] タブの [サービス名] で、ステップ 3: タスク定義を使用してサービスを作成する に作成したサービスを選択します。
5. [タスク] タブ > サービス内のタスクの順に選択します。
6. [タスク] ページの [設定] セクションの [パブリック IP] で、[オープンアドレス] を選択します。

ステップ 5: クリーンアップ

Amazon ECS クラスターの使用が終了したら、使用していないリソースに対する料金が発生しないよう、それに関連付けられたリソースをクリーンアップする必要があります。

タスク、サービス、クラスター、コンテナインスタンスなど、一部の Amazon ECS リソースは、Amazon ECS コンソールを使用してクリーンアップします。Amazon EC2 インスタンス、Elastic Load Balancing ロードバランサー、Auto Scaling グループなど他のリソースは、Amazon EC2 コンソールで手動でクリーンアップするか、それを作成した AWS CloudFormation スタックを削除することでクリーンアップする必要があります。

1. ナビゲーションペインで [Clusters] (クラスター) を選択します。
2. [クラスター] ページで、このチュートリアル用に作成したクラスターを選択します。
3. [サービス] タブを選択します。
4. サービス > [削除] の順に選択します。
5. 確認プロンプトで、delete (削除) と入力し、[Delete] (削除) を選択します。

   サービスが削除されるまでお待ちください。

6. [Delete Cluster] を選択します。確認プロンプトで、delete ***cluster-name***と入力し、[Delete] (削除) を選択します。クラスターを削除すると、Auto Scaling グループ、VPC、ロードバランサーなどを含むクラスターで作成された関連リソースがクリーンアップされます。

EC2 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。

EC2 起動タイプを使用して Amazon ECS を開始するには、タスク定義を登録し、クラスターを作成し、コンソールにサービスを作成します。

EC2 起動タイプを使用して、Amazon ECS を開始するには、以下の手順を完了します。

前提条件

開始する前に、Amazon ECS を使用するようにセットアップする のステップを完了し、AWS ユーザーに `AdministratorAccess` IAM ポリシー例で指定されているアクセス許可があることを確認します。

コンソールは、Fargate タスクに必要なタスク実行 IAM ロールを自動で作成しようとします。コンソールがこの IAM ロールを作成できるようにするには、次のいずれかがtrueである必要があります。

- ユーザーが管理者権限を持っていることが必要です。詳細については、「Amazon ECS を使用するようにセットアップする」を参照してください。
- ユーザーがサービスロールを作成するための IAM 権限を持っていることが必要です。詳細については、「AWS サービスにアクセス許可を委任するロールの作成」を参照してください。
- 管理者権限を持つユーザーは、タスク実行ロールを手動で作成することにより、使用するアカウントで有効にできます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

> **Important**
>
> タスク定義を使用してサービスを作成するときに選択するセキュリティグループには、インバウンドトラフィック用にポート 80 が開いている必要があります。セキュリティグループに次のインバウンドルールを追加します。セキュリティグループの作成方法については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンス用のセキュリティグループの作成」を参照してください。

- [Type]: HTTP
- [Protocol]: TCP
- ポート範囲: 80
- ソース: 任意の場所 (`0.0.0.0/0`)

ステップ 1: クラスターを作成する

Amazon ECS クラスターはタスク、サービス、およびコンテナインスタンスの論理グループです。

以下では、1 つの Amazon EC2 インスタンスが登録されたクラスターを作成し、そこでタスクを実行できるようにするステップについて説明します。特定のフィールドが示されていない場合は、コンソールのデフォルト値のままにします。

新しいクラスターを作成するには (Amazon ECS コンソール)

開始する前に、適切な IAM アクセス許可を割り当ててください。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [Cluster configuration] (クラスター設定) で、[Cluster name] (クラスター名) に一意の名前を入力します。

   名前には、最大 255 文字 (大文字と小文字)、数字、およびハイフンを含めることができます。
6. (オプション) タスクとサービスが起動する VPC とサブネットを変更するには、[Networking] (ネットワーク) で、次のいずれかのオペレーションを実行します。

   - サブネットを削除するには、[Subnets] (サブネット) で、削除するサブネットごとに [X] を選択します。
   - [default] (デフォルト) VPC 以外の VPC に変更するには、[VPC] で既存の [VPC] を選択し、[Subnets] (サブネット) で各サブネットを選択します。

7. クラスターに Amazon EC2 インスタンスを追加するには、[インフラストラクチャー] を展開して [Amazon EC2 インスタンス] を選択します。次に、キャパシティープロバイダーとして機能する Auto Scaling グループを設定します。

   a. 既存の Auto Scaling グループを使用するには、[Auto Scaling group (ASG)] (Auto Scaling グループ) からグループを選択します。

   b. Auto Scaling グループを作成するには、Auto Scaling group(ASG) (Auto Scaling グループ) から、[Create new group] (新しいグループの作成) を選択し、グループに関する以下の詳細情報を入力します。

      - Operating system/Architecture (オペレーティングシステム/アーキテクチャ) を使用する場合、Auto Scaling グループインスタンスの Amazon ECS 最適化 AMI を選択します。
      - [EC2 instance type] (EC2 インスタンスタイプ) を使用する場合、ワークロードのインスタンスタイプを選択します。さまざまなインスタンスタイプに関する詳細については、Amazon EC2 インスタンスを参照してください。

        マネージドスケーリングは、Auto Scaling グループが同じインスタンスタイプまたは類似のインスタンスタイプを使用している場合に最適です。
      - [SSH key pair] (SSH キーペア) を使用する場合、インスタンスに接続する際に ID を証明するペアを選択してください。
      - [Capacity] (キャパシティー) には、Auto Scaling グループで起動するインスタンスの最小数と最大数を入力します。Amazon EC2 instances が AWS リソースに存在する間、コストが発生します。詳細については、Amazon EC2 の料金表を参照してください。

8. (オプション) Container Insights を有効にするには、[Monitoring] (モニタリング) を展開し、[Use Container Insights] (Container Insights を使用する) をオンにします。

9. (オプション) クラスタータグを管理するには、[Tags] (タグ) を展開し、次のいずれかのオペレーションを実行します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。

10. [Create] (作成) を選択します。

ステップ 2: タスク定義を登録する

AWS Management Console を使用してサンプルタスク定義を登録するには

1. ナビゲーションペインで、[タスク定義] を選択します。
2. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
3. 以下のタスク定義の例をコピーしてボックスに貼り付け、[保存] を選択します。

```
{
    "containerDefinitions": [
        {
            "command": ["New-Item -Path C:\\inetpub\\wwwroot\\index.html
 -Type file -Value '<html> <head> <title>Amazon ECS Sample App</title>
 <style>body {margin-top: 40px; background-color: #333;} </style> </head><body>
 <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
 <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p>'; C:\\ServiceMonitor.exe w3svc"],
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "essential": true,
            "cpu": 2048,
            "memory": 4096,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "name": "sample_windows_app",
            "portMappings": [
                {
                    "hostPort": 443,
                    "containerPort": 80,
                    "protocol": "tcp"
                }
            ]
        }
    ],
    "memory": "4096",
    "cpu": "2048",
    "family": "windows-simple-iis-2019-core",
    "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
    "runtimePlatform": {"operatingSystemFamily": "WINDOWS_SERVER_2019_CORE"},
```

```
    "requiresCompatibilities": ["EC2"]
}
```

4. 情報を確認し、[Create] (作成) を選択します。

ステップ 3: サービスを作成する

Amazon ECS サービスを使用すると、Amazon ECS クラスター内で、タスク定義の指定した数のインスタンスを同時に実行して維持するのに役立ちます。タスクが何らかの理由で失敗または停止した場合、 Amazon ECS サービススケジューラは、タスク定義の別のインスタンスを起動してそれに置き換え、サービスで必要な数のタスクを維持します。サービスの詳細については、「Amazon ECS サービス」を参照してください。

サービスを作成するには

1. ナビゲーションペインで [Clusters] (クラスター) を選択します。
2. ステップ 1: クラスターを作成する で作成したクラスターを選択します。
3. [Services (サービス)] タブで、[Create (作成]) を選択します。
4. [Environment] (環境) セクションで、以下を実行します。
   a. [Compute options] (コンピューティングオプション) では、[Launch type] (起動タイプ) を選択します。
   b. [起動タイプ] で [EC2] をクリックします。
5. [Deployment configuration] (デプロイ設定) セクションで、以下を実行します。
   a. [Family] (ファミリー) で、ステップ 2: タスク定義を登録する で作成したタスク定義を選択します。
   b. [Service name] (サービス名) でサービスの名前を入力します。
   c. [Desired tasks] (必要なタスク) に、1と入力します。
6. オプションを確認し [作成] を選択します。
7. [View service (サービスの表示)] を選択して、サービスを確認します。

ステップ 4: サービスを表示する

このサービスはウェブベースのアプリケーションであるため、ウェブブラウザでコンテナを表示できます。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. サービスを実行したクラスターを選択します。
4. [サービス] タブの [サービス名] で、ステップ 3: サービスを作成する に作成したサービスを選択します。
5. [タスク] タブ > サービス内のタスクの順に選択します。
6. [タスク] ページの [設定] セクションの [パブリック IP] で、[オープンアドレス] を選択します。以下のスクリーンショットは想定される出力です。

ステップ 5: クリーンアップ

Amazon ECS クラスターの使用が終了したら、使用していないリソースに対する料金が発生しないよう、それに関連付けられたリソースをクリーンアップする必要があります。

タスク、サービス、クラスター、コンテナインスタンスなど、一部の Amazon ECS リソースは、Amazon ECS コンソールを使用してクリーンアップします。Amazon EC2 インスタンス、Elastic Load Balancing ロードバランサー、Auto Scaling グループなど他のリソースは、Amazon EC2 コンソールで手動でクリーンアップするか、それを作成した AWS CloudFormation スタックを削除することでクリーンアップする必要があります。

1. ナビゲーションペインで [Clusters] (クラスター) を選択します。
2. [クラスター] ページで、このチュートリアル用に作成したクラスターを選択します。
3. [サービス] タブを選択します。
4. サービス > [削除] の順に選択します。
5. 確認プロンプトで、delete (削除) と入力し、[Delete] (削除) を選択します。

サービスが削除されるまでお待ちください。

6. [Delete Cluster] を選択します。確認プロンプトで、delete ***cluster-name***と入力し、[Delete] (削除) を選択します。クラスターを削除すると、Auto Scaling グループ、VPC、ロードバランサーなどを含むクラスターで作成された関連リソースがクリーンアップされます。

AWS CDK を使用した Amazon ECS リソースの作成

AWS Cloud Development Kit (AWS CDK) は、選択したプログラミング言語を使用して、AWS クラウドインフラストラクチャの定義に使用できる、Infrastructure as Code (IAC) フレームワークです。独自のクラウドインフラストラクチャを定義するには、最初に、(CDK でサポートされている言語のいずれかで) 1 つ以上のスタックが含まれるアプリケーションを記述します。次に、それを AWS CloudFormation テンプレートに合成して、AWS アカウント にリソースをデプロイします。このトピックのステップに従って、Amazon Elastic Container Service (Amazon ECS) と Fargate 上の AWS CDK で、コンテナ化されたウェブサーバーをデプロイしてください。

CDK に含まれる AWS 構成ライブラリは、AWS のサービス が提供するリソースのモデル化に使用できるモジュールを提供します。一般的なサービスでは、ライブラリが、スマートなデフォルトとベストプラクティスを持つ厳選された構成を提供します。これらのモジュールの 1 つである `aws-ecs-patterns` は、コンテナ化されたサービスと必要なすべてのサポートリソースをほんの数行のコードで定義するために使用できる、高レベルの抽象化を提供します。

このトピックでは、`ApplicationLoadBalancedFargateService` 構成を使用します。この構成は、Application Load Balancer の背後にある Fargate に Amazon ECS サービスをデプロイします。この `aws-ecs-patterns` モジュールには、Network Load Balancer を使用したり、Amazon EC2 で実行したりする構成も含まれています。

このタスクを開始する前に、AWS CDK 開発環境をセットアップし、次のコマンドを実行して AWS CDK をインストールします。AWS CDK 開発環境のセットアップ方法については、「Getting Started With the AWS CDK - Prerequisites」(の使用を開始する - 前提条件) を参照してください。

```
npm install -g aws-cdk
```

> **Note**
>
> これらの手順は、AWS CDK v2 を使用していることを前提としています。

トピック

ステップ 1:AWS CDK プロジェクトを設定する

新しいAWS CDKアプリケーションのディレクトリを作成し、プロジェクトを初期化します。

TypeScript

```
mkdir hello-ecs
cd hello-ecs
cdk init --language typescript
```

JavaScript

```
mkdir hello-ecs
cd hello-ecs
cdk init --language javascript
```

Python

```
mkdir hello-ecs
cd hello-ecs
cdk init --language python
```

プロジェクトが開始されたら、プロジェクトの仮想環境をアクティブにし、AWS CDK のベースラインの依存関係をインストールします。

```
source .venv/bin/activate
python -m pip install -r requirements.txt
```

Java

```
mkdir hello-ecs
```

```
cd hello-ecs
cdk init --language java
```

この Maven プロジェクトを Java IDE にインポートします。例えば Eclipse では、[File] (ファイル) > [Import] (インポート) > [Maven] > [Existing Maven Projects] (既存の Maven プロジェクト) を使用します。

C#

```
mkdir hello-ecs
cd hello-ecs
cdk init --language csharp
```

Go

```
mkdir hello-ecs
cd hello-ecs
cdk init --language go
```

> **Note**
>
> AWS CDKアプリケーションテンプレートは、プロジェクトディレクトリの名前を使用し、ソースファイルとクラスの名前を生成します。この例では、ディレクトリ名は `hello-ecs` です。別のプロジェクトディレクトリ名を使用する場合、アプリケーションはこれらの指示と一致しません。

AWS CDK v2 は、`aws-cdk-lib` と呼ばれる単一パッケージですべての AWS のサービス の安定した構成を含んでいます。このパッケージは、プロジェクト開始時に依存関係としてインストールされます。特定のプログラミング言語で作業する場合、パッケージはプロジェクトを初めて構築するときにインストールされます。このトピックでは、Amazon ECS の使用時に高レベルの抽象化を提供する、Amazon ECS Patterns 構成の使用方法について説明します。このモジュールは、Amazon ECS 構成およびその他の構成に依存し、Amazon ECS アプリケーションに必要なリソースをプロビジョニングします。

これらのライブラリを CDK アプリケーションにインポートする際に使用する名前は、使用するプログラミング言語によって若干異なります。参考として、サポートされている各 CDK プログラミング言語で使用される名前を以下に示します。

TypeScript

```
aws-cdk-lib/aws-ecs
aws-cdk-lib/aws-ecs-patterns
```

JavaScript

```
aws-cdk-lib/aws-ecs
aws-cdk-lib/aws-ecs-patterns
```

Python

```
aws_cdk.aws_ecs
aws_cdk.aws_ecs_patterns
```

Java

```
software.amazon.awscdk.services.ecs
software.amazon.awscdk.services.ecs.patterns
```

C#

```
Amazon.CDK.AWS.ECS
Amazon.CDK.AWS.ECS.Patterns
```

Go

```
github.com/aws/aws-cdk-go/awscdk/v2/awsecs
github.com/aws/aws-cdk-go/awscdk/v2/awsecspatterns
```

ステップ 2: AWS CDK を使用して、Fargate 上のコンテナ化されたウェブサーバーを定義する

DockerHub のコンテナイメージ amazon-ecs-sample を使用します。このイメージには、Amazon Linux 2 で実行される PHP ウェブアプリケーションが含まれています。

作成した AWS CDK プロジェクトで、スタック定義を含むファイルを次の例のいずれかと同様に編集します。

> **Note**
>
> スタックはデプロイの単位です。すべてのリソースがスタック内にある必要があり、スタック内のすべてのリソースは同時にデプロイされます。リソースのデプロイに失敗すると、既にデプロイされている他のリソースはロールバックされます。AWS CDK アプリケーションには複数のスタックを含めることができ、あるスタック内のリソースは別のスタック内のリソースを参照できます。

TypeScript

`lib/hello-ecs-stack.ts` を更新すると次のようになります。

```
import * as cdk from 'aws-cdk-lib';
import { Construct } from 'constructs';
import * as ecs from 'aws-cdk-lib/aws-ecs';
import * as ecsp from 'aws-cdk-lib/aws-ecs-patterns';

export class HelloEcsStack extends cdk.Stack {
  constructor(scope: Construct, id: string, props?: cdk.StackProps) {
    super(scope, id, props);

    new ecsp.ApplicationLoadBalancedFargateService(this, 'MyWebServer', {
      taskImageOptions: {
        image: ecs.ContainerImage.fromRegistry('amazon/amazon-ecs-sample'),
      },
      publicLoadBalancer: true
    });
  }
}
```

JavaScript

`lib/hello-ecs-stack.js` を更新すると次のようになります。

```
const cdk = require('aws-cdk-lib');
const { Construct } = require('constructs');
const ecs = require('aws-cdk-lib/aws-ecs');
const ecsp = require('aws-cdk-lib/aws-ecs-patterns');

class HelloEcsStack extends cdk.Stack {
  constructor(scope = Construct, id = string, props = cdk.StackProps) {
```

```
    super(scope, id, props);

    new ecsp.ApplicationLoadBalancedFargateService(this, 'MyWebServer', {
      taskImageOptions: {
        image: ecs.ContainerImage.fromRegistry('amazon/amazon-ecs-sample'),
      },
      publicLoadBalancer: true
    });
  }
}

module.exports = { HelloEcsStack }
```

Python

hello-ecs/hello_ecs_stack.py を更新すると次のようになります。

```
import aws_cdk as cdk
from constructs import Construct

import aws_cdk.aws_ecs as ecs
import aws_cdk.aws_ecs_patterns as ecsp

class HelloEcsStack(cdk.Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        ecsp.ApplicationLoadBalancedFargateService(self, "MyWebServer",
            task_image_options=ecsp.ApplicationLoadBalancedTaskImageOptions(
                image=ecs.ContainerImage.from_registry("amazon/amazon-ecs-sample")),
            public_load_balancer=True
        )
```

Java

src/main/java/com.myorg/HelloEcsStack.java を更新すると次のようになります。

```
package com.myorg;

import software.constructs.Construct;
import software.amazon.awscdk.Stack;
import software.amazon.awscdk.StackProps;
```

```
import software.amazon.awscdk.services.ecs.ContainerImage;
import
 software.amazon.awscdk.services.ecs.patterns.ApplicationLoadBalancedFargateService;
import
 software.amazon.awscdk.services.ecs.patterns.ApplicationLoadBalancedTaskImageOptions;

public class HelloEcsStack extends Stack {
    public HelloEcsStack(final Construct scope, final String id) {
        this(scope, id, null);
    }

    public HelloEcsStack(final Construct scope, final String id, final StackProps
 props) {
        super(scope, id, props);

        ApplicationLoadBalancedFargateService.Builder.create(this, "MyWebServer")
         .taskImageOptions(ApplicationLoadBalancedTaskImageOptions.builder()
           .image(ContainerImage.fromRegistry("amazon/amazon-ecs-sample"))
           .build())
         .publicLoadBalancer(true)
         .build();
    }
}
```

C#

src/HelloEcs/HelloEcsStack.cs を更新すると次のようになります。

```
using Amazon.CDK;
using Constructs;
using Amazon.CDK.AWS.ECS;
using Amazon.CDK.AWS.ECS.Patterns;
namespace HelloEcs
{
    public class HelloEcsStack : Stack
    {
        internal HelloEcsStack(Construct scope, string id, IStackProps props =
 null) : base(scope, id, props)
        {
            new ApplicationLoadBalancedFargateService(this, "MyWebServer",
                new ApplicationLoadBalancedFargateServiceProps
                {
                    TaskImageOptions = new ApplicationLoadBalancedTaskImageOptions
```

```
                    {
                        Image = ContainerImage.FromRegistry("amazon/amazon-ecs-
sample")
                    },
                    PublicLoadBalancer = true
                });
        }
    }
}
```

Go

hello-ecs.go を更新すると次のようになります。

```
package main

import (
 "github.com/aws/aws-cdk-go/awscdk/v2"
 // "github.com/aws/aws-cdk-go/awscdk/v2/awssqs"
 "github.com/aws/aws-cdk-go/awscdk/v2/awsecs"
 "github.com/aws/aws-cdk-go/awscdk/v2/awsecspatterns"
 "github.com/aws/constructs-go/constructs/v10"
 "github.com/aws/jsii-runtime-go"
)

type HelloEcsStackProps struct {
 awscdk.StackProps
}

func NewHelloEcsStack(scope constructs.Construct, id string, props
 *HelloEcsStackProps) awscdk.Stack {
 var sprops awscdk.StackProps
 if props != nil {
  sprops = props.StackProps
 }
 stack := awscdk.NewStack(scope, &id, &sprops)

 // The code that defines your stack goes here

 // example resource
 // queue := awssqs.NewQueue(stack, jsii.String("HelloEcsQueue"),
 &awssqs.QueueProps{
 //  VisibilityTimeout: awscdk.Duration_Seconds(jsii.Number(300)),
 // })
```

```
 res := awsecspatterns.NewApplicationLoadBalancedFargateService(stack,
 jsii.String("MyWebServer"),
  &awsecspatterns.ApplicationLoadBalancedFargateServiceProps{
   TaskImageOptions: &awsecspatterns.ApplicationLoadBalancedTaskImageOptions{
    Image: awsecs.ContainerImage_FromRegistry(jsii.String("amazon/amazon-ecs-
sample"), &awsecs.RepositoryImageProps{}),
   },
  },
 )
 awscdk.NewCfnOutput(stack, jsii.String("LoadBalancerDNS"),
 &awscdk.CfnOutputProps{Value: res.LoadBalancer().LoadBalancerDnsName()})

 return stack
}

func main() {
 defer jsii.Close()

 app := awscdk.NewApp(nil)

 NewHelloEcsStack(app, "HelloEcsStack", &HelloEcsStackProps{
  awscdk.StackProps{
   Env: env(),
  },
 })

 app.Synth(nil)
}

// env determines the AWS environment (account+region) in which our stack is to
// be deployed. For more information see: https://docs.aws.amazon.com/cdk/latest/
guide/environments.html
func env() *awscdk.Environment {
 // If unspecified, this stack will be "environment-agnostic".
 // Account/Region-dependent features and context lookups will not work, but a
 // single synthesized template can be deployed anywhere.
 //---------------------------------------------------------------------------
 return nil

 // Uncomment if you know exactly what account and region you want to deploy
 // the stack to. This is the recommendation for production stacks.
 //---------------------------------------------------------------------------
 // return &awscdk.Environment{
 //  Account: jsii.String("123456789012"),
```

```
 //  Region:  jsii.String("us-east-1"),
 // }

 // Uncomment to specialize this stack for the AWS Account and Region that are
 // implied by the current CLI configuration. This is recommended for dev
 // stacks.
 //---------------------------------------------------------------------------
 // return &awscdk.Environment{
 //  Account: jsii.String(os.Getenv("CDK_DEFAULT_ACCOUNT")),
 //  Region:  jsii.String(os.Getenv("CDK_DEFAULT_REGION")),
 // }
}
```

前述の短いスニペットには次のものが含まれます。

- サービスの論理名: `MyWebServer`。
- DockerHub から取得したコンテナイメージ: `amazon/amazon-ecs-sample`。
- ロードバランサーが公開アドレスを持ち、インターネットからアクセスできる事実といった、その他の関連情報。

AWS CDK は、次のリソースを含む、ウェブサーバーのデプロイに必要なすべてのリソースを作成します。この例では、これらのリソースは省略されています。

- Amazon ECS クラスター
- Amazon VPC と Amazon EC2 インスタンス
- Auto Scaling グループ
- Application Load Balancer
- IAM ロールとポリシー

自動プロビジョニングされたリソースの一部は、スタックで定義されているすべての Amazon ECS サービスにより共有されます。

ソースファイルを保存し、アプリケーションのメインディレクトリで `cdk synth` コマンドを実行します。AWS CDK はアプリケーションを実行し、そのアプリケーションから AWS CloudFormation テンプレートを合成して、テンプレートを表示します。テンプレートは約 600 行の YAML ファイルです。ファイルの先頭は以下のとおりです。テンプレートはこの例と異なる場合があります。

```
Resources:
  MyWebServerLB3B5FD3AB:
    Type: AWS::ElasticLoadBalancingV2::LoadBalancer
    Properties:
      LoadBalancerAttributes:
        - Key: deletion_protection.enabled
          Value: "false"
      Scheme: internet-facing
      SecurityGroups:
        - Fn::GetAtt:
            - MyWebServerLBSecurityGroup01B285AA
            - GroupId
      Subnets:
        - Ref: EcsDefaultClusterMnL3mNNYNVpcPublicSubnet1Subnet3C273B99
        - Ref: EcsDefaultClusterMnL3mNNYNVpcPublicSubnet2Subnet95FF715A
      Type: application
    DependsOn:
      - EcsDefaultClusterMnL3mNNYNVpcPublicSubnet1DefaultRouteFF4E2178
      - EcsDefaultClusterMnL3mNNYNVpcPublicSubnet2DefaultRouteB1375520
    Metadata:
      aws:cdk:path: HelloEcsStack/MyWebServer/LB/Resource
  MyWebServerLBSecurityGroup01B285AA:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Automatically created Security Group for ELB
 HelloEcsStackMyWebServerLB06757F57
      SecurityGroupIngress:
        - CidrIp: 0.0.0.0/0
          Description: Allow from anyone on port 80
          FromPort: 80
          IpProtocol: tcp
          ToPort: 80
      VpcId:
        Ref: EcsDefaultClusterMnL3mNNYNVpc7788A521
    Metadata:
      aws:cdk:path: HelloEcsStack/MyWebServer/LB/SecurityGroup/Resource
# and so on for another few hundred lines
```

AWS アカウント でサービスをデプロイするには、cdk deploy コマンドをアプリケーションのメインディレクトリで実行します。AWS CDK が生成した IAM ポリシーを、承認するよう求められます。

デプロイには数分かかり、その間に AWS CDK は複数のリソースを作成します。デプロイからの出力の末尾数行に、ロードバランサーの公開ホスト名と、新しいウェブサーバーの URL が含まれます。その内容は次のとおりです。

```
Outputs:
HelloEcsStack.MyWebServerLoadBalancerDNSXXXXXXXX = Hello-MyWeb-ZZZZZZZZZZZZZ-
ZZZZZZZZZZ.us-west-2.elb.amazonaws.com
HelloEcsStack.MyWebServerServiceURLYYYYYYYY = http://Hello-MyWeb-ZZZZZZZZZZZZZ-
ZZZZZZZZZZ.us-west-2.elb.amazonaws.com
```

ステップ 3: ウェブサーバーをテストする

デプロイ出力から URL をコピーし、ウェブブラウザに貼り付けます。ウェブサーバーからの次のウェルカムメッセージが表示されます。

ステップ 4: クリーンアップする

ウェブサーバーの使用が終了したら、CDK を使用して `cdk destroy` コマンドをアプリケーションのメインディレクトリで実行し、サービスを終了します。これにより、将来的に想定外の請求が発生するのを防げます。

次のステップ

AWS CDK を使用して AWS インフラストラクチャを開発する方法の詳細については、「AWS CDK デベロッパーガイド」を参照してください。

選択した言語で AWS CDK アプリケーションを記述する方法については、以下を参照してください。

TypeScript

TypeScript で AWS CDK を操作

JavaScript

JavaScript で AWS CDK を操作

Python

Python で AWS CDK を捜査

Java

Java で AWS CDK を操作

C#

C# で AWS CDK を操作

Go

Go での AWS CDK の操作

このトピックで使用する AWS 構成ライブラリモジュールの詳細は、以下の AWS CDK API リファレンスの概要を参照してください。

- aws-ecs
- aws-ecs-patterns

AWS CloudFormation を使用した Amazon ECS リソースの作成

Amazon ECS は AWS CloudFormation と統合されています。これは、ユーザーが定義したテンプレートで AWS リソースをモデル化してセットアップする際に使用できるサービスです。これにより、リソースとインフラストラクチャの作成、管理に費やす時間を短縮できます。AWS CloudFormation を使用して、特定の Amazon ECS クラスターなど、必要なすべての AWS リソースを説明するテンプレートを作成できます。次に、AWS CloudFormation はプロビジョニングと必要なリソースの設定を行います。

AWS CloudFormation を使用すると、テンプレートを再利用して Amazon ECS リソースを一貫して繰り返しセットアップできます。リソースを一度記述すると、複数の AWS アカウント および AWS リージョン 全体で同じリソースを再度プロビジョニングできます。

AWS CloudFormation テンプレート

Amazon ECS および関連サービスのリソースをプロビジョニングして設定するには、AWS CloudFormation テンプレートについて理解しておく必要があります。AWS CloudFormation テンプレートは、AWS CloudFormation スタックでプロビジョニングするリソースを記述する JSON または YAML 形式のテキストファイルです。JSON や YAML 形式に不慣れな方は、AWS CloudFormation Designer を使用することで AWS CloudFormation テンプレートの使用を開始できます。詳細については、AWS CloudFormation ユーザーガイドの AWS CloudFormationDesigner とは を参照してください。

Amazon ECS は、クラスター、タスク定義、サービス、タスクセットの作成を AWS CloudFormation でサポートしています。以下の例では、AWS CLI を使用して、これらのテンプレートによってリソースを作成する方法を説明しています。これらのリソースは、AWS CloudFormation コンソールを使用して作成することもできます。AWS CloudFormation コンソールを使用してリソースを作成する方法の詳細については、「AWS CloudFormation ユーザーガイド」を参照してください。

テンプレートの例

別のスタックを使用して Amazon ECS リソースを作成する

以下の例では、リソースごとに別のスタックを使用して Amazon ECS リソースを作成する方法を説明しています。

タスク定義

以下のテンプレートを使用して、Fargate Linux タスクを作成できます。

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Resources": {
       "ECSTaskDefinition": {
          "Type": "AWS::ECS::TaskDefinition",
          "Properties": {
              "ContainerDefinitions": [
                  {
                      "Command": [
                          "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS
Sample App</title> <style>body {margin-top: 40px; background-color: #333;} </style>
```

```
 </head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</
h1> <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html &&
 httpd-foreground\""
                        ],
                        "EntryPoint": [
                            "sh",
                            "-c"
                        ],
                        "Essential": true,
                        "Image": "public.ecr.aws/docker/library/httpd:2.4",
                        "LogConfiguration": {
                            "LogDriver": "awslogs",
                            "Options": {
                                "awslogs-group": "/ecs/fargate-task-definition",
                                "awslogs-region": "us-east-1",
                                "awslogs-stream-prefix": "ecs"
                            }
                        },
                        "Name": "sample-fargate-app",
                        "PortMappings": [
                            {
                                "ContainerPort": 80,
                                "HostPort": 80,
                                "Protocol": "tcp"
                            }
                        ]
                    }
                ],
                "Cpu": 256,
                "ExecutionRoleArn": "arn:aws:iam::aws_account_id:role/
ecsTaskExecutionRole",
                "Family": "task-definition-cfn",
                "Memory": 512,
                "NetworkMode": "awsvpc",
                "RequiresCompatibilities": [
                    "FARGATE"
                ],
                "RuntimePlatform": {
                    "OperatingSystemFamily": "LINUX"
                }
            }

        }
```

```
        }
    }
```

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  ECSTaskDefinition:
    Type: 'AWS::ECS::TaskDefinition'
    Properties:
      ContainerDefinitions:
        - Command:
            - >-
              /bin/sh -c "echo '<html> <head> <title>Amazon ECS Sample
              App</title> <style>body {margin-top: 40px; background-color:
              #333;} </style> </head><body> <div
              style=color:white;text-align:center> <h1>Amazon ECS Sample
              App</h1> <h2>Congratulations!</h2> <p>Your application is now
              running on a container in Amazon ECS.</p> </div></body></html>' >
              /usr/local/apache2/htdocs/index.html && httpd-foreground"
          EntryPoint:
            - sh
            - '-c'
          Essential: true
          Image: 'public.ecr.aws/docker/library/httpd:2.4'
          LogConfiguration:
            LogDriver: awslogs
            Options:
              awslogs-group: /ecs/fargate-task-definition
              awslogs-region: us-east-1
              awslogs-stream-prefix: ecs
          Name: sample-fargate-app
          PortMappings:
            - ContainerPort: 80
              HostPort: 80
              Protocol: tcp
      Cpu: 256
      ExecutionRoleArn: 'arn:aws:iam::aws_account_id:role/ecsTaskExecutionRole'
      Family: task-definition-cfn
      Memory: 512
      NetworkMode: awsvpc
      RequiresCompatibilities:
        - FARGATE
```

```
      RuntimePlatform:
        OperatingSystemFamily: LINUX
```

クラスター

以下のテンプレートを使用して、空のクラスターを作成できます。

JSON

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
        "ECSCluster": {
            "Type": "AWS::ECS::Cluster",
            "Properties": {
                "ClusterName": "MyEmptyCluster"
            }
        }
    }
}
```

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  ECSCluster:
    Type: 'AWS::ECS::Cluster'
    Properties:
      ClusterName: MyEmptyCluster
```

AL2023 Amazon ECS-Optimized-AMI を使用してクラスターを作成する

キャパシティープロバイダーを使用して Amazon EC2 で AL2023 インスタンスを起動するクラスターを定義します。

> **Important**
>
> 最新の AMI ID については、「Amazon Elastic Container Service デベロッパーガイド」の「Amazon ECS-optimized AMI」(Amazon ECS に最適化された AMI) を参照してください。

JSON

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Description": "EC2 ECS cluster that starts out empty, with no EC2 instances
 yet. An ECS capacity provider automatically launches more EC2 instances as required
 on the fly when you request ECS to launch services or standalone tasks.",
    "Parameters": {
        "InstanceType": {
            "Type": "String",
            "Description": "EC2 instance type",
            "Default": "t2.medium",
            "AllowedValues": [
                "t1.micro",
                "t2.2xlarge",
                "t2.large",
                "t2.medium",
                "t2.micro",
                "t2.nano",
                "t2.small",
                "t2.xlarge",
                "t3.2xlarge",
                "t3.large",
                "t3.medium",
                "t3.micro",
                "t3.nano",
                "t3.small",
                "t3.xlarge"
            ]
        },
        "DesiredCapacity": {
            "Type": "Number",
            "Default": "0",
            "Description": "Number of EC2 instances to launch in your ECS cluster."
        },
        "MaxSize": {
            "Type": "Number",
            "Default": "100",
            "Description": "Maximum number of EC2 instances that can be launched in
 your ECS cluster."
        },
        "ECSAMI": {
            "Description": "The Amazon Machine Image ID used for the cluster",
            "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
```

```
            "Default": "/aws/service/ecs/optimized-ami/amazon-linux-2023/
recommended/image_id"
        },
        "VpcId": {
            "Type": "AWS::EC2::VPC::Id",
            "Description": "VPC ID where the ECS cluster is launched",
            "Default": "vpc-1234567890abcdef0"
        },
        "SubnetIds": {
            "Type": "List<AWS::EC2::Subnet::Id>",
            "Description": "List of subnet IDs where the EC2 instances will be
 launched",
            "Default": "subnet-021345abcdef67890"
        }
    },
    "Resources": {
        "ECSCluster": {
            "Type": "AWS::ECS::Cluster",
            "Properties": {
                "ClusterSettings": [
                    {
                        "Name": "containerInsights",
                        "Value": "enabled"
                    }
                ]
            }
        },
        "ECSAutoScalingGroup": {
            "Type": "AWS::AutoScaling::AutoScalingGroup",
            "DependsOn": [
                "ECSCluster",
                "EC2Role"
            ],
            "Properties": {
                "VPCZoneIdentifier": {
                    "Ref": "SubnetIds"
                },
                "LaunchTemplate": {
                    "LaunchTemplateId": {
                        "Ref": "ContainerInstances"
                    },
                    "Version": {
                        "Fn::GetAtt": [
                            "ContainerInstances",
```

```
                            "LatestVersionNumber"
                        ]
                    }
                },
                "MinSize": 0,
                "MaxSize": {
                    "Ref": "MaxSize"
                },
                "DesiredCapacity": {
                    "Ref": "DesiredCapacity"
                },
                "NewInstancesProtectedFromScaleIn": true
            },
            "UpdatePolicy": {
                "AutoScalingReplacingUpdate": {
                    "WillReplace": "true"
                }
            }
        },
        "ContainerInstances": {
            "Type": "AWS::EC2::LaunchTemplate",
            "Properties": {
                "LaunchTemplateName": "asg-launch-template-2",
                "LaunchTemplateData": {
                    "ImageId": {
                        "Ref": "ECSAMI"
                    },
                    "InstanceType": {
                        "Ref": "InstanceType"
                    },
                    "IamInstanceProfile": {
                        "Name": {
                            "Ref": "EC2InstanceProfile"
                        }
                    },
                    "SecurityGroupIds": [
                        {
                            "Ref": "ContainerHostSecurityGroup"
                        }
                    ],
                    "UserData": {
                        "Fn::Base64": {
                            "Fn::Sub": "#!/bin/bash -xe\n echo ECS_CLUSTER=
${ECSCluster} >> /etc/ecs/ecs.config\n yum install -y aws-cfn-bootstrap\n /opt/aws/
```

```
bin/cfn-init -v --stack ${AWS::StackId} --resource ContainerInstances --configsets
 full_install --region ${AWS::Region} &\n"
                        }
                    },
                    "MetadataOptions": {
                        "HttpEndpoint": "enabled",
                        "HttpTokens": "required"
                    }
                }
            }
        },
        "EC2InstanceProfile": {
            "Type": "AWS::IAM::InstanceProfile",
            "Properties": {
                "Path": "/",
                "Roles": [
                    {
                        "Ref": "EC2Role"
                    }
                ]
            }
        },
        "CapacityProvider": {
            "Type": "AWS::ECS::CapacityProvider",
            "Properties": {
                "AutoScalingGroupProvider": {
                    "AutoScalingGroupArn": {
                        "Ref": "ECSAutoScalingGroup"
                    },
                    "ManagedScaling": {
                        "InstanceWarmupPeriod": 60,
                        "MinimumScalingStepSize": 1,
                        "MaximumScalingStepSize": 100,
                        "Status": "ENABLED",
                        "TargetCapacity": 100
                    },
                    "ManagedTerminationProtection": "ENABLED"
                }
            }
        },
        "CapacityProviderAssociation": {
            "Type": "AWS::ECS::ClusterCapacityProviderAssociations",
            "Properties": {
                "CapacityProviders": [
```

```
                {
                    "Ref": "CapacityProvider"
                }
            ],
            "Cluster": {
                "Ref": "ECSCluster"
            },
            "DefaultCapacityProviderStrategy": [
                {
                    "Base": 0,
                    "CapacityProvider": {
                        "Ref": "CapacityProvider"
                    },
                    "Weight": 1
                }
            ]
        }
    },
    "ContainerHostSecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Access to the EC2 hosts that run containers",
            "VpcId": {
                "Ref": "VpcId"
            }
        }
    },
    "EC2Role": {
        "Type": "AWS::IAM::Role",
        "Properties": {
            "AssumeRolePolicyDocument": {
                "Statement": [
                    {
                        "Effect": "Allow",
                        "Principal": {
                            "Service": [
                                "ec2.amazonaws.com"
                            ]
                        },
                        "Action": [
                            "sts:AssumeRole"
                        ]
                    }
                ]
```

```
                },
                "Path": "/",
                "ManagedPolicyArns": [
                    "arn:aws:iam::aws:policy/service-role/
AmazonEC2ContainerServiceforEC2Role",
                    "arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore"
                ]
            }
        },
        "ECSTaskExecutionRole": {
            "Type": "AWS::IAM::Role",
            "Properties": {
                "AssumeRolePolicyDocument": {
                    "Statement": [
                        {
                            "Effect": "Allow",
                            "Principal": {
                                "Service": [
                                    "ecs-tasks.amazonaws.com"
                                ]
                            },
                            "Action": [
                                "sts:AssumeRole"
                            ],
                            "Condition": {
                                "ArnLike": {
                                    "aws:SourceArn": {
                                        "Fn::Sub": "arn:${AWS::Partition}:ecs:
${AWS::Region}:${AWS::AccountId}:*"
                                    }
                                },
                                "StringEquals": {
                                    "aws:SourceAccount": {
                                        "Fn::Sub": "${AWS::AccountId}"
                                    }
                                }
                            }
                        }
                    ]
                },
                "Path": "/",
                "ManagedPolicyArns": [
                    "arn:aws:iam::aws:policy/service-role/
AmazonECSTaskExecutionRolePolicy"
```

```
                ]
            }
        }
    },
    "Outputs": {
        "ClusterName": {
            "Description": "The ECS cluster into which to launch resources",
            "Value": "ECSCluster"
        },
        "ECSTaskExecutionRole": {
            "Description": "The role used to start up a task",
            "Value": "ECSTaskExecutionRole"
        },
        "CapacityProvider": {
            "Description": "The cluster capacity provider that the service should
 use to request capacity when it wants to start up a task",
            "Value": "CapacityProvider"
        }
    }
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Description: EC2 ECS cluster that starts out empty, with no EC2 instances yet. An
 ECS capacity provider automatically launches more EC2 instances as required on the
 fly when you request ECS to launch services or standalone tasks.
Parameters:
  InstanceType:
    Type: String
    Description: EC2 instance type
    Default: t2.medium
    AllowedValues:
      - t1.micro
      - t2.2xlarge
      - t2.large
      - t2.medium
      - t2.micro
      - t2.nano
      - t2.small
      - t2.xlarge
      - t3.2xlarge
      - t3.large
```

```
      - t3.medium
      - t3.micro
      - t3.nano
      - t3.small
      - t3.xlarge
  DesiredCapacity:
    Type: Number
    Default: '0'
    Description: Number of EC2 instances to launch in your ECS cluster.
  MaxSize:
    Type: Number
    Default: '100'
    Description: Maximum number of EC2 instances that can be launched in your ECS
 cluster.
  ECSAMI:
    Description: The Amazon Machine Image ID used for the cluster
    Type: AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>
    Default: /aws/service/ecs/optimized-ami/amazon-linux-2023/recommended/image_id
  VpcId:
    Type: AWS::EC2::VPC::Id
    Description: VPC ID where the ECS cluster is launched
    Default: vpc-1234567890abcdef0
  SubnetIds:
    Type: List<AWS::EC2::Subnet::Id>
    Description: List of subnet IDs where the EC2 instances will be launched
    Default: subnet-021345abcdef67890
Resources:
  ECSCluster:
    Type: AWS::ECS::Cluster
    Properties:
      ClusterSettings:
        - Name: containerInsights
          Value: enabled
  ECSAutoScalingGroup:
    Type: AWS::AutoScaling::AutoScalingGroup
    DependsOn:
      - ECSCluster
      - EC2Role
    Properties:
      VPCZoneIdentifier: !Ref SubnetIds
      LaunchTemplate:
        LaunchTemplateId: !Ref ContainerInstances
        Version: !GetAtt ContainerInstances.LatestVersionNumber
      MinSize: 0
```

```
      MaxSize: !Ref MaxSize
      DesiredCapacity: !Ref DesiredCapacity
      NewInstancesProtectedFromScaleIn: true
    UpdatePolicy:
      AutoScalingReplacingUpdate:
        WillReplace: 'true'
  ContainerInstances:
    Type: AWS::EC2::LaunchTemplate
    Properties:
      LaunchTemplateName: asg-launch-template-2
      LaunchTemplateData:
        ImageId: !Ref ECSAMI
        InstanceType: !Ref InstanceType
        IamInstanceProfile:
          Name: !Ref EC2InstanceProfile
        SecurityGroupIds:
          - !Ref ContainerHostSecurityGroup
        UserData: !Base64
          Fn::Sub: |
            #!/bin/bash -xe
            echo ECS_CLUSTER=${ECSCluster} >> /etc/ecs/ecs.config
            yum install -y aws-cfn-bootstrap
            /opt/aws/bin/cfn-init -v --stack ${AWS::StackId} --resource
ContainerInstances --configsets full_install --region ${AWS::Region} &
        MetadataOptions:
          HttpEndpoint: enabled
          HttpTokens: required
  EC2InstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      Path: /
      Roles:
        - !Ref EC2Role
  CapacityProvider:
    Type: AWS::ECS::CapacityProvider
    Properties:
      AutoScalingGroupProvider:
        AutoScalingGroupArn: !Ref ECSAutoScalingGroup
        ManagedScaling:
          InstanceWarmupPeriod: 60
          MinimumScalingStepSize: 1
          MaximumScalingStepSize: 100
          Status: ENABLED
          TargetCapacity: 100
```

```
      ManagedTerminationProtection: ENABLED
  CapacityProviderAssociation:
    Type: AWS::ECS::ClusterCapacityProviderAssociations
    Properties:
      CapacityProviders:
        - !Ref CapacityProvider
      Cluster: !Ref ECSCluster
      DefaultCapacityProviderStrategy:
        - Base: 0
          CapacityProvider: !Ref CapacityProvider
          Weight: 1
  ContainerHostSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Access to the EC2 hosts that run containers
      VpcId: !Ref VpcId
  EC2Role:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
  ECSTaskExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ecs-tasks.amazonaws.com
            Action:
              - sts:AssumeRole
            Condition:
              ArnLike:
```

```
                aws:SourceArn: !Sub arn:${AWS::Partition}:ecs:${AWS::Region}:
${AWS::AccountId}:*
              StringEquals:
                aws:SourceAccount: !Sub ${AWS::AccountId}
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy
Outputs:
  ClusterName:
    Description: The ECS cluster into which to launch resources
    Value: ECSCluster
  ECSTaskExecutionRole:
    Description: The role used to start up a task
    Value: ECSTaskExecutionRole
  CapacityProvider:
    Description: The cluster capacity provider that the service should use to
 request capacity when it wants to start up a task
    Value: CapacityProvider
```

サービスをデプロイします。

次のテンプレートは、キャパシティープロバイダーを使用して AL2023 キャパシティーの実行をリクエストするサービスを定義しています。コンテナは、オンラインになると AL2023 インスタンスで起動します。

JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "An example service that deploys in AWS VPC networking mode on
 EC2 capacity. Service uses a capacity provider to request EC2 instances to run
 on. Service runs with networking in private subnets, but still accessible to the
 internet via a load balancer hosted in public subnets.",
  "Parameters": {
      "VpcId": {
          "Type": "String",
          "Description": "The VPC that the service is running inside of"
      },
      "PublicSubnetIds": {
          "Type": "List<AWS::EC2::Subnet::Id>",
          "Description": "List of public subnet ID's to put the load balancer in"
      },
```

```
    "PrivateSubnetIds": {
        "Type": "List<AWS::EC2::Subnet::Id>",
        "Description": "List of private subnet ID's that the AWS VPC tasks are in"
    },
    "ClusterName": {
        "Type": "String",
        "Description": "The name of the ECS cluster into which to launch
capacity."
    },
    "ECSTaskExecutionRole": {
        "Type": "String",
        "Description": "The role used to start up an ECS task"
    },
    "CapacityProvider": {
        "Type": "String",
        "Description": "The cluster capacity provider that the service should use
to request capacity when it wants to start up a task"
    },
    "ServiceName": {
        "Type": "String",
        "Default": "web",
        "Description": "A name for the service"
    },
    "ImageUrl": {
        "Type": "String",
        "Default": "public.ecr.aws/docker/library/nginx:latest",
        "Description": "The url of a docker image that contains the application
process that will handle the traffic for this service"
    },
    "ContainerCpu": {
        "Type": "Number",
        "Default": 256,
        "Description": "How much CPU to give the container. 1024 is 1 CPU"
    },
    "ContainerMemory": {
        "Type": "Number",
        "Default": 512,
        "Description": "How much memory in megabytes to give the container"
    },
    "ContainerPort": {
        "Type": "Number",
        "Default": 80,
        "Description": "What port that the application expects traffic on"
    },
```

```
        "DesiredCount": {
            "Type": "Number",
            "Default": 2,
            "Description": "How many copies of the service task to run"
        }
    },
    "Resources": {
        "TaskDefinition": {
            "Type": "AWS::ECS::TaskDefinition",
            "Properties": {
                "Family": {
                    "Ref": "ServiceName"
                },
                "Cpu": {
                    "Ref": "ContainerCpu"
                },
                "Memory": {
                    "Ref": "ContainerMemory"
                },
                "NetworkMode": "awsvpc",
                "RequiresCompatibilities": [
                    "EC2"
                ],
                "ExecutionRoleArn": {
                    "Ref": "ECSTaskExecutionRole"
                },
                "ContainerDefinitions": [
                    {
                        "Name": {
                            "Ref": "ServiceName"
                        },
                        "Cpu": {
                            "Ref": "ContainerCpu"
                        },
                        "Memory": {
                            "Ref": "ContainerMemory"
                        },
                        "Image": {
                            "Ref": "ImageUrl"
                        },
                        "PortMappings": [
                            {
                                "ContainerPort": {
                                    "Ref": "ContainerPort"
```

```
                            },
                            "HostPort": {
                                "Ref": "ContainerPort"
                            }
                        }
                    ],
                    "LogConfiguration": {
                        "LogDriver": "awslogs",
                        "Options": {
                            "mode": "non-blocking",
                            "max-buffer-size": "25m",
                            "awslogs-group": {
                                "Ref": "LogGroup"
                            },
                            "awslogs-region": {
                                "Ref": "AWS::Region"
                            },
                            "awslogs-stream-prefix": {
                                "Ref": "ServiceName"
                            }
                        }
                    }
                }
            ]
        }
    },
    "Service": {
        "Type": "AWS::ECS::Service",
        "DependsOn": "PublicLoadBalancerListener",
        "Properties": {
            "ServiceName": {
                "Ref": "ServiceName"
            },
            "Cluster": {
                "Ref": "ClusterName"
            },
            "PlacementStrategies": [
                {
                    "Field": "attribute:ecs.availability-zone",
                    "Type": "spread"
                },
                {
                    "Field": "cpu",
                    "Type": "binpack"
```

```
                }
            ],
            "CapacityProviderStrategy": [
                {
                    "Base": 0,
                    "CapacityProvider": {
                        "Ref": "CapacityProvider"
                    },
                    "Weight": 1
                }
            ],
            "NetworkConfiguration": {
                "AwsvpcConfiguration": {
                    "SecurityGroups": [
                        {
                            "Ref": "ServiceSecurityGroup"
                        }
                    ],
                    "Subnets": {
                        "Ref": "PrivateSubnetIds"
                    }
                }
            },
            "DeploymentConfiguration": {
                "MaximumPercent": 200,
                "MinimumHealthyPercent": 75
            },
            "DesiredCount": {
                "Ref": "DesiredCount"
            },
            "TaskDefinition": {
                "Ref": "TaskDefinition"
            },
            "LoadBalancers": [
                {
                    "ContainerName": {
                        "Ref": "ServiceName"
                    },
                    "ContainerPort": {
                        "Ref": "ContainerPort"
                    },
                    "TargetGroupArn": {
                        "Ref": "ServiceTargetGroup"
                    }
```

```
                }
            ]
        }
    },
    "ServiceSecurityGroup": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Security group for service",
            "VpcId": {
                "Ref": "VpcId"
            }
        }
    },
    "ServiceTargetGroup": {
        "Type": "AWS::ElasticLoadBalancingV2::TargetGroup",
        "Properties": {
            "HealthCheckIntervalSeconds": 6,
            "HealthCheckPath": "/",
            "HealthCheckProtocol": "HTTP",
            "HealthCheckTimeoutSeconds": 5,
            "HealthyThresholdCount": 2,
            "TargetType": "ip",
            "Port": {
                "Ref": "ContainerPort"
            },
            "Protocol": "HTTP",
            "UnhealthyThresholdCount": 10,
            "VpcId": {
                "Ref": "VpcId"
            },
            "TargetGroupAttributes": [
                {
                    "Key": "deregistration_delay.timeout_seconds",
                    "Value": 0
                }
            ]
        }
    },
    "PublicLoadBalancerSG": {
        "Type": "AWS::EC2::SecurityGroup",
        "Properties": {
            "GroupDescription": "Access to the public facing load balancer",
            "VpcId": {
                "Ref": "VpcId"
```

```
            },
            "SecurityGroupIngress": [
                {
                    "CidrIp": "0.0.0.0/0",
                    "IpProtocol": -1
                }
            ]
        }
    },
    "PublicLoadBalancer": {
        "Type": "AWS::ElasticLoadBalancingV2::LoadBalancer",
        "Properties": {
            "Scheme": "internet-facing",
            "LoadBalancerAttributes": [
                {
                    "Key": "idle_timeout.timeout_seconds",
                    "Value": "30"
                }
            ],
            "Subnets": {
                "Ref": "PublicSubnetIds"
            },
            "SecurityGroups": [
                {
                    "Ref": "PublicLoadBalancerSG"
                }
            ]
        }
    },
    "PublicLoadBalancerListener": {
        "Type": "AWS::ElasticLoadBalancingV2::Listener",
        "Properties": {
            "DefaultActions": [
                {
                    "Type": "forward",
                    "ForwardConfig": {
                        "TargetGroups": [
                            {
                                "TargetGroupArn": {
                                    "Ref": "ServiceTargetGroup"
                                },
                                "Weight": 100
                            }
                        ]
```

```
                    }
                }
            ],
            "LoadBalancerArn": {
                "Ref": "PublicLoadBalancer"
            },
            "Port": 80,
            "Protocol": "HTTP"
        }
    },
    "ServiceIngressfromLoadBalancer": {
        "Type": "AWS::EC2::SecurityGroupIngress",
        "Properties": {
            "Description": "Ingress from the public ALB",
            "GroupId": {
                "Ref": "ServiceSecurityGroup"
            },
            "IpProtocol": -1,
            "SourceSecurityGroupId": {
                "Ref": "PublicLoadBalancerSG"
            }
        }
    },
    "LogGroup": {
        "Type": "AWS::Logs::LogGroup"
    }
  }
}
```

YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Description: >-
  An example service that deploys in AWS VPC networking mode on EC2 capacity.
  Service uses a capacity provider to request EC2 instances to run on. Service
  runs with networking in private subnets, but still accessible to the internet
  via a load balancer hosted in public subnets.
Parameters:
  VpcId:
    Type: String
    Description: The VPC that the service is running inside of
  PublicSubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
```

```
    Description: List of public subnet ID's to put the load balancer in
  PrivateSubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
    Description: List of private subnet ID's that the AWS VPC tasks are in
  ClusterName:
    Type: String
    Description: The name of the ECS cluster into which to launch capacity.
  ECSTaskExecutionRole:
    Type: String
    Description: The role used to start up an ECS task
  CapacityProvider:
    Type: String
    Description: >-
      The cluster capacity provider that the service should use to request
      capacity when it wants to start up a task
  ServiceName:
    Type: String
    Default: web
    Description: A name for the service
  ImageUrl:
    Type: String
    Default: 'public.ecr.aws/docker/library/nginx:latest'
    Description: >-
      The url of a docker image that contains the application process that will
      handle the traffic for this service
  ContainerCpu:
    Type: Number
    Default: 256
    Description: How much CPU to give the container. 1024 is 1 CPU
  ContainerMemory:
    Type: Number
    Default: 512
    Description: How much memory in megabytes to give the container
  ContainerPort:
    Type: Number
    Default: 80
    Description: What port that the application expects traffic on
  DesiredCount:
    Type: Number
    Default: 2
    Description: How many copies of the service task to run
Resources:
  TaskDefinition:
    Type: 'AWS::ECS::TaskDefinition'
```

```
    Properties:
      Family: !Ref ServiceName
      Cpu: !Ref ContainerCpu
      Memory: !Ref ContainerMemory
      NetworkMode: awsvpc
      RequiresCompatibilities:
        - EC2
      ExecutionRoleArn: !Ref ECSTaskExecutionRole
      ContainerDefinitions:
        - Name: !Ref ServiceName
          Cpu: !Ref ContainerCpu
          Memory: !Ref ContainerMemory
          Image: !Ref ImageUrl
          PortMappings:
            - ContainerPort: !Ref ContainerPort
              HostPort: !Ref ContainerPort
          LogConfiguration:
            LogDriver: awslogs
            Options:
              mode: non-blocking
              max-buffer-size: 25m
              awslogs-group: !Ref LogGroup
              awslogs-region: !Ref AWS::Region
              awslogs-stream-prefix: !Ref ServiceName
  Service:
    Type: AWS::ECS::Service
    DependsOn: PublicLoadBalancerListener
    Properties:
      ServiceName: !Ref ServiceName
      Cluster: !Ref ClusterName
      PlacementStrategies:
        - Field: 'attribute:ecs.availability-zone'
          Type: spread
        - Field: cpu
          Type: binpack
      CapacityProviderStrategy:
        - Base: 0
          CapacityProvider: !Ref CapacityProvider
          Weight: 1
      NetworkConfiguration:
        AwsvpcConfiguration:
          SecurityGroups:
            - !Ref ServiceSecurityGroup
          Subnets: !Ref PrivateSubnetIds
```

```
      DeploymentConfiguration:
        MaximumPercent: 200
        MinimumHealthyPercent: 75
      DesiredCount: !Ref DesiredCount
      TaskDefinition: !Ref TaskDefinition
      LoadBalancers:
        - ContainerName: !Ref ServiceName
          ContainerPort: !Ref ContainerPort
          TargetGroupArn: !Ref ServiceTargetGroup
  ServiceSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Security group for service
      VpcId: !Ref VpcId
  ServiceTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      HealthCheckIntervalSeconds: 6
      HealthCheckPath: /
      HealthCheckProtocol: HTTP
      HealthCheckTimeoutSeconds: 5
      HealthyThresholdCount: 2
      TargetType: ip
      Port: !Ref ContainerPort
      Protocol: HTTP
      UnhealthyThresholdCount: 10
      VpcId: !Ref VpcId
      TargetGroupAttributes:
        - Key: deregistration_delay.timeout_seconds
          Value: 0
  PublicLoadBalancerSG:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Access to the public facing load balancer
      VpcId: !Ref VpcId
      SecurityGroupIngress:
        - CidrIp: 0.0.0.0/0
          IpProtocol: -1
  PublicLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Scheme: internet-facing
      LoadBalancerAttributes:
        - Key: idle_timeout.timeout_seconds
```

```
          Value: '30'
      Subnets: !Ref PublicSubnetIds
      SecurityGroups:
        - !Ref PublicLoadBalancerSG
  PublicLoadBalancerListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      DefaultActions:
        - Type: forward
          ForwardConfig:
            TargetGroups:
              - TargetGroupArn: !Ref ServiceTargetGroup
                Weight: 100
      LoadBalancerArn: !Ref PublicLoadBalancer
      Port: 80
      Protocol: HTTP
  ServiceIngressfromLoadBalancer:
    Type: 'AWS::EC2::SecurityGroupIngress'
    Properties:
      Description: Ingress from the public ALB
      GroupId: !Ref ServiceSecurityGroup
      IpProtocol: -1
      SourceSecurityGroupId: !Ref PublicLoadBalancerSG
  LogGroup:
    Type: 'AWS::Logs::LogGroup'
```

1 つのスタックに複数の Amazon ECS リソースを作成する

以下のサンプルテンプレートを使用して、1 つのスタックに複数の Amazon ECS リソースを作成できます。テンプレートは、`CFNCluster` という名前の Amazon ECS クラスターを作成します。クラスターには、Web サーバーをセットアップする Linux Fargate タスク定義が含まれています。このテンプレートは、タスク定義で定義されたタスクを起動して維持する、`cfn-service` という名前のサービスも作成します。このテンプレートを使用する前に、サービスの `NetworkConfiguration` のサブネット ID とセキュリティグループ ID がすべて同じ VPC に属していること、およびセキュリティグループに必要なルールがあることを確認してください。セキュリティグループのルールの詳細については、Amazon VPC ユーザーガイドの「セキュリティグループのルール」を参照してください。

JSON

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
        "ECSCluster": {
            "Type": "AWS::ECS::Cluster",
            "Properties": {
                "ClusterName": "CFNCluster"
            }
        },
        "ECSTaskDefinition": {
            "Type": "AWS::ECS::TaskDefinition",
            "Properties": {
                "ContainerDefinitions": [
                    {
                        "Command": [
                            "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS
 Sample App</title> <style>body {margin-top: 40px; background-color: #333;} </style>
 </head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</
h1> <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html &&
 httpd-foreground\""
                        ],
                        "EntryPoint": [
                            "sh",
                            "-c"
                        ],
                        "Essential": true,
                        "Image": "public.ecr.aws/docker/library/httpd:2.4",
                        "LogConfiguration": {
                            "LogDriver": "awslogs",
                            "Options": {
                                "awslogs-group": "/ecs/fargate-task-definition",
                                "awslogs-region": "us-east-1",
                                "awslogs-stream-prefix": "ecs"
                            }
                        },
                        "Name": "sample-fargate-app",
                        "PortMappings": [
                            {
                                "ContainerPort": 80,
                                "HostPort": 80,
                                "Protocol": "tcp"
```

```
                            }
                        ]
                    }
                ],
                "Cpu": 256,
                "ExecutionRoleArn": "arn:aws:iam::aws_account_id::role/
ecsTaskExecutionRole",
                "Family": "task-definition-cfn",
                "Memory": 512,
                "NetworkMode": "awsvpc",
                "RequiresCompatibilities": [
                    "FARGATE"
                ],
                "RuntimePlatform": {
                    "OperatingSystemFamily": "LINUX"
                }
            }
        },
        "ECSService": {
            "Type": "AWS::ECS::Service",
            "Properties": {
                "ServiceName": "cfn-service",
                "Cluster": {
                    "Ref": "ECSCluster"
                },
                "DesiredCount": 1,
                "LaunchType": "FARGATE",
                "NetworkConfiguration": {
                    "AwsvpcConfiguration": {
                        "AssignPublicIp": "ENABLED",
                        "SecurityGroups": [
                            "sg-abcdef01234567890"
                        ],
                        "Subnets": [
                            "subnet-abcdef01234567890"
                        ]
                    }
                },
                "TaskDefinition": {
                    "Ref": "ECSTaskDefinition"
                }
            }
        }
    }
```

```
}
```

YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  ECSCluster:
    Type: 'AWS::ECS::Cluster'
    Properties:
      ClusterName: CFNCluster
  ECSTaskDefinition:
    Type: 'AWS::ECS::TaskDefinition'
    Properties:
      ContainerDefinitions:
        - Command:
            - >-
              /bin/sh -c "echo '<html> <head> <title>Amazon ECS Sample
              App</title> <style>body {margin-top: 40px; background-color:
              #333;} </style> </head><body> <div
              style=color:white;text-align:center> <h1>Amazon ECS Sample
              App</h1> <h2>Congratulations!</h2> <p>Your application is now
              running on a container in Amazon ECS.</p> </div></body></html>' >
              /usr/local/apache2/htdocs/index.html && httpd-foreground"
          EntryPoint:
            - sh
            - '-c'
          Essential: true
          Image: 'public.ecr.aws/docker/library/httpd:2.4'
          LogConfiguration:
            LogDriver: awslogs
            Options:
              awslogs-group: /ecs/fargate-task-definition
              awslogs-region: us-east-1
              awslogs-stream-prefix: ecs
          Name: sample-fargate-app
          PortMappings:
            - ContainerPort: 80
              HostPort: 80
              Protocol: tcp
      Cpu: 256
      ExecutionRoleArn: 'arn:aws:iam::aws_account_id:role/ecsTaskExecutionRole'
      Family: task-definition-cfn
      Memory: 512
```

```
      NetworkMode: awsvpc
      RequiresCompatibilities:
        - FARGATE
      RuntimePlatform:
        OperatingSystemFamily: LINUX
  ECSService:
    Type: 'AWS::ECS::Service'
    Properties:
      ServiceName: cfn-service
      Cluster: !Ref ECSCluster
      DesiredCount: 1
      LaunchType: FARGATE
      NetworkConfiguration:
        AwsvpcConfiguration:
          AssignPublicIp: ENABLED
          SecurityGroups:
            - sg-abcdef01234567890
          Subnets:
            - subnet-abcdef01234567890
      TaskDefinition: !Ref ECSTaskDefinition
```

AWS CLI を使用してテンプレートからリソースを作成する

以下のコマンドを実行すると、ecs-template-body.json という名前のテンプレート本文ファイルを使用する、ecs-stack というスタックが作成されます。テンプレート本文ファイルが JSON または YAML 形式であることを確認します。ファイルの場所は、--template-body パラメータで指定されます。この場合、テンプレート本文ファイルは現在のディレクトリにあります。

```
aws cloudformation create-stack \
      --stack-name ecs-stack \
      --template-body file://ecs-template-body.json
```

リソースが正しく作成されていることを確認するには、Amazon ECS コンソールを確認するか、次のコマンドを使用します。

- 次のコマンドを実行すると、すべてのタスク定義が一覧表示されます。

  ```
  aws ecs list-task-definitions
  ```

- 次のコマンドを実行すると、すべてのクラスターが一覧表示されます。

```
aws ecs list-clusters
```

- 次のコマンドを実行すると、クラスター *CFNCluster* で定義されたすべてのサービスが一覧表示されます。*CFNCluster* を、サービスを作成するクラスター名に置換します。

```
aws ecs list-services \
      --cluster CFNCluster
```

AWS CloudFormation の詳細はこちら

AWS CloudFormation の詳細については、以下のリソースを参照してください。

- AWS CloudFormation
- AWS CloudFormation ユーザーガイド
- AWS CloudFormation コマンドラインインターフェイスユーザーガイド

AWS Copilot コマンドラインインターフェイスを使用した Amazon ECS リソースの作成

AWS Copilot コマンドラインインターフェイス (CLI) コマンドは、ローカル開発環境から、Amazon ECS での本番稼働対応のコンテナ化されたアプリケーションの構築、リリース、および運用を簡素化します。AWS Copilot CLI は、Infrastructure as Code 使用することから、ユーザーの代わりにプロビジョニングされた CI/CD パイプラインを作成することまで、最新のアプリケーションのベストプラクティスをサポートするデベロッパーワークフローと連携 Infrastructure as CodeInfrastructure as Code します。AWS Copilot CLI を毎日の開発の一部として使用し、AWS Management Console の代替としてテストのサイクルを使用します。

AWS Copilot は現在 Linux、macOS、Windows システムをサポートしています。AWS Copilot CLI の最新バージョンの詳細については、「リリース」を参照してください。

> **Note**
>
> AWS Copilot CLI のソースコードは GitHub で入手できます。含める変更について、問題とプルリクエストを送信することをお勧めします。ただし、現在、Amazon Web Services では、AWS Copilot コードの変更されたコピーの実行をサポートしていません。AWS Copilot

の問題は、「Gitter」 または「GitHub」 でご連絡ください。問題を開いたり、フィードバックを提供したり、バグを報告したりすることができます。

トピック

- AWS Copilot CLI のインストール
- AWS Copilot CLI を使用してサンプル Amazon ECS アプリケーションをデプロイする

AWS Copilot CLI の追加ドキュメントは、AWS Copilot ウェブサイトで入手できます。

AWS Copilot CLI のインストール

以下の手順を使用して、Homebrew を使用するか、バイナリを手動でダウンロードして、AWS Copilot CLI をインストールできます。

Homebrew の使用

次のコマンドは、Homebrew を使用して macOS または Linux システムに AWS Copilot CLIをインストールするために使用されます。インストールする前に、Homebrew をインストールする必要があります。詳細については、「Homebrew」を参照してください。

```
brew install aws/tap/copilot-cli
```

バイナリのダウンロード

Homebrew の代わりに、macOS、Windows、または Linux システムに手動で AWS Copilot CLI をインストールできます。ご使用のオペレーティングシステムに合わせて次のコマンドを使用して、バイナリをダウンロードします。macOS と Linux の例には、バイナリに実行アクセス許可を適用するコマンドが含まれているほか、インストールが機能していることを検証するためのヘルプメニューがリストされています。

macOS

macOS の場合:

```
sudo curl -Lo /usr/local/bin/copilot https://github.com/aws/copilot-cli/releases/
latest/download/copilot-darwin \
   && sudo chmod +x /usr/local/bin/copilot \
   && copilot --help
```

macOS ARM システムの場合:

```
sudo curl -Lo /usr/local/bin/copilot https://github.com/aws/copilot-cli/releases/
latest/download/copilot-darwin-arm64 \
   && sudo chmod +x /usr/local/bin/copilot \
   && copilot --help
```

Linux

Linux x86 (64 ビット) システムの場合:

```
sudo curl -Lo /usr/local/bin/copilot https://github.com/aws/copilot-cli/releases/
latest/download/copilot-linux \
   && sudo chmod +x /usr/local/bin/copilot \
   && copilot --help
```

Linux ARM システムの場合:

```
sudo curl -Lo /usr/local/bin/copilot https://github.com/aws/copilot-cli/releases/
latest/download/copilot-linux-arm64 \
   && sudo chmod +x /usr/local/bin/copilot \
   && copilot --help
```

Windows

PowerShell を使用して、次のコマンドを実行します。

```
New-Item -Path 'C:\copilot' -ItemType directory; `
  Invoke-WebRequest -OutFile 'C:\copilot\copilot.exe' https://github.com/aws/
copilot-cli/releases/latest/download/copilot-windows.exe
```

(任意) PGP 署名を使用した手動でインストールした AWS Copilot CLI の検証

AWS Copilot CLI の実行可能ファイルは、PGP 署名を使用して暗号で署名されます。PGP 署名を使用して、AWS Copilot CLI 実行可能ファイルの妥当性を検証できます。GnuPG ツールを使用してこの署名を検証するには、次のステップを行います。

1. GnuPG をダウンロードし、インストールします。詳細については、GnuPG のウェブサイトを参照してください。

macOS

Homebrew の使用をお勧めします。製品ウェブサイトの手順に従って、Homebrew をインストールします。詳細については、「Homebrew」を参照してください。Homebrew がインストールされたら、macOS 端末から次のコマンドを使用します。

```
brew install gnupg
```

Linux

任意の Linux のパッケージマネージャーを使用して gpg をインストールします。

Windows

GnuPG ウェブサイトから Windows の簡易インストーラをダウンロードし、管理者としてインストールします。GnuPG をインストールしたら、管理者向け PowerShell を閉じてから再度開きます。

詳細については、「GnuPG のダウンロード」を参照してください。

2. GnuPG パスが環境パスに追加されていることを確認します。

macOS

```
echo $PATH
```

出力に GnuPG パスが表示されない場合は、次のコマンドを実行してパスに追加します。

```
PATH=$PATH:<path to GnuPG executable files>
```

Linux

```
echo $PATH
```

出力に GnuPG パスが表示されない場合は、次のコマンドを実行してパスに追加します。

```
export PATH=$PATH:<path to GnuPG executable files>
```

Windows

```
Write-Output $Env:PATH
```

出力に GnuPG パスが表示されない場合は、次のコマンドを実行してパスに追加します。

```
$Env:PATH += ";<path to GnuPG executable files>"
```

3. ローカルプレーンテキストファイルを作成します。

macOS

ターミナルで、次のように入力します。

```
touch <public_key_filename.txt>
```

TextEdit でファイルを開きます。

Linux

gedit など、テキストエディタでテキストファイルを作成します。public_key_filename.txt として保存します。

Windows

Notepad など、テキストエディタでテキストファイルを作成します。public_key_filename.txt として保存します。

4. 次の Amazon ECS PGP パブリックキーの内容を追加し、ファイルを保存します。

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQINBFq1SasBEADliGcT1NVJ1ydfN8DqebYYe9ne3dt6jqKFmKowLmm6LLGJe7HU
jGtqhCWRDkN+qPpHqdArRgDZAtn2pXY5fEipHgar4CP8QgRnRMO2fl74lmavr4Vg
7K/KH8VHlq2uRw32/B94XLEgRbGTMdWFdKuxoPCttBQaMj3LGn6Pe+6xVWRkChQu
BoQAhjBQ+bEm0kNy0LjNgjNlnL3UMAG56t8E3LANIgGgEnpNsB1UwfWluPoGZoTx
N+6pHBJrKIL/1v/ETU4FXpYw2zvhWNahxeNRnoYj3uycHkeliCrw4kj0+skizBgO
2K7oVX8Oc3j5+ZilhL/qDLXmUCb2az5cMM1mOoF8EKX5HaNuq1KfwJxqXE6NNIcO
lFTrT7QwD5fMNld3FanLgv/ZnIrsSaqJOL6zRSq8O4LN1OWBVbndExk2Kr+5kFxn
5lBPgfPgRj5hQ+KTHMa9Y8Z7yUc64BJiN6F9Nl7FJuSsfqbdkvRLsQRbcBG9qxX3
rJAEhieJzVMEUNl+EgeCkxj5xuSkNU7zw2c3hQZqEcrADLV+hvFJktOz9Gm6xzbq
```

```
lTnWWCz4xrIWtuEBA2qE+MlDheVd78a3gIsEaSTfQq0osYXaQbvlnSWOoc1y/5Zb
zizHTJIhLtUyls9WisP2s0emeHZicVMfW61EgPrJAiupgc7kyZvFt4YwfwARAQAB
tCRBbWF6b24gRUNTIDxlY3Mtc2VjdXJpdHlAYW1hem9uLmNvbT6JAhwEEAECAAYF
AlrjL0YACgkQHivRXs0TaQrg1g/+JppwPqHnlVPmv7lessB8I5UqZeD6p6uVpHd7
Bs3pcPp8BV7BdRbs3sPLt5bV1+rkqOlw+0gZ4Q/ue/YbWtOAt4qY0OcEo0HgcnaX
lsB827QIfZIVtGWMhuh94xzm/SJkvngml6KB3YJNnWP61A9qJ37/VbVVLzvcmazA
McWB4HUMNrhd0JgBCo0gIpqCbpJEvUc02Bjn23eEJsS9kC7OUAHyQkVnx4d9UzXF
4OoISF6hmQKIBoLnRrAlj5Qvs3GhvHQ0ThYq0Grk/KMJJX2CSqt7tWJ8gk1n3H3Y
SReRXJRnv7DsDDBwFgT6r5Q2HW1TBUvaoZy5hF6maD09nHcNnvBjqADzeT8Tr/Qu
bBCLzkNSYqqkpgtwv7seoD2P4n1giRvDAOEfMZpVkUr+C252IaH1HZFEz+TvBVQM
Y8OWWxmIJW+J6evjo3N1eO19UHv71jvoF8zljbI4bsL2c+QTJmOv7nRqzDQgCWyp
Id/v2dUVVTk1j9omuLBBwNJzQCB+72LcIzJhYmaP1HC4LcKQG+/f41exuItenatK
lEJQhYtyVXcBlh6Yn/wzNg2NWOwb3vqY/F7m6u9ixAwgtIMgPCDE4aJ86zrrXYFz
N2HqkTSQh77Z8KPKmyGopsmN/reMuilPdINb249nA0dzoN+nj+tTFOYCIaLaFyjs
Z0r1QAOJAjkEEwECACMFAlq1SasCGwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIX
gAAKCRC86dmkLVF4T9iFEACEnkm1dNXsWUx34R3c0vamHrPxvfkyI1FlEUen8D1h
uX9xy6jCEROHWEp0rjGK4QDPgM93sWJ+s1UAKg214QRVzft0y9/DdR+twApA0fzy
uavIthGd6+03jAAo6udYDE+cZC3P7XBbDiYEWk4XAF9I1JjB8hTZUgvXBL046JhG
eM17+crgUyQeetkiOQemLbsbXQ40Bd9V7zf7XJraFd8VrwNUwNb+9KFtgAsc9rk+
YIT/PEf+YOPysgcxI4sTWghtyCulVnuGoskgDv4v73PALU0ieUrvvQVqWMRvhVx1
0X90J7cC1KOyhlEQQ1aFTgmQjmXexVTwIBm8LvysFK6YXM41KjOrlz3+6xBIm/qe
bFyLUnf4WoiuOplAaJhK9pRY+XEnGNxdtN4D26Kd0F+PLkm3Tr3Hy3b1Ok34FlGr
KVHUq1TZD7cvMnnNKEELTUcKX+1mV3an16nmAg/my1JSUt6BNK2rJpY1s/kkSGSE
XQ4zuF2IGCpvBFhYAlt5Un5zwqkwwQR3/n2kwAoDzonJcehDw/C/cGos5D0aIU7I
K2X2aTD3+pA7Mx3IMe2hqmYqRt9X42yF1PIEVRneBRJ3HDezAgJrNh0GQWRQkhIx
gz6/cTR+ekr5TptVszS9few2GpI5bCgBKBisZIssT89aw7mAKWut0Gcm4qM9/yK6
1bkCDQRatUmrARAAxNPvVwreJ2yAiFcUpdRlVhsuOgnxvs1QgsIw3H7+Pacr9Hpe
8uftYZqdC82KeSKhpHq7c8gMTMucIINtH25x9BCc73E33EjCL9Lqov1TL7+QkgHe
T+JIhZwdD8Mx2K+LVVVu/aWkNrfMuNwyDUciSI4D5QHa8T+F8fgN4OTpwYjirzel
5yoICMr9hVcbzDNv/ozKCxjx+XKgnFc3wrnDfJfntfDAT7ecwbUTL+viQKJ646s+
psiqXRYtVvYInEhLVrJ0aV6zHFoigE/Bils6/g7ru1Q6CEHqEw++APs5CcE8VzJu
WAGSVHZgun5Y9N4quR/M9Vm+IPMhTxrAg7rOvyRN9cAXfeSMf77I+XTifigNna8x
t/MOdjXr1fjF4pThEi5u6WsuRdFwjY2azEv3vevodTi4HoJReH6dFRa6y8c+UDgl
2iHiOKIpQqLbHEfQmHcDd2fix+AaJKMnPGNku9qCFEMbgSRJpXz6BfwnY1QuKE+I
R6jA0frUNt2jhiGG/F8RceXzohaaC/Cx7LUCUFWc0n7z32C9/Dtj7I1PMOacdZzz
bjJzRKO/ZDv+UN/c9dwAkllzAyPMwGBkUaY68EBstnIliW34aWm6IiHhxioVPKSp
VJfyiXPO0EXqujtHLAeChfjcns3I12YshT1dv2PafG53fp33ZdzeUgsBo+EAEQEA
AYkCHwQYAQIACQUCWrVJqwIbDAAKCRC86dmkLVF4T+ZdD/9x/8APzgNJF3o3STrF
jvnV1ycyhWYGAeBJiu7wjsNWwzMFOv15tLjB7AqeVxZn+WKDD/mIOQ45OZvnYZuy
X7DR0JszaH9wrYTxZLVruAu+t6UL0y/XQ4L1GZ9QR6+r+7t1Mvbfy7BlHbvX/gYt
Rwe/uwdibI0CagEzyX+2D3kTOlHO5XThbXaNf8AN8zha91Jt2Q2UR2X5T6JcwtMz
FBvZnl3LSmZyE0EQehS2iUurU4uWOpGppuqVnbi0jbCvCHKgDGrqZ0smKNAQng54
F365W3g8AfY48s8XQwzmcliowYX9bT8PZiEi0J4QmQh0aXkpqZyFefuWeOL2R94S
XKzr+gRh3BAULoqF+qK+IUMxTip9KTPNvYDpiC66yBiT6gFDji5Ca9pGpJXrC3xe
```

```
TXiKQ8DBWDhBPVPrruLIaenTtZEOsPc4I85yt5U9RoPTStcOr34s3w5yEaJagt6S
Gc5r9ysjkfH6+6rbi1ujxMgROSqtqr+RyB+V9A5/OgtNZc8llK6u4UoOCde8jUUW
vqWKvjJB/Kz3u4zaeNu2ZyyHaOqOuH+TETcW+jsY9IhbEzqN5yQYGi4pVmDkY5vu
lXbJnbqPKpRXgM9BecV9AMbPgbDq/5LnHJJXg+G8YQOgp4lR/hC1TEFdIp5wM8AK
CWsENyt2o1rjgMXiZOMF8A5oBLkCDQRatUuSARAAr77kj7j2QR2SZeOSlFBvV7oS
mFeSNnz9xZssqrsm6bTwSHM6YLDwc7Sdf2esDdyzONETwqrVCg+FxgL8hmo9hS4c
rR6tmrP0mOmptr+xLLsKcaP7ogIXsyZnrEAEsvW8PnfayoiPCdc3cMCR/lTnHFGA
7EuR/XLBmi7Qg9tByVYQ5Yj5wB9V4B2yeCt3XtzPqeLKvaxl7PNelaHGJQY/xo+m
V0bndxf9IY+4oFJ4blD32WqvyxESo7vW6WBh7oqv3Zbm0yQrr8a6mDBpqLkvWwNI
3kpJR974tg5o5LfDu1BeeyHWPSGm4U/G4JB+JIG1ADy+RmoWEt4BqTCZ/knnoGvw
D5sTCxbKdmuOmhGyTssoG+3OOcGYHV7pWYPhazKHMPm201xKCjH1RfzRULzGKjD+
yMLT1I3AXFmLmZJXikAOlvE3/wgMqCXscbycbLjLD/bXIuFWo3rzoezeXjgi/DJx
jKBAyBTYO5nMcth1O9oaFd9d0HbsOUDkIMnsgGBE766Piro6MHo0T0rXl07Tp4pI
rwuSOsc6XzCzdImj0Wc6axS/HeUKRXWdXJwno5awTwXKRJMXGfhCvSvbcbc2Wx+L
IKvmB7EB4K3fmjFFE67yolmiw2qRcUBfygtH3eL5XZU28MiCpue8Y8GKJoBAUyvf
KeM1rO8Jm3iRAc5a/D0AEQEAAYkEPgQYAQIACQUCWrVLkgIbAgIpCRC86dmkLVF4
T8FdIAQZAQIABgUCWrVLkgAKCRDePL1hra+LjtHYD/9MucxdFe6bXO1dQR4tKhhQ
P0LRqy6zlBY9ILCLowNdGZdqorogUiUymgn3VhEhVtxTOoHcN7qOuM01PNsRnOeS
EYjf8Xrb1clzkD6xULwmOclTb9bBxnBc/4PFvHAbZW3QzusaZniNgkuxt6BTfloS
Of4inq71kjmGK+TlzQ6mUMQUg228NUQC+a84EPqYyAeY1sgvgB7hJBhYL0QAxhcW
6m20Rd8iEc6HyzJ3yCOCsKip/nRWAbf0OvfHfRBp0+m0ZwnJM8cPRFjOqqzFpKH9
HpDmTrC4wKP1+TL52LyEqNh4yZitXmZNV7giSRIkk0eDSko+bFy6VbMzKUMkUJK3
D3eHFAMkujmbfJmSMTJOPGn5SB1HyjCZNx6bhIIbQyEUB9gKCmUFaqXKwKpF6rj0
iQXAJxLR/shZ5Rk96VxzOphUl7T90m/PnUEEPwq8KsBhnMRgxa0RFidDP+n9fgtv
HLmrOqX9zBCVXh0mdWYLrWvmzQFWzG7AoE55fkf8nAEPsalrCdtaNUBHRXA0OQxG
AHMOdJQQvBsmqMvuAdjkDWpFu5y0My5ddU+hiUzUyQLjL5Hhd5LOUDdewlZgIw1j
xrEAUzDKetnemM8GkHxDgg8koev5frmShJuce7vSjKpCNg3EIJSgqMOPFjJuLWtZ
vjHeDNbJy6uNL65ckJy6WhGjEADS2WAW1D6Tfekkc21SsIXk/LqEpLMR/0g5OUif
wcEN1rS9IJXBwIy8MelN9qr5KcKQLmfdfBNEyyceBhyVl0MDyHOKC+7PofMtkGBq
13QieRHv5GJ8LB3fclqHV8pwTTo3Bc8z2g0TjmUYAN/ixETdReDoKavWJYSE9yoM
aaJu279ioVTrwpECse0XkiRyKToTjwOb73CGkBZZpJyqux/rmCV/fp4ALdSW8zbz
FJVORaivhoWwzjpfQKhwcU9lABXi2UvVm14v0AfeI7oiJPSU1zM4fEny4oiIBXlR
zhFNih1UjIu82X16mTm3BwbIga/s1fnQRGzyhqUIMii+mWra23EwjChaxpvjjcUH
5ilLc5Zq781aCYRygYQw+hu5nFkOH1R+Z50Ubxjd/aqUfnGIAX7kPMD3Lof4KldD
Q8ppQriUvxVo+4nPV6rpTy/PyqCLWDjkguHpJsEFsMkwajrAz0QNSAU5CJ0G2Zu4
yxvYlumHCEl7nbFrm0vIiA75Sa8KnywTDsyZsu3XcOcf3g+g1xWTpjJqy2bYXlqz
9uDOWtArWHOis6bq8l9RE6xr1RBVXS6uqgQIZFBGyq66b0dIq4D2JdsUvgEMaHbc
e7tBfeB1CMBdA64e9Rq7bFR7Tvt8gasCZYlNr3lydh+dFHIEkH53HzQe6l88HEic
+0jVnLkCDQRa55wJARAAyLya2Lx6gyoWoJN1a6740q3o8e9d4KggQOfGMTCflmeq
ivuzgN+3DZHN+9ty2KxXMtn0mhHBerZdbNJyjMNT1gAgrhPNB4HtXBXum2wS57WK
DNmade914L7FWTPAWBG2Wn448OEHTqsClICXXWy9IICgclAEyIq0Yq5mAdTEgRJS
Z8t4GpwtDL9gNQyFXaWQmDmkAsCygQMvhAlmu9xOIzQG5CxSnZFk7zcuL60k14Z3
Cmt49k4T/7ZU8goWi8tt+rU78/IL3J/fF9+1civ1OwuUidgfPCSvOUW1JojsdCQA
L+RZJcoXq7lfOFj/eNjeOSstCTDPfTCL+kThE6E5neDtbQHBYkEX1BRiTedsV4+M
```

```
ucgiTrdQFWKf89G72xdv8ut9AYYQ2BbEYU+JAYhUH8rYYui2dHKJIgjNvJscuUWb
+QEqJIRleJRhrO+/CHgMs4fZAkWF1VFhKBkcKmEjLn1f7EJJUUW84ZhKXjO/AUPX
1CHsNjziRceuJCJYox1cwsoq6jTE50GiNzcIxTn9xUc0UMKFeggNAFys1K+TDTm3
Bzo8H5ucjCUEmUm9lhkGwqTZgOlRX5eqPX+JBoSaObqhgqCa5IPinKRa6MgoFPHK
6sYKqroYwBGgZm6Js5chpNchvJMs/3WXNOEVg0J3z3vP0DMhxqWm+r+n9zlW8qsA
EQEAAYkEPgQYAQgACQUCWuecCQIbAgIpCRC86dmkLVF4T8FdIAQZAQgABgUCWuec
CQAKCRBQ3szEcQ5hr+ykD/4tOLRHFHXuKUcxgGaubUcVtsFrwBKma1cYjqaPms8u
6Sk0wfGRI32G/GhOrp0Ts/MOkbObq6VLTh8N5Yc/53MEl8zQFw9Y5AmRoW4PZXER
ujs5s7p4oR7xHMihMjCCBn1bvrR+34YPfgzTcgLiOEFHYT8UTxwnGmXOvNkMM7md
xD3CV5q6VAte8WKBo/220II3fcQlc9r/oWX4kXXkb0v9hoGwKbDJ1tzqTPrp/xFt
yohqnvImpnlz+Q9zXmbrWYL9/g8VCmW/NN2gju2G3Lu/TlFUWIT4v/5OPK6TdeNb
VKJO4+S8bTayqSG9CML1S57KSgCo5HUhQWeSNHI+fpe5oX6FALPT9JLDce8OZz1i
cZZ0MELP37mOOQun0AlmHm/hVzf0f311PtbzcqWaE51tJvgUR/nZFo6Ta3O5Ezhs
3VlEJNQ1Ijf/6DH87SxvAoRIARCuZd0qxBcDK0avpFzUtbJd24lRA3WJpkEiMqKv
RDVZkE4b6TW61f0o+LaVfK6E8oLpixegS4fiqC16mFrOdyRk+RJJfIUyz0WTDVmt
g0U1CO1ezokMSqkJ7724pyjr2xf/r9/sC6aOJwB/lKgZkJfC6NqL7TlxVA31dUga
LEOvEJTTE4gl+tYtfsCDvALCtqL0jduSkUo+RXcBItmXhA+tShW0pbS2Rtx/ixua
KohVD/0R4QxiSwQmICNtm9mw9ydIl1yjYXX5a9x4wMJracNY/LBybJPFnZnT4dYR
z4XjqysDwvvYZByaWoIe3QxjX84V6MlI2IdAT/xImu8gbaCI8tmyfpIrLnPKiR9D
VFYfGBXuAX7+HgPPSFtrHQONCALxxzlbNpS+zxt9r0MiLgcLyspWxSdmoYGZ6nQP
RO5Nm/ZVS+u2imPCRzNUZEMa+dlE6kHx0rS0dPiuJ4O7NtPeYDKkoQtNagspsDvh
cK7CSqAiKMq06UBTxqlTSRkm62eOCtcs3p3OeHu5GRZF1uzTET0ZxYkaPgdrQknx
ozjP5mC7X+45lcCfmcVt94TFNL5HwEUVJpmOgmzILCI8yoDTWzloo+i+fPFsXX4f
kynhE83mSEcr5VHFYrTY3mQXGmNJ3bCLuc/jq7ysGq69xiKmTlUeXFm+aojcRO5i
zyShIRJZ0GZfuzDYFDbMV9amA/YQGygLw//zP5ju5SW26dNxlf3MdFQE5JJ86rn9
MgZ4gcpazHEVUsbZsgkLizRp9imUiH8ymLqAXnfRGlU/LpNSefnvDFTtEIRcpOHc
bhayG0bk51Bd4mioOXnIsKy4j63nJXA27x5EVVHQ1sYRN8Ny4Fdr2tMAmj2O+X+J
qX2yy/UX5nSPU492e2CdZ1UhoU0SRFY3bxKHKB7SDbVeav+K5g==
=Gi5D
-----END PGP PUBLIC KEY BLOCK-----
```

Amazon ECS PGP パブリックキーの詳細を参照用として以下に示します。

```
Key ID: BCE9D9A42D51784F
Type: RSA
Size: 4096/4096
Expires: Never
User ID: Amazon ECS
Key fingerprint: F34C 3DDA E729 26B0 79BE AEC6 BCE9 D9A4 2D51 784F
```

5. ターミナルで次のコマンドを使用して、Amazon ECS PGP パブリックキーを持ったファイルをインポートします。

```
gpg --import <public_key_filename.txt>
```

6. AWS Copilot CLI 署名をダウンロードします。署名は、ASCII でデタッチ済みの PGP 署名で、拡張子が .asc のファイルに保存されています。この署名ファイルには、対応する実行可能ファイルと同じ名前が付けられており、拡張子は .asc です。

   macOS

   macOS システムでは、次のコマンドを実行します。

   ```
   sudo curl -Lo copilot.asc https://github.com/aws/copilot-cli/releases/latest/download/copilot-darwin.asc
   ```

   Linux

   Linux システム x86 (64 ビット) の場合は、次のコマンドを実行します。

   ```
   sudo curl -Lo copilot.asc https://github.com/aws/copilot-cli/releases/latest/download/copilot-linux.asc
   ```

   Linux ARM システムの場合は、次のコマンドを実行します。

   ```
   sudo curl -Lo copilot.asc https://github.com/aws/copilot-cli/releases/latest/download/copilot-linux-arm64.asc
   ```

   Windows

   PowerShell を使用して、次のコマンドを実行します。

   ```
   Invoke-WebRequest -OutFile 'C:\copilot\copilot.asc' https://github.com/aws/copilot-cli/releases/latest/download/copilot-windows.exe.asc
   ```

7. 次のコマンドを使用して、署名を検証します。

   - macOS および Linux システムの場合:

     ```
     gpg --verify copilot.asc /usr/local/bin/copilot
     ```

   - Windows システムの場合:

```
gpg --verify 'C:\copilot\copilot.asc' 'C:\copilot\copilot.exe'
```

正常な出力:

```
gpg: Signature made Tue Apr  3 13:29:30 2018 PDT
gpg:                using RSA key DE3CBD61ADAF8B8E
gpg: Good signature from "Amazon ECS <ecs-security@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: F34C 3DDA E729 26B0 79BE  AEC6 BCE9 D9A4 2D51 784F
     Subkey fingerprint: EB3D F841 E2C9 212A 2BD4  2232 DE3C BD61 ADAF 8B8E
```

> **Important**
>
> 出力に警告が表示されることがありますが、問題ありません。これは、個人 PGP キー (持っている場合) と Amazon ECS PGP キーの間に信頼チェーンがないために表示されます。詳細については、「信用の輪 (Web of Trust)」を参照してください。

8. Windows のインストールの場合は、PowerShell で次のコマンドを実行して、AWS Copilot ディレクトリをパスに追加します。

```
$Env:PATH += ";<path to Copilot executable files>"
```

AWS Copilot CLI を使用してサンプル Amazon ECS アプリケーションをデプロイする

AWS Copilot CLI をインストールしたら、以下の手順に従ってサンプルアプリケーションをデプロイし、デプロイを検証し、リソースをクリーンアップできます。

前提条件

開始する前に、以下の前提条件を満たしていることを確認してください。

- AWS CLI をインストールして設定します。詳細については、「AWS コマンドラインインターフェイス」を参照してください。

- `aws configure` を実行して、AWSコパイロット CLI がアプリケーションとサービスの管理に使用するデフォルトプロファイルを設定します。
- Docker のインストールと実行 詳細については、「Docker の開始方法」を参照してください。

単一コマンドを使用したサンプル Amazon ECS アプリケーションのデプロイ

1. 次のコマンドを使用して、GitHub リポジトリからクローンされたサンプルウェブアプリケーションをデプロイします。AWS Copilot `init` とそのフラグの詳細については、AWS Copilot ドキュメントを参照してください。

```
git clone https://github.com/aws-samples/aws-copilot-sample-service.git demo-app &&
 \
cd demo-app &&                                \
copilot init --app demo                       \
  --name api                                  \
  --type 'Load Balanced Web Service'          \
  --dockerfile './Dockerfile'                 \
  --port 80                                   \
  --tag  latest                               \
  --deploy
```

2. デプロイが完了すると、AWS Copilot CLI はデプロイの検証に使用できる URL を返します。次のコマンドを使用して、アプリケーションのステータスを確認することもできます。

   - AWS コパイロットのアプリケーションを一覧を表示します。

     ```
     copilot app ls
     ```

   - アプリケーション内の環境およびサービスに関する情報を表示します。

     ```
     copilot app show
     ```

   - 環境に関する情報を表示します。

     ```
     copilot env ls
     ```

   - エンドポイント、キャパシティー、関連リソースなど、サービスに関する情報を表示します。

     ```
     copilot svc show
     ```

- アプリケーション内のすべてのサービスのリスト。

```
copilot svc ls
```

- デプロイされたサービスのログを表示します。

```
copilot svc logs
```

- サービスのステータスを表示する

```
copilot svc status
```

3. このデモが終了したら、次のコマンドを実行して関連付けられたリソースをクリーンアップし、未使用のリソースに対する料金が発生しないようにしてください。

```
copilot app delete
```

Amazon ECS のベストプラクティス

以下のページを使用して、Amazon ECS ネットワーキングに関する最も重要な運用上のベストプラクティスを学習できます。

ベストプラクティスの概要	詳細はこちら
アプリケーションをインターネットに接続する	Amazon ECS アプリケーションをインターネットに接続する
インターネットから Amazon ECS へのインバウンド接続を受信する	インターネットから Amazon ECS へのインバウンド接続を受信するためのベストプラクティス
Amazon ECS を VPC 内の他の AWS サービスに接続する	Amazon ECS を VPC 内から AWS サービスに接続するためのベストプラクティス
AWS アカウント と VPC 間のネットワークサービス	AWS アカウントおよび VPC の間で Amazon ECS サービスをネットワーキングするためのベストプラクティス
ネットワークの問題のトラブルシューティング	Amazon ECS ネットワーキングのトラブルシューティングのための AWS サービス

以下のページを使用して、Fargate on Amazon ECS に関する最も重要な運用上のベストプラクティスを学習できます。

ベストプラクティスの概要	詳細はこちら
Fargate のセキュリティ	Amazon ECS の Fargate セキュリティのベストプラクティス
Fargate のセキュリティに関する考慮事項	Amazon ECS の Fargate のセキュリティに関する考慮事項
Fargate 上の Linux コンテナにおけるコンテナイメージのプル動作	Fargate 上の Linux コンテナにおける Amazon ECS のコンテナイメージのプル動作
Fargate 上の Windows コンテナにおけるコンテナイメージのプル動作	Fargate 上の Windows コンテナにおける Amazon ECS のコンテナイメージのプル動作
Fargate のタスク廃止	AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス

以下のページを使用して、タスク定義に関する最も重要な運用上のベストプラクティスを学習できます。

ベストプラクティスの概要	詳細はこちら
コンテナイメージ	Amazon ECS コンテナイメージのベストプラクティス
タスクサイズ	Amazon ECS タスクサイズのベストプラクティス
ボリュームのベストプラクティス	Amazon ECS タスクのストレージオプション

以下のページを使用して、クラスターとキャパシティに関する最も重要な運用上のベストプラクティスを学習できます。

ベストプラクティスの概要	詳細はこちら
Fargate のセキュリティ	Amazon ECS の Fargate セキュリティのベストプラクティス
EC2 コンテナインスタンスのセキュリティに関する考慮事項	Amazon ECS の Amazon EC2 コンテナインスタンスのセキュリティに関する考慮事項
クラスターの自動スケーリング	Amazon ECS クラスターの自動スケーリングの最適化

以下のページを使用して、タスクとサービスに関する最も重要な運用上のベストプラクティスを学習できます。

ベストプラクティスの概要	詳細はこちら
タスクの起動時間を最適化する	Amazon ECS タスクの起動時間を最適化する
サービスパラメータ	Amazon ECS サービスパラメータのベストプラクティス
ロードバランサーのヘルスチェックパラメータを最適化する	Amazon ECS のロードバランサーのヘルスチェックパラメータを最適化する
ロードバランサーの Connection Draining パラメータを最適化する	Amazon ECS のロードバランサー Connection Draining パラメータを最適化する
サービス自動スケーリングを最適化する	Amazon ECS のサービス自動スケーリングを最適化する

以下のページを使用して、セキュリティに関する最も重要な運用上のベストプラクティスを学習できます。

ベストプラクティスの概要	詳細はこちら	
ネットワークセキュリティ	Amazon ECS のネットワークセキュリティのベストプラクティス	
タスクとコンテナのセキュリティ	Amazon ECS タスクおよびコンテナのセキュリティのベストプラクティス	

Amazon ECS の AWS Fargate

AWS Fargate Fargate はAmazon ECSで使用できるテクノロジーであり、サーバーやAmazon EC2 インスタンスの クラスターを管理することなくコンテナを実行できます。AWS Fargate を使用すると、コンテナを実行するために仮想マシンのクラスターをプロビジョニング、設定、スケールする必要がありません。これにより、サーバータイプの選択、クラスターをスケールするタイミングの決定、クラスターのパッキングの最適化を行う必要がなくなります。

Fargate 起動タイプを使用してタスクやサービスを実行する場合、アプリケーションをコンテナにパッケージ化し、CPU とメモリ要件を指定して、ネットワークとIAM ポリシーを定義して、アプリケーションを起動します。各Fargate タスクは、独自の分離境界を持ち、基盤となるカーネル、CPU リソース、メモリリソース、Elastic Network Interface を別のタスクと共有しません。Fargate のタスク定義を構成するには、`requiresCompatibilities` タスク定義パラメータを `FARGATE` に設定します。詳細については、「起動タイプ」を参照してください。

Fargate は、Amazon Linux 2 (プラットフォームバージョン 1.3.0)、Bottlerocket オペレーティングシステム (プラットフォームバージョン 1.4.0)、および Microsoft Windows 2019 Server Full Edition および Core Edition 用のプラットフォームバージョンを提供しています。特に指定がない限り、このページの情報はすべての Fargate プラットフォームに適用されます。

このトピックでは、Fargate タスクおよびサービスのさまざまなコンポーネントを説明し、Amazon ECSで Fargate を使用する際の特別な考慮事項を示しています。

Fargate で Linux コンテナをサポートするリージョンの情報については、「the section called “AWS Fargate 上の Linux コンテナ”」を参照してください。

Fargate で Windows コンテナをサポートするリージョンの情報については、「the section called “AWS Fargate 上の Windows コンテナ”」を参照してください。

チュートリアル

コンソールの使用開始方法については、以下を参照してください。

- Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する方法について説明します。
- Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。

AWS CLI の使用開始方法については、以下を参照してください。

- AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する
- AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する

キャパシティープロバイダー

以下のキャパシティプロバイダーが利用可能です。

- Fargate
- Fargate Spot - 割り込み許容のある Amazon ECS タスクを、AWS Fargate 料金と比較して割引料金で実行します。Fargate Spot は、予備のコンピュートキャパシティーでタスクを実行します。AWS がキャパシティーを戻す必要がある場合、タスクは中断され、2 分間の警告が表示されます。詳細については、「Fargate 起動タイプ用の Amazon ECS クラスター 」を参照してください。

タスク定義

Fargate 起動タイプを使用するタスクは利用可能な Amazon ECS タスク定義パラメータのすべてをサポートするわけではありません。一部のパラメータはサポートされていません。また、Fargate タスクでは動作が異なるパラメータがあります。詳細については、「タスク CPU とメモリ」を参照してください。

プラットフォームのバージョン

AWS Fargate プラットフォームのバージョンを使って、Fargate タスクインフラストラクチャの特定のランタイム環境を参照できます。これは、カーネルとコンテナのランタイムバージョンの組み合わせです。同一のタスクを多数管理するためのタスク実行時、またはそのためのサービス作成時には、プラットフォームバージョンを選択します。

ランタイム環境の進化に合わせて、新しいプラットフォームバージョンがリリースされます。例えば、カーネルやオペレーティングシステムの更新、新機能の追加、バグ修正、セキュリティの更新があった場合が当てはまります。Fargate プラットフォームのバージョンは、新しいプラットフォームバージョンのリビジョンを行うことで更新されます。各タスクは、そのライフサイクルを通じて、単一のプラットフォームバージョンのリビジョンで実行されます。最新のプラットフォームバージョンのリビジョンを使用する場合は、新たにタスクを開始する必要があります。Fargate で実行される新しいタスクは、常にプラットフォームバージョンの最新リビジョンで実行されます。これにより、タスクは必ず、安全でパッチ適用済みのインフラストラクチャで開始されることが保証されます。

既存のプラットフォームのバージョンに影響を与えるセキュリティ上の問題が見つかった場合、AWS は、そのプラットフォームバージョンのパッチ済みリビジョンを新たに作成します。また、脆弱性のあるリビジョンで実行しているタスクは廃止されます。場合によっては、Fargate で使用しているタスクについて、廃止の予定が通知されることがあります。詳細については、「AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス」を参照してください。

詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。

サービスの負荷分散

AWS Fargate の Amazon ECS サービスは、オプションで Elastic Load Balancing を使用して、サービスのタスク間でトラフィックを均等に分散するように設定できます。

AWS Fargate の Amazon ECS サービスでは、Application Load Balancer と Network Load Balancer のタイプがサポートされています。アプリケーションロードバランサーは、HTTP/HTTPS (またはレイヤー 7) トラフィックをルーティングするために使用されます。ネットワークロードバランサーは、TCP または UDP (またはレイヤー 4)トラフィックをルーティングするために使用されます。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。

また、このようなサービスのターゲットグループを作成する場合は、ターゲットタイプとして `instance` ではなく、`ip` を選択する必要があります。これは、`awsvpc` ネットワークモードを使用するタスクは、Amazon EC2インスタンスではなく、Elastic Network Interface に関連付けられているためです。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。

Network Load Balancer を使用して AWS Fargate タスクの Amazon ECS に UDP トラフィックをルーティングするには、プラットフォームバージョン 1.4 移行を使用する場合にのみサポートされます。

使用状況メトリクス

CloudWatch 使用状況メトリクスを使用して、アカウントのリソースの使用状況を把握できます。これらのメトリクスを使用して、CloudWatch グラフやダッシュボードで現在のサービスの使用状況を可視化できます。

AWS Fargate 使用状況メトリクスは、AWS のサービスクォータに対応しています。使用量がサービスクォータに近づいたときに警告するアラームを設定することもできます。AWS Fargate のサービスクォータの詳細については、「AWS Fargate Service Quotas」を参照してください。

AWS Fargate 使用状況メトリクスの詳細については、「AWS Fargate 使用状況メトリクス」を参照してください。

Fargate 起動タイプをどのような場合に使用するかについての Amazon ECS セキュリティ上の考慮事項

タスクの強力な分離を求めているお客様には、Fargate を使用することをお勧めします。Fargate はハードウェア仮想化環境で各タスクを実行します。これにより、これらのコンテナ化されたワークロードがネットワークインターフェイス、Fargate の一時ストレージ、CPU、またはメモリを他のタスクと共有しないことが保証されます。詳細については、「AWS Fargate のセキュリティの概要」をご参照ください。

Amazon ECS の Fargate セキュリティのベストプラクティス

AWS Fargate を使用する際には、次のベストプラクティスを考慮することをお勧めします。その他のガイダンスについては、「AWS Fargate のセキュリティ概要」を参照してください。

AWS KMS を使用して Fargate のエフェメラルストレージを暗号化する

エフェメラルストレージは、 AWS KMS または独自のカスタマーマネージドキーで暗号化する必要があります。バージョン `1.4.0` 以降のプラットフォームを使用していて、Fargate でホストされているタスクの場合は、最低 20 GiB のエフェメラルストレージを受け取ります。詳細については、「カスタマーマネージドキー (CMK)」を参照してください。エフェメラルストレージの総量は、タスク定義で `ephemeralStorage` パラメータを指定することによって、最大 200 GiB まで増やすことができます。2020 年 5 月 28 日以降に起動されたこのようなタスクでは、エフェメラルストレージは、Fargate によって管理される暗号化キーを使用して、AES-256 暗号化アルゴリズムによって暗号化されます。

詳細については、「Amazon ECS タスクのストレージオプション」を参照してください。

例: Fargate プラットフォーム バージョン 1.4.0 で、エフェメラルストレージの暗号化を使用してタスクを起動する

次のコマンドは、Fargate プラットフォームバージョン 1.4 でタスクを起動します。このタスクは Amazon ECS クラスターの一部として起動されるため、自動的に暗号化された 20 GiB のエフェメラルストレージが使用されます。

```
aws ecs run-task --cluster clustername \
  --task-definition taskdefinition:version \
  --count 1
  --launch-type "FARGATE" \
  --platform-version 1.4.0 \
  --network-configuration
 "awsvpcConfiguration={subnets=[subnetid],securityGroups=[securitygroupid]}" \
  --region region
```

Fargate を使用したカーネルシステムコールトレーシングの SYS_PTRACE 機能

コンテナに追加または削除される Linux 機能のデフォルト設定は、Docker が行います。

Fargate で起動したタスクでは、SYS_PTRACE カーネル機能の追加のみがサポートされます。

Sysdig Falco プロジェクトでこの機能を使用する方法を示す以下の動画。

#ContainersFromTheCouch - SYS_PTRACE 機能を使用した Fargate タスクのトラブルシューティング

前のビデオで説明したコードは、こちらの GitHub にあります。

Fargate Runtime Monitoring で Amazon GuardDuty を使用する

Amazon GuardDuty は、AWS 環境内のアカウント、コンテナ、ワークロード、データを保護する脅威検知サービスです。GuardDuty は、機械学習（ML）モデル、異常および脅威検出機能を使用して、さまざまなログソースとランタイムアクティビティを継続的に監視し、環境内の潜在的なセキュリティリスクと悪意のあるアクティビティを特定して優先順位を付けます。

GuardDuty のランタイムモニタリングは、AWS ログとネットワークアクティビティを継続的に監視して悪意のある動作や不正な動作を特定することで、Fargate で実行されているワークロードを保護します。ランタイムモニタリングは、軽量でフルマネージド型の GuardDuty セキュリティエージェントを使用して、ファイルアクセス、プロセス実行、ネットワーク接続などのホスト上動作を分析します。これは、Amazon EC2 インスタンスおよびコンテナワークロードでの権限の昇格、流出した認証情報の使用、悪意のある IP アドレスやドメインとの通信、マルウェアの存在などの問題に対応

しています。詳細については、「GuardDuty ユーザーガイド」の「GuardDuty ランタイムモニタリング」を参照してください。

Amazon ECS の Fargate のセキュリティに関する考慮事項

Fargate は各ワークロードを独立した仮想環境で実行するため、各タスクには専用のインフラストラクチャ容量があります。Fargate で実行されるワークロードは、ネットワークインターフェイス、エフェメラルストレージ、CPU、またはメモリを他のタスクと共有しません。アプリケーションコンテナやサイドカーコンテナを含む複数のコンテナをタスク内で実行することも、単にサイドカーを実行することもできます。サイドカーは Amazon ECS タスク内のアプリケーションコンテナと一緒に実行されるコンテナです。アプリケーションコンテナはコアアプリケーションコードを実行しますが、サイドカーで実行されるプロセスはアプリケーションを拡張できます。サイドカーはアプリケーションの機能を専用のコンテナに分離するのに役立ち、アプリケーションの一部を簡単に更新することができます。

同じタスクに属するコンテナは、常に同じホスト上で実行され、コンピュートリソースを共有するため、Fargate 起動タイプのリソースを共有します。これらのコンテナは、Fargate が提供するエフェメラルストレージも共有しています。タスク内の Linux コンテナは、IP アドレスやネットワークポートを含むネットワーク名前空間を共有します。タスク内では、タスクに属するコンテナが localhost を介して相互通信できます。

Fargate のランタイム環境では、EC2 インスタンスでサポートされている特定のコントローラー機能を使用できません。Fargate で実行されるワークロードを設計するときは、次の点を考慮してください。

- 特権コンテナまたはアクセスなし - 特権コンテナやアクセスなどの機能は現在、Fargate では利用できません。これは Docker 内で Docker を実行するなどのユースケースに影響します。
- Linux 機能への制限付きアクセス - Fargate 上でコンテナが動作する環境はロックダウンされています。CAP_SYS_ADMIN や CAP_NET_ADMIN などのそのほかの Linux 機能は、権限昇格を防ぐために制限されています。Fargateは、タスクに CAP_SYS_PTRACE Linux機能を追加することをサポートしています。これにより、タスク内にデプロイされたオブザーバビリティツールとセキュリティツールがコンテナ化されたアプリケーションを監視できるようになります。
- 基盤となるホストにはアクセスできない - お客様も AWS オペレーターも、お客様のワークロードを実行しているホストには接続できません。ECS Exec を使用して、Fargate で実行されているコンテナでコマンドを実行したり、シェルを取得したりできます。ECS Exec を使用すると、デバッグ用の診断情報を収集できます。また、Fargate は、コンテナがファイルシステム、デバイス、ネットワーク、コンテナランタイムなどの基盤となるホストのリソースにアクセスするのを防ぎます。

- ネットワーク - セキュリティグループとネットワーク ACL を使用して、インバウンドトラフィックとアウトバウンドトラフィックをコントロールできます。Fargate のタスクは VPC 内の設定済みサブネットから IP アドレスを受け取ります。

Amazon ECS 向け Fargate プラットフォームバージョン

AWS Fargate プラットフォームのバージョンを使って、Fargate タスクインフラストラクチャの特定のランタイム環境を参照できます。これは、カーネルとコンテナのランタイムバージョンの組み合わせです。同一のタスクを多数管理するためのタスク実行時、またはそのためのサービス作成時には、プラットフォームバージョンを選択します。

ランタイム環境の進化に合わせて、新しいプラットフォームバージョンがリリースされます。例えば、カーネルやオペレーティングシステムの更新、新機能の追加、バグ修正、セキュリティの更新があった場合が当てはまります。Fargate プラットフォームのバージョンは、新しいプラットフォームバージョンのリビジョンを行うことで更新されます。各タスクは、そのライフサイクルを通じて、単一のプラットフォームバージョンのリビジョンで実行されます。最新のプラットフォームバージョンのリビジョンを使用する場合は、新たにタスクを開始する必要があります。Fargate で実行される新しいタスクは、常にプラットフォームバージョンの最新リビジョンで実行されます。これにより、タスクは必ず、安全でパッチ適用済みのインフラストラクチャで開始されることが保証されます。

既存のプラットフォームのバージョンに影響を与えるセキュリティ上の問題が見つかった場合、AWS は、そのプラットフォームバージョンのパッチ済みリビジョンを新たに作成します。また、脆弱性のあるリビジョンで実行しているタスクは廃止されます。場合によっては、Fargate で使用しているタスクについて、廃止の予定が通知されることがあります。詳細については、「AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス」を参照してください。

プラットフォームバージョンは、タスクを実行するとき、またはサービスをデプロイするときに指定します。

プラットフォームのバージョンを指定する際には、次の点を検討してください。

- `1.4.0`、LATEST など、特定のバージョン番号を指定できます。

  [LATEST] の Linux プラットフォームバージョンは `1.4.0` です。

  [LATEST] の Windows プラットフォームバージョンは `1.0.0` です。
- サービスのプラットフォームバージョンを更新する場合は、デプロイを作成します。例えば、Linux のプラットフォームバージョン `1.3.0` で、タスクを実行しているサービスがあるとし

ます。Linux プラットフォームバージョン 1.4.0 でタスクを実行するようにサービスを変更するには、サービスを更新し、新しいプラットフォームバージョンを指定します。タスクは、最新のプラットフォームバージョンと最新のプラットフォームバージョンのリビジョンで再デプロイされます。デプロイの詳細については、「Amazon ECS サービス」を参照してください。

- サービスがプラットフォームバージョンを更新しないでスケールアップされた場合、これらのタスクには、サービスの最新のデプロイで指定されたプラットフォームのバージョンが提供されます。例えば、Linux のプラットフォームバージョン 1.3.0 で、タスクを実行しているサービスがあるとします。このサービスについて必要とされる数を増加した場合、サービススケジューラーは、プラットフォームバージョン 1.3.0 の最新のプラットフォームバージョンのリビジョンを使用して、新しいタスクを開始します。
- 新しいタスクは、常にプラットフォームバージョンの最新リビジョンで実行されます。この結果、タスクは常にセキュリティで保護されパッチが適用されたインフラストラクチャ上になります。
- Fargate の Linux コンテナと Windows コンテナのプラットフォームバージョンの番号は相互に独立しています。例えば、Fargate の Windows コンテナのプラットフォームバージョン 1.0.0 で使用される動作、機能、およびソフトウェアは、Fargate の Linux コンテナのプラットフォームバージョン 1.0.0 の動作、機能、およびソフトウェアとは比較できません。
- Fargate Windows プラットフォームバージョンには、以下が適用されます。

  Microsoft Windows Server のコンテナイメージは、特定のバージョンの Windows Server から作成する必要があります。Windows Server コンテナイメージに適合したタスクの実行やサービスの作成を行う場合は、platformFamily で同じバージョンの Windows Server を選択する必要があります。さらに、タスク定義で一致させる operatingSystemFamily を指定して、間違った Windows バージョンでタスクが実行されないようにできます。詳細については、Microsoft Learn のウェブサイトで「コンテナホストのバージョンとコンテナイメージのバージョンを一致させる」を参照してください。

Amazon ECS 上の Linux プラットフォームバージョン 1.4.0 への移行

FargateタスクのAmazon ECSをプラットフォームバージョン 1.0.0、1.1.0、1.2.0、または 1.3.0 からプラットフォームバージョン 1.4.0 に移行する場合は、次のことを考慮してください。タスクを移行する前に、そのタスクがプラットフォームバージョン 1.4.0 で正しく動作するのを確認することがベストプラクティスです。

- タスクとの間のネットワークトラフィック動作を更新しました。プラットフォームバージョン 1.4.0 以降では、Fargate タスクでのすべての Amazon ECS は単一の Elastic Network Interface (以降タスク ENI)を受け取り、すべてのネットワークトラフィックは VPC 内でこの ENI を通過しま

す。このトラフィックは VPC フローログを通じて表示されます。詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。

- インターフェイス VPC エンドポイントを使用する場合は、次の点を考慮してください。
  - Amazon ECR でホストされているコンテナイメージでは、次のエンドポイントが必要です。詳細については、Amazon Elastic コンテナレジストリ ユーザーガイドの Amazon ECR Interface VPC エンドポイント(AWS PrivateLink)を参照してください。
    - [com.amazonaws.***region***.ecr.dkr] Amazon ECR VPC エンドポイント
    - [com.amazonaws.***region***.ecr.api] Amazon ECR VPC エンドポイント
    - Amazon S3 ゲートウェイエンドポイント
  - コンテナの機密データを取得する際にタスク定義が Secrets Manager シークレットを参照する場合は、Secrets Manager のインターフェイス VPC エンドポイントを作成する必要があります。詳細については、AWS Secrets Manager ユーザーガイドのVPC EndpointでSecrets Managerを使用するを参照してください。
  - コンテナの機密データを取得する際にタスク定義が Systems Manager Parameter Store パラメータを参照する場合は、SystemsManager のインターフェイス VPC エンドポイントを作成する必要があります。詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。
  - タスクに関連付けられた Elastic Network Interface (ENI) のセキュリティグループには、タスクと VPC エンドポイントとの間のトラフィックを許可するセキュリティグループルールが必要です。

Fargate Linux プラットフォームバージョンの変更ログ

使用できる Linux プラットフォームのバージョンは以下のとおりです。プラットフォームバージョンの廃止については、「AWS Fargate Linux プラットフォームバージョンの廃止」を参照してください。

1.4.0

以下は、プラットフォームバージョンの変更履歴です`1.4.0`。

- 2020 年 11 月 5 日以降、プラットフォームバージョン`1.4.0`を使用して Fargate で起動されたすべての新しい Amazon ECS タスクで次の機能を使用できるようになります:

  - Secrets Managerを使用して機密データを保存する場合、特定の JSON キーまたは特定のシークレットのバージョンを環境変数またはログ設定に挿入できます。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。
  - `environmentFiles` コンテナ定義パラメータを使用して、環境変数を一括で指定します。詳細については、「個々の環境変数を Amazon ECS コンテナに渡す」を参照してください。
  - VPC で実行されるタスクと IPv6 が有効になっているサブネットには、プライベート IPv4 アドレスと IPv6 アドレスの両方が割り当てられます。詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。
  - タスクメタデータエンドポイントバージョン 4 には、タスク起動タイプ、コンテナの Amazon リソースネーム (ARN)、使用されるログドライバーとログドライバーオプションなど、タスクとコンテナに関する追加のメタデータが提供されます。`/stats` エンドポイントに対してクエリを実行すると、コンテナのネットワークレート統計も受け取ります。詳細については、「タスクメタデータエンドポイントバージョン 4」を参照してください。
- 2020 年 7 月 30 日以降、プラットフォームバージョン `1.4.0` を使用して Fargate で起動されたすべての新しい Amazon ECS タスクは、Network Load Balancer を使用して、UDP トラフィックを Fargate タスク上の Amazon ECS にルーティングできるようになります。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。
- 2020 年 5 月 28 日以降、プラットフォームバージョン`1.4.0`を使用してFargate で起動されたすべての新しい Amazon ECS タスクにはAWS 所有する暗号化キーを使用して AES-256 暗号化アルゴリズムで暗号化されたエフェメラルストレージが搭載されます。詳細については、Amazon ECS 向けの Fargate タスクエフェメラルストレージおよびAmazon ECS タスクのストレージオプションを参照してください。
- 永続的なタスクストレージとして Amazon EFS ファイルシステムボリュームを使用するためにサポートを追加しました。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。
- エフェメラルタスクストレージは、タスクごとに最低 20 GB に増加しました。詳細については、「Amazon ECS 向けの Fargate タスクエフェメラルストレージ」を参照してください。
- タスクとの間のネットワークトラフィック動作を更新しました。プラットフォームバージョン 1.4.0 以降、すべての Fargate タスクは単一の Elastic Network Interface (タスク ENI と呼ばれる) を受け取り、すべてのネットワークトラフィックは VPC 内でこの ENI を通過し、VPC フローログを通じて表示されます。Amazon EC2 起動タイプのネットワークの詳細については、「EC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。Fargate 起動タイプのネットワークの詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。

- タスク ENI は、ジャンボフレームのサポートを追加しています。ネットワークインターフェイスは、最大転送単位 (MTU) で設定されます。MTU は、1 つのフレームに収まるペイロードの最大サイズです。MTU が大きいほど、1 つのフレーム内に収まるアプリケーションのペイロードが増えるため、フレームあたりのオーバーヘッドが減少し、効率が向上します。ジャンボフレームをサポートすると、オーバーヘッドが減ります。タスクと転送先とのネットワークパスでジャンボフレームをサポートすると、VPC 内に残っているすべてのトラフィックなどのオーバーヘッドが軽減されます。
- CloudWatch Container Insights には、Fargate タスクのネットワークパフォーマンスメトリクスが含まれます。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。
- タスクメタデータエンドポイントバージョン 4 のサポートを追加しました。これにより、タスクのネットワーク統計情報や、タスクが実行されているアベイラビリティーゾーンなど、Fargate タスクに関する追加情報が提供されます。詳細については、Amazon ECS タスクメタデータエンドポイントバージョン 4およびFargate のタスク用の Amazon ECS タスクメタデータエンドポイントバージョン 4を参照してください。
- コンテナの定義に SYS_PTRACE Linux パラメータのサポートを追加しました。詳細については、「Linux パラメータ」を参照してください。
- Fargateコンテナエージェントは、Amazon ECS コンテナエージェントの使用をすべての Fargate タスクに置き換えます。通常、この変更は、タスクの実行方法には影響しません。
- コンテナランタイムは Docker の代わりに Containerd を使用するようになりました。ほとんどの場合、この変更はタスクの実行方法には影響しません。コンテナランタイムで発生するいくつかのエラーメッセージは、より一般的な内容になり、Docker には言及されなくなります。詳細については、「Amazon ECS の停止したタスクのエラーメッセージ」を参照してください。
- Amazon Linux 2 に基づく。

1.3.0

以下は、プラットフォームバージョンの変更履歴です`1.3.0`。

- 2019 年 9 月 30 日以降、起動されたすべての新しい Fargate タスクでは、`awsfirelens`ログドライバーをサポートします。タスク定義パラメータを使用して、AWS のサービスまたは AWS パートナーネットワーク (APN) の送信先に、ログをルーティングし保存および分析を行うように、FireLens for Amazon ECS を設定します。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。

- Fargateタスクのタスクリサイクルが追加されました。これは、Amazon ECS サービスの一部であるタスクを更新するプロセスです。詳細については、「AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス」。
- 2019 年 3 月 27 日以降、起動されたすべての新しい Fargate タスクでは、プロキシ設定、コンテナのスタートアップとシャットダウンの依存関係、コンテナ別の起動と停止のタイムアウト値を定義するための追加タスク定義パラメータを使用できます。詳細については、「プロキシ設定」、「コンテナの依存関係」、および「[コンテナのタイムアウト]」を参照してください。
- 2019 年 4 月 2 日以降、起動されたすべての新しい Fargate タスクでは、機密データをAWS Secrets Managerシークレットまたは AWS Systems Managerパラメーターストアのパラメーターのいずれかに保存し、コンテナ定義でそれらを参照することにより、コンテナへの機密データの挿入をサポートします。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。
- 2019 年 5 月 1 日以降、起動された新しい Fargate タスクでは、`secretOptions` コンテナ定義パラメータを使用してコンテナのログ設定内の機密データを参照できます。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。
- 2019 年 5 月 1 日以降、起動されるすべての新しいFargate タスクでは、`splunk`ログドライバーに加えて `awslogs`ログドライバーがサポートされます。詳細については、「ストレージとログ記録」を参照してください。
- 2019 年 7 月 9 日以降に新しく起動された Fargate タスクでは、 CloudWatch Container Insights がサポートされています。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。
- 2019 年 12 月 3 日より、Fargate Spot キャパシティープロバイダーがサポートされます。詳細については、「Fargate 起動タイプ用の Amazon ECS クラスター 」を参照してください。
- Amazon Linux 2 に基づく。

AWS Fargate Linux プラットフォームバージョンの廃止

このページでは、AWS Fargate が非推奨にされたか、または廃止が予定されている Linux プラットフォームのバージョンを示しています。これらのプラットフォームのバージョンは、公開された廃止日までは引き続き利用できます。

廃止予定のプラットフォームのバージョンごとに、強制更新日が提供されます。強制更新日に、廃止予定のプラットフォームバージョンを指すLATEST プラットフォームバージョンを使用するすべてのサービスは、強制新規デプロイオプションを使用して更新されます。強制新規デプロイオプションを使用してサービスを更新すると、廃止予定のプラットフォームバージョンで実行されているすべての

タスクが停止され、新しいタスクはLATESTタグがその時に指すプラットフォームのバージョンを使用して起動されます。明示的なプラットフォームバージョンが設定されているスタンドアロンのタスクまたはサービスは、強制更新日の影響を受けません。

サービスのスタンドアロンタスクを更新して、最新のプラットフォームバージョンを使用することをお勧めします。最新のプラットフォームバージョンへの移行の詳細については、Amazon ECS 上の Linux プラットフォームバージョン 1.4.0 への移行を参照してください。

プラットフォームバージョンが廃止日に達すると、そのプラットフォームのバージョンは新しいタスクやサービスで使用できなくなります。非推奨のプラットフォームバージョンを明示的に使用するスタンドアロンのタスクまたはサービスは、タスクが停止されるまでそのプラットフォームバージョンを使用し続けます。廃止日を過ぎると、非推奨のプラットフォームバージョンはセキュリティのアップデートやバグの修正を受けなくなります。

プラットフォームバージョン	強制更新日	廃止日
1.0.0	2020 年 10 月 26 日	2020 年 12 月 14 日
1.1.0	2020 年 10 月 26 日	2020 年 12 月 14 日
1.2.0	2020 年 10 月 26 日	2020 年 12 月 14 日

現在のプラットフォームバージョンの詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。

廃止された Fargate Linux バージョンに関する変更ログ

1.2.0

以下は、プラットフォームバージョンの変更履歴です`1.2.0`。

> **Note**
>
> プラットフォームバージョン `1.2.0` は今後利用できません。プラットフォームバージョンの廃止については、AWS Fargate Linux プラットフォームバージョンの廃止を参照してください。

- AWS Secrets Manager を使用したプライベートレジストリ認証のサポートが追加されました。詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

1.1.0

以下は、プラットフォームバージョンの変更履歴です1.1.0。

> **Note**
>
> プラットフォームバージョン 1.1.0 は今後利用できません。プラットフォームバージョンの廃止については、AWS Fargate Linux プラットフォームバージョンの廃止を参照してください。

- Amazon ECSタスクメタデータエンドポイントのサポートを追加しました。詳細については、「Fargate のタスクで使用できる Amazon ECS タスクメタデータ」を参照してください。
- コンテナ定義に追加された Docker ヘルスチェックのサポート。詳細については、「ヘルスチェック」を参照してください。
- Amazon ECSサービス検出のサポートを追加しました。詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。

1.0.0

以下は、プラットフォームバージョンの変更履歴です1.0.0。

> **Note**
>
> プラットフォームバージョン 1.0.0 は今後利用できません。プラットフォームバージョンの廃止については、AWS Fargate Linux プラットフォームバージョンの廃止を参照してください。

- Amazon Linux 2017.09 に基づく。
- 初回リリース。

Fargate Windows プラットフォームバージョンの変更ログ

Windows コンテナに使用できるプラットフォームのバージョンは以下のとおりです。

1.0.0

以下は、プラットフォームバージョンの変更履歴です`1.0.0`。

- 以下の Microsoft Windows Server オペレーティングシステムに対応した初期リリース。
  - Windows Server 2019 Full
  - Windows Server 2019 Core
  - Windows Server 2022 Full
  - Windows Server 2022 Core

Amazon ECS における Fargate 上の Windows コンテナに関する考慮事項

AWS Fargate で Windows コンテナを実行する場合の相違点と考慮事項は次のとおりです。

Linux と Windows のコンテナでタスクを実行する必要がある場合は、オペレーティングシステムごとに別々のタスク定義を作成する必要があります。

オペレーティングシステムのライセンス管理は、AWS が担当します。したがって、お客様は、追加の Microsoft ライセンスの必要はありません。

AWS Fargate の Windows コンテナは以下のオペレーティングシステムをサポートしています。

- Windows Server 2019 Full
- Windows Server 2019 Core
- Windows Server 2022 Full
- Windows Server 2022 Core

AWS Fargate の Windows コンテナは、awslogs ドライバをサポートしています。詳細については、「the section called “CloudWatch にログを送信する ”」を参照してください。

Fargate の Windows コンテナでは、以下の機能はサポートされていません。

- Amazon FSx
- ENI トランキング
- Windows コンテナ向け gMSA
- タスク用 App Mesh サービスとプロキシの統合
- タスク用 Firelens ログルーターの統合
- EFS ボリューム
- EBS ボリューム
- 以下に示すタスク定義パラメータ。
  - `maxSwap`
  - `swappiness`
  - `environmentFiles`
- Fargate Spot キャパシティープロバイダー
- イメージボリューム

  Dockerfile `volume` オプションは無視されます。代わりに、タスクの定義でバインドマウントを使用します。詳細については、「Amazon ECS でのバインドマウントの使用」を参照してください。
- Windows コンテナーでは、タスクレベルの CPU およびメモリパラメーターは無視されます。Windows コンテナではコンテナレベルリソースを指定することをお勧めします。
- タスクのメモリ
- コンテナのメモリ予約

Amazon ECS 向けの Fargate タスクエフェメラルストレージ

AWS Fargate の Linux コンテナでホストされている各 Amazon ECS タスクはプロビジョニング時にバインドマウントのために次のエフェメラルストレージを受け取ります。これらをマウントし、タスク定義内で `volumes`、`mountPoints` および `volumesFrom` パラメータを使用しているコンテナ間で共有することが可能です。この設定は AWS Fargate の Windows コンテナではサポートされません。

Fargate Linux コンテナプラットフォームのバージョン

バージョン 1.4.0 以降

プラットフォームバージョン `1.4.0` 以降を使用している Fargate でホストされている Amazon ECS タスクは、デフォルトで、最低 20 GiB のエフェメラルストレージを受け取ります。エフェメラルストレージの総量は、最大 200 GiB まで増やすことができます。これを行うには、タスク定義内で `ephemeralStorage` パラメータを設定します。

プル、圧縮、および非圧縮されたコンテナイメージは、エフェメラルストレージに格納されます。タスクを使用するエフェメラルストレージの総量を判断するには、タスクが割り当てられているエフェメラルストレージの総量から、コンテナイメージが使用するストレージの容量を差し引く必要があります。

2020 年 5 月 28 日以降に開始されたプラットフォームバージョン `1.4.0` 以降を使用するタスクでは、エフェメラルストレージが AES-256 暗号化アルゴリズムにより暗号化されます。このアルゴリズムは AWS が所有する暗号化キーを使用するか、独自のカスタマーマネージドキーを作成できます。詳細については、「Customer managed keys for AWS Fargate ephemeral storage」を参照してください。

2022 年 11 月 18 日以降に開始されたプラットフォームバージョン `1.4.0` 以降を使用するタスクでは、エフェメラルストレージの使用量がタスクメタデータエンドポイントを通じて報告されます。タスク内のアプリケーションは、タスクメタデータエンドポイントのバージョン 4 に対してクエリを実行して、エフェメラルストレージの予約サイズと使用量を取得できます。

さらに、Container Insights をオンにすると、エフェメラルストレージの予約サイズと使用量が Amazon CloudWatch Container Insights に送信されます。

> **Note**
>
> Fargate はディスク上のスペースを予約します。スペースは Fargate によってのみ使用されます。これには課金されることはありません。これらのメトリクスには表示されません。ただし、この追加ストレージは、`df` などの他のツールでも確認できます。

バージョン 1.3.0 以前

プラットフォームバージョン `1.3.0` 以前を使用する Fargate タスクでの Amazon ECS の場合、各タスクは次のエフェメラルストレージを受け取ります。

- 10 GB の Docker Layer ストレージ

> **Note**
>
> この量には、圧縮および非圧縮のコンテナイメージのアーティファクトの両方が含まれます。

- ボリュームマウント用の追加 4 GB。これらをマウントし、タスク定義内で `volumes`、`mountPoints` および `volumesFrom` パラメータを使用しているコンテナ間で共有することが可能です。

Fargate Windows コンテナプラットフォームのバージョン

バージョン 1.0.0 以降

プラットフォームバージョン `1.0.0` 以降を使用している Fargate でホストされている Amazon ECS タスクは、デフォルトで、最低 20 GiB のエフェメラルストレージを受け取ります。エフェメラルストレージの総量は、最大 200 GiB まで増やすことができます。これを行うには、タスク定義内で `ephemeralStorage` パラメータを設定します。

プル、圧縮、および非圧縮されたコンテナイメージは、エフェメラルストレージに格納されます。タスクが使用するエフェメラルストレージの総量を判断するには、タスクに割り当てられたエフェメラルストレージの総量から、コンテナイメージが使用するストレージの容量を差し引く必要があります。

詳細については、「Amazon ECS でのバインドマウントの使用」を参照してください。

Amazon ECS 向け AWS Fargate エフェメラルストレージ用のカスタマーマネージドキー

AWS Fargate は、エフェメラルストレージに保存されている Amazon ECS タスクのデータを暗号化するカスタマーマネージドキーをサポートし、規制の影響を受けるお客様が内部セキュリティポリシーを満たすことができるよう支援しています。お客様は、Fargate のサーバーレスのメリットを引き続き享受しながら、コンプライアンス監査者に対してセルフマネージドストレージ暗号化の強化された可視性を提供できます。Fargate は、デフォルトで Fargate 管理のエフェメラルストレージ暗号化を備えていますが、お客様は財務情報や健康関連情報などの機密データを暗号化する際に、独自のセルフマネージドキーを使用することもできます。

AWS KMS に独自のキーをインポートするか、AWS KMS でキーを作成できます。これらのセルフマネージドキーは AWS KMS に保存され、ローテーション、無効化、削除などの標準的な AWS KMS のライフサイクルアクションを実行します。CloudTrail ログで、キーのアクセスと使用状況を監査できます。

デフォルトでは、KMS キーはキーごとに 50,000 の許可をサポートします。Fargate は、各カスタマーマネージドキーのタスクに 1 つの AWS KMS 許可を使用するため、1 つのキーに対して最大 50,000 の同時タスクをサポートします。この数を増やしたい場合は、ケースバイケースで承認される制限の引き上げをリクエストすることができます。

Fargate では、カスタマーマネージドキーの使用に追加の料金は発生しません。ストレージと API リクエストに AWS KMS キーを使用するための標準料金のみが請求されます。

トピック

- Amazon ECS 向け Fargate エフェメラルストレージの暗号化キーを作成する
- Amazon ECS 向け Fargate エフェメラルストレージの AWS KMS キーを管理する

Amazon ECS 向け Fargate エフェメラルストレージの暗号化キーを作成する

Fargate エフェメラルストレージに保存されているデータを暗号化するためのカスタマーマネージドキーを作成します。

> **Note**
>
> カスタマーマネージドキーによる Fargate エフェメラルストレージの暗号化は、Windows タスククラスターでは利用できません。
> カスタマーマネージドキーによる Fargate エフェメラルストレージの暗号化は、`1.4.0` より前のバージョンの `platformVersions` では利用できません。
> Fargate は、Fargate のみが使用するエフェメラルストレージのスペースを予約します。そのスペースに対して料金は発生しません。割り当ては、カスタマー管理以外のキータスクとは異なる場合がありますが、スペースの合計は変わりません。この変更については、`df` などのツールで確認できます。
> マルチリージョンキーは、Fargate エフェメラルストレージではサポートされていません。
> KMS キーエイリアスは、Fargate エフェメラルストレージではサポートされていません。

AWS KMS で Fargate のエフェメラルストレージを暗号化するカスタマーマネージドキー (CMK) を作成するには、次のステップに従ってください。

1. https://console.aws.amazon.com/kms に移動します。
2. 手順については、「AWS Key Management Service デベロッパーガイド」の「Creating Keys」を参照してください。
3. AWS KMS キーを作成するときは、キーポリシーで Fargate サービスに関連する AWS KMS オペレーションのアクセス許可を必ず付与してください。Amazon ECS クラスターリソースでカスタマー管理キーを使用するには、ポリシーで次の API オペレーションを許可する必要があります。

   - `kms:GenerateDataKeyWithoutPlainText` - `GenerateDataKeyWithoutPlainText` を呼び出し、提供された AWS KMS キーから暗号化されたデータキーを生成します。
   - `kms:CreateGrant` - カスタマーマネージドキーに許可を追加します。指定された AWS KMS キーへのアクセス制御を付与します。これは、Amazon ECS Fargate が必要なグラントオペレーションへのアクセスを許可するものです。詳細については、「AWS Key Management Service デベロッパーガイド」の「Using Grants」を参照してください。これにより、Amazon ECS Fargate で以下を行うことができます。
     - `Decrypt` から AWS KMS を呼び出し、エフェメラルストレージのデータを復号するための暗号化キーを取得します。
     - `RetireGrant` にサービスが許可するための、廃止するプリンシパルを設定します。
   - `kms:DescribeKey` — カスタマーマネージドキーの詳細を提供し、キーが対称、かつ有効である場合に、Amazon ECS がキーを検証できるようにします。

   次の例は、暗号化するターゲットキーに適用する AWS KMS キーポリシーを示しています。ポリシーステートメントの例を使用する際は、*###############*を独自の情報に置き換えます。通常どおり、必要なアクセス許可のみを設定しますが、エラーを回避するために、少なくとも 1 人のユーザーにアクセス許可付きの AWS KMS を提供する必要があります。

```
{
      "Sid": "Allow generate data key access for Fargate tasks.",
      "Effect": "Allow",
      "Principal": { "Service":"fargate.amazonaws.com" },
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Condition": {
        "StringEquals": {
          "kms:EncryptionContext:aws:ecs:clusterAccount": [
            "customerAccountId"
```

```
          ],
          "kms:EncryptionContext:aws:ecs:clusterName": [
             "clusterName"
          ]
        }
      },
      "Resource": "*"
    },
    {
      "Sid": "Allow grant creation permission for Fargate tasks.",
      "Effect": "Allow",
      "Principal": { "Service":"fargate.amazonaws.com" },
      "Action": [
        "kms:CreateGrant"
      ],
      "Condition": {
        "StringEquals": {
          "kms:EncryptionContext:aws:ecs:clusterAccount": [
            "customerAccountId"
          ],
          "kms:EncryptionContext:aws:ecs:clusterName": [
             "clusterName"
          ]
        },
       "ForAllValues:StringEquals": {
          "kms:GrantOperations": [
             "Decrypt"
          ]
       }
      },
      "Resource": "*"
    },
    {
      "Sid": "Allow describe key permission for cluster operator - CreateCluster
 and UpdateCluster.",
      "Effect": "Allow",
      "Principal": { "AWS":"arn:aws:iam::customerAccountId:role/customer-chosen-
role" },
      "Action": [
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
```

Fargate タスクでは、キーを使用する暗号化オペレーションに aws:ecs:clusterAccount および aws:ecs:clusterName 暗号化コンテキストキーを使用します。特定のアカウントやクラスターへのアクセスを制限するには、これらのアクセス許可を追加する必要があります。クラスターを指定するときは、ARN ではなくクラスター名を使用してください。

詳しくは、AWS KMS デベロッパーガイドの Encryption context を参照してください。

クラスターを作成または更新する場合、条件キー fargateEphemeralStorageKmsKeyId を使用するオプションを利用できます。この条件キーにより、お客様は IAM ポリシーをよりきめ細かく制御できます。fargateEphemeralStorageKmsKeyId 設定の更新は、新しいサービスのデプロイでのみ有効になります。

以下は、お客様が特定の承認された AWS KMS キーのセットにのみアクセス許可を付与できるようにする例です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:CreateCluster",
        "ecs:UpdateCluster"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ecs:fargate-ephemeral-storage-kms-key": "arn:aws:kms:us-
west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        }
      }
    }
  ]
}
```

次に、クラスターに既に関連付けられている AWS KMS キーの削除を拒否する例を示します。

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

```
    "Effect": "Deny",
    "Action": [
        "ecs:CreateCluster",
        "ecs:UpdateCluster"
    ],
    "Resource": "*",
    "Condition": {
      "Null": {
        "ecs:fargate-ephemeral-storage-kms-key": "true"
      }
    }
  }
}
```

お客様は、AWS CLI、`describe-tasks`、`describe-cluster` または `describe-services` コマンドを使用して、管理されていないタスクまたはサービスタスクが、キーを使用して暗号化されているかどうかを確認できます。

詳細については、「AWS KMS デベロッパーガイド」の「Condition keys for AWS KMS」を参照してください。

AWS Management Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. 左側のナビゲーションで [クラスター]を選択し、右上で [クラスターの作成] を選択するか、既存のクラスターを選択します。既存のクラスターの場合は、右上の [クラスターの更新] を選択します。
3. ワークフローの [暗号化] セクションでは、[マネージド型ストレージ] と [Fargate エフェメラルストレージ] で AWS KMS キーを選択することもできます。ここで [AWS KMS キーの作成] を選択することもできます。
4. 新しいクラスターの作成が完了したら [作成] を選択し、既存のクラスターを更新する場合は [更新] を選択します。

AWS CLI

以下は、クラスターを作成し、AWS CLI を使用して Fargate エフェメラルストレージを設定する例です (*##*の値は独自の値に置き換えてください)。

```
aws ecs create-cluster --cluster clusterName \
```

```
--configuration '{"managedStorageConfiguration":
{"fargateEphemeralStorageKmsKeyId":"arn:aws:kms:us-
west-2:012345678901:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"}}'
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:012345678901:cluster/clusterName",
        "clusterName": "clusterName",
        "configuration": {
            "managedStorageConfiguration": {
                "fargateEphemeralStorageKmsKeyId": "arn:aws:kms:us-
west-2:012345678901:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        },
        "status": "ACTIVE",
        "registeredContainerInstancesCount": 0,
        "runningTasksCount": 0,
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [],
        "settings": [],
        "capacityProviders": [],
        "defaultCapacityProviderStrategy": []
    },
    "clusterCount": 5
}
```

AWS CloudFormation

以下は、クラスターを作成し、AWS CloudFormation を使用して Fargate エフェメラルストレージを設定するテンプレートの例です (##の値は独自の値に置き換えてください)。

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  MyCluster:
    Type: AWS::ECS::Cluster
    Properties:
      ClusterName: "clusterName"
      Configuration:
        ManagedStorageConfiguration:
          FargateEphemeralStorageKmsKeyId: "arn:aws:kms:us-
west-2:012345678901:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Amazon ECS 向け Fargate エフェメラルストレージの AWS KMS キーを管理する

Fargate エフェメラルストレージを暗号化するための AWS KMS キーを作成またはインポートしたら、他の AWS KMS キーと同じ方法で管理します。

AWS KMS キーの自動ローテーション

キーの自動ローテーションを有効にするか、手動でローテーションすることができます。キーの自動ローテーションは、キーの新しい暗号化マテリアルを生成することによって、キーを毎年ローテーションします。AWS KMS は、暗号化マテリアルの以前のバージョンもすべて保存するため、以前のキーバージョンを使用したデータを復号化することができます。ローテーションされたマテリアルは、キーを削除するまで AWS KMS によって削除されることはありません。

キーの自動ローテーションはオプションであり、いつでも有効または無効にできます。

AWS KMS キーの無効化または取り消し

AWS KMS でカスタマーマネージドキーを無効にした場合でも、タスクの実行に影響はなく、ライフサイクルを通じて引き続き機能します。無効化または取り消しされたキーが新しいタスクで使用されている場合は、キーにアクセスできないためタスクは失敗します。CloudWatch アラームなどを設定し、既に暗号化されたデータを復号するために無効化されたキーが再び必要になることがないことを確認する必要があります。

AWS KMS キーの削除

キーの削除は最終的な手段であり、削除されたキーが再び必要になることがないと確信している場合にのみ実行する必要があります。削除されたキーを使用しようとする新しいタスクは、そのキーにアクセスできないため失敗します。AWS KMS では、キーを削除するのではなく、キーを無効にすることをお勧めしています。キーを削除する必要があると思われる場合は、最初にキーを無効にした後、CloudWatch アラームを設定して、不要であることを確認することをお勧めします。キーを削除する場合、AWS KMS では少なくとも 7 日間の猶予期間が付与されているため、その期間に削除を撤回することも可能です。

AWS KMS キーアクセスの監査

CloudTrail ログを使用して、AWS KMS キーへのアクセスを監査できます。AWS KMS オペレーション `CreateGrant`、`GenerateDataKeyWithoutPlaintext`、および `Decrypt` を確認できます。これらのオペレーションでは、`EncryptionContext` がログインした CloudTrail の一部として `aws:ecs:clusterAccount` および `aws:ecs:clusterName` も表示されます。

以下は、GenerateDataKeyWithoutPlaintext、GenerateDataKeyWithoutPlaintext (DryRun)、CreateGrant、CreateGrant (DryRun)、RetireGrant の CloudTrail イベントの例です (*##*の値は独自の値に置き換えてください)。

GenerateDataKeyWithoutPlaintext


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ec2-frontend-api.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:08:13Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyWithoutPlaintext",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "ec2-frontend-api.amazonaws.com",
    "userAgent": "ec2-frontend-api.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 64,
        "keyId": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "encryptionContext": {
            "aws:ecs:clusterAccount": "account-id",
            "aws:ebs:id": "vol-xxxxxxx",
            "aws:ecs:clusterName": "cluster-name"
        }
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account-id",
```

```
    "sharedEventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventCategory": "Management"
}
```

GenerateDataKeyWithoutPlaintext (DryRun)

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "fargate.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:08:11Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyWithoutPlaintext",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "fargate.amazonaws.com",
    "userAgent": "fargate.amazonaws.com",
    "errorCode": "DryRunOperationException",
    "errorMessage": "The request would have succeeded, but the DryRun option is
 set.",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "dryRun": true,
        "numberOfBytes": 64,
        "encryptionContext": {
            "aws:ecs:clusterAccount": "account-id",
            "aws:ecs:clusterName": "cluster-name"
        }
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": true,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account-id",
    "sharedEventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventCategory": "Management"
}
```

CreateGrant

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "ec2-frontend-api.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:08:13Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "ec2-frontend-api.amazonaws.com",
    "userAgent": "ec2-frontend-api.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "granteePrincipal": "fargate.us-west-2.amazonaws.com",
        "operations": [
            "Decrypt"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:ecs:clusterAccount": "account-id",
                "aws:ebs:id": "vol-xxxx",
                "aws:ecs:clusterName": "cluster-name"
            }
        },
        "retiringPrincipal": "ec2.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
        "keyId": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
```

```
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account-id",
    "sharedEventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventCategory": "Management"
}
```

CreateGrant (DryRun)

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "fargate.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:08:11Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "fargate.amazonaws.com",
    "userAgent": "fargate.amazonaws.com",
    "errorCode": "DryRunOperationException",
    "errorMessage": "The request would have succeeded, but the DryRun option is
 set.",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "granteePrincipal": "fargate.us-west-2.amazonaws.com",
        "dryRun": true,
        "operations": [
            "Decrypt"
        ],
```

```
        "constraints": {
            "encryptionContextSubset": {
                "aws:ecs:clusterAccount": "account-id",
                "aws:ecs:clusterName": "cluster-name"
            }
        }
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account-id",
    "sharedEventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventCategory": "Management"
}
```

RetireGrant

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-04-20T18:37:38Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": {
```

```
        "keyId": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "additionalEventData": {
        "grantId":
 "e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:account-id:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "account-id",
    "sharedEventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
    "eventCategory": "Management"
}
```

AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス

AWS は、AWS Fargate の基盤インフラストラクチャを維持する責任を負います。AWS は、プラットフォームバージョンのリビジョンを、インフラストラクチャ用の新しいリビジョンに置き換える必要があるタイミングを決定します。これはタスクの廃止と呼ばれます。プラットフォームバージョンのリビジョンが廃止されると、AWS からタスクの廃止通知が送信されます。サポート対象のプラットフォームバージョンを定期的に更新して、Fargate ランタイムソフトウェアと、オペレーティングシステムやコンテナランタイムなどの内在的な依存関係の更新を含む新しいリビジョンを導入しています。新しいリビジョンが利用可能になった後、すべてのお客様のワークロードが Fargate プラットフォームバージョンの最新リビジョンで実行されるように、古いリビジョンを廃止します。リビジョンが廃止されると、そのリビジョンで実行されていたすべてのタスクが停止します。

Amazon ECS タスクは、サービスタスクまたはスタンドアロンタスクのどちらかに分類されます。サービスタスクは、Amazon ECS サービスの一部としてデプロイされ、Amazon ECS スケジューラによって制御されます。詳細については、「Amazon ECS サービス」を参照してください。スタ

ンドアロンタスクとは、Amazon ECS RunTask API によって開始されるタスクであり、直接または、Amazon EventBridge によって開始されるスケジュールされたタスク、AWS Batch、AWS Step Functions などの外部スケジューラにより開始されます。Amazon ECS スケジューラはタスクを自動的に置き換えるため、サービスタスクのタスク廃止への対応のために措置を講じる必要はありません。

スタンドアロンタスクについては、タスク廃止への対応として追加の処理を実行する必要が生じる場合があります。詳細については、「Amazon ECS はスタンドアロンタスクを自動的に処理できますか?」を参照してください。

サービスタスクについては、AWS よりも前にこれらのタスクを置き換える場合を除き、タスク廃止に対する措置を講じる必要はありません。Amazon ECS スケジューラーはタスクを停止すると、`maximumPercent` を使用して新しいタスクを起動し、サービスに必要な数を維持しようとします。AWS Fargate のタスク廃止による影響を最小限に抑えるには、ワークロードをデプロイするときに Amazon ECS のベストプラクティスに従う必要があります。REPLICA サービススケジューラを使用するサービスのデフォルトの `maximumPercent` 値は 200% です。そのため、AWS Fargate が廃止タスクを開始すると、Amazon ECS はまず新しいタスクをスケジュールし、それが実行されるのを待ってから、古いタスクを廃止します。`maximumPercent` 値を 100% に設定すると、Amazon ECS は最初にタスクを停止し、次にタスクを置き換えます。

スタンドアロンタスクの廃止では、AWS タスク廃止日およびそれ以降のタスクを停止します。タスクが停止したとき、Amazon ECS は代替のタスクを起動しません。これらのタスクを継続して実行する必要がある場合は、通知で示された時間より前に、実行中のタスクを停止し、代替タスクを起動する必要があります。そのためユーザーには、スタンドアロンタスクの状態をモニタリングすることと、必要に応じて停止したタスクを置き換えるロジックの実装が推奨されます。

タスクが停止したシナリオに関係なく、`describe-tasks` を実行することができます。レスポンス内の `stoppedReason` は `ECS is performing maintenance on the underlying infrastructure hosting the task` です。

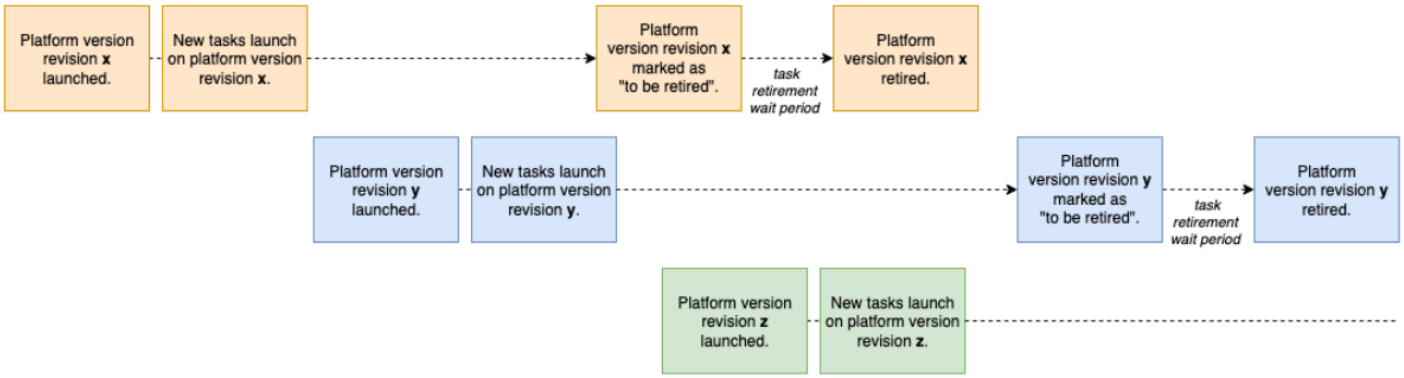
タスクのメンテナンスは、新しいプラットフォームバージョンのリビジョンを新しいリビジョンで置き換える必要があるときに適用されます。内在する Fargate ホストに問題がある場合、Amazon ECS はタスク終了通知を行わず、ホストを交換します。

タスク廃止通知の概要

AWS がプラットフォームバージョンリビジョンを要廃止としてマークすると、そのプラットフォームバージョンリビジョンで実行されているすべてのタスクがすべてのリージョンで特定されます。次

に、リージョンごとにアカウントあたり 1 件の通知が送信されます。これには、影響を受けるタスクやサービスと、廃止が開始される日付が記載されています。

以下の図は、新しいリビジョンの起動からプラットフォームリビジョンの廃止までの、Fargate プラットフォームバージョンリビジョンのライフサイクルを示しています。



以下は、ライフサイクルの詳細情報です。

- 新しいプラットフォームバージョンリビジョンが起動されたら、新しいタスクのすべてがこのリビジョンでスケジュールされます。
- 実行されているスケジュール済みの既存のタスクは、タスクの期間が終わるまで元々設定されていたリビジョンに残り、新しいリビジョンには移行されません。
- 新しいタスク (サービスの更新や Fargate のタスク廃止の一環として行われるタスクなど) は、起動時に利用可能な最新のプラットフォームバージョンリビジョンに設定されます。

タスク廃止通知は、AWS Health ダッシュボード、および登録された E メールアドレスへの E メールを通じて送信され、以下の情報が含まれています。

- タスクの廃止日 - タスクは、この日またはそれ以降に停止されます。
- タスクの ID (スタンドアロンタスクの場合)。
- サービスが実行されるクラスターの ID とサービスの ID (サービスタスクの場合)。
- 次に実行する必要があるステップ。

通常、AWS リージョン のサービスタスクとスタンドアロンのタスクについて、それぞれ 1 件の通知が送信されます。ただし、場合によっては、タスクタイプごとに複数のイベントを受け取ることがあります。たとえば、廃止するタスクが多すぎて通知メカニズムの制限を超える場合などです。

廃止がスケジュールされているタスクは次の方法で識別できます。

- AWS Health Dashboard

AWS Health 通知は Amazon EventBridge 経由で Amazon Simple Storage Service などのアーカイブストレージに送信すること、AWS Lambda 関数の実行などの自動化されたアクションを取ること、または Amazon Simple Notification Service などのその他の通知システムに送信することができます。詳細については「Amazon EventBridge による AWS Health イベントのモニタリング」を参照してください。Amazon Chime、Slack、または Microsoft Teams に通知を送信するための設定例については、GitHub の「AWS Health Aware」リポジトリを参照してください。

EventBridge イベントの例を次に示します。

```
{
    "version": "0",
    "id": "3c268027-f43c-0171-7425-1d799EXAMPLE",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-08-16T23:18:51Z",
    "region": "us-east-1",
    "resources": [
        "cluster|service",
        "cluster|service"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/ECS/
AWS_ECS_TASK_PATCHING_RETIREMENT/AWS_ECS_TASK_PATCHING_RETIREMENT_test1",
        "service": "ECS",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId":
 "7988399e2e6fb0b905ddc88e0e2de1fd17e4c9fa60349577446d95a18EXAMPLE",
        "lastUpdatedTime": "Wed, 16 Aug 2023 23:18:52 GMT",
        "eventRegion": "us-east-1",
        "eventTypeCode": "AWS_ECS_TASK_PATCHING_RETIREMENT",
        "eventTypeCategory": "scheduledChange",
        "startTime": "Wed, 16 Aug 2023 23:18:51 GMT",
        "endTime": "Fri, 18 Aug 2023 23:18:51 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "\\nA software update has been deployed to
 Fargate which includes CVE patches or other critical patches. No action is required
 on your part. All new tasks launched automatically uses the latest software
```

```
 version. For existing tasks, your tasks need to be restarted in order for these
 updates to apply. Your tasks running as part of the following ECS Services will
 be automatically updated beginning Wed, 16 Aug 2023 23:18:51 GMT.\\n\\nAfter Wed,
 16 Aug 2023 23:18:51 GMT, the ECS scheduler will gradually replace these tasks,
 respecting the deployment settings for your service. Typically, services should
 see little to no interruption during the update and no action is required. When AWS
 stops tasks, AWS uses the minimum healthy percent (1) and launches a new task in
 an attempt to maintain the desired count for the service. By default, the minimum
 healthy percent of a service is 100 percent, so a new task is started first before
 a task is stopped. Service tasks are routinely replaced in the same way when
 you scale the service or deploy configuration changes or deploy task definition
 revisions. If you would like to control the timing of this restart you can update
 the service before Wed, 16 Aug 2023 23:18:51 GMT, by running the update-service
 command from the ECS command-line interface specifying force-new-deployment for
 services using Rolling update deployment type. For example:\\n\\n$ aws ecs update-
service -service service_name \\\n--cluster cluster_name -force-new-deployment\
\n\\nFor services using Blue/Green deployment type with AWS CodeDeploy:\\nPlease
 refer to create-deployment document (2) and create new deployment using same task
 definition revision.\\n\\nFor further details on ECS deployment types, please
 refer to ECS Deployment Developer Guide (1).\\nFor further details on Fargate's
 update process, please refer to the AWS Fargate User Guide (3).\\nIf you have
 any questions or concerns, please contact AWS Support (4).\\n\\n(1) https://
docs.aws.amazon.com/AmazonECS/latest/developerguide/deployment-types.html\\n(2)
 https://docs.aws.amazon.com/cli/latest/reference/deploy/create-deployment.html\\n(3)
 https://docs.aws.amazon.com/AmazonECS/latest/userguide/task-maintenance.html\\n(4)
 https://aws.amazon.com/support\\n\\nA list of your affected resources(s) can be
 found in the 'Affected resources' tab in the 'Cluster/ Service' format in the AWS
 Health Dashboard. \\n\\n"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cluster|service"
            },
            {
                "entityValue": "cluster|service"
            }
        ]
    }
}
```

- E メール

  AWS アカウント ID に対して登録された E メールアドレスに E メールが送信されます。

タスク廃止の準備を行う方法については、「Amazon ECS での AWS Fargate タスク廃止に備える」を参照してください。

タスク廃止をオプトアウトすることはできますか?

いいえ。AWS の責任共有モデルの一環として、AWS は AWS Fargate の基盤となるインフラストラクチャの管理と維持に対する責任を担います。これには、セキュリティと安定性を確保するための定期的なプラットフォーム更新の実施が含まれます。これらの更新は AWS が自動的に適用するため、お客様がオプトアウトすることはできません。これは、EC2 インスタンスでワークロードを実行する代わりに AWS Fargate を使用するときの主なメリットであり、基盤となるプラットフォームを維持する責任は AWS が担います。このモデルは、インフラストラクチャのメンテナンスではなく、アプリケーションに集中することを可能にします。AWS は、これらのプラットフォーム更新を自動的に適用することによって、お客様からのアクションを必要とすることなく、Fargate 環境を最新かつセキュアに保つことができます。これは、Fargate でワークロードを実行するための、セキュアで信頼性が高いコンテナ化された環境の提供に役立ちます。

他の AWS サービスを通じてタスク終了通知を受け取ることはできますか?

AWS は、タスク終了通知を、AWS Health Dashboard および AWS アカウント の主要メール連絡先に送信します。AWS Health Dashboard は、EventBridge を含む他の AWS サービスとのさまざまな統合を提供します。EventBridge を使用して、通知の可視性を自動化できます (たとえば、メッセージを ChatOps ツールに転送するなど) 。詳細については、「ソリューションの概要: タスク廃止通知の取得」を参照してください。

タスクの廃止はスケジュールされた後に変更できますか?

いいえ。スケジュールはタスクの廃止待ち時間に基づいており、デフォルトでは 7 日間です。さらに時間が必要な場合は、待機期間を 14 日間に設定することもできます。詳細については、「ステップ 2: タスク廃止通知をキャプチャしてチームに警告し、措置を講じる」を参照してください。この構成の変更は、今後予定されている廃止に適用されます。現在予定されている廃止には影響しません。ご不明な点がある場合は、サポート までお問い合わせください。

Amazon ECS はサービスの一部であるタスクをどのように処理しますか?

サービスタスクについては、AWS よりも前にこれらのタスクを置き換える場合を除き、タスク廃止に対応するための措置を講じる必要はありません。Amazon ECS スケジューラは、タスクを停止する際、最小正常稼働率を使用して新しいタスクを起動し、サービスに必要とされる数を維持しようとします。Fargate のタスク廃止による影響を最小限に抑えるには、Amazon ECS のベストプラク

ティスに従ってワークロードをデプロイする必要があります。例えば、ウェブまたは API サーバーなど、Amazon ECS サービスとしてステートレスアプリケーションをデプロイする場合、お客様は複数のタスクレプリカをデプロイして、minimumHealthyPercent を 100% に設定する必要があります。サービスの最小ヘルス率はデフォルトで 100% です。そのため、Fargate が廃止タスクを開始すると、Amazon ECS はまず新しいタスクをスケジュールし、それが実行されるのを待ってから、古いタスクを廃止します。サービスタスクは、サービスをスケールする、設定変更をデプロイする、またはタスク定義リビジョンをデプロイするときと同じ方法で、タスク廃止の一環として定期的に置き換えられます。タスク廃止プロセスへの準備を行うには、「Amazon ECS での AWS Fargate タスク廃止に備える」を参照してください。

Amazon ECS はスタンドアロンタスクを自動的に処理できますか?

いいえ。AWS は、RunTask が開始したスタンドアロンタスク、スケジュールされたタスク (EventBridge Scheduler の使用など)、AWS Batch、AWS Step Functions に対する交換タスクを作成できません。Amazon ECS はサービスの一部であるタスクのみを管理します。

Amazon ECS での AWS Fargate タスク廃止に備える

タスク廃止への準備を行うには、以下の手順を実行します。

1. タスク廃止の待機期間を設定します。
2. タスク廃止通知をキャプチャして、チームメンバーに通知します。
3. タスク廃止の正確なタイミングを制御することはできませんが、force-deployment オプションを使用してサービスを更新することで、タスクの置き換えを制御することができます。

ステップ 1: タスクの待機時間を設定する

Fargate がタスク廃止を開始する時間を設定できます。アップデートをすぐに適用する必要があるワークロードの場合は、即時設定 (0) を選択します。特定の時間帯にしかタスクを停止できない場合など、詳細な制御が必要な場合は、7 日 (7) または 14 日 (14) のオプションを設定します。

新しいプラットフォームバージョンのリビジョンを早く取得できるように、待機時間を短くすることをお勧めします。

待機時間を設定するには、ルートユーザーまたは管理者ユーザーで put-account-setting-default または put-account-setting を実行します。fargateTaskRetirementWaitPeriod オプションを name に使用し、value オプションを次のいずれかの値に設定します。

- 0 - AWS から通知が送信され、影響を受けたタスクが直ちに廃止されます。
- 7 - AWS から通知が送信され、7 日間待機してから、影響を受けたタスクの廃止が開始されます。
- 14 - AWS から通知が送信され、14 日間待機してから、影響を受けたタスクの廃止が開始されます。

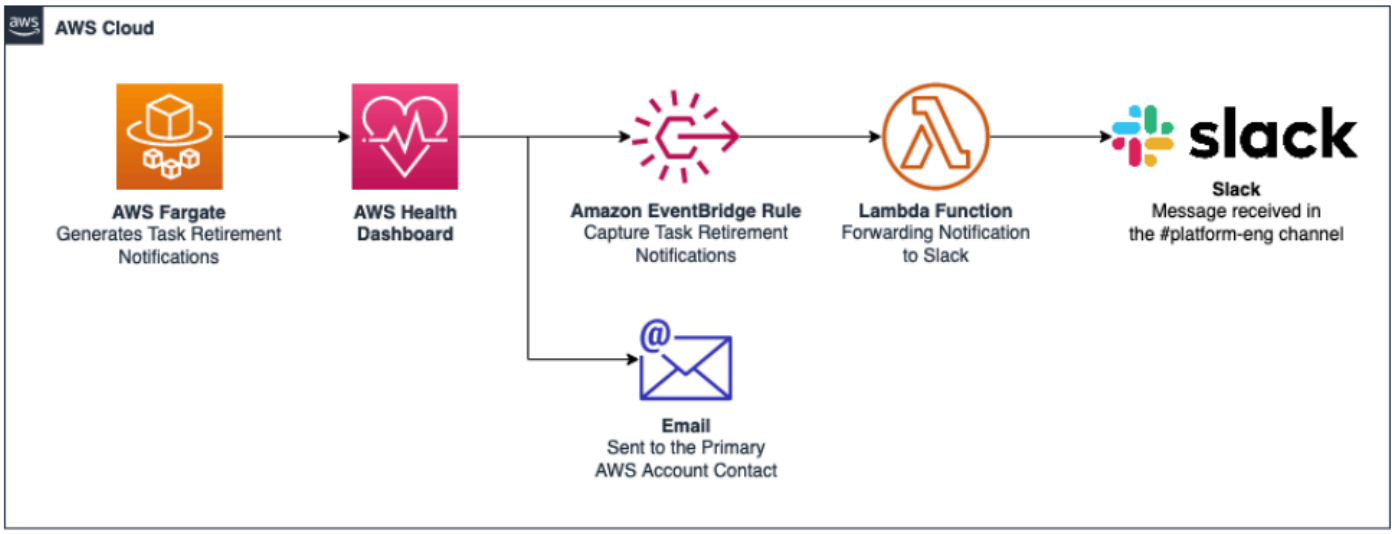
デフォルトは 7 日間です。

詳細については、「Amazon Elastic Container Service API リファレンス」の「put-account-setting-default」と「put-account-setting」を参照してください。

ステップ 2: タスク廃止通知をキャプチャしてチームに警告し、措置を講じる

近日実施されるタスク廃止があるときは、AWS が AWS Health ダッシュボード、および AWS アカウント の主要 E メール連絡先にタスク廃止通知を送信します。AWS Health ダッシュボードは、Amazon EventBridge を含めた他の AWS サービスとの統合を多数提供しています。EventBridge を使用して、ChatOps ツールにメッセージを転送して次回の廃止の視認性を高めるなど、タスク廃止通知からオートメーションを構築することができます。AWS HealthAware は、AWS Health ダッシュボードの能力と、組織全体に通知を配布する方法を説明するリソースです。タスク廃止通知は、Slack などのチャットアプリケーションに転送できます。

以下の図は、このソリューションの概要です。



以下は、ソリューションの詳細情報です。

- Fargate がタスク廃止通知を AWS Health ダッシュボードに送信します。

- AWS Health ダッシュボードが AWS アカウント の主要 E メール連絡先に E メールを送信し、EventBridge に通知します。
- EventBridge には、廃止通知をキャプチャするルールがあります。

  このルールは、イベント詳細タイプが `"AWS Health Event" and the Event Detail Type Code: "AWS_ECS_TASK_PATCHING_RETIREMENT"` のイベントを探します。
- ルールが、Slack Incoming Webhook を使用して情報を Slack に転送する Lambda 関数をトリガーします。詳細については、「Incoming Webhooks」を参照してください。

コード例については、Github で「Capturing AWS Fargate Task Retirement Notifications」を参照してください。

ステップ 3: タスクの置き換えを制御する

タスク廃止の正確なタイミングを制御することはできませんが、待機時間を定義することは可能です。独自のスケジュールに従ってタスクの置き換えを制御する場合は、タスク廃止通知をキャプチャして、タスク廃止の日付を把握することから始めます。その後、サービスを再度デプロイして代替タスクを起動することができます。スタンドアロンタスクも同様に置き換えます。ローリングデプロイを使用するサービスの場合は、廃止の開始時刻の前に、`force-deployment` オプションがある `update-service` を使用してサービスを更新します。

次の `update-service` 例では、`force-deployment` オプションを使用しています。

```
aws ecs update-service —-service service_name \
    --cluster cluster_name \
     --force-new-deployment
```

ブルー/グリーンデプロイを使用するサービスの場合は、AWS CodeDeploy で新しいデプロイメントを作成する必要があります。デプロイを作成する方法については、AWS Command Line Interface リファレンスの「create-deployment」を参照してください。

AWS Fargate で使用する Amazon ECS でサポートされているリージョン

次の表を参照すると、AWS Fargate 上の Linux コンテナおよび AWS Fargate 上の Windows コンテナのリージョンサポートを確認できます。

AWS Fargate 上の Linux コンテナ

AWS Fargate の Amazon ECS Linux コンテナは次の AWS リージョン でサポートされています。該当する場合、サポートされているアベイラビリティーゾーン ID が記載されています。

リージョン名	リージョン
米国東部 (オハイオ)	us-east-2
米国東部 (バージニア北部)	us-east-1
米国西部 (北カリフォルニア)	us-west-1 (usw1-az1 &usw1-az3のみ)
米国西部 (オレゴン)	us-west-2
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (東京)	ap-northeast-1 (apne1-az1 、apne1-az2 、&apne1-az4 のみ)
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (ジャカルタ)	ap-southeast-3
アジアパシフィック (メルボルン)	ap-southeast-4
アジアパシフィック (マレーシア)	ap-southeast-5
カナダ (中部)	ca-central-1

リージョン名	リージョン
カナダ西部 (カルガリー)	ca-west-1
中国 (北京)	cn-north-1 (cnn1-az1 &cnn1-az2のみ)
中国 (寧夏)	cn-northwest-1
欧州 (フランクフルト)	eu-central-1
欧州 (チューリッヒ)	eu-central-2
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
欧州 (パリ)	eu-west-3
欧州 (ミラノ)	eu-south-1
欧州 (スペイン)	eu-south-2
欧州 (ストックホルム)	eu-north-1
南米 (サンパウロ)	sa-east-1
イスラエル (テルアビブ)	il-central-1
中東 (バーレーン)	me-south-1
中東 (UAE)	me-central-1
AWS GovCloud (米国東部)	us-gov-east-1
AWS GovCloud (米国西部)	us-gov-west-1

AWS Fargate 上の Windows コンテナ

AWS Fargate の Amazon ECS Windows コンテナは次の AWS リージョン でサポートされています。該当する場合、サポートされているアベイラビリティーゾーン ID が記載されています。

リージョン名	リージョン
米国東部 (オハイオ)	us-east-2
米国東部 (バージニア北部)	us-east-1 (use1-az1、use1-az2、use1-az4、use1-az5、& use1-az6 のみ)
米国西部 (北カリフォルニア)	us-west-1 (usw1-az1 &usw1-az3のみ)
米国西部 (オレゴン)	us-west-2
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (メルボルン)	ap-southeast-4
アジアパシフィック (マレーシア)	ap-southeast-5
アジアパシフィック (東京)	ap-northeast-1 (apne1-az1 、apne1-az2 、&apne1-az4 のみ)
カナダ (中部)	ca-central-1 (cac1-az1 &cac1-az2のみ)
カナダ西部 (カルガリー)	ca-west-1
中国 (北京)	cn-north-1 (cnn1-az1 &cnn1-az2のみ)
中国 (寧夏)	cn-northwest-1

リージョン名	リージョン
欧州 (フランクフルト)	eu-central-1
欧州 (チューリッヒ)	eu-central-2
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
欧州 (パリ)	eu-west-3
欧州 (ミラノ)	eu-south-1
欧州 (スペイン)	eu-south-2
欧州 (ストックホルム)	eu-north-1
南米 (サンパウロ)	sa-east-1
イスラエル (テルアビブ)	il-central-1
中東 (UAE)	me-central-1
中東 (バーレーン)	me-south-1

Amazon ECS のソリューションの構築

Amazon ECS を使用する前に、Amazon ECS リソースを正しく設定できるように、容量、ネットワーク、アカウント設定、ロギングについて決定する必要があります。

容量

容量は、コンテナが実行されるインフラストラクチャです。以下のオプションが利用できます。

- Amazon EC2 インスタンス
- サーバーレス (AWS Fargate)
- オンプレミス仮想マシン (VM) またはサーバー

クラスターを作成する際、インフラストラクチャを指定します。タスク定義を登録する際、インフラストラクチャタイプも指定します。タスク定義では、インフラストラクチャを「起動タイプ」と呼びます。スタンドアロンタスクを実行する、またはサービスをデプロイする際にも起動タイプを使用します。起動タイプのオプションについては、Amazon ECS 起動タイプ を参照してください。

ネットワーク

AWS リソースはサブネットに作成されます。EC2 インスタンスを使用する場合、Amazon ECS はクラスターの作成時に指定したサブネットでインスタンスを起動します。タスクはインスタンスのサブネットで実行されます。Fargate またはオンプレミス仮想マシンの場合は、タスクを実行するとき、またはサービスを作成するときにサブネットを指定します。

アプリケーションに応じて、サブネットはプライベートサブネットでもパブリックサブネットでもよく、サブネットは次の AWS リソースのどれにあってもかまいません。

- アベイラビリティーゾーン
- ローカルゾーン
- Wavelength Zone
- AWS リージョン
- AWS Outposts

詳細については、「共有サブネット、Local Zones、および Wavelength Zones の Amazon ECS アプリケーション」または「AWS OutpostsのAmazon Elastic Container Service」を参照してください。

次のいずれかの方法を使用して、アプリケーションをインターネットに接続できます。

- インターネットゲートウェイを持つパブリックサブネット

  大量の帯域幅や最小のレイテンシーを必要とするパブリックアプリケーションがある場合は、パブリックサブネットを使用してください。該当するシナリオには、ビデオストリーミングやゲームサービスが含まれます。

- NAT ゲートウェイを持つプライベートサブネット

  外部からの直接アクセスからコンテナを保護するには、プライベートサブネットを使用してください。該当するシナリオには、支払い処理システムや、ユーザーデータとパスワードを格納するコンテナなどがあります。

- AWS PrivateLink

  トラフィックをパブリックインターネットに公開することのない、VPC、AWS サービス、オンプレミスネットワークの間のプライベート接続を提供するには、AWS PrivateLink を使用してください。

機能アクセス

Amazon ECS アカウント設定を使用して、次の機能にアクセスできます。

- Container Insights

  CloudWatch Container Insights は、コンテナ化されたアプリケーションとマイクロサービスのメトリクスとログを収集、集約、要約します。このメトリクスには、CPU、メモリ、ディスク、ネットワークなどのリソース使用率が含まれます。

- `awsvpc` トランキング

  特定の EC2 インスタンスタイプでは、新しく起動したコンテナインスタンスで追加のネットワークインターフェイス (ENI) を使用できます。

- タグ付け認可

  ユーザーには、リソースを作成するアクションの許可が必要です (`ecsCreateCluster` など)。リソース作成アクションでタグが指定されている場合、AWS は `ecs:TagResource` アクションに

対して追加の認可を実行して、ユーザーまたはロールがタグを作成するための許可を持っているかどうかを確認します。

- Fargate FIPS-140 コンプライアンス

  Fargate は、機密情報を保護する暗号モジュールのセキュリティ要件を指定する連邦情報処理標準 (FIPS-140) をサポートしています。これは現在の米国およびカナダの政府標準であり、Federal Information Security Management Act (FISMA) または Federal Risk and Authorization Management Program (FedRAMP) への準拠が要求されるシステムに適用されます。
- Fargate タスクの廃止時間の変更

  Fargate タスクが廃止されるまでの待機時間を設定できます。
- デュアルスタック VPC

  タスクが IPv4、IPv6、またはその両方を介して通信できるようにします。
- Amazon リソースネーム (ARN) 形式

  タグ付け認可などの特定の機能には、新しい Amazon リソースネーム (ARN) 形式が必要です。

詳細については、「アカウント設定による Amazon ECS 機能へのアクセス」を参照してください。

IAM ロール

IAM ロールは、特定の許可があり、 アカウントで作成できる IAM アイデンティティです。Amazon ECS では、コンテナやサービスなどの Amazon ECS リソースにアクセス許可を付与するロールを作成できます。

Amazon ECS の一部の機能にはロールが必要です。詳細については、「Amazon ECS の IAM ロール」を参照してください。

ロギング

ログ記録およびモニタリングは、Amazon ECS ワークロードの信頼性、可用性、パフォーマンスを維持する上で重要な要素です。以下のオプションが利用できます。

- Amazon CloudWatch ログ- ログを Amazon CloudWatch にルーティングする
- Amazon ECS 用 FireLens - ログを AWS サービスまたは AWS Partner Network の宛先にルーティングして、ログの保存と分析を行います。AWS Partner Network は、プログラム、専門知識、リ

ソースを活用して顧客向けサービスの構築、マーケティング、販売を行うパートナーのグローバルコミュニティです。

Amazon ECS 起動タイプ

タスク定義の起動タイプは、タスクを実行できる容量を定義します。例: AWS Fargate

起動タイプを選択すると、Amazon ECS は、設定したタスク定義パラメータが起動タイプで機能することを確認します。

次の表は、利用可能なタイプを説明しています。

起動タイプ		詳細はこちら
Fargate	Fargate はサーバーレスの従量制料金計算エンジンであり、サーバーを管理することなく、アプリケーションの構築に集中できます。	Amazon ECS の Fargate 起動タイプ
EC2	インスタンスタイプ、インスタンス数を選択し、キャパシティを管理します。	Amazon ECS の EC2 起動タイプ
オンプレミス仮想マシン (VM) またはサーバー	Amazon ECS Anywhere は、オンプレミスサーバーや仮想マシン (VM) などの外部インスタンスをクラスターに登録するためのサポートを提供します。	Amazon ECS の外部 (Amazon ECS Anywhere) 起動タイプ

Amazon ECS の Fargate 起動タイプ

Fargate はサーバーレスの従量制料金計算エンジンであり、サーバーを管理することなく、アプリケーションの構築に集中できます。Fargate を選択する場合、EC2 インフラストラクチャを管理する必要はありません。必要なのは、コンテナイメージを構築し、アプリケーションを実行するクラス

ターを定義することだけです。Fargate は、次のような AWS サービスとネイティブに統合されています。

- Amazon VPC
- Auto Scaling
- エラスティックロードバランシング
- IAM
- Secrets Manager

アプリケーションが必要とする正確な CPU とメモリを選択できるため、ユーザーは EC2 よりも Fargate でより多くの制御を行えます。Fargate が容量のスケールアウトを処理するため、トラフィックの急増を心配する必要はありません。つまり、Fargate では運用上の労力が少なくて済みます。

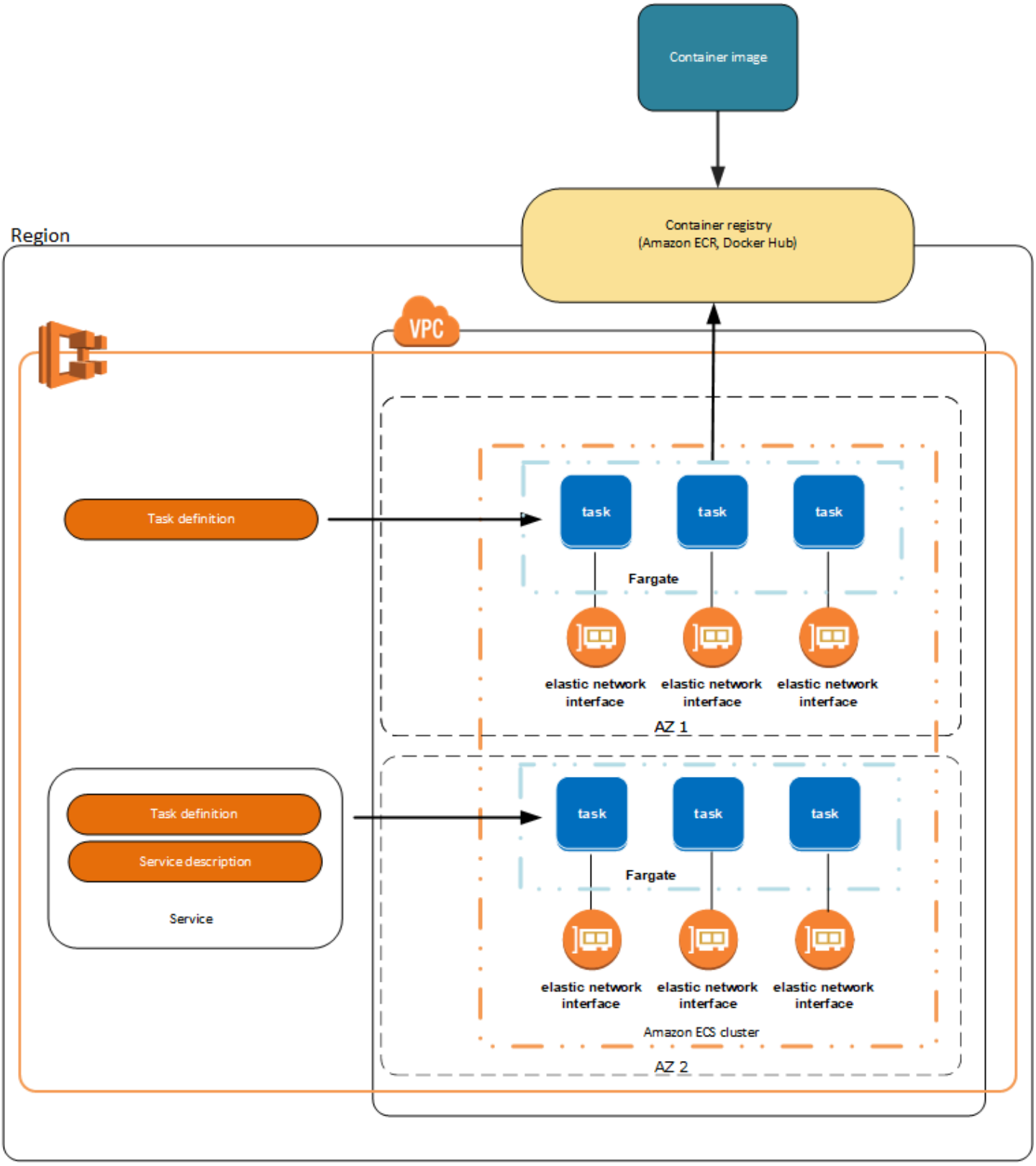
Fargate は、PCI、FIPS 140-2、FedRAMP、HIPAA などのコンプライアンスプログラムの基準を満たしています。詳細については、「コンプライアンスプログラムによる対象 AWS サービス」を参照してください。

Fargate は、次のワークロードに適しています:

- 運用上で低いオーバーヘッドを必要とする大規模なワークロード
- 時折バーストが発生する小さなワークロード
- 小さなワークロード
- バッチワークロード

Fargate をサポートするリージョンの情報については、「the section called “AWS Fargate リージョン”」 を参照してください。

次の図に、一般的なアーキテクチャを示します。



Fargate の Amazon ECS の詳細については、「Amazon ECS の AWS Fargate」を参照してください。

Fargate 上の Linux コンテナにおける Amazon ECS のコンテナイメージのプル動作

すべての Fargate タスクは、専用のシングルユース、シングルテナントのインスタンスで実行されます。Fargate 上で Linux コンテナを実行すると、コンテナイメージまたはコンテナイメージレイヤーはインスタンスにキャッシュされません。したがって、タスクで定義されたコンテナイメージごとに、コンテナイメージ全体を各 Fargate タスクのコンテナイメージレジストリからプルする必要があります。イメージをプルするのにかかる時間は、Fargate タスクを開始するのにかかる時間と直接相関しています。

イメージのプル時間を最適化するために、次の点を考慮してください。

コンテナイメージの近接性

コンテナイメージのダウンロードにかかる時間を短縮するには、データをコンピューティングにできるだけ近い場所に配置します。コンテナイメージをインターネット経由または AWS リージョン 間でプルすると、ダウンロード時間に影響する可能性があります。コンテナイメージは、タスクを実行するのと同じリージョンに保存することをお勧めします。コンテナイメージを Amazon ECR に保存する場合は、VPC インターフェイスエンドポイントを使用することでイメージのプル時間をさらに短縮できます。詳細については、「Amazon ECR ユーザーガイド」の「Amazon ECR 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。

コンテナイメージのサイズ削減

コンテナイメージのサイズは、ダウンロード時間に直接影響します。コンテナイメージのサイズまたはコンテナイメージレイヤーの数を減らすことで、イメージのダウンロードにかかる時間を短縮できます。軽量なベースイメージ (最小の Amazon Linux 2023 コンテナイメージなど) は、従来のオペレーティングシステムのベースイメージに基づくイメージよりも大幅に小さくすることができます。最小イメージの詳細については、「Amazon Linux 2023 ユーザーガイド」の「AL2023 の最小コンテナイメージ」を参照してください。

代替の圧縮アルゴリズム

多くの場合、コンテナイメージレイヤーは、コンテナイメージレジストリにプッシュされるときに圧縮されます。コンテナイメージレイヤーを圧縮することで、ネットワーク経由で転送され、コンテナイメージレジストリに保存されるデータの量を削減できます。コンテナランタイムによってコンテナイメージレイヤーがインスタンスにダウンロードされた後、そのレイヤーは解凍されます。使用される圧縮アルゴリズムとランタイムに使用できる vCPU の量は、コンテナイメージの解凍にかかる時間に影響します。Fargate では、タスクのサイズを増やすか、よりパフォーマンスの高い zstd 圧縮アルゴリズムを利用することで、解凍にかかる時間を短縮できます。詳細については、GitHub の「zstd」を参照してください。Fargate のイメージを実装

する方法については、「Reducing AWS Fargate Startup Times with zstd Compressed Container Images」を参照してください。

コンテナイメージの遅延読み込み

大きなコンテナイメージ (> 250 mb) の場合、すべてのコンテナイメージをダウンロードするのではなく、コンテナイメージを遅延読み込みするのが最適である場合があります。Fargate では、Seekable OCI (SOCI) を使用して、コンテナイメージレジストリからコンテナイメージを遅延読み込みできます。詳細については、GitHub の「soci-snapshotter」と「Seekable OCI (SOCI) を使ったコンテナイメージの遅延読み込み」を参照してください。

Fargate 上の Windows コンテナにおける Amazon ECS のコンテナイメージのプル動作

Fargate Windows は、Microsoft から提供された直近の月と前月のサーバーコアのベースイメージをキャッシュします。これらのイメージは、毎週火曜日のパッチで更新される KB /ビルド番号のパッチと一致します。例えば、Microsoft は 2024 年 4 月 9 日に Windows Server 2019 用の KB5036896 (17763.5696) をリリースしました。前月の KB (2024 年 3 月 12 日) は KB5035849 (17763.5576) でした。そのため、プラットフォーム `WINDOWS_SERVER_2019_CORE` および `WINDOWS_SERVER_2019_FULL` では、以下のコンテナイメージがキャッシュされました。

- `mcr.microsoft.com/windows/servercore:ltsc2019`
- `mcr.microsoft.com/windows/servercore:10.0.17763.5696`
- `mcr.microsoft.com/windows/servercore:10.0.17763.5576`

さらに、Microsoft は 2024 年 4 月 9 日に Windows Server 2022 用の KB5036909 (20348.2402) をリリースしました。前月の KB (2024 年 3 月 12 日) は KB5035857 (20348.2340) でした。そのため、プラットフォーム `WINDOWS_SERVER_2022_CORE` および `WINDOWS_SERVER_2022_FULL` では以下のコンテナイメージがキャッシュされました。

- `mcr.microsoft.com/windows/servercore:ltsc2022`
- `mcr.microsoft.com/windows/servercore:10.0.20348.2402`
- `mcr.microsoft.com/windows/servercore:10.0.20348.2340`

Amazon ECS の EC2 起動タイプ

EC2 起動タイプは、料金を最適化する必要がある大規模なワークロードに適しています。

EC2 起動タイプを使用してタスク定義とサービスをモデル化する方法を検討する際には、一緒に実行する必要があるプロセスはどれか、また、各コンポーネントをどのようにスケーリングするかについて検討することをお勧めします。

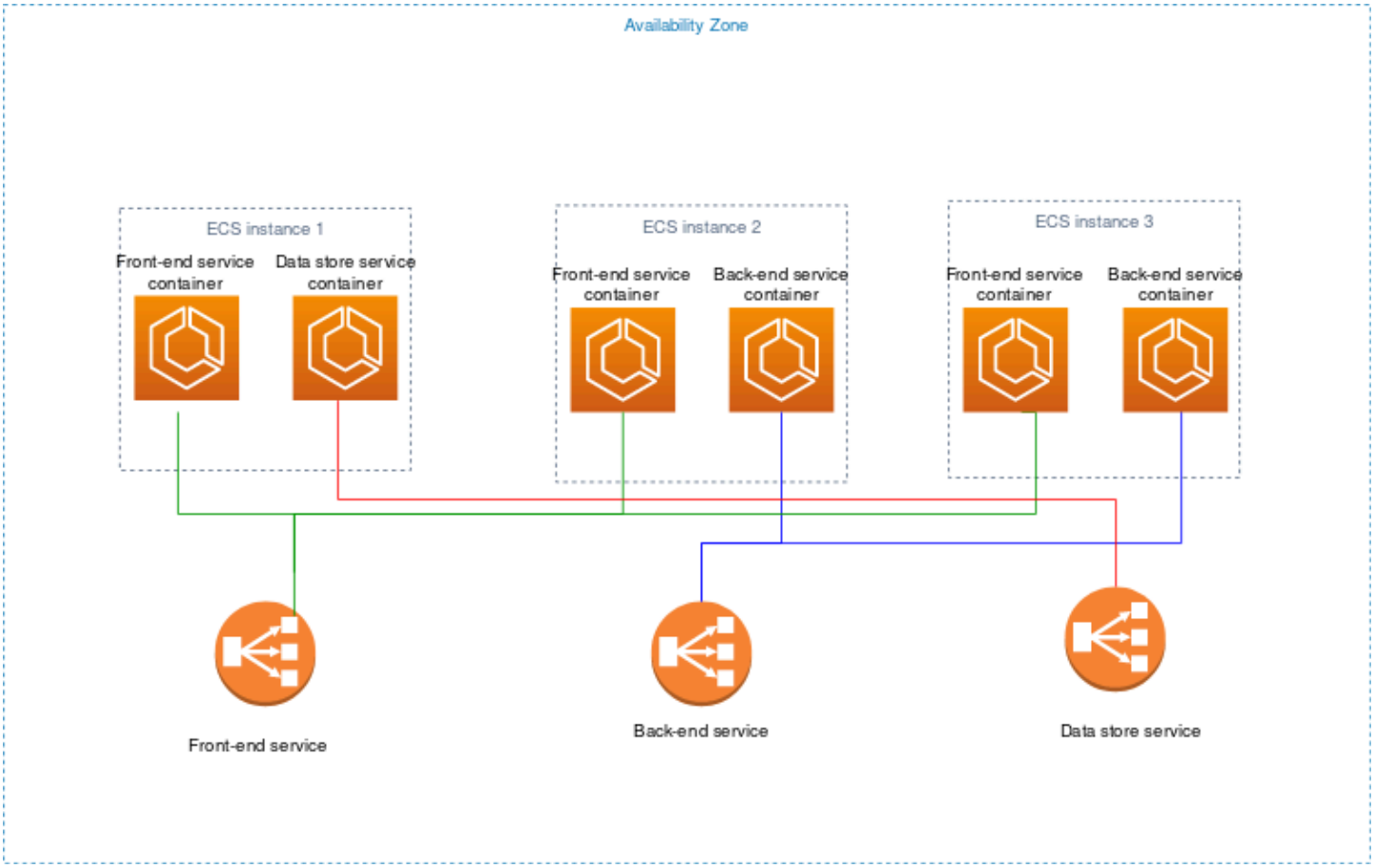
例えば、以下のコンポーネントで構成されるアプリケーションがあるとします。

- ウェブページに情報を表示するフロントエンドサービス
- フロントエンドサービスに API を提供するバックエンドサービス
- データストア

この例では、共通の目的で使用されるコンテナをまとめてグループ化するタスク定義を作成します。異なるコンポーネントは、複数の個別なタスク定義に分割します。以下の例のクラスターでは、3 つのコンテナインスタンスにより、3 つのフロントエンドサービスコンテナ、2 つのバックエンドサービスコンテナ、さらに 1 つのデータストアサービスコンテナを実行しています。

一緒に実行する必要のあるリンクされたコンテナなど、関連するコンテナをタスク定義にグループ化できます。例えば、フロントエンドサービスに追加するログストリーミングコンテナは、同じタスク定義に含めることができます。

タスク定義を作成したら、それらの定義からサービスを作成して、使用可能なタスクの必要数を維持できます。詳細については、「コンソールを使用した Amazon ECS サービスの作成」を参照してください。サービスでは、コンテナを Elastic Load Balancing ロードバランサーに関連付けることができます。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。アプリケーションの要件が変更された際には、サービスを更新してタスクの必要数を増減できます。あるいは、サービスを更新して、タスクに新しいバージョンのコンテナをデプロイすることも可能です。詳細については、「コンソールを使用した Amazon ECS サービスの更新」を参照してください。



EC2 起動タイプと Amazon ECS の外部起動タイプのコンテナイメージのプル動作

コンテナーの起動にかかる時間は、基礎となるコンテナイメージによって異なります。たとえば、太いイメージ (Debian、Ubuntu、Amazon 1/2 のフルバージョン) は、それぞれのスリムバージョン (Debian-Slim、Ubuntu-Slim、Amazon-Slim) や小さいベースイメージ (Alpine) と比較して、コンテナ内で実行されるサービスの数が多いため、起動に時間がかかる場合があります。

Amazon ECS エージェントはタスクを開始すると、リモートレジストリから Docker イメージを取得し、ローカルコピーをキャッシュします。アプリケーションのリリースごとに新しいイメージタグを使用する場合、この動作は不要です。

`ECS_IMAGE_PULL_BEHAVIOR` エージェントパラメータはイメージのプル動作を決定します。以下のオプションが利用できます。

- `ECS_IMAGE_PULL_BEHAVIOR: default`

  イメージはリモートでプルされます。プルが失敗した場合、インスタンスにキャッシュされたイメージが使用されます。

- ECS_IMAGE_PULL_BEHAVIOR: always

  イメージはリモートでプルされます。プルに失敗した場合、そのタスクは失敗します。

デプロイをスピードアップするには、Amazon ECS エージェントパラメータを次のいずれかの値に設定します。

- ECS_IMAGE_PULL_BEHAVIOR: once

  同じコンテナインスタンスの以前のタスクによりイメージがプルされていないか、自動クリーンアッププロセスによってキャッシュされたイメージが削除された場合にのみ、イメージがリモートでプルされます。それ以外の場合は、インスタンスにキャッシュされたイメージが使用されます。これにより、不要なイメージのプルがなくなります。

- ECS_IMAGE_PULL_BEHAVIOR: prefer-cached

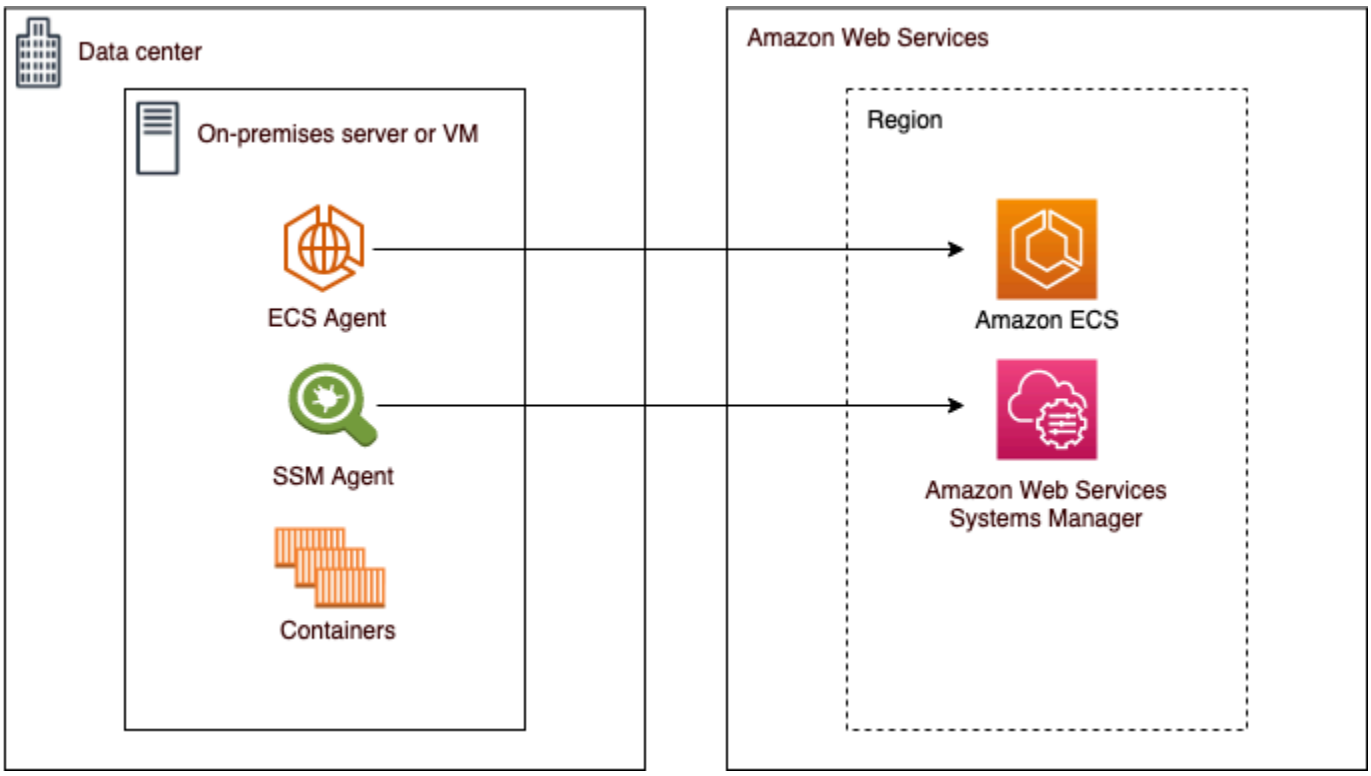
  キャッシュされたイメージがない場合に、リモートでイメージがプルされます。それ以外の場合は、インスタンスにキャッシュされたイメージが使用されます。キャッシュされたイメージが削除されないように、そのコンテナの自動イメージクリーンアップはオフになっています。

ECS_IMAGE_PULL_BEHAVIOR パラメータを前述の値のいずれかに設定すると、Amazon ECS エージェントはダウンロードされた既存のイメージを使用するため、時間を節約できます。Docker イメージのサイズが大きい場合、ダウンロード時間がネットワーク経由で取得されるまでに 10 ~ 20 秒かかることがあります。

Amazon ECS の外部 (Amazon ECS Anywhere) 起動タイプ

Amazon ECS Anywhere は、オンプレミスサーバーや仮想マシン (VM) などの外部インスタンスを Amazon ECS クラスターに登録するためのサポートを提供します。外部インスタンスは、アウトバウンドトラフィックを生成したり、データを処理したりするアプリケーションを実行するために最適化されています。アプリケーションがインバウンドトラフィックを必要とする場合、Elastic Load Balancing のサポートがないため、これらのワークロードの実行効率が低下します。Amazon ECS は、新しいEXTERNAL起動タイプで、サービスを作成したり、外部インスタンスでタスクを実行したりできます。

以下に、Amazon ECS Anywhere の高レベルのシステムアーキテクチャの概要を示します。オンプレミスサーバーには、Amazon ECS エージェントと SSM エージェントの両方がインストールされています。



詳細については、「外部起動タイプ用の Amazon ECS クラスター」を参照してください。

共有サブネット、Local Zones、および Wavelength Zones の Amazon ECS アプリケーション

Amazon ECS は、低レイテンシーまたはローカルデータ処理が必要な場合に、Local Zones、Wavelength Zone、および AWS Outposts を利用するワークロードをサポートします。

- Local Zones を AWS リージョン の拡張に使用して、エンドユーザーにより近い複数の場所にリソースを配置できます。
- Wavelength Zone を使用すると、5G デバイスやエンドユーザーに非常に低いレイテンシーを提供するアプリケーションを構築できます。Wavelength は標準の AWS コンピューティングおよびストレージサービスを通信事業者の 5G ネットワークのエッジにデプロイします。
- AWS Outposts では、ネイティブの AWS のサービス、インフラストラクチャ、運用モデルをほぼすべてのデータセンター、コロケーションスペース、オンプレミスの施設で利用できます。

> **Important**
>
> AWS Fargate ワークロードの Amazon ECS は、現時点では、Local Zones、Wavelength Zone、または AWS Outposts ではサポートされていません。

Local Zones、Wavelength Zone、および AWS Outposts の違いについては、「AWS Wavelength のよくある質問」の「低レイテンシーやローカルデータ処理を必要とするアプリケーションに、AWS Wavelength、AWS Local Zones、または AWS Outposts をいつ使用するとよいですか?」を参照してください。

共有サブネット

VPC 共有を使用して、同じ AWS Organizations 内でサブネットを他の AWS アカウントと共有できます。

EC2 の起動タイプには共有 VPC を使用できますが、次の点を考慮してください。

- VPC サブネットの所有者は、参加者アカウントで Amazon ECS リソース用にサブネットを使用する前に、そのサブネットをそのアカウントに共有する必要があります。
- VPC のデフォルトセキュリティグループは所有者に属しているため、コンテナインスタンスには VPC のデフォルトセキュリティグループを使用できません。また、参加者は、他の参加者または所有者が所有するセキュリティグループを使用してインスタンスを起動することはできません。
- 共有サブネットでは、参加者と所有者がそれぞれのアカウント内のセキュリティグループを個別に管理します。サブネットの所有者は、参加者が作成したセキュリティグループを表示できますが、これらのグループに対してアクションを実行することはできません。サブネットの所有者がこれらのセキュリティグループの削除または変更を希望する場合は、セキュリティグループを作成した参加者がそのアクションを実行する必要があります。
- 共有 VPC の所有者は、参加者が共有サブネット内に作成したクラスターを表示、更新、削除することはできません。これは、アカウントごとに異なるアクセス権を持つ VPC リソースに加えて適用されます。詳細については、「Amazon VPC ユーザーガイド」の「所有者および参加者の責任と権限」を参照してください。

Fargate の起動タイプには共有 VPC を使用できますが、次の点を考慮してください。

- VPC サブネットの所有者は、参加者アカウントで Amazon ECS リソース用にサブネットを使用する前に、そのサブネットをそのアカウントに共有する必要があります。

- VPC のデフォルトセキュリティグループは所有者に属しているため、デフォルトのセキュリティグループを使用してサービスを作成したりタスクを実行したりすることはできません。また、参加者は、他の参加者または所有者が所有するセキュリティグループを使用してサービスを作成したりタスクを実行したりすることはできません。
- 共有サブネットでは、参加者と所有者がそれぞれのアカウント内のセキュリティグループを個別に管理します。サブネットの所有者は、参加者が作成したセキュリティグループを表示できますが、これらのグループに対してアクションを実行することはできません。サブネットの所有者がこれらのセキュリティグループの削除または変更を希望する場合は、セキュリティグループを作成した参加者がそのアクションを実行する必要があります。
- 共有 VPC の所有者は、参加者が共有サブネット内に作成したクラスターを表示、更新、削除することはできません。これは、アカウントごとに異なるアクセス権を持つ VPC リソースに加えて適用されます。詳細については、「Amazon VPC ユーザーガイド」の「所有者および参加者の責任と権限」を参照してください。

VPC サブネット共有の詳細については、「Amazon VPC ユーザーガイド」の「VPC を他のアカウントと共有する」を参照してください。

ローカルゾーン

Local Zones は、ユーザーに近い場所に位置する AWS リージョンの拡張です。Local Zones は、インターネットへの独自の接続を持ち、AWS Direct Connect をサポートします。Local Zones で作成したリソースは、低いレイテンシーの通信をローカルユーザーに提供できます。詳細については、AWS Local Zonesを参照してください。

Local Zones を表すには、リージョンコードに続けて場所を示す識別子を使用します (例: `us-west-2-lax-1a`)。

Local Zones を使用するには、まずゾーンにオプトインする必要があります。オプトインしたら、Local Zones に Amazon VPC およびサブネットを作成する必要があります。

Amazon ECS クラスターとタスクに使用する Amazon EC2 インスタンス、Amazon FSx ファイルサーバー、Application Load Balancer を起動できます。

詳細についてはAWS ローカルゾーンユーザーガイドの「AWS ローカルゾーンとは」を参照してください。

Wavelength Zone

AWS Wavelength を使用することで、モバイルデバイスおよびエンドユーザー向けに、非常にレイテンシーが低いアプリケーションを構築できます。Wavelength は標準の AWS コンピューティングおよびストレージサービスを通信事業者の 5G ネットワークのエッジにデプロイします。Amazon Virtual Private Cloud は、1 つまたは複数の Wavelength Zone に拡張できます。その後、Amazon EC2 インスタンスなどの AWS リソースを使用して、極めて低いレイテンシーやリージョンの AWS のサービス への接続を必要とするアプリケーションを実行できます。

Wavelength Zone は、Wavelength インフラストラクチャをデプロイする先のキャリアロケーション内の独立したゾーンです。Wavelength Zone は、AWS リージョンに関連付けられています。Wavelength Zone はリージョンの論理的な拡張であり、リージョンの制御プレーンによって管理されます。

Wavelength Zone は、リージョンコードに続けて Wavelength Zone を示す識別子で表されます (例: `us-east-1-wl1-bos-wlz-1`)。

Wavelength Zone を使用するには、まずゾーンにオプトインする必要があります。オプトインしたら、Wavelength Zone に Amazon VPC およびサブネットを作成する必要があります。その後、Amazon ECS クラスターとタスクに使用する Amazon EC2 インスタンスを Zone で起動することができます。

詳細については、AWS Wavelengthデベロッパーガイドの「の使用開始AWS Wavelength」を参照してください。

Wavelength Zone は、すべての AWS リージョンで利用できるわけではありません。Wavelength Zone をサポートするリージョンについてはAWS Wavelength デベロッパーガイドの利用可能な Wavelength Zone をご参照ください。

AWS OutpostsのAmazon Elastic Container Service

AWS Outposts は、オンプレミス施設でネイティブ AWS サービス、インフラストラクチャ、運用モデルを有効にします。AWS Outposts 環境では、AWS で使用するのと同じ AWS クラウド API、ツール、インフラストラクチャを使用できます。

AWS Outposts の Amazon ECS は、オンプレミスのデータやアプリケーションの近くで実行が必要な、低レイテンシーのワークロードに最適です。

AWS Outposts の詳細については、AWS Outposts ユーザーガイドを参照してください。

考慮事項

AWS Outposts で Amazon ECS を使用する際の考慮事項は以下のとおりです。

- Amazon Elastic Container Registry、AWS Identity and Access Management、Network Load Balancer は、AWS Outposts ではなく AWS リージョンで実行されます。これにより、これらのサービスとコンテナ間のレイテンシーが増加します。
- AWS Fargate は AWS Outposts で使用できません。

以下に、AWS Outposts のネットワーク接続に関する考慮事項を示します。

- AWS Outposts とその AWS リージョン間のネットワーク接続が失われた場合、クラスターは引き続き実行されます。ただし、接続が復元されるまで、新しいクラスターを作成したり、既存のクラスターで新しいアクションを実行したりすることはできません。インスタンスに障害が発生した場合、インスタンスは自動的に置き換えられません。The CloudWatch Logs エージェントは、ログとイベントデータを更新できません。
- AWS OutpostsとAWS リージョン間で、信頼性が高く、可用性が高く、低レイテンシーの接続を提供することをお勧めします。

前提条件

AWS Outposts で Amazon ECS を使用するための前提条件は以下のとおりです。

- オンプレミスのデータセンターに Outpost をインストールして設定しておく必要があります。
- Outpost とその AWS リージョンとの間に、信頼できるネットワーク接続が必要です。

AWS Outposts でのクラスター作成の概要

以下は、設定の概要です。

1. AWS Outposts に対する権限を持つロールとポリシーを作成します。
2. AWS Outposts の権限を持つ IAM インスタンスプロファイルを作成します。
3. VPC を作成、または AWS Outposts と同じリージョンにある既存の VPC を使用します。
4. サブネットを作成、または AWS Outposts に関連付けられている既存のサブネットを使用します。

これは、コンテナインスタンスが実行されるサブネットです。

5. クラスター内にあるコンテナインスタンスのセキュリティグループを作成します。
6. Amazon ECS クラスターを作成します。
7. クラスターでインスタンスを起動するための、Amazon ECS コンテナエージェント環境変数を定義します。
8. コンテナを実行します。

Amazon ECS を AWS Outposts に統合する方法の詳細については、「Extend Amazon ECS across two AWS Outposts rack」を参照してください。

次の例では、AWS Outposts に Amazon ECS クラスターを作成します。

1. AWS Outposts に対する権限を持つロールとポリシーを作成します。

   `role-policy.json` ファイルは、リソースに対する効果とアクションを含むポリシードキュメントです。ファイル形式の情報については、「IAM API リファレンス」の「PutRolePolicy」を参照してください。

```
aws iam create-role --role-name ecsRole \
    --assume-role-policy-document file://ecs-policy.json
aws iam put-role-policy --role-name ecsRole --policy-name ecsRolePolicy \
    --policy-document file://role-policy.json
```

2. AWS Outposts の権限を持つ IAM インスタンスプロファイルを作成します。

```
aws iam create-instance-profile --instance-profile-name outpost
aws iam add-role-to-instance-profile --instance-profile-name outpost \
    --role-name ecsRole
```

3. VPC を作成します。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16
```

4. AWS Outposts に関連付けられたサブネットを作成します。

```
aws ec2 create-subnet \
    --cidr-block 10.0.3.0/24 \
    --vpc-id vpc-xxxxxxxx \
```

```
    --outpost-arn arn:aws:outposts:us-west-2:123456789012:outpost/op-
xxxxxxxxxxxxxxxx \
    --availability-zone-id usw2-az1
```

5. コンテナインスタンスのセキュリティグループを作成し、AWS Outposts に適切な CIDR 範囲を指定します。(この手順は、AWS Outposts では異なります。)

```
aws ec2 create-security-group --group-name MyOutpostSG
aws ec2 authorize-security-group-ingress --group-name MyOutpostSG --protocol tcp \
    --port 22 --cidr 10.0.3.0/24
aws ec2 authorize-security-group-ingress --group-name MyOutpostSG --protocol tcp \
    --port 80 --cidr 10.0.3.0/24
```

6. クラスターを作成します。

7. Amazon ECS コンテナエージェント環境変数を定義して、前のステップで作成したクラスターにインスタンスを起動し、クラスター (例えば、クラスターが Outpost 用であることを示す Outpost など) を識別するのに役立つタグを追加し、定義します。

```
#! /bin/bash
cat << 'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
ECS_IMAGE_PULL_BEHAVIOR=prefer-cached
ECS_CONTAINER_INSTANCE_TAGS={"environment": "Outpost"}
EOF
```

> **Note**
>
> リージョン内の Amazon ECR からコンテナイメージをプルすることによる遅延を回避するには、イメージキャッシュを使用します。これを行うには、タスクを実行するたびに、ECS_IMAGE_PULL_BEHAVIOR を prefer-cached に設定して、インスタンス自体でキャッシュされたイメージを使用するように Amazon ECS エージェントをデフォルトに設定します。

8. コンテナインスタンスを作成し、このインスタンスを実行する AWS Outposts の VPC とサブネットを指定して、AWS Outposts で使用できるインスタンスタイプを指定します。(この手順は、AWS Outposts では異なります。)

   userdata.txt ファイルは、インスタンスの起動後にそのインスタンスが一般的な自動設定タスクを実行したり、スクリプトを実行したりするために使用できるユーザーデータが含まれてい

ます。API コールのファイルの情報については、「Amazon EC2 ユーザーガイド」の「起動時に Linux インスタンスでコマンドを実行する」を参照してください。

```
aws ec2 run-instances --count 1 --image-id ami-xxxxxxxx --instance-type c5.large \
    --key-name aws-outpost-key --subnet-id subnet-xxxxxxxxxxxxxxxxx \
    --iam-instance-profile Name outpost --security-group-id sg-xxxxxx \
    --associate-public-ip-address --user-data file://userdata.txt
```

> **Note**
>
> このコマンドは、クラスターにインスタンスを追加する場合にも使用されます。クラスターにデプロイされたコンテナは、その特定の AWS Outposts に配置されます。

Amazon ECS のキャパシティーと可用性の最適化

アプリケーションの可用性は、エラーのないエクスペリエンスを提供し、アプリケーションのレイテンシーを最小限に抑えるために不可欠です。可用性は、需要を満たすのに十分なキャパシティーのある利用可能なリソースがあるかどうかで変わります。AWS では、可用性を管理するためのメカニズムが複数用意されています。Amazon ECS でホストされるアプリケーションの場合、自動スケーリングやアベイラビリティーゾーン (AZ) などがあります。自動スケーリングは、定義したメトリクスに基づいてタスクやインスタンスの数を管理します。一方、アベイラビリティーゾーンを使用すると、分離されているが地理的に近い場所でアプリケーションをホストできます。

タスクサイズと同様に、キャパシティーと可用性には考慮する必要がある特定のトレードオフが存在します。理想は、キャパシティーと需要が完全に一致することです。低レイテンシーやエラー率などのサービスレベル目標 (SLO) を満たすために、リクエストを処理し、ジョブを処理するのに十分なキャパシティーが常に確保されます。キャパシティーが大きすぎて過度のコストがかかったり、キャパシティーが小さすぎてレイテンシーやエラー率が高くなったりすることはありません。

自動スケーリングは潜在的なプロセスです。最初に、リアルタイムメトリクスを CloudWatch に配信する必要があります。次に、それらを分析のために集計する必要があります。メトリクスの詳細度によっては数分かかる場合があります。CloudWatch は、メトリクスをアラームのしきい値と比較して、リソースの不足や超過を特定します。不安定な状態を回避するために、設定されたしきい値を超えた状態が数分間続かないとアラームが作動しないようにアラームを設定します。また、新しいタスクをプロビジョニングしたり、不要になったタスクを終了したりするのにも時間がかかります。

説明されているシステムではこのような遅延が発生する可能性があるため、オーバープロビジョニングによってある程度の余裕を維持することが重要です。これにより、短期的な需要の急増に対応できるようになります。また、アプリケーションが飽和状態に達することなく追加のリクエストを処理するのにも役立ちます。スケーリングのターゲットは、使用率の 60 ~ 80 % に設定することをお勧めします。これにより、追加のキャパシティーがプロビジョニングされている間も、アプリケーションは追加需要の急増をより適切に処理できるようになります。

オーバープロビジョニングが推奨されるもう 1 つの理由は、アベイラビリティーゾーンの障害に迅速に対応できるようにするためです。本番ワークロードは複数のアベイラビリティーゾーンから提供することをお勧めします。これは、1 つのアベイラビリティーゾーンに障害が発生した場合でも、残りのアベイラビリティーゾーンで実行されているタスクが引き続き需要を処理できるためです。アプリケーションが 2 つのアベイラビリティーゾーンで実行されている場合は、通常のタスク数を 2 倍にする必要があります。これは、潜在的な障害の発生時に即時にキャパシティーを提供できるようにするためです。アプリケーションが 3 つのアベイラビリティーゾーンで実行されている場合は、通常のタスク数の 1.5 倍を実行することをお勧めします。つまり、通常のサービス提供に必要な 2 つのタスクごとに 3 つのタスクを実行します。

スケーリング速度の最大化

自動スケーリングは事後対応型プロセスであるため、効果が現れるまでに時間がかかります。ただし、スケールアウトに必要な時間を最小限に抑えるための方法がいくつかあります。

イメージサイズを最小限に抑えます。イメージが大きいほど、イメージリポジトリからのダウンロードと解凍にかかる時間が長くなります。したがって、イメージサイズを小さくすることで、コンテナの起動に必要な時間が短縮されます。イメージサイズを小さくするには、以下の特定の推奨事項に従ってください。

- 静的バイナリを構築できるか、Golang を使用する場合は、イメージを`FROM`ゼロから構築し、作成されたイメージにバイナリアプリケーションのみを含めます。
- Amazon Linux や Ubuntu など、アップストリームのディストリビューションベンダーが提供する最小限のベースイメージを使用します。
- 最終イメージにはビルドアーティファクトを含めないでください。マルチステージビルドを使用することで、これを実現できます。
- 可能な限り、`RUN` ステージをコンパクトにします。各 `RUN` ステージで新しいイメージレイヤーが作成され、そのレイヤーをダウンロードするための追加のラウンドトリップが発生します。`&&` によって複数のコマンドが結合された単一の `RUN` ステージでは、複数の `RUN` ステージの場合よりレイヤーが少なくなります。

- 最終イメージに ML 推論データなどのデータを含める場合は、起動とトラフィック処理の開始に必要なデータのみを含めます。サービスに影響を与えずに Amazon S3 または他のストレージからオンデマンドでデータを取得する場合は、代わりにそれらの場所にデータを保存します。

イメージを近くに保持します。ネットワークレイテンシーが高いほど、イメージのダウンロードにかかる時間が長くなります。ワークロードと同じ リージョンのリポジトリでイメージをホストします。Amazon ECR は、Amazon ECS を使用可能なすべてのリージョンで使用できる高性能のイメージリポジトリです。インターネットや VPN リンクを経由してコンテナイメージをダウンロードすることは避けてください。同じリージョンでイメージをホストすることで、全体的な信頼性が向上します。この結果、別のリージョンでのネットワーク接続の問題や可用性の問題が発生するリスクを軽減できます。または、Amazon ECR クロスリージョンレプリケーションを実装して、これを実現することもできます。

ロードバランサーのヘルスチェックのしきい値を下げます。ロードバランサーは、アプリケーションにトラフィックを送信する前にヘルスチェックを実行します。ターゲットグループのデフォルトのヘルスチェック設定には、90 秒以上かかる場合があります。この間に、ロードバランサーはヘルスステータスをチェックし、リクエストを受信します。ヘルスチェックの間隔としきい値のカウントを下げることで、アプリケーションがトラフィックをより迅速に受け入れ、他のタスクの負荷を減らすことができます。

コールドスタートのパフォーマンスを考慮します。一部のアプリケーションでは、Java などのランタイムを使用して実行時 (JIT) コンパイルを実行します。コンパイルプロセスは、少なくとも開始時に、アプリケーションのパフォーマンスを減速させる場合があります。回避策は、レイテンシーが重要となるワークロードの部分を、コールドスタート時にパフォーマンスの低下を引き起こさない言語で書き換えることです。

ターゲット追跡スケーリングポリシーではなく、ステップスケーリングポリシーを使用します。タスクに対する Application Auto Scaling オプションは複数あります。ターゲットトラッキングは最も使いやすいモードです。これにより、CPU 平均使用率などのメトリクスの目標値を設定するだけです。次に、オートスケーラーは、その値を達成するために必要なタスクの数を自動的に管理します。ステップスケーリングを使用すると、スケーリングメトリクスの特定のしきい値と、しきい値を超えたときに追加または削除するタスクの数を定義できるため、需要の変化に迅速に対応できます。さらに重要なことは、しきい値アラームが超過する時間を最小限に抑えることで、需要の変化に非常に迅速に対応できることです。詳細については、「Service Auto Scaling」を参照してください。

Amazon EC2 インスタンスを使用してクラスターキャパシティーを提供する場合は、以下の推奨事項を考慮してください。

より大きい Amazon EC2 インスタンスと、より高速な Amazon EBS ボリュームを使用します。より大きい Amazon EC2 インスタンスとより高速な Amazon EBS ボリュームを使用することで、イメージのダウンロードと準備の速度を向上させることができます。特定のインスタンスファミリー内では、インスタンスサイズが大きくなると、ネットワークと Amazon EBS の最大スループットが増加します (例えば、`m5.xlarge` から `m5.2xlarge`)。さらに、Amazon EBS ボリュームをカスタマイズして、そのスループットと IOPS を向上させることもできます。例えば、gp2 ボリュームを使用する場合は、ベースラインスループットが増える、より大きなボリュームを使用します。gp3 ボリュームを使用する場合は、ボリュームの作成時にスループットと IOPS を指定します。

Amazon EC2 インスタンスで実行されるタスクには、ブリッジネットワークモードを使用します。Amazon EC2 で `bridge` ネットワークモードを使用するタスクは、`awsvpc` ネットワークモードを使用するタスクよりも速く開始されます。`awsvpc` ネットワークモードを使用すると、Amazon ECS はタスクを起動する前に Elastic Network Interface (ENI) をインスタンスにアタッチします。これにより、レイテンシーが大きくなります。ただし、ブリッジネットワークの使用には、いくつかのトレードオフがあります。これらのタスクは独自のセキュリティグループを取得しないため、ロードバランシングにいくつかの影響を及ぼします。詳細については、「Elastic Load Balancing ユーザーガイド」の「Load balancer target groups」を参照してください。

需要ショックへの対処

一部のアプリケーションでは、需要が急激に増大することがあります。これは、ニュースイベント、大セール、メディアイベント、急速に拡散されるその他のイベント (トラフィックが非常に短期間で急速かつ大幅に増加する原因となる) など、さまざまな理由で発生します。計画外の場合、これによって使用可能なリソースを需要が急速に上回る可能性があります。

需要ショックに対処する最善の方法は、それらを予測して適切に計画することです。自動スケーリングには時間がかかる場合があるため、需要ショックが始まる前にアプリケーションをスケールアウトすることをお勧めします。最良の結果を得るために、共有カレンダーを使用するチーム間の緊密なコラボレーションを含むビジネス計画を立てることをお勧めします。イベントを計画しているチームは、事前にアプリケーションを担当するチームと緊密に連携する必要があります。これにより、そのチームは明確なスケジューリング計画を立てるのに十分な時間を確保できます。イベント前にスケールアウトし、イベント後にスケールインするキャパシティーをスケジュールできます。詳細については、「Application Auto Scaling ユーザーガイド」の「スケジュールされたスケーリング」を参照してください。

エンタープライズサポートプランをご利用の場合は、テクニカルアカウントマネージャー (TAM) とも連携してください。TAM はサービスクォータを検証し、イベントの開始前に必要なクォータが引き上げられるようにします。これにより、誤ってサービスクォータに達することがなくなります。ま

た、ロードバランサーなどのサービスの暖気運転を行って、イベントのスムーズな進行をサポートすることもできます。

予定外の需要ショックに対処することは、より難しい問題です。予定外のショックが発生し、その振幅が非常に大きい場合、需要がすぐにキャパシティーを超える可能性があります。また、自動スケーリングが反応する能力を上回る可能性もあります。予定外のショックに備える最善の方法は、リソースをオーバープロビジョニングすることです。予想される最大トラフィック需要をいつでも処理できる十分なリソースを確保しておく必要があります。

予定外の需要ショックに備えて最大キャパシティーを維持すると、コストがかかる可能性があります。コストへの影響を軽減するには、大きな需要ショックが差し迫っていることを予測する先行指標となるメトリクスやイベントを見つけます。メトリクスやイベントによって十分な事前通知が確実に提供される場合、イベントが発生したとき、またはメトリクスが設定した特定のしきい値を超えたときには、すぐにスケールアウトプロセスを開始してください。

アプリケーションが突然の予定外の需要ショックを受けやすい場合は、高性能モードをアプリケーションに追加することを検討してください。このモードでは、重要ではない機能を犠牲にして、顧客にとって重要な機能を保持します。例えば、ご使用のアプリケーションでは、コストがかかる高価なカスタマイズされたレスポンスの生成から静的レスポンスページの提供に切り替えることができるとします。このシナリオでは、アプリケーションをまったくスケーリングせずに、スループットを大幅に向上させることができます。

より良く需要ショックに対処するために、モノリシックサービスの分離を検討できます。ご使用のアプリケーションが、実行にコストがかかり、スケーリングに時間がかかるモノリシックサービスである場合、パフォーマンスが重要となる部分を抽出または書き換えて、別のサービスとして実行できる可能性があります。これらの新しいサービスは、重要度の低いコンポーネントから独立してスケーリングできます。パフォーマンスが重要となる機能をアプリケーションの他の部分とは別にスケールアウトする柔軟性を持つことで、キャパシティーの追加にかかる時間の短縮とコストの削減の両方を実現できます。

Amazon ECS ネットワーキングのベストプラクティス

最近のアプリケーションは通常、相互に通信する複数の分散コンポーネントから構築されています。例えば、モバイルアプリケーションやウェブアプリケーションは API エンドポイントと通信したり、その API はインターネット経由で通信する複数のマイクロサービスによって動作していたりします。

インターネットへの接続アプリケーションのベストプラクティスについては、「Amazon ECS アプリケーションをインターネットに接続する」を参照してください。

インターネットから Amazon ECS へのインバウンド接続を受信するためのベストプラクティスについては、「インターネットから Amazon ECS へのインバウンド接続を受信するためのベストプラクティス」を参照してください。

Amazon ECS を他の AWS サービスに接続するためのベストプラクティスについては、「Amazon ECS を VPC 内から AWS サービスに接続するためのベストプラクティス」を参照してください。

VPC 内のサービスに接続するためのベストプラクティスについては、「VPC で Amazon ECS サービスを接続するためのベストプラクティス」を参照してください。

AWS アカウント間および VPC 間でのサービスのネットワーキングに関するベストプラクティスについては、「AWS アカウントおよび VPC の間で Amazon ECS サービスをネットワーキングするためのベストプラクティス」を参照してください。

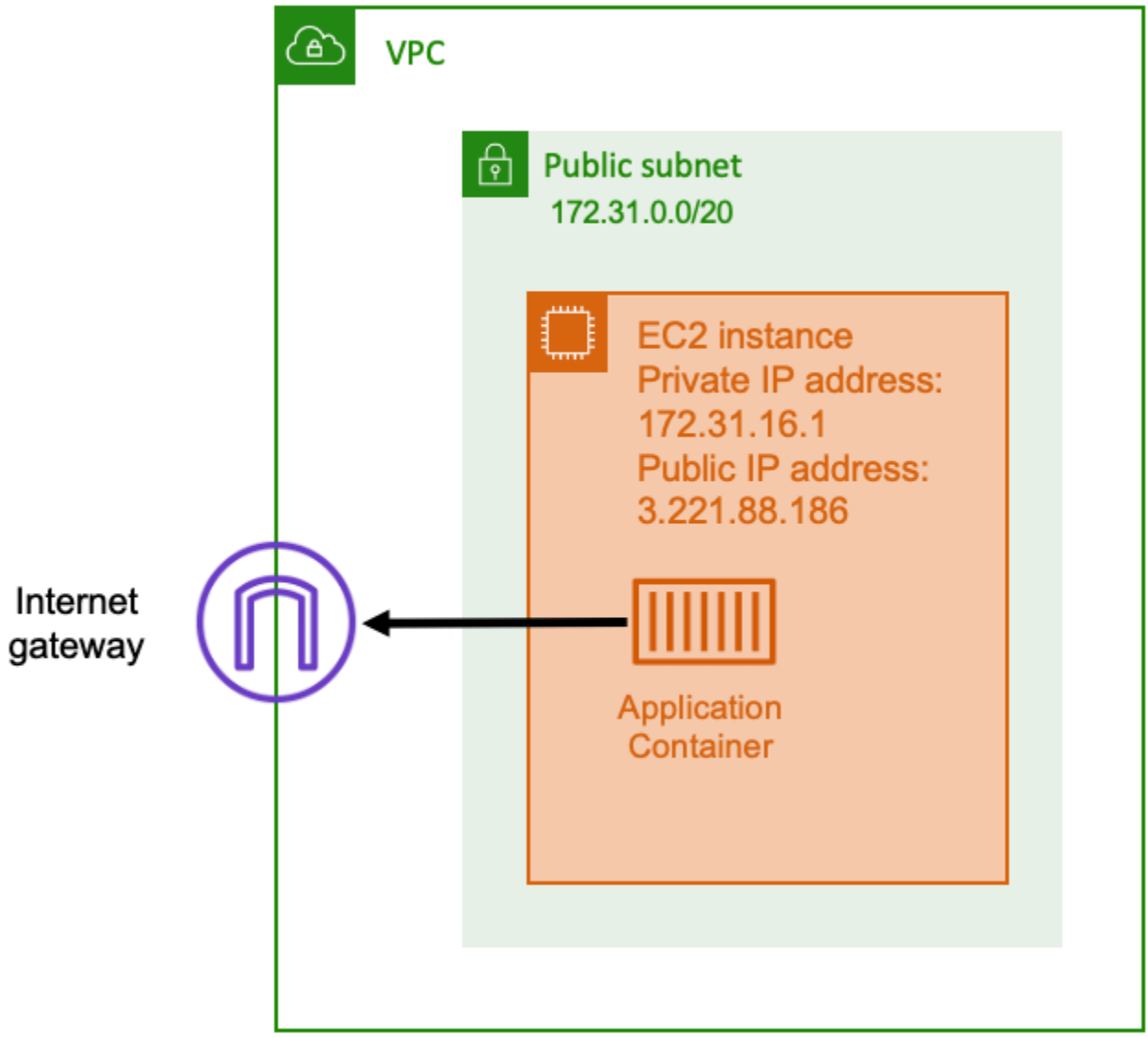
ネットワーキングの問題をトラブルシューティングするサービスに関するベストプラクティスについては、「Amazon ECS ネットワーキングのトラブルシューティングのための AWS サービス」を参照してください。

Amazon ECS アプリケーションをインターネットに接続する

ほとんどのコンテナ化されたアプリケーションには、少なくとも、インターネットへのアウトバウンドアクセスを必要とするいくつかのコンポーネントが含まれています。たとえば、モバイルアプリのバックエンドでは、プッシュ通知へのアウトバウンドアクセスが必要です。

Amazon Virtual Private Cloud には、VPC とインターネット間の通信を円滑にする主な方法が 2 つあります。

パブリックサブネットとインターネットゲートウェイ



インターネットゲートウェイへのルートがあるパブリックサブネットを使用すると、コンテナ化されたアプリケーションは、パブリックサブネットの VPC 内のホストで実行できます。コンテナを実行するホストには、パブリック IP アドレスが割り当てられます。このパブリック IP アドレスは、インターネットからルーティング可能です。詳細については、Amazon VPC ユーザーガイドの「インターネットゲートウェイ」を参照してください。

このネットワークアーキテクチャにより、アプリケーションを実行するホストとインターネット上の他のホストとの直接通信が容易になります。通信は双方向です。つまり、インターネット上の他のホストへのアウトバウンド接続を確立できるだけでなく、インターネット上の他のホストもそのホストに接続を試みる可能性があります。そのため、セキュリティグループとファイアウォールのルールに

は細心の注意を払う必要があります。これにより、インターネット上の他のホストは、開くべきでない接続を開くことができなくなります。

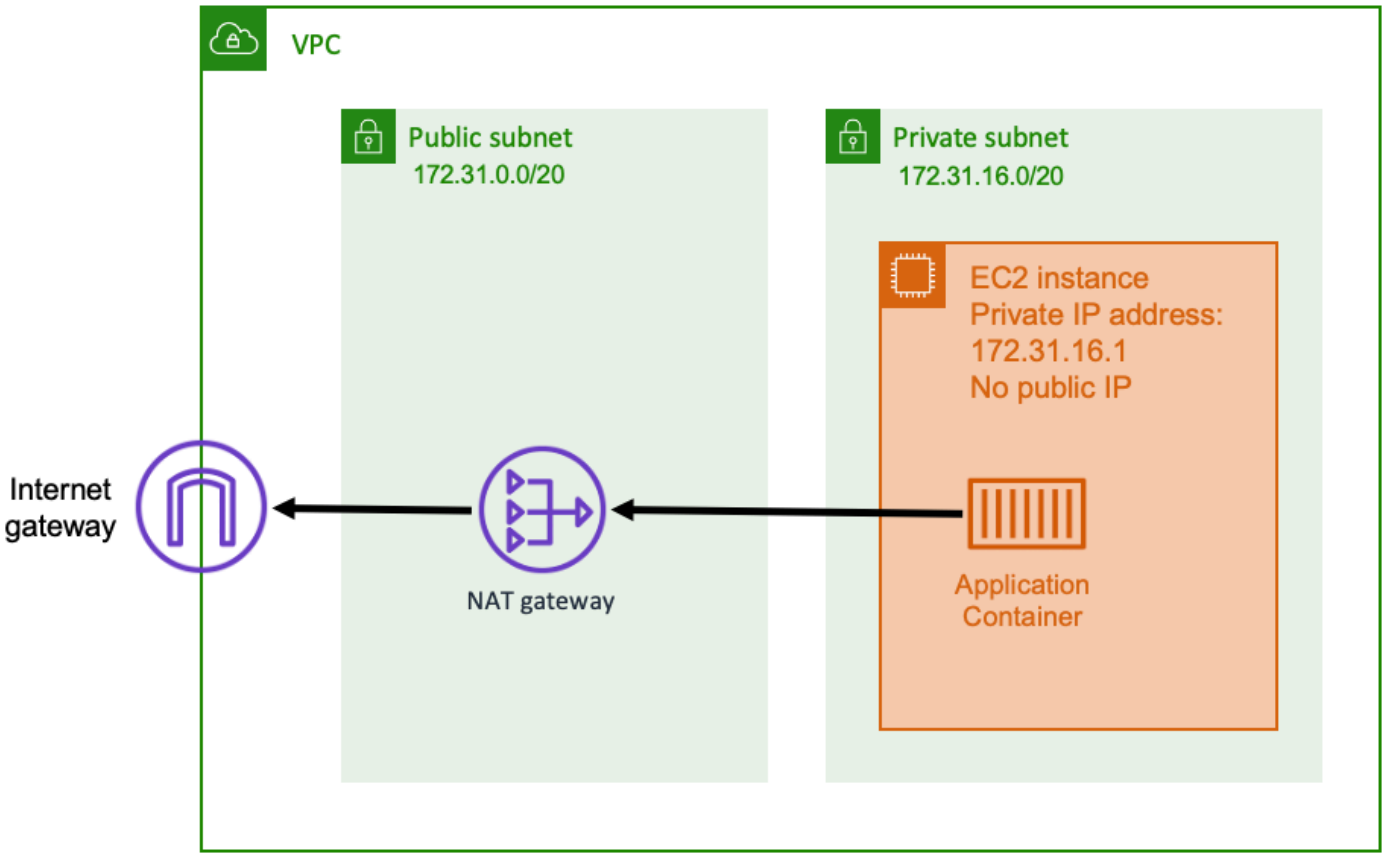
たとえば、アプリケーションが Amazon EC2 で実行されている場合は、SSH アクセス用のポート 22 が開いていないことを確認してください。そうしないと、インスタンスがインターネット上の悪意のあるボットが継続的に SSH 接続を試みる可能性があります。これらのボットはパブリック IP アドレスを総当たり的に調べます。空いている SSH ポートが見つかると、そのようなボットはパスワードをブルートフォース攻撃してインスタンスにアクセスしようとします。このため、多くの組織はパブリックサブネットの使用を制限し、すべてではないにしてもほとんどのリソースをプライベートサブネット内に置くことを好みます。

ネットワークにパブリックサブネットを使用することは、大量の帯域幅や最小のレイテンシーを必要とするパブリックアプリケーションに適しています。該当するユースケースには、ビデオストリーミングやゲームサービスが含まれます。

このネットワークアプローチは、Amazon ECS を Amazon EC2 で使用する場合と、AWS Fargate で使用する場合の両方でサポートされます。

- Amazon EC2 — パブリックサブネットで EC2 インスタンスを起動できます。Amazon ECS はこれらの EC2 インスタンスをクラスター容量として使用し、インスタンス上で実行されるすべてのコンテナは、ホストの基礎となるパブリック IP アドレスをアウトバウンドネットワークに使用できます。これは `host` および `bridge` ネットワークモードの両方に当てはまります。ただし、`awsvpc` ネットワークモードでは、タスク ENI にパブリック IP アドレスが提供されません。そのため、インターネットゲートウェイを直接使用することはできません。
- Fargate — Amazon ECS サービスを作成するときは、サービスのネットワーク設定にパブリックサブネットを指定し、[パブリック IP アドレスの割り当て] オプションを使用してください。各 Fargate タスクはパブリックサブネットでネットワーク化されており、インターネットと直接通信するための独自のパブリック IP アドレスを持っています。

プライベートサブネットと NAT ゲートウェイ



プライベートサブネットと NAT ゲートウェイを使用すると、プライベートサブネット内のホストでコンテナ化されたアプリケーションを実行できます。そのため、このホストのプライベート IP アドレスは VPC 内ではルーティング可能ですが、インターネットからはルーティングできません。つまり、VPC 内の他のホストはプライベート IP アドレスを使用してホストに接続できますが、インターネット上の他のホストはそのホストとのインバウンド通信を行うことができません。

プライベートサブネットでは、ネットワークアドレス変換 (NAT) ゲートウェイを使用して、プライベートサブネット内のホストがインターネットに接続できるようにします。インターネット上のホストは、パブリックサブネット内の NAT ゲートウェイのパブリック IP アドレスから送信されているように見えるインバウンド接続を受信します。NAT ゲートウェイは、インターネットとプライベートサブネットの間のブリッジとして機能します。この構成では、VPC がインターネット上の攻撃者による直接アクセスから保護されるため、多くの場合セキュリティ上望ましいものです。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。

このプライベートネットワークアプローチは、外部からの直接アクセスからコンテナを保護するシナリオに適しています。該当するシナリオには、支払い処理システムや、ユーザーデータとパスワード

を格納するコンテナなどがあります。アカウントで NAT ゲートウェイを作成して使用するには料金がかかります。NAT ゲートウェイの時間単位の使用料金とデータ処理料金も適用されます。冗長性を確保するために、アベイラビリティーゾーンごとに NAT ゲートウェイが必要です。こうすることで、1 つのアベイラビリティーゾーンの可用性が失われても、アウトバウンド接続が損なわれなくなります。このため、ワークロードが少ない場合は、プライベートサブネットと NAT ゲートウェイを使用する方が費用対効果が高い可能性があります。

このネットワークアプローチは、Amazon ECS を Amazon EC2 で使用する場合と、AWS Fargate で使用する場合の両方でサポートされます。

- Amazon EC2 — プライベートサブネットで EC2 インスタンスを起動できます。これらの EC2 ホストで実行されるコンテナは、基盤となるホストのネットワークを使用し、アウトバウンドリクエストは NAT ゲートウェイを経由します。
- Fargate — Amazon ECS サービスを作成するときは、サービスのネットワーク設定にプライベートサブネットを指定してください。[パブリック IP アドレスの割り当て] オプションは使用しないでください。各 Fargate タスクはプライベートサブネットでホストされます。そのアウトバウンドトラフィックは、そのプライベートサブネットに関連付けた NAT ゲートウェイを経由してルーティングされます。

インターネットから Amazon ECS へのインバウンド接続を受信するためのベストプラクティス

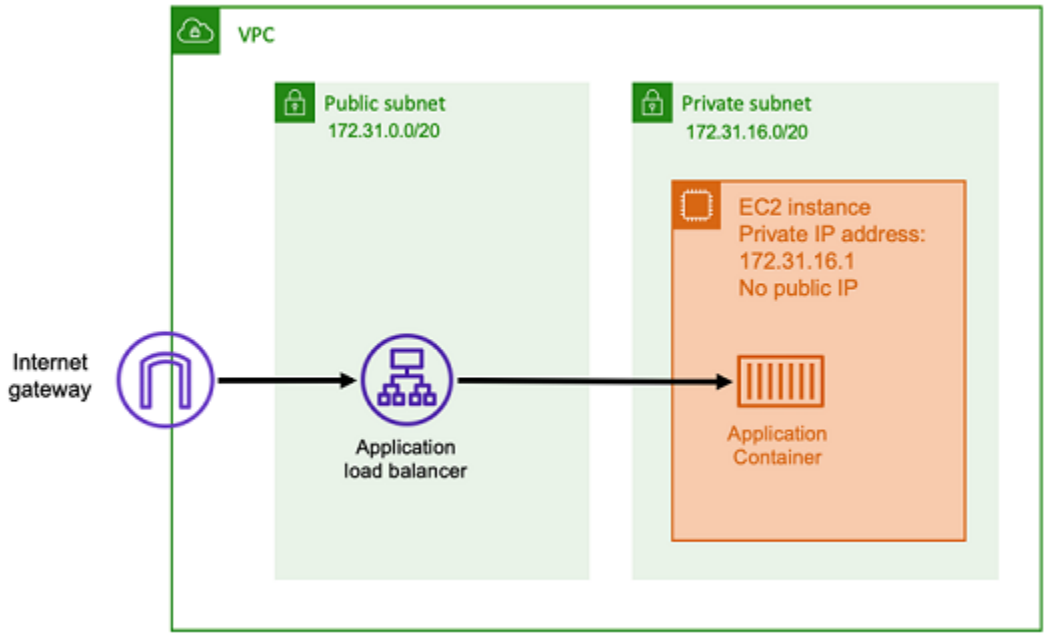
パブリックサービスを運営している場合は、インターネットからのインバウンドトラフィックを受け入れる必要があります。たとえば、公開 Web サイトはブラウザからのインバウンド HTTP リクエストを受け入れる必要があります。このような場合、インターネット上の他のホストもアプリケーションのホストへのインバウンド接続を開始する必要があります。

この問題に対する 1 つの方法は、パブリック IP アドレスを持つパブリックサブネット内のホスト上でコンテナを起動することです。ただし、大規模なアプリケーションにこれを行うことは推奨しません。このような場合は、インターネットとアプリケーションの間にスケーラブルな入力層を設けるのがより適切なアプローチです。このアプローチでは、このセクションに記載されている AWS サービスのいずれかを入力として使用できます。

Application Load Balancer

Application Load Balancer はアプリケーション層で機能します。これは、開放型システム間相互接続 (OSI) モデルの第 7 層です。これにより、Application Load Balancer はパブリック HTTP サービ

スに適しています。ウェブサイトまたは HTTP REST API を使用している場合は、Application Load Balancer がこのワークロードに適したロードバランサーです。詳細については、Application Load Balancers ユーザーガイドの Application Load Balancer とは を参照してください。



このアーキテクチャでは、パブリックサブネットに Application Load Balancer を作成します。これにより、パブリック IP アドレスが割り当てられ、インターネットからのインバウンド接続を受信できるようになります。Application Load Balancer は、インバウンド接続、より具体的には HTTP リクエストを受信すると、プライベート IP アドレスを使用してアプリケーションへの接続を開きます。次に、リクエストを内部接続経由で転送します。

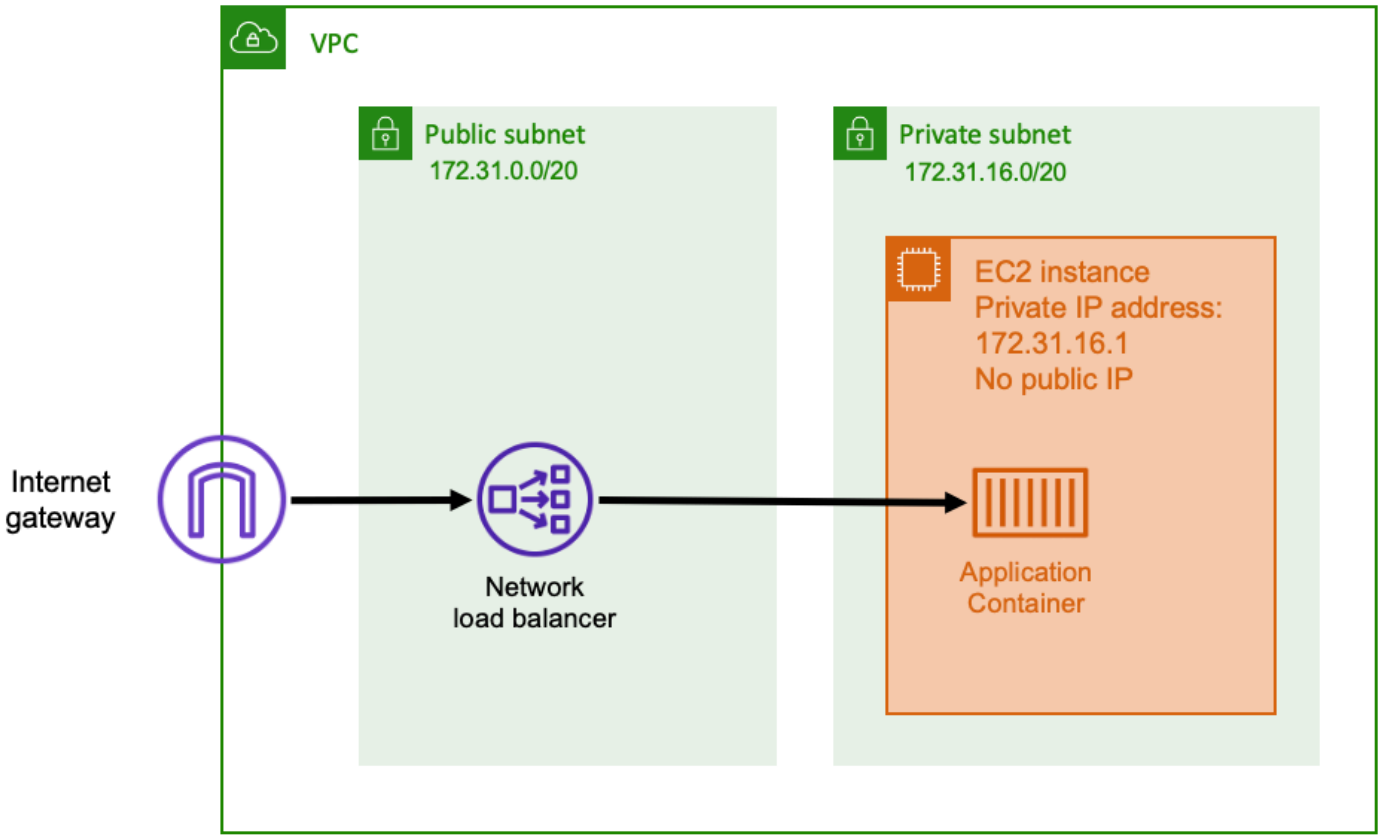
Application Load Balancer には以下の利点があります。

- SSL/TLS ターミネーション — Application Load Balancer は、クライアントとの通信用の安全な HTTPS 通信と証明書を維持できます。必要に応じて SSL 接続をロードバランサーレベルで終了できるため、独自のアプリケーションで証明書を処理する必要がありません。
- 高度なルーティング — Application Load Balancer は複数の DNS ホスト名を持つことができます。また、ホスト名やリクエストのパスなどのメトリックに基づいて、受信した HTTP リクエストをさまざまな宛先に送信する高度なルーティング機能も備えています。つまり、単一の Application Load Balancer をさまざまな内部サービス、さらには REST API のさまざまなパスにあるマイクロサービスの入力として使用できます。
- gRPC サポートとウェブソケット — Application Load Balancer は HTTP 以外も処理できます。また、HTTP/2 サポートにより、gRPC およびウェブソケットベースのサービスの負荷分散も可能です。

- セキュリティ — Application Load Balancer は、悪意のあるトラフィックからアプリケーションを保護するのに役立ちます。HTTP 同期解除対策などの機能が含まれており、AWS Web Application Firewall (AWS WAF) と統合されています。AWS WAF は、SQL インジェクションやクロスサイトスクリプティングなどの攻撃パターンを含む可能性のある悪意のあるトラフィックをさらに効果的に除外できます。

Network Load Balancer

Network Load Balancer は、開放型システム間相互接続 (OSI) モデルの第 4 層で機能します。HTTP 以外のプロトコルや、エンドツーエンドの暗号化が必要なシナリオに適していますが、Application Load Balancer と同じ HTTP 固有の機能はありません。そのため、Network Load Balancer は HTTP を使用しないアプリケーションに最適です。詳細については、Network Load Balancers ユーザーガイドの「Network Load Balancer とは」を参照してください。



Network Load Balancer を入力として使用すると、Application Load Balancer と同様に機能します。これは、パブリックサブネットで作成されており、インターネット上でアクセスできるパブリック IP アドレスがあるためです。次に、Network Load Balancer は、コンテナを実行しているホストの

プライベート IP アドレスへの接続を開き、パブリック側からプライベート側にパケットを送信します。

Network Load Balancer の機能

Network Load Balancer はネットワークスタックの下位レベルで動作するため、機能セットは Application Load Balancer と同じではありません。ただし、以下の重要な機能を備えています。

- エンドツーエンドの暗号化 — Network Load Balancer は OSI モデルの第 4 層で動作するため、パケットの内容を読み取ることはありません。これにより、エンドツーエンドの暗号化を必要とする負荷分散通信に適しています。
- TLS 暗号化 — エンドツーエンドの暗号化に加えて、Network Load Balancer は TLS 接続を終了することもできます。これにより、バックエンドアプリケーションが独自の TLS を実装する必要がなくなります。
- UDP サポート — Network Load Balancer は OSI モデルの第 4 層で動作するため、HTTP 以外のワークロードや TCP 以外のプロトコルに適しています。

接続を終了する

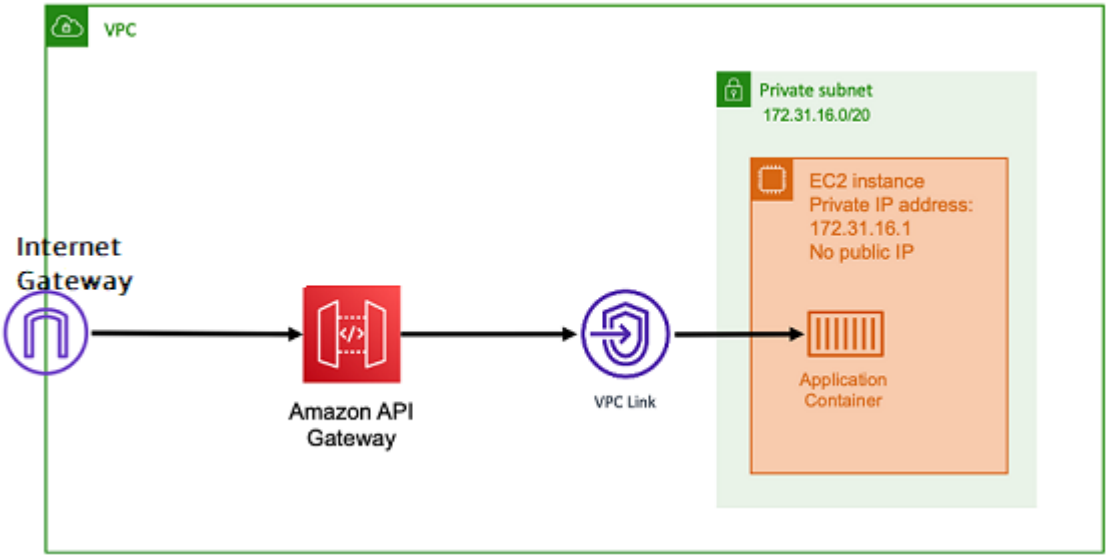
Network Load Balancer は OSI モデルの上位層ではアプリケーションプロトコルを監視しないため、それらのプロトコルのクライアントにクロージャメッセージを送信することはできません。Application Load Balancer とは異なり、これらの接続はアプリケーションによって閉じられる必要があります。または、タスクが停止または置換されたときに、第 4 レイヤーの接続を閉じるように Network Load Balancer を設定することもできます。Network Load Balancer のドキュメントで、Network Load Balancer のターゲットグループの接続終了設定を参照してください。

Network Load Balancer に第 4 層で接続を終了させると、クライアントがそれを処理しない場合、クライアントが望ましくないエラーメッセージを表示する恐れがあります。推奨されるクライアント設定の詳細については、「こちらの」 Builders Library を参照してください。

接続を閉じる方法はアプリケーションによって異なりますが、1 つの方法は、Network Load Balancer のターゲット登録解除の遅延時間をクライアントの接続タイムアウトよりも長くすることです。クライアントは最初にタイムアウトし、Network Load Balancer を介して次のタスクに正常に再接続し、同時に古いタスクではすべてのクライアントがゆっくりとドレインされます。Network Load Balancer のターゲット登録解除を遅延させる方法の詳細については、Network Load Balancer のドキュメントを参照してください。

Amazon API Gateway HTTP API

Amazon API Gateway は、リクエスト量が突然急増する、またはリクエスト量が少ない HTTP アプリケーションに適しています。詳細については、API Gateway デベロッパーガイドの「Amazon API Gateway とは」を参照してください。



Application Load Balancer および Network Load Balancer の料金モデルには、ロードバランサーがインバウンド接続を常時受け付けられるようにするための時間単位の料金が含まれています。これとは対照的に、API Gateway ではリクエストごとに個別に請求されます。これには、リクエストを受信しない限り課金されないという効果があります。トラフィック負荷が高い場合、Application Load Balancer または Network Load Balancer は、API Gateway よりも安いリクエストあたりの料金で大量のリクエストを処理できます。ただし、全体的にリクエスト数が少ない場合やトラフィックが少ない期間がある場合は、使用率が低いロードバランサーを維持するために時間単位の料金を支払うよりも、API Gateway を使用する場合の累積料金の方が費用対効果が高くなるでしょう。API Gateway は API レスポンスをキャッシュすることもできるため、バックエンドのリクエスト率が軽減される可能性があります。

API Gateway は、AWS マネージドサービスがプライベート IP アドレスを使用して VPC のプライベートサブネット内のホストに接続できるようにする VPC リンクを使用する機能です。Amazon ECS Service Discovery によって管理されている AWS Cloud Map サービス検出レコードを調べることで、これらのプライベート IP アドレスを検出できます。

API Gateway は、次の機能をサポートしています。

- API Gateway の動作はロードバランサーに似ていますが、API 管理に固有の追加機能があります。

- API Gateway は、クライアントの承認、使用レベル、リクエスト/レスポンスの変更に関する追加機能を備えています。詳細については、「Amazon API Gateway の機能」を参照してください。
- API Gateway は、エッジ、リージョン、プライベート API ゲートウェイのエンドポイントをサポートできます。エッジエンドポイントは、マネージド CloudFront ディストリビューションを通じて利用できます。リージョナルエンドポイントとプライベートエンドポイントはどちらもリージョンに対してローカルです。
- SSL/TLS ターミネーション
- 異なる HTTP パスを別々のバックエンドマイクロサービスにルーティングする

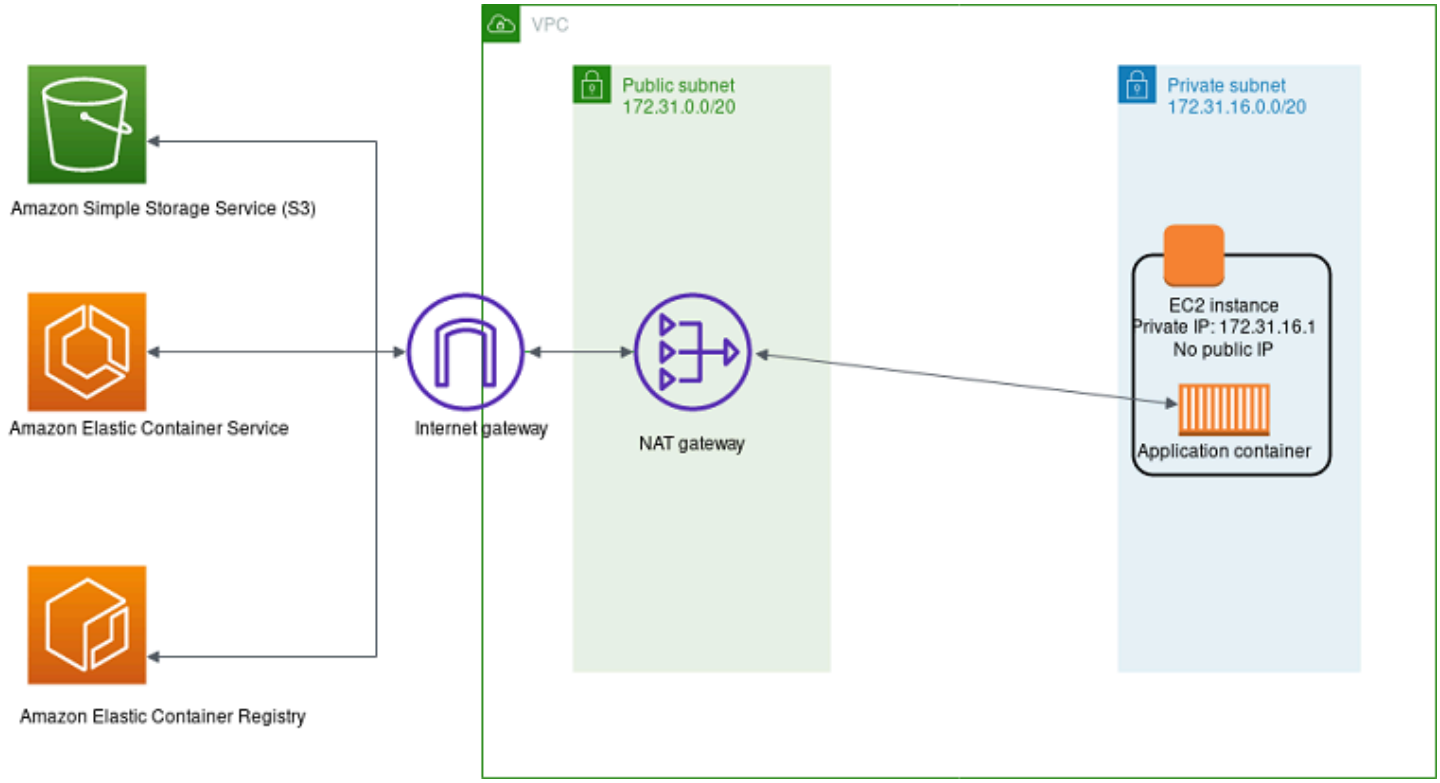
API Gateway は、前述の機能に加えて、API を不正使用から保護するために使用できるカスタム Lambda オーソライザーの使用もサポートしています。詳細については、「フィールドノート:Amazon ECS と Amazon API Gateway を使用したサーバーレスコンテナベースの API」を参照してください。

Amazon ECS を VPC 内から AWS サービスに接続するためのベストプラクティス

Amazon ECS が正しく機能するためには、各ホストで実行される Amazon ECS コンテナエージェントは Amazon ECS コントロールプレーンと通信する必要があります。コンテナイメージを Amazon ECR に保存している場合、Amazon EC2 ホストは Amazon ECR サービスエンドポイントと、およびイメージレイヤーが保存されている Amazon S3 と通信する必要があります。DynamoDB に保存されているデータの保持など、コンテナ化されたアプリケーションに他の AWS サービスを使用する場合は、必要なネットワーキングのサポートもこのサービスにあることを再確認してください。

NAT ゲートウェイ

NAT ゲートウェイの使用は、Amazon ECS タスクが他の AWS サービスにアクセスできるようになる最も簡単な方法です。この方法の詳細については、「プライベートサブネットと NAT ゲートウェイ」を参照してください。



この方法の利用における欠点は次のとおりです。

- NAT ゲートウェイが通信できる宛先を制限することはできません。また、VPC からのすべてのアウトバウンド通信を中断することなく、バックエンド層が通信できる宛先を制限することはできません。
- NAT ゲートウェイは、通過するデータの GB ごとに課金されます。NAT ゲートウェイを次のいずれかの操作に使用すると、帯域幅の GB ごとに課金されます。
  - Amazon S3 からの大きなファイルのダウンロード
  - DynamoDB に対する大量のデータベースクエリの実行
  - Amazon ECR からのイメージのプル

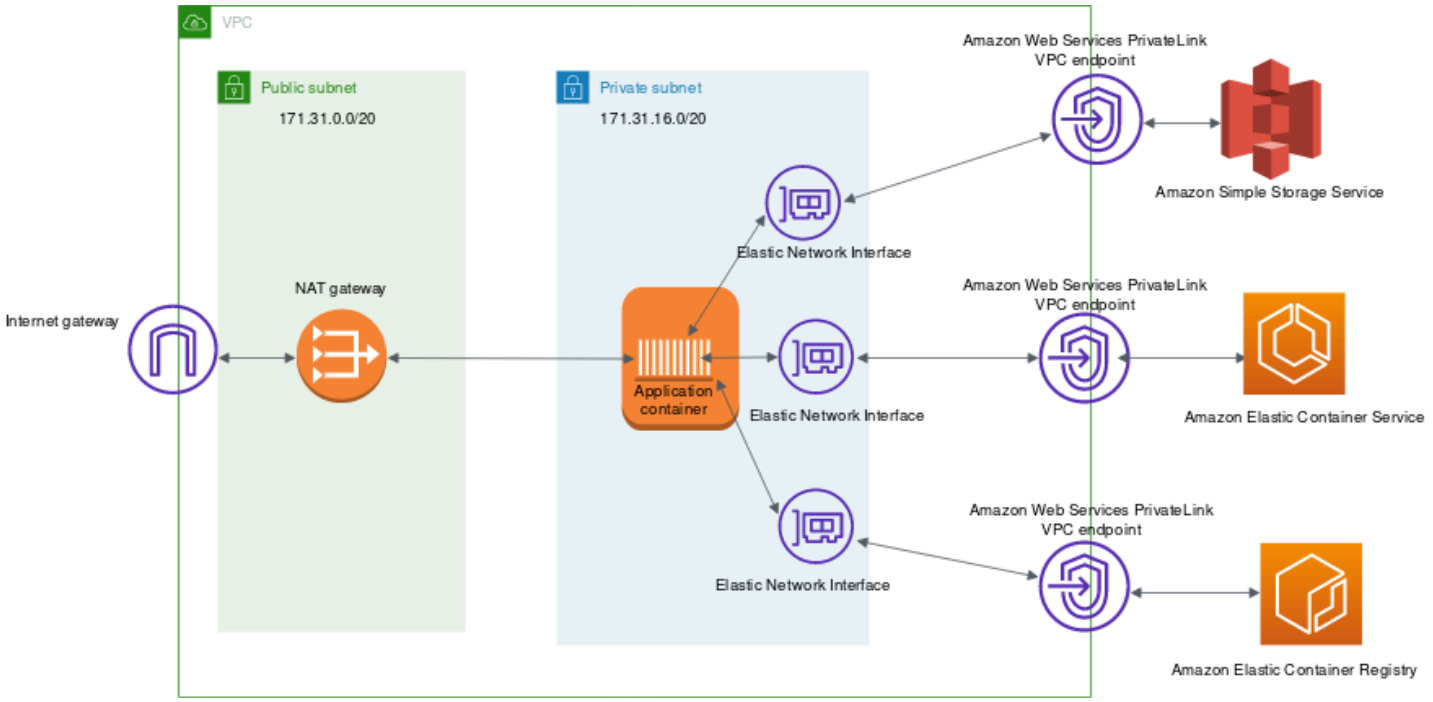
  さらに、NAT ゲートウェイは 5 Gbps の帯域幅をサポートしており、45 Gbps まで自動的にスケールアップします。1 つの NAT ゲートウェイを介してルーティングする場合、非常に大きな帯域幅の接続を必要とするアプリケーションでは、ネットワーク上の制約が発生する可能性があります。回避策として、ワークロードを複数のサブネットに分割し、各サブネットに独自の NAT ゲートウェイを与えることができます。

AWS PrivateLink

AWS PrivateLink は、トラフィックをパブリックインターネットに公開することのない、VPC、AWS サービス、オンプレミスネットワークの間のプライベート接続を提供します。

VPC エンドポイントにより、VPC とサポートされている AWS サービスおよび VPC エンドポイントサービスとの間のプライベート接続が可能になります。VPC と他のサービス間のトラフィックは、Amazon ネットワークを離れることはありません。VPC エンドポイントは、インターネットゲートウェイ、仮想プライベートゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を必要としません。VPC の Amazon EC2 インスタンスでは、サービスのリソースと通信するのにパブリック IP アドレスを必要としません。

次の図は、インターネットゲートウェイではなく VPC エンドポイントを使用している場合に、AWS サービスへの通信がどのように機能するかを示しています。AWS PrivateLink はサブネット内で Elastic Network Interface (ENI) をプロビジョニングし、ENI 経由でサービスホスト名への通信を宛先の AWS サービスに直接送信するのに、VPC ルーティングルールが使用されています。このトラフィックは、NAT ゲートウェイまたはインターネットゲートウェイを使用する必要がなくなっています。



以下は、Amazon ECS サービスで使用される一般的な VPC エンドポイントの一部です。

- Amazon S3 のゲートウェイエンドポイント
- DynamoDB VPC エンドポイント

- Amazon ECS VPC エンドポイント
- Amazon ECR VPC エンドポイント

他の多くの AWS サービスは VPC エンドポイントをサポートしています。いずれかの AWS サービスを大量に使用する場合は、そのサービスの特定のドキュメントと、そのトラフィックにおいて VPC エンドポイントを作成する方法を調べる必要があります。

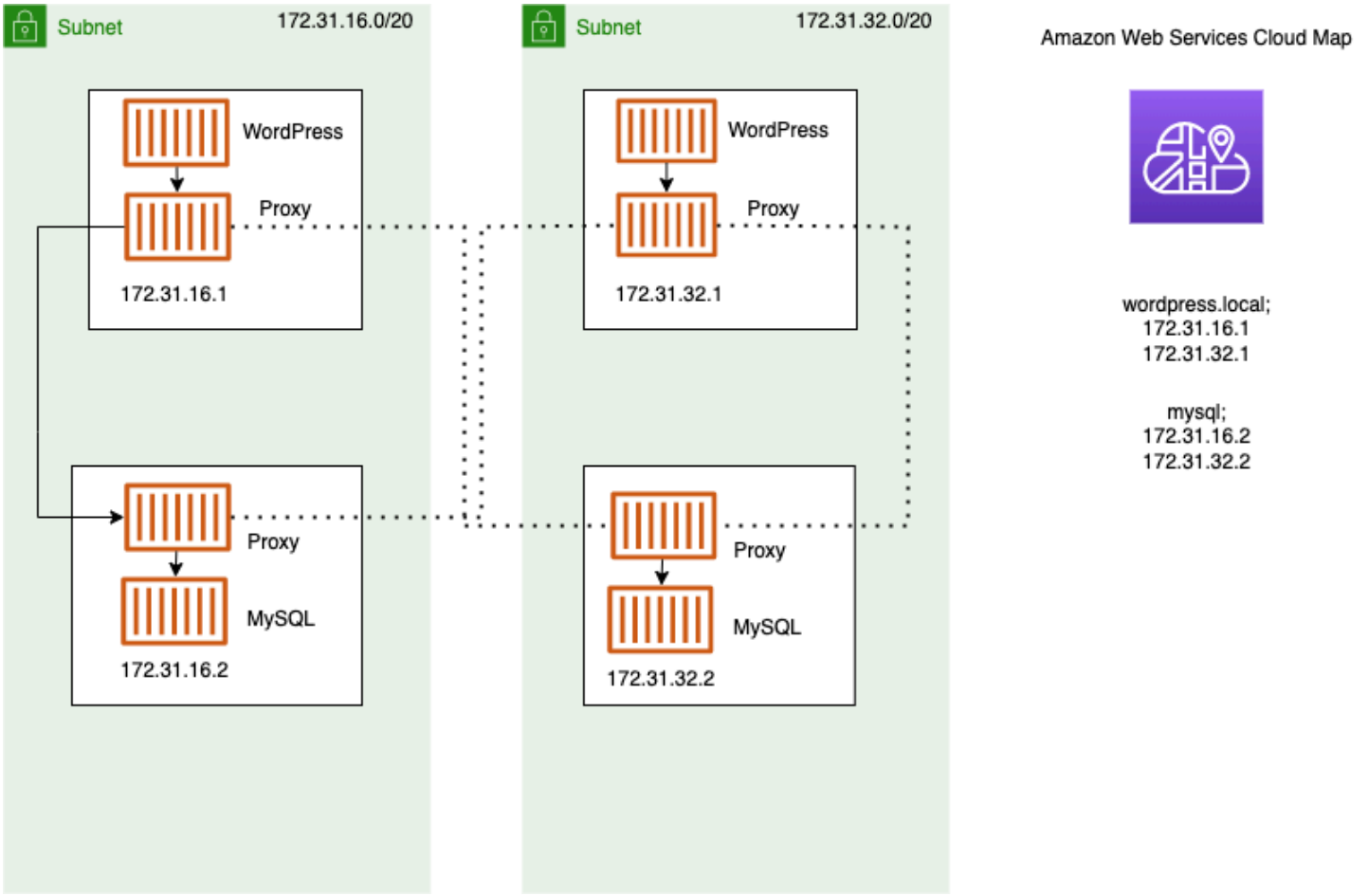
VPC で Amazon ECS サービスを接続するためのベストプラクティス

VPC で Amazon ECS タスクを使用すると、モノリシックアプリケーションを、安全な環境で個別にデプロイおよびスケーリングできる別々の部分に分割できます。このアーキテクチャは、サービス指向アーキテクチャ (SOA) またはマイクロサービスといいます。ただし、VPC の内外両方で、これらのすべての部分が相互に通信できるようにするのが難しい場合があります。通信を促進する方法は複数ありますが、すべてにさまざまな利点と欠点があります。

Service Connect の使用

サービス検出、接続、トラフィックモニタリング用の Amazon ECS 設定を提供する Service Connect をお勧めします。Service Connect を使用すると、アプリケーションは短縮名と標準ポートを使用して、同じクラスターや他のクラスター (同じリージョンの VPC 間を含む) 内のサービスに接続できます。詳細については、「Amazon ECS Service Connect」を参照してください。

Service Connect を使用すると、Amazon ECS がサービス検出のすべての部分を管理します。つまり、検出可能な名前の作成、タスクの開始と終了時に各タスクのエントリを動的に管理すること、名前を検出するように設定された各タスクでのエージェントの実行などです。アプリケーションは DNS 名の標準機能を使用して接続することで名前を検索できます。アプリケーションがすでにこれを実行している場合、Service Connect を使用する際に、アプリケーションを変更する必要はありません。



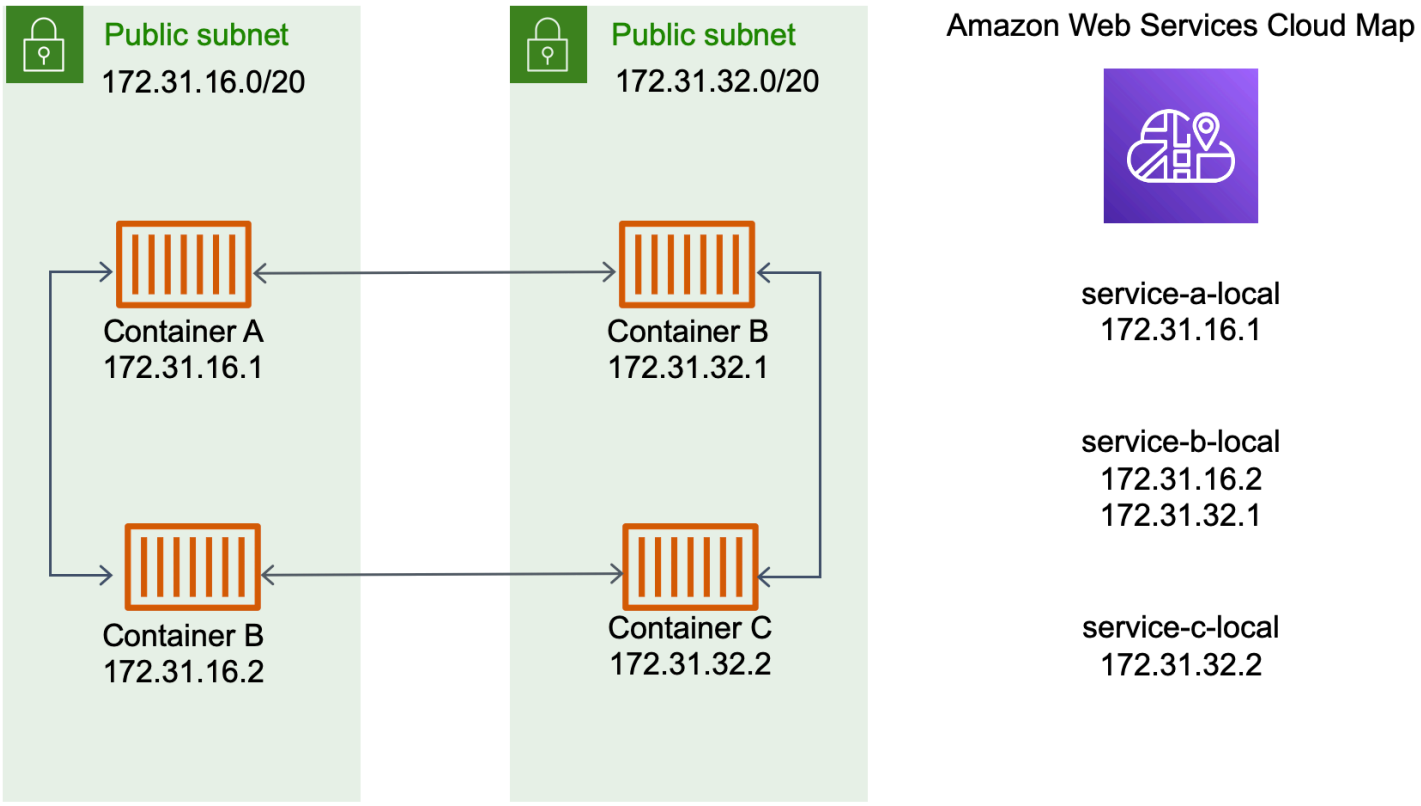
変更はデプロイ中にのみ発生します

各サービスとタスク定義内で完全な設定を行います。Amazon ECS は、デプロイ内のすべてのタスクが同じように動作するように、サービスデプロイごとにこの設定の変更を管理します。たとえば、サービス検出の DNS でよくある問題は、移行の制御です。新しい IP アドレスを指すように DNS 名を変更すると、すべてのクライアントが新しいサービスの使用を開始するまでに最大 TTL 時間がかかることがあります。Service Connect では、クライアントデプロイメントがクライアントタスクを置き換えて設定を更新します。他のデプロイと同様に、Service Connect の変更に影響するように、デプロイサーキットブレーカーやその他のデプロイ設定を設定できます。

サービス検出の使用

サービス間の通信のもう 1 つのアプローチは、サービス検出を使用する直接的な通信です。このアプローチでは、Amazon ECS との AWS Cloud Map サービス検出の統合を使用できます。Amazon ECS はサービス検出を使用して、起動されたタスクのリストを AWS Cloud Map に同期します。このホスト名は特定のサービスの 1 つ以上のタスクの内部 IP アドレスに解決される DNS ホスト名を保持します。Amazon VPC の他のサービスは、この DNS ホスト名を使用して、内部 IP アドレスを

使用してトラフィックを別のコンテナに直接送信できます。詳細については、「サービス検出」を参照してください。



前出の図では、サービスが 3 つあります。`service-a-local` はコンテナが 1 つあり、コンテナが 2 つある `service-b-local` と通信します。`service-b-local` は、コンテナが 1 つある `service-c-local` とも通信する必要があります。これら 3 つのサービスすべての各コンテナは、AWS Cloud Map の内部 DNS 名を使用して、通信する必要があるダウンストリームサービスからコンテナの内部 IP アドレスを見つけることができます。

このサービス間通信のアプローチでは、レイテンシが低くなります。一見すると、コンテナ間に余分なコンポーネントがないためシンプルでもあります。トラフィックは 1 つのコンテナから別のコンテナに直接移動します。

この方法は、各タスクに固有の IP アドレスが割り当てられる `awsvpc` ネットワークモードを使用する場合に適しています。ほとんどのソフトウェアは、IP アドレスに直接変換される DNS `A` レコードの使用のみをサポートしています。`awsvpc` ネットワークモードを使用する場合、各タスクの IP アドレスは `A` レコードになります。ただし、`bridge` ネットワークモードを使用している場合は、複数のコンテナが同じ IP アドレスを共有している可能性があります。さらに、動的ポートマッピングでは、その 1 つの IP アドレスのポート番号がコンテナにランダムに割り当てられます。この時点では、`A` レコードだけではサービス検出には不十分です。`SRV` レコードも使用する必要があります。

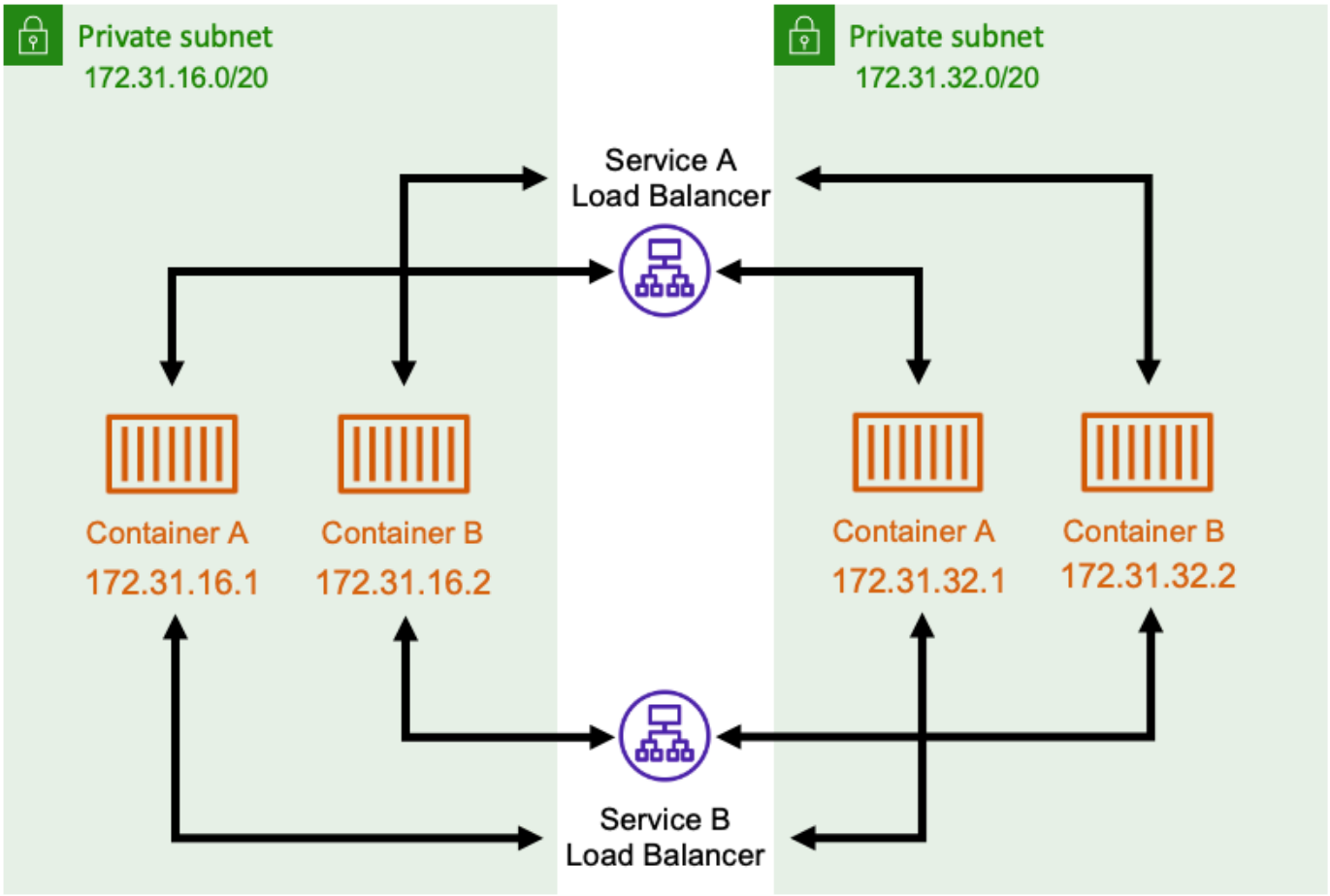
このタイプのレコードは IP アドレスとポート番号の両方を記録できますが、アプリケーションを適切に設定する必要があります。使用するビルド済みアプリケーションの中には、SRV レコードをサポートしていないものもあります。

awsvpc ネットワークモードのもう 1 つの利点は、サービスごとに固有のセキュリティグループがあることです。このセキュリティ グループを設定して、そのサービスと通信する必要がある特定のアップストリームサービスからの受信接続のみを許可することができます。

サービス検出を使用するサービス間直接的な通信の主な欠点は、再試行や接続障害に対処するためのロジックを追加する必要があることです。DNS レコードには、キャッシュされる時間を制御する有効期限 (TTL) があります。DNS レコードが更新されてキャッシュが期限切れになり、アプリケーションが最新バージョンの DNS レコードを取得できるようになるまでには、ある程度の時間がかかります。そのため、アプリケーションが DNS レコードを解決して、もう存在しない別のコンテナを指すようになってしまう可能性があります。アプリケーションには再試行を処理し、不正なバックエンドを無視するロジックが必要です。

内部ロードバランサーの使用

サービス間通信のもう 1 つの方法は、内部ロードバランサーを使用することです。内部ロードバランサーは完全に VPC 内に存在し、VPC 内のサービスにのみアクセスできます。



ロードバランサーは、冗長リソースを各サブネットにデプロイすることで、高可用性を維持します。serviceA のコンテナが serviceB のコンテナと通信する必要がある場合、ロードバランサーへの接続が開きます。次に、ロードバランサーは service B からコンテナへの接続を開きます。ロードバランサーは、各サービス間のすべての接続を管理するための一元的な場所として機能します。

serviceB のコンテナが停止すると、ロードバランサーはそのコンテナをプールから削除できます。また、ロードバランサーはそのプール内の各ダウンストリームターゲットに対してヘルスチェックを行い、再び正常になるまでプールから不正なターゲットを自動的に削除できます。アプリケーションは、ダウンストリームコンテナの数を認識する必要がなくなりました。ロードバランサーへの接続を開くだけです。

この方法は、すべてのネットワークモードで有益です。ロードバランサーは、awsvpc ネットワークモードを使用する場合のタスク IP アドレスと、bridge ネットワークモードを使用する場合の IP アドレスとポートのより高度な組み合わせを追跡できます。また、実際に複数のコンテナが異なるポー

トにおいて同じ Amazon EC2 インスタンスでホストされている場合でも、すべての IP アドレスとポートの組み合わせにトラフィックを均等に分散します。

この方法の欠点の 1 つはコストです。可用性を高めるために、ロードバランサーには各アベイラビリティーゾーンにリソースが必要です。この結果、ロードバランサーとロードバランサーを通過するトラフィック量に対して支払うオーバーヘッドにより、追加コストが追加されます。

ただし、複数のサービスでロードバランサーを共有することで、オーバーヘッドコストを削減できます。これは、Application Load Balancer を使用する REST サービスに特に適しています。ユーザーは、異なるサービスにトラフィックをルーティングするパスベースのルーティングルールを作成できます。例えば、`/api/user/*` は `user` サービスの一部であるコンテナにルーティングし、`/api/order/*` は関連付けられた `order` サービスにルーティングできます。この方法では、1 つの Application Load Balancer に対してのみ料金が発生し、API の URL が一貫した 1 つになります。ただし、トラフィックをバックエンドのさまざまなマイクロサービスに分割することはできます。

AWS アカウントおよび VPC の間で Amazon ECS サービスをネットワーキングするためのベストプラクティス

複数のチームや部門を有する組織に属している場合は、おそらく共有 AWS アカウント内の個別の VPC または複数の個別の AWS アカウントに関連付けられている VPC に、サービスを個別にデプロイするでしょう。どの方法でサービスをデプロイしても、VPC 間でトラフィックをルーティングできるようにネットワークコンポーネントを補完することをお勧めします。そのためには、複数の AWS サービスを使用して、既存のネットワークコンポーネントを補完することができます。

- AWS Transit Gateway – このネットワーキングサービスを最初に検討する必要があります。このサービスは、Amazon VPC、AWS アカウントおよびオンプレミスネットワーク間の接続をルーティングするための中央ハブとして機能します。詳細については、「Amazon VPC Transit Gateway ガイド」の「Transit Gateway とは」を参照してください。
- Amazon VPC および VPN サポート – このサービスを使用して、オンプレミスネットワークを VPC に接続するためのサイト間 VPN 接続を作成できます。詳細については、『AWS Site-to-Site VPN ユーザーガイド』の「What is AWS Site-to-Site VPN? (とは ?)」 を参照してください。
- Amazon VPC – 同じアカウント内または複数のアカウント間で複数の VPC を接続できる、Amazon VPC ピアリングを使用できます。詳細については、Amazon VPC Peering Guideの「VPC ピア機能とは」を参照してください。
- 共有 VPC – 複数の AWS アカウントで VPC と VPC サブネットを使用できます。詳細については、「Amazon VPC ユーザーガイド」の「共有 VPC の使用」を参照してください。

Amazon ECS ネットワーキングのトラブルシューティングのための AWS サービス

以下のサービスと機能は、ネットワークとサービスの設定に関するインサイトを得るのに役立ちます。この情報を使用することで、ネットワーキング問題のトラブルシューティングを行い、サービスをより適切に最適化できます。

CloudWatch Container Insights

CloudWatch Container Insights は、コンテナ化されたアプリケーションとマイクロサービスのメトリクスとログを収集、集約、要約します。メトリクスには、CPU、メモリ、ディスク、ネットワークなどのリソースの使用率が含まれています。メトリクスは CloudWatch 自動ダッシュボードで使用できます。詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon ECS での Container Insights のセットアップ」を参照してください。

AWS X-Ray

AWS X-Ray は、アプリケーションが行うネットワークリクエストに関する情報を収集するのに使用できるトレースサービスです。SDK を使用することで、アプリケーションをインストルメント化し、サービス間、およびサービスと AWS サービスエンドポイントとの間のトラフィックのタイミングとレスポンスコードをキャプチャできます。詳細については、「AWS X-Ray デベロッパーガイド」の「AWS X-Ray とは」を参照してください。

また、サービスがどのように相互にネットワーキングされているかについての AWS X-Ray グラフを見ることもできます。または、これらを使用して、各サービス間リンクのパフォーマンスに関する総合統計情報を見ることができます。最後に、特定のトランザクションを詳しく調べることで、ネットワーク呼び出しを表すセグメントがその特定のトランザクションにどのように関連付けられているかを確認できます。

これらの機能を使用することで、ネットワーキングのボトルネックがあるかどうか、またはネットワーク内の特定のサービスが期待どおりに動作していないかどうかを特定できます。

VPC フローログ

Amazon VPC フローログを使用して、ネットワークパフォーマンスを分析したり、接続の問題をデバッグしたりできます。VPC フローログを有効にすると、VPC 内のすべての接続のログをキャプチャできます。この接続には、Elastic Load Balancing、Amazon RDS、NAT ゲートウェイ、および使用している可能性があるその他の主要な AWS サービスに関連付けられているネットワークインターフェイスへの接続が含まれます。詳細については、「Amazon VPC ユーザーガイド」の「VPC フローログ」を参照してください。

ネットワーク調整のヒント

ネットワーキングを改善するために微調整できる設定がいくつかあります。

nofile ulimit

アプリケーションのトラフィックが多く、多数の同時接続を処理することが予想される場合は、許可されるファイル数に対しシステムクォータを考慮する必要があります。多数のネットワークソケットが開いている場合は、それぞれをファイル記述子で表す必要があります。ファイル記述子のクォータが低すぎると、ネットワークソケットが制限されます。この結果、接続が失敗したり、エラーが発生したりします。コンテナ固有のクォータは、Amazon ECS タスク定義内のファイル数に合わせて更新できます。(AWS Fargate ではなく) Amazon EC2 で実行している場合は、基盤となる Amazon EC2 インスタンスでこれらのクォータを調整する必要もあります。

sysctl ネット

もう 1 つのカテゴリの調整可能な設定は、`sysctl` ネット設定です。選択した Linux ディストリビューションの特定の設定を参照する必要があります。この設定の多くでは、読み取りバッファと書き込みバッファのサイズが調整されます。これは、コンテナが多数ある大規模な Amazon EC2 インスタンスを実行する場合に役立つことがあります。

アカウント設定による Amazon ECS 機能へのアクセス

Amazon ECS アカウント設定に移動して、特定の機能をオプトインまたはオプトアウトできます。各 AWS リージョンについて、アカウントレベルまたは特定のユーザーまたはロールで、各アカウント設定をオプトインまたはオプトアウトすることができます。

次のいずれかの条件が関係する場合は、特定の機能をオプトインまたはオプトアウトすることが考えられます。

- ユーザーまたはロールは、個々のアカウントのために特定のアカウント設定をオプトインまたはオプトアウトできます。
- ユーザーまたはロールはアカウントのすべてのユーザーに対してデフォルトのオプトインまたはオプトアウト設定を定義できます。
- ルートユーザーまたは管理者権限を持つユーザーは、アカウントの任意の種類のロールまたはユーザーについて、オプトインまたはオプトアウトすることができます。ルートユーザーのアカウント設定が変更されると、個別にアカウント設定が選択されなかったすべてのユーザーとロールに対してデフォルト値が設定されます。

> **Note**
>
> フェデレーションユーザーは、ルートユーザーのアカウント設定を想定しており、明示的にアカウント設定を個別に設定することはできません。

以下のアカウント設定を使用できます。アカウント設定ごとに、オプトインおよびオプトアウトする必要があります。

リソース名	詳細はこちら
`containerInsights`	Container Insights

`serviceLongArnFormat`
`taskLongArnFormat`
`containerInstanceLongArnFormat`
	Amazon リソースネーム (ARN) と ID

`tagResourceAuthorization`	タグ付け認可
`fargateFIPSMode`	AWS Fargate 連邦情報処理標準 (FIPS-140) コンプライアンス
`fargateTaskRetirementWaitPeriod`	AWS Fargate タスク廃止の待機時間
`guardDutyActivate`	Runtime Monitoring (Amazon GuardDuty 統合)
`dualStackIPv6`	デュアルスタック IPv6 VPC
`awsvpcTrunking`	Linux コンテナインスタンスのネットワークインターフェイスを増やす

Amazon リソースネーム (ARN) と ID

Amazon ECS リソースの作成時に、各リソースには一意の Amazon リソースネーム (ARN) と一意のリソース識別子 (ID) が割り当てられます。コマンドラインツールまたは Amazon ECS API を使用して Amazon ECS を操作する場合、特定のコマンドにはリソース ARNまたはリソース ID が必要にな

ります。例えば、タスクを停止するために stop-task AWS CLI コマンドを使用する場合は、そのコマンドでタスクの ARN または ID を指定する必要があります。

Amazon ECS では、Amazon ECS サービス、タスク、コンテナインスタンスの Amazon リソース名 (ARN) とリソース ID の新しい形式が導入されました。各リソースタイプのオプトインステータスによって、リソースが使用する Amazon リソースネーム (ARN) の形式が決まります。そのリソースタイプのリソースタグ付けなどの機能を使用するには、新しい ARN の形式にオプトインする必要があります。

新しい Amazon リソースネーム (ARN) およびリソース ID の形式は、リージョンごとにオプトインおよびオプトアウトできます。現在、新しく作成されたアカウントはデフォルトでオプトインされています。

新形式の Amazon リソースネーム (ARN) およびリソース ID はいつでもオプトインまたはオプトアウトできます。オプトイン後、作成するすべての新しいリソースは新しい形式を使用します。

> **Note**
>
> リソース ID が作成後に変更することはありません。したがって、新しい形式をオプトインまたはオプトアウトしても、既存のリソース ID には影響しません。

以下のセクションでは、ARN およびリソース ID 形式がどのように変更されているかについて説明します。新しい形式への移行の詳細については、「Amazon Elastic Container Service のよくある質問」を参照してください。

Amazon リソースネーム (ARN) 形式

一部のリソースには、`production` という名前のサービスなど、わかりやすい名前があります。それ以外の場合は、Amazon リソースネーム (ARN) 形式を使用してリソースを指定する必要があります。Amazon ECS のタスク、サービス、およびコンテナインスタンスの新しい ARN 形式には、クラスター名が含まれます。新しい ARN 形式へのオプトインの詳細については、「Amazon ECS アカウント設定の変更」を参照してください。

各リソースタイプでの現在の形式と新しい形式を次の表に示しています。

リソースタイプ	ARN
コンテナインスタンス	現在: `arn:aws:ecs:` *`region`*`:`*`aws_account_id`*` :container-instance/` *`container-instance-id`*

リソースタイプ	ARN
	新: arn:aws:ecs: *region*:*aws_account_id* :container-instance/ *cluster-name* /*container-instance-id*
Amazon ECS サービス	現在: arn:aws:ecs: *region*:*aws_account_id* :service/ *service-name* 新: arn:aws:ecs: *region*:*aws_account_id* :service/ *cluster-name* /*service-name*
Amazon ECS タスク	現在: arn:aws:ecs: *region*:*aws_account_id* :task/*task-id* 新: arn:aws:ecs: *region*:*aws_account_id* :task/*cluster-name* /*task-id*

リソース ID の長さ

リソース ID は文字と数字の一意の組み合わせです。新しいリソース ID 形式には、Amazon ECS タスクおよびコンテナインスタンス用の短い ID が含まれます。現在のリソース ID の形式の長さは 36 文字です。新しい ID は 32 文字の形式で、ハイフンは含まれません。新しい リソース ID 形式をオプトインする方法の詳細については、「Amazon ECS アカウント設定の変更」を参照してください。

デフォルト: enabled。

オプトインした後に起動されたリソースだけが、新形式の ARN とリソース ID を受け取ります。既存のリソースは、いずれも影響を受けません。Amazon ECS サービスとタスクを新しい ARN およびリソース ID の形式に移行するには、サービスまたはタスクを再作成する必要があります。コンテナインスタンスを新しい ARN およびリソース ID 形式に移行するには、そのコンテナインスタンスを空にし、新規コンテナインスタンスを起動してクラスターに登録する必要があります。

> **Note**
>
> Amazon ECS サービスが 2018 年 11 月 16 日以降に作成されていて、そのサービスを作成したユーザーがタスクの新形式をオプトインしている場合、そのサービスによって起動されたタスクだけが新形式の ARN とリソース ID になります。

ARN およびリソース ID 形式のタイムライン

新しい Amazon リソースネーム (ARN) と Amazon ECS リソースのリソース ID 形式のための、オプトインおよびオプトアウト期間のタイムラインは、2021 年 4 月 1 日に終了しました。デフォルトでは、すべてのアカウントが新しい形式にオプトインされています。新しく作成されたすべてのリソースには新しい形式が適用され、オプトアウトできなくなります。

Container Insights

2024 年 12 月 2 日、AWS で Amazon ECS 用にオブザーバビリティが強化された Container Insights がリリースされました。このバージョンでは、Amazon EC2 および Fargate 起動タイプを使用して Amazon ECS 用に強化されたオブザーバビリティがサポートされます。Amazon ECS でオブザーバビリティが強化された Container Insights を設定したら、Container Insights は環境内のクラスターレベルからコンテナレベルまでの詳細なインフラストラクチャテレメトリを自動収集し、さまざまなメトリクスとディメンションを示すダッシュボードにデータを表示します。その後、Container Insights コンソールでこれらのすぐに使えるダッシュボードを使用して、コンテナの健全性とパフォーマンスをよりよく理解し、異常を特定することで問題を迅速に軽減することができます。

コンテナ環境で詳細な可視性を提供し、解決までの平均時間を短縮するため、Container Insights ではなく、オブザーバビリティが強化された Container Insights を使用することをお勧めします。詳細については、「Amazon CloudWatchユーザーガイド」の「Amazon ECS 用にオブザーバビリティメトリクスが強化された Container Insights」を参照してください。

`containerInsights` アカウントのデフォルトは、`disabled` です。

オブザーバビリティが強化された Container Insights

次のコマンドを使用し、オブザーバビリティが強化された Container Insights を有効にします。

`containerInsights` アカウント設定を `enhanced` に設定します。

```
aws ecs put-account-setting --name containerInsights --value enhanced
```

出力例

```
{
    "setting": {
        "name": "containerInsights",
```

```
        "value": "enhanced",
        "principalArn": "arn:aws:iam::123456789012:johndoe",
         "type": user
    }
}
```

このアカウント設定を行ったら、すべての新しいクラスターはオブザーバビリティが強化された Container Insights を自動的に使用します。update-cluster-settings コマンドを使用してオブザーバビリティが強化された Container Insights を既存のクラスターに追加するか、Container Insightsからオブザーバビリティが強化されたContainer Insightsにクラスターをアップグレードします。

```
aws ecs update-cluster-settings --cluster cluster-name --settings
 name=containerInsights,value=enhanced
```

コンソールを使用して、オブザーバビリティが強化された Container Insights を設定することもできます。詳細については、「Amazon ECS アカウント設定の変更」を参照してください。

Container Insights

containerInsights アカウント設定を enabled に設定すると、すべての新しいクラスターはデフォルトで Container Insights が有効になります。update-cluster-settings を使用して既存のクラスターを変更できます。

Container Insights を使用するには、containerInsights アカウント設定を enabled に設定します。次のコマンドを使用して Container Insights を有効にします。

```
aws ecs put-account-setting --name containerInsights --value enabled
```

出力例

```
{
    "setting": {
        "name": "containerInsights",
        "value": "enabled",
        "principalArn": "arn:aws:iam::123456789012:johndoe",
         "type": user
    }
}
```

containerInsights アカウント設定を enabled に設定すると、すべての新しいクラスターはデフォルトで Container Insights が有効になります。update-cluster-settings コマンドを使用して Container Insights を既存のクラスターに追加します。

```
aws ecs update-cluster-settings --cluster cluster-name --settings
 name=containerInsights,value=enabled
```

コンソールを使用して Container Insights を設定することもできます。詳細については、「Amazon ECS アカウント設定の変更」を参照してください。

AWS Fargate 連邦情報処理標準 (FIPS-140) コンプライアンス

Fargate は、機密情報を保護する暗号モジュールのセキュリティ要件を指定する連邦情報処理標準 (FIPS-140) をサポートしています。これは現在の米国およびカナダの政府標準であり、Federal Information Security Management Act (FISMA) または Federal Risk and Authorization Management Program (FedRAMP) への準拠が要求されるシステムに適用されます。

リソース名は fargateFIPSMode です。

デフォルト: disabled。

Fargate で連邦情報処理標準 (FIPS-140) コンプライアンスをオンにする必要があります。詳細については、「the section called “AWS Fargate FIPS-140 コンプライアンス”」を参照してください。

> **Important**
>
> fargateFIPSMode アカウント設定は、Amazon ECS API または AWS CLI を使用してのみ変更できます。詳細については、「Amazon ECS アカウント設定の変更」を参照してください。

fargateFIPSMode オプションを enabled に設定して put-account-setting-default を実行します。詳細については、「Amazon Elastic Container Service API リファレンス」の「put-account-setting-default」を参照してください。

- 次のコマンドを使用して、FIPS-140 コンプライアンスをオンにできます。

  ```
  aws ecs put-account-setting-default --name fargateFIPSMode --value enabled
  ```

  出力例

```
{
    "setting": {
        "name": "fargateFIPSMode",
        "value": "enabled",
        "principalArn": "arn:aws:iam::123456789012:root",
         "type": user
    }
}
```

list-account-settings を実行して、現在の FIPS-140 コンプライアンスステータスを表示できます。effective-settings オプションを使用して、アカウントレベルの設定を表示します。

```
aws ecs list-account-settings --effective-settings
```

タグ付け認可

Amazon ECS は、リソース作成のためのタグ付け認可を導入しています。ecsCreateCluster などのリソースを作成するアクションには、ユーザーがタグ付けのアクセス許可を持っている必要があります。リソースを作成し、そのリソースのタグを指定すると、AWS は、追加の認可を実行して、タグを作成するための許可があることを検証します。したがって、ecs:TagResource アクションを使用するための明示的な許可を付与する必要があります。詳細については、「the section called "リソース作成時のタグ付け"」を参照してください。

タグ付け認可にオプトインするには、tagResourceAuthorization オプションを enable に設定して put-account-setting-default を実行します。詳細については、「Amazon Elastic Container Service API リファレンス」の「put-account-setting-default」を参照してください。list-account-settings を実行して、現在のタグ付け認可ステータスを表示できます。

- 次のコマンドを使用して、タグ付け認可を有効にできます。

```
aws ecs put-account-setting-default --name tagResourceAuthorization --value on --
region region
```

出力例

```
{
    "setting": {
        "name": "tagResourceAuthorization",
```

```
        "value": "on",
        "principalArn": "arn:aws:iam::123456789012:root",
        "type": user
    }
}
```

タグ付け認可を有効にしたら、作成時にユーザーがリソースにタグ付けできるように、適切なアクセス許可を設定する必要があります。詳細については、「the section called “リソース作成時のタグ付け”」を参照してください。

`list-account-settings` を実行して、現在のタグ付け認可ステータスを表示できます。`effective-settings` オプションを使用して、アカウントレベルの設定を表示します。

```
aws ecs list-account-settings --effective-settings
```

タグ付け認可のタイムライン

`list-account-settings` を実行して `tagResourceAuthorization` 値を表示することで、タグ付け認可がアクティブかどうかを確認できます。値が on である場合、タグ付け認可が使用されています。詳細については、「Amazon Elastic Container Service API リファレンス」の「list-account-settings」を参照してください。

タグ付け認可に関連する重要な日付を次に示します。

- 2023 年 4 月 18 日 – タグ付け認可が導入されました。この機能を使用するには、新規および既存のすべてのアカウントでオプトインする必要があります。タグ付け認可の使用開始をオプトインできます。オプトインすることにより、適切な許可を付与する必要があります。
- 2024 年 2 月 9 日から 2024 年 3 月 6 日 — すべての新しいアカウントと影響を受けていない既存のアカウントでは、タグ付け認可がデフォルトで有効になります。`tagResourceAuthorization` アカウント設定を有効/無効にすると、IAM ポリシーを確認できます。

  AWS は、影響を受けたアカウントに通知しました。

  この機能を無効にするには、`tagResourceAuthorization` オプションを `off` に設定して `put-account-setting-default` を実行します。
- 2024 年 3 月 7 日 — タグ付け認可を有効にしている場合、アカウント設定を無効にすることはできなくなります。

この日までに IAM ポリシーのテストを完了することをお勧めします。

- 2024 年 3 月 29 日 — すべてのアカウントがタグ付け認可を使用するようになります。アカウントレベルの設定は、Amazon ECS コンソールまたは AWS CLI では使用できなくなります。

AWS Fargate タスク廃止の待機時間

廃止の対象としてマークされたプラットフォームバージョンリビジョン上で実行している Fargate タスクがある場合、AWS から通知が送信されます。詳細については、「AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス」を参照してください。

AWS Fargate の基盤となるインフラストラクチャに対する、パッチ適用とメンテナンスは、AWS が担当します。Fargate でホストされている Amazon ECS タスクにおいて、セキュリティまたはインフラストラクチャの更新が必要であると AWS が判断した場合、対象のタスクを停止し、それらを置き換えるための新しいタスクを起動する必要があります。Fargate タスクが廃止されるまでの待機時間を設定できます。タスクをすぐに廃止するか、7 暦日または 14 暦日待つかを選択できます。

この設定はアカウントレベルで適用されます。

Fargate がタスク廃止を開始する時間を設定できます。アップデートをすぐに適用する必要があるワークロードの場合は、即時設定 (0) を選択します。特定の時間帯にしかタスクを停止できない場合など、詳細な制御が必要な場合は、7 日 (7) または 14 日 (14) のオプションを設定します。

新しいプラットフォームバージョンのリビジョンを早く取得できるように、待機時間を短くすることをお勧めします。

待機時間を設定するには、ルートユーザーまたは管理者ユーザーで `put-account-setting-default` または `put-account-setting` を実行します。`fargateTaskRetirementWaitPeriod` オプションを `name` に使用し、`value` オプションを次のいずれかの値に設定します。

- `0` - AWS から通知が送信され、影響を受けたタスクが直ちに廃止されます。
- 7 - AWS から通知が送信され、7 日間待機してから、影響を受けたタスクの廃止が開始されます。
- 14 - AWS から通知が送信され、14 日間待機してから、影響を受けたタスクの廃止が開始されます。

デフォルトは 7 日間です。

詳細については、「Amazon Elastic Container Service API リファレンス」の「put-account-setting-default」と「put-account-setting」を参照してください。

次のコマンドを実行して、待機時間を 14 日間に設定できます。

```
aws ecs put-account-setting-default --name fargateTaskRetirementWaitPeriod --value 14
```

出力例

```
{
    "setting": {
        "name": "fargateTaskRetirementWaitPeriod",
        "value": "14",
        "principalArn": "arn:aws:iam::123456789012:root",
        "type: user"
    }
}
```

現在の Fargate タスク廃止の待機時間は、`list-account-settings` を実行して表示できます。`effective-settings` オプションを使用する

```
aws ecs list-account-settings --effective-settings
```

Linux コンテナインスタンスのネットワークインターフェイスを増やす

`awsvpc` ネットワークモードを使用する各 Amazon ECS タスクには、独自の Elastic Network Interface (ENI) が割り当てられ、その ENI はそれをホストするコンテナインスタンスにアタッチされます。Amazon EC2 インスタンスにアタッチできるネットワークインターフェイスの数にはデフォルトの制限があり、プライマリネットワークインターフェイスも 1 つとしてカウントされます。例えば、デフォルトでは `c5.large` インスタンスには最大 3 つの ENI がアタッチされています。このインスタンスのプライマリネットワークインターフェイスも 1 つとしてカウントされるため、このインスタンスに追加でアタッチできる ENI は 2 つです。`awsvpc` ネットワークモードを使用する各タスクには ENI が必要なため、通常このインスタンスタイプでは、このようなタスクを 2 つだけ実行できます。

Amazon ECS は、サポートされている Amazon EC2 インスタンスタイプを使用して、ENI 密度が高いコンテナインスタンスの起動をサポートしています。これらのインスタンスタイプを使用し、`awsvpcTrunking` アカウント設定を有効にすると、新しく起動されたコンテナインスタンスで

追加の ENI を利用できます。この設定により、各コンテナインスタンスにより多くのタスクを配置できます。

例えば、awsvpcTrunking を持つ c5.large インスタンスでは、ENI の制限が 12 に引き上げられています。コンテナインスタンスはプライマリネットワークインターフェイスを持ち、Amazon ECS はコンテナインスタンスの「トランク」ネットワークインターフェイスを作成およびアタッチします。したがって、この設定では、現在の 2 個ではなく 10 個のタスクをコンテナインスタンスで起動できます。

Runtime Monitoring (Amazon GuardDuty 統合)

Runtime Monitoring は、AWS ログとネットワークアクティビティを継続的に監視して悪意のある動作や不正な動作を特定することで、Fargate および EC2 で実行されているワークロードを保護するインテリジェントな脅威検出サービスです。

guardDutyActivate パラメータは Amazon ECS では読み取り専用で、Amazon ECS アカウントのセキュリティ管理者によってランタイムモニタリングが有効になっているか無効になっているかを示します。GuardDuty は、ユーザーに代わってこのアカウント設定を制御します。詳細については、「Runtime Monitoring で Amazon ECS ワークロードを保護する」を参照してください。

list-account-settings を実行して、現在の GuardDuty 統合設定を表示できます。

```
aws ecs list-account-settings
```

出力例

```
{
    "setting": {
        "name": "guardDutyActivate",
        "value": "on",
        "principalArn": "arn:aws:iam::123456789012:doej",
        "type": aws-managed"
    }
}
```

デュアルスタック IPv6 VPC

Amazon ECS は、プライマリプライベート IPv4 アドレスに加えて IPv6 アドレスを備えたタスクの提供をサポートします。

タスクが IPv6 アドレスを受信するには、タスクが awsvpc ネットワークモードを使用し、デュアルスタックモードに設定された VPC で起動し、dualStackIPv6 アカウント設定を有効にする必要があります。その他の要件について詳しくは、EC2 起動タイプに関しては デュアルスタックモードでの VPC の使用、Fargate 起動タイプに関しては デュアルスタックモードでの VPC の使用 を参照してください。

> **Important**
>
> dualStackIPv6 アカウント設定は、Amazon ECS API または AWS CLI を使用してのみ変更できます。詳細については、「Amazon ECS アカウント設定の変更」を参照してください。

2020 年 10 月 1 日から 2020 年 11 月 2 日の間に、IPv6 が有効なサブネットで awsvpc ネットワークモードを使用してタスクを実行している場合、タスクが実行されていたリージョンの既定の dualStackIPv6 アカウント設定は disabled です。この条件が満たされない場合、リージョンのデフォルト dualStackIPv6 設定は enabled です。

デフォルト: disabled。

コンソールを使用して Amazon ECS のアカウント設定を表示する

コンソールでアカウント設定を表示して、アクセスできる機能を確認します。

> **Important**
>
> dualStackIPv6、fargateFIPSMode、fargateTaskRetirementWaitPeriod のアカウントの設定は、AWS CLI を使用してのみ表示または変更できます。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. 上部にあるナビゲーションバーで、アカウント設定を表示するリージョンを選択します。
3. ナビゲーションペインで [Account Settings] (アカウント設定) を選択します。

Amazon ECS アカウント設定の変更

アカウント設定を変更して Amazon ECS 機能にアクセスします。

`guardDutyActivate` パラメータは Amazon ECS では読み取り専用で、Amazon ECS アカウントのセキュリティ管理者によってランタイムモニタリングが有効になっているか無効になっているかを示します。GuardDuty は、ユーザーに代わってこのアカウント設定を制御します。詳細については、「Runtime Monitoring で Amazon ECS ワークロードを保護する」を参照してください。

> **Important**
>
> `dualStackIPv6`、`fargateFIPSMode`、`fargateTaskRetirementWaitPeriod` のアカウントの設定は、AWS CLI を使用してのみ表示または変更できます。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. 上部にあるナビゲーションバーで、アカウント設定を表示するリージョンを選択します。
3. ナビゲーションペインで [Account Settings] (アカウント設定) を選択します。
4. [Update] (更新) を選択します。
5. 各 EC2 インスタンスの awsvpc ネットワークモードで実行できるタスク数を増減するには、[AWSVPC トランキング] で [AWSVPC トランキング] を選択します。
6. クラスターで CloudWatch Container Insights をデフォルトで使用、または使用を停止するには、CloudWatch Container Insights オブザーバビリティ で、次のいずれかのオプションを選択します。
   - オブザーバビリティが強化された Container Insights を使用するには、[オブザーバビリティが強化された Container Insights] を選択します。
   - Container Insights を使用するには、[Container Insights] を選択します。
   - Container Insights の使用を停止するには、[オフ]を選択します。
7. タグ付け認可を有効または無効にするには、[リソースのタグ付け認可] で、[リソースのタグ付け認可] を選択または選択解除します。
8. [Save changes] (変更の保存) をクリックします。
9. 確認画面で [Confirm (確認)] を選択すると、選択内容が保存されます。

次のステップ

オブザーバビリティが強化された Container Insights または Container Insights を有効にした場合、オプションで既存のクラスターを更新してその機能を使用できます。詳細については、「Amazon ECS クラスターを更新する」を参照してください。

デフォルトの Amazon ECS アカウント設定の復元

AWS Management Console を使用して、Amazon ECS アカウント設定をデフォルトに戻せます。

[Revert to account default] (アカウントのデフォルトに戻す) オプションは、アカウント設定がデフォルト設定ではなくなった場合にのみ使用できます。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. 上部にあるナビゲーションバーで、アカウント設定を表示するリージョンを選択します。
3. ナビゲーションペインで [Account Settings] (アカウント設定) を選択します。
4. [Update] (更新) を選択します。
5. [Revert to account default] (アカウントのデフォルトに戻す) を選択します。
6. 確認画面で [Confirm (確認)] を選択すると、選択内容が保存されます。

AWS CLI を使用した Amazon ECS アカウント設定の管理

アカウント設定は、Amazon ECS API、AWS CLI、または SDK を使用して管理することができます。`dualStackIPv6`、`fargateFIPSMode`、`fargateTaskRetirementWaitPeriod` のアカウント設定は、それらのツールを使用してのみ表示または変更できます。

タスク定義に使用できる API アクションの詳細については、「Amazon Elastic Container Service API リファレンス」の「アカウント設定アクション」を参照してください。

アカウントのすべてのユーザーまたはロールのデフォルトアカウント設定を変更するには、以下のいずれかのコマンドを使用します。これらの変更は、ユーザーまたはロールがこれらの設定を明示的に上書きしない限り、AWS アカウント全体に適用されます。

- put-account-setting-default (AWS CLI)

```
aws ecs put-account-setting-default --name serviceLongArnFormat --value enabled --
region us-east-2
```

  このコマンドを使用して、他のアカウント設定を変更することもできます。そのためには、`name` パラメータを対応するアカウント設定に置き換えます。

- Write-ECSAccountSetting (AWS Tools for Windows PowerShell)

```
Write-ECSAccountSettingDefault -Name serviceLongArnFormat -Value enabled -Region us-
east-1 -Force
```

ユーザーアカウントのアカウント設定を変更するには (AWS CLI)

自分のユーザーのアカウント設定を変更するには、以下のいずれかのコマンドを使用します。ルートユーザーとしてこれらのコマンドを使用する場合、ユーザーまたはロールが対象の設定を明示的に上書きしない限り、この変更内容が AWS アカウント全体に適用されます。

- put-account-setting (AWS CLI)

  ```
  aws ecs put-account-setting --name serviceLongArnFormat --value enabled --region us-
  east-1
  ```

  このコマンドを使用して、他のアカウント設定を変更することもできます。そのためには、name パラメータを対応するアカウント設定に置き換えます。
- Write-ECSAccountSetting (AWS Tools for Windows PowerShell)

  ```
  Write-ECSAccountSetting -Name serviceLongArnFormat -Value enabled -Force
  ```

特定のユーザーまたはロールのアカウント設定を変更するには (AWS CLI)

特定のユーザーまたはロールのアカウント設定を変更するには、以下のいずれかのコマンドを使用して、リクエストの中でユーザー、ロール、またはルートユーザーの ARN を指定します。

- put-account-setting (AWS CLI)

  ```
  aws ecs put-account-setting --name serviceLongArnFormat --value enabled --principal-
  arn arn:aws:iam::aws_account_id:user/principalName --region us-east-1
  ```

  このコマンドを使用して、他のアカウント設定を変更することもできます。そのためには、name パラメータを対応するアカウント設定に置き換えます。
- Write-ECSAccountSetting (AWS Tools for Windows PowerShell)

  ```
  Write-ECSAccountSetting -Name serviceLongArnFormat -Value enabled -PrincipalArn
   arn:aws:iam::aws_account_id:user/principalName -Region us-east-1 -Force
  ```

Amazon ECS の IAM ロール

IAM ロールは、特定の許可があり、 アカウントで作成できる IAM アイデンティティです。Amazon ECS では、コンテナやサービスなどの Amazon ECS リソースにアクセス許可を付与するロールを作成できます。

Amazon ECS が必要とするロールは、タスク定義の起動タイプと使用する機能によって異なります。次の表を参照して、Amazon ECS に必要な IAM ロールを決定します。

ロール	定義	必要な場合	詳細情報
タスク実行ロール	このロールにより、Amazon ECS がお客様に代わって他の AWS サービスを利用できるようにします。	タスクは AWS Fargate または外部インスタンスホストされています。また、 • Amazon ECR プライベートリポジトリからコンテナイメージをプルします。 • タスクを実行するアカウントとは別のアカウントの Amazon ECR プライベートリポジトリからコンテナイメージをプルします。 • `awslogs` ログドライバーを使用して CloudWatch Logs にコンテナログを送信します。 タスクは、AWS Fargate または	Amazon ECS タスク実行IAM ロール

ロール	定義	必要な場合	詳細情報
		Amazon EC2 インスタンスでホストされています。また、 • プライベートレジストリの認証を使用します。 • Runtime Monitoring を使用します。 • タスク定義は、Secrets Manager のシークレットまたは AWS Systems Manager Parameter Store のパラメータを使用して機密データを参照します。	
タスクロール	このロールにより、(コンテナ上の) アプリケーションコードが他の AWS サービスを使用できるようになります。	アプリケーションは、Amazon S3 などの他の AWS サービスにアクセスします。	Amazon ECS タスクの IAM ロール
コンテナインスタンスのロール	このロールにより、EC2 インスタンスまたは外部インスタンスをクラスターに登録できます。	タスクは Amazon EC2 インスタンスまたは外部インスタンスでホストされています。	Amazon ECS コンテナインスタンスの IAM ロール

ロール	定義	必要な場合	詳細情報
Amazon ECS Anywhere ロール	このロールにより、外部インスタンスが AWS API にアクセスできるようになります。	タスクは外部インスタンスでホストされています。	Amazon ECS Anywhere IAM ロール
Amazon ECS CodeDeploy ロール	このロールにより、CodeDeploy はサービスを更新できます。	CodeDeploy のブルー/グリーンデプロイタイプを使用して、サービスをデプロイします。	Amazon ECS CodeDeploy IAM ロール
Amazon ECS EventBridge ロール	このロールにより、EventBridge はサービスを更新できます。	EventBridge のルールとターゲットを使用してタスクをスケジュールします。	Amazon ECS EventBridge IAM ロール

ロール	定義	必要な場合	詳細情報
Amazon ECS インフラストラクチャロール	このロールにより、Amazon ECS はクラスター内のインフラストラクチャリソースを管理できます。	• Amazon EBS ボリュームを Fargate または EC2 起動タイプの Amazon ECS タスクにアタッチできます。インフラストラクチャロールにより、Amazon ECS はタスクの Amazon EBS ボリュームを管理できます。 • Amazon ECS Service Connect サービス間のトラフィックを暗号化するには、Transport Layer Security (TLS) を使用します。 • VPC Lattice ターゲットグループを作成する場合。	Amazon ECS インフラストラクチャ IAM ロール

Amazon ECSの タスク定義

タスク定義はアプリケーションのブループリントです。これは、アプリケーションを形成するパラメータと 1 つ以上のコンテナを記述する JSON 形式のテキストファイルです。

以下に示したのは、タスク定義の中で指定できるパラメータの一部です。

- 使用する起動タイプ、これによりタスクをホストするインフラストラクチャを決定
- タスクの各コンテナで使用する Docker イメージ
- 各タスクで、またはタスク内の各コンテナで使用する CPU とメモリの量
- メモリと CPU の要件
- タスクが実行されるコンテナのオペレーションシステム
- タスクのコンテナで使用する Docker ネットワーキングモード
- タスクで使用するログ記録設定
- コンテナが終了または失敗した場合にタスクを実行し続けるかどうか
- コンテナの開始時に実行するコマンド
- タスク内でコンテナが使用するデータボリューム
- タスクで使用される IAMロール

タスク定義パラメータの完全なリストについては、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」を参照してください。

タスク定義を作成したら、タスク定義をタスクまたはサービスとして実行できます。

- タスクはクラスター内のタスク定義のインスタンス化です。Amazon ECS でアプリケーションのタスク定義を作成後、クラスターで実行するタスクの数を指定できます。
- Amazon ECS サービスは、Amazon ECS クラスターで必要な数のタスクを同時に実行して維持します。仕組みとしては、タスクがいずれかの理由で失敗または停止した場合に、Amazon ECS サービススケジューラがタスク定義に基づいて別のインスタンスを起動することによって動作します。これは、それを置き換え、サービス内の必要な数のタスクを維持するために行われます。

トピック

- Amazon ECS タスク定義の状態

- Amazon ECS 用のアプリケーションの構築
- コンソールを使用した Amazon ECS タスク定義の作成
- コンソールを使用した Amazon ECS タスク定義の更新
- 新しいコンソールを使用した Amazon ECS タスク定義リビジョンの登録解除
- コンソールを使用した Amazon ECS タスク定義リビジョンの削除
- Amazon ECS タスク定義のユースケース
- Fargate 起動タイプでの Amazon ECS タスク定義パラメータ
- EC2 起動タイプの Amazon ECS タスク定義パラメータ
- Amazon ECS タスク定義テンプレート
- Amazon ECS のタスク定義の例

Amazon ECS タスク定義の状態

タスク定義を作成、登録解除、または削除すると、タスク定義の状態が変わります。タスク定義の状態は、コンソール上で、または DescribeTaskDefinition を使用して確認できます。

タスク定義は、以下の状態を取ることがあります。

ACTIVE

Amazon ECS に登録された後のタスク定義は ACTIVE の状態になります。ACTIVE 状態にあるタスク定義では、タスクを実行することやサービスを作成することができます。

INACTIVE

タスク定義の登録を解除すると、そのタスク定義の状態は ACTIVE から INACTIVE に遷移します。DescribeTaskDefinition を呼び出すと、INACTIVE 状態のタスク定義を取得できます。INACTIVE 状態のタスク定義を使用して、新しいタスクを実行することや新しいサービスを作成することはできません。既存のサービスやタスクには影響を与えません。

DELETE_IN_PROGRESS

タスク定義の削除をリクエストすると、そのタスク定義の状態が INACTIVE から DELETE_IN_PROGRESS に遷移します。タスク定義の状態が DELETE_IN_PROGRESS に遷移した後、Amazon ECS は、そのタスク定義がアクティブなタスクやデプロイによって参照されていないことを周期的に確認した上で、タスク定義を完全に削除します。DELETE_IN_PROGRESS 状態のタスク定義を使用して、新しいタスクを実行することや新しいサービスを作成することはでき

ません。タスク定義の削除は、既存のタスクやサービスに影響を与えることなく、任意のタイミングでリクエストできます。

DELETE_IN_PROGRESS 状態にあるタスク定義はコンソールに表示できます。また、DescribeTaskDefinition を呼び出すと、そのタスク定義を取得できます。

すべての INACTIVE タスク定義リビジョンを削除すると、タスク定義名はコンソールで表示されず、API でも返されません。タスク定義リビジョンが DELETE_IN_PROGRESS 状態にある場合、タスク定義名はコンソールに表示され、API で返されます。タスク定義名は Amazon ECS によって保持され、次回その名前を使用してタスク定義を作成するときにリビジョンがインクリメントされます。

タスク定義の管理に AWS Config を使用してしている場合は、すべてのタスク定義の登録について AWS Config による課金が行われます。登録解除については、ACTIVE の状態にある最新のタスク定義の解除に対してのみ課金されます。タスク定義の削除には料金はかかりません。料金の詳細については、「AWS Config 料金表」を参照してください。

削除をブロックできる Amazon ECS リソース

タスク定義リビジョンに依存する Amazon ECS リソースがある場合、タスク定義の削除リクエストは完了しません。次のリソースが原因で、タスク定義が削除されない場合があります。

- Amazon ECS スタンドアロンタスク – タスクを正常に動作させるには、タスク定義が必要です。
- Amazon ECS サービスタスク - タスクを正常に動作させるには、タスク定義が必要です。
- Amazon ECS サービスのデプロイとタスクセット - Amazon ECS のデプロイまたはタスクセットのスケーリングイベントが開始される場合は、タスク定義が必要です。

タスク定義が DELETE_IN_PROGRESS の状態のままである場合は、コンソールまたは AWS CLI を使用して、タスク定義の削除をブロックしているリソースを特定し、停止できます。

ブロックされたリソースが削除された後のタスク定義の削除

タスク定義の削除をブロックするリソースを削除すると、次のルールが適用されます。

- Amazon ECS タスク - タスク定義の削除は、タスクが停止されてから完了するまでに最大 1 時間かかる場合があります。
- Amazon ECS サービスのデプロイとタスクセット - タスク定義の削除は、デプロイまたはタスクセットが削除されてから完了するまでに最大 24 時間かかる場合があります。

Amazon ECS 用のアプリケーションの構築

アプリケーションのタスク定義を作成して、アプリケーションを構築します。タスク定義には、次のようなアプリケーションに関する情報を定義するパラメータが含まれます。

- 使用する起動タイプ、これによりタスクをホストするインフラストラクチャを決定します。

  EC2 起動タイプを使用する場合、インスタンスタイプも選択します。GPU などの一部のインスタンスタイプでは、さらに追加のパラメータを設定する必要があります。詳細については、「Amazon ECS タスク定義のユースケース」を参照してください。
- コンテナイメージには、アプリケーションコードと、アプリケーションコードの実行に必要なすべての依存関係が保持されます。
- タスクのコンテナで使用するネットワーキングモード

  ネットワークモードにより、タスクがネットワーク上で通信する方法が決定します。

  EC2 インスタンスで実行されるタスクについては、複数のオプションがありますが、その中でも awsvpc ネットワークモードの使用をお勧めします。awsvpc ネットワークモードを使用すると、コンテナネットワークが簡素化されます。また、アプリケーション間およびそのアプリケーションと VPC 内の他のサービスとの相互通信をより強力にコントロールできます。

  Fargate で実行されるタスクについては、awsvpc ネットワークモードのみが使用可能です。
- タスクで使用するログ記録設定。
- タスク内のコンテナで使用するデータボリューム。

タスク定義パラメータの完全なリストについては、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」を参照してください。

タスク定義を作成する際には、次のガイドラインに従ってください。

- 各タスク定義ファミリーは 1 つのビジネス目的にのみ使用してください。

  複数の種類のアプリケーションコンテナを同じタスク定義にグループ化する場合、それらのコンテナを個別にスケールすることはできません。例えば、ウェブサイトと API の両方が同じレートでスケールアウトする必要がある可能性はほとんどありません。トラフィックが増加すると、API コンテナとは異なる数のウェブコンテナが必要になります。これらの 2 つのコンテナが同じタスク定義にデプロイされる場合、各タスクは同じ数のウェブコンテナと API コンテナを実行します。

- 各アプリケーションのバージョンを、タスク定義ファミリー内のタスク定義リビジョンと一致させます。

  タスク定義ファミリー内では、各タスク定義リビジョンを、特定のコンテナイメージの設定のポイントインタイムスナップショットとみなします。これは、コンテナがアプリケーションコードの特定のバージョンを実行するために必要なすべてもののスナップショットであるのと似ています。

  アプリケーションコードのバージョン、コンテナイメージタグ、およびタスク定義リビジョンの間に 1 対 1 のマッピングがあることを確認してください。一般的なリリースプロセスには、git commit SHA でタグ付けされたコンテナイメージに変換される git commit が含まれます。その後、そのコンテナイメージタグは、独自の Amazon ECS タスク定義リビジョンを取得します。最後に、Amazon ECS サービスが更新され、新しいタスク定義リビジョンをデプロイするように指示されます。
- タスク定義ファミリーごとに異なる IAM ロールを使用します。

  各タスク定義を独自の IAM ロールで定義します。この推奨事項は、各ビジネスコンポーネントに独自のタスク定義ファミリーを提供するという推奨事項と合わせて実行される必要があります。これらのベストプラクティスを両方実装することで、各サービスが AWS アカウント内のリソースにどの程度アクセスできるかを制限できます。例えば、パスワードデータベースに接続するためのアクセス権を認証サービスに付与できます。同時に、注文サービスのみがクレジットカードの支払情報にアクセスできるようにすることもできます。

Amazon ECS コンテナイメージのベストプラクティス

コンテナイメージは、コンテナの構築方法に関する一連の指示です。コンテナイメージには、アプリケーションコードと、アプリケーションコードの実行に必要なすべての依存関係が保持されます。アプリケーションの依存関係には、アプリケーションコードが依存するソースコードパッケージ、インタープリタ型言語の言語ランタイム、および動的にリンクされたコードが依存するバイナリパッケージが含まれます。

コンテナイメージを設計および構築する際には、次のガイドラインに従ってください。

- すべてのアプリケーションの依存関係をコンテナイメージ内に静的ファイルとして保存することで、コンテナイメージを完成させます。

  コンテナイメージ内の何かを変更する場合は、変更内容を反映した新しいコンテナイメージを構築します。
- コンテナ内で単一のアプリケーションプロセスを実行します。

コンテナの有効期間は、アプリケーションプロセスが実行されている期間です。Amazon ECS は、クラッシュしたプロセスを置き換えると共に、置き換え後のプロセスをどこで起動するかを決定します。適切に完成されたイメージは、デプロイ全体の耐障害性を高めます。

- アプリケーションが SIGTERM を処理できるようにします。

  Amazon ECS は、タスクを停止する場合、まず SIGTERM シグナルをそのタスクに送信し、アプリケーションを終了してシャットダウンする必要があることを通知します。その後、Amazon ECS は SIGKILL のメッセージを送信します。アプリケーションが SIGTERM を無視した場合、Amazon ECS サービスはしばらく待ってからプロセスを終了する SIGKILL シグナルを送信する必要があります。

  アプリケーションが作業を完了するまでにかかる時間を特定して、アプリケーションが確実に SIGTERM シグナルに対応できるようにしてください。アプリケーションによるシグナル対応においては、アプリケーションがそれ以上新しい作業を取得するのをストップするとともに、進行中の作業を完了するか、または完了までに長い時間がかかる場合は、タスクの外部のストレージに未完了の作業を保存する必要があります。

- ログを stdout および stderr に書き込むように、コンテナ化されたアプリケーションを設定します。

  ログ処理をアプリケーションコードから分離することで、ログ処理をインフラストラクチャレベルでより柔軟に調整できるようになります。その一例として、ロギングシステムの変更があります。サービスを変更したり、新しいコンテナイメージを構築してデプロイする代わりに、設定の調整により対応できます。

- タグを使用してコンテナイメージをバージョニングします。

  コンテナイメージはコンテナレジストリに保存されます。レジストリ内の各イメージはタグによって識別されます。latest というタグがあります。このタグは、git リポジトリの HEAD と同様に、アプリケーションコンテナイメージの最新バージョンに対するポインターとして機能します。latest タグはテストのみに使用することが推奨されます。ベストプラクティスとして、ビルドごとにコンテナイメージに一意のタグを付けます。イメージの構築に使用された git コミットの git SHA を使用してイメージにタグ付けすることをお勧めします。

  コミットごとにコンテナイメージを構築する必要はありません。ただし、特定のコードコミットを本番環境にリリースするたびに、新しいコンテナイメージを構築することをお勧めします。また、イメージに対して、イメージ内のコードの git commit に対応するタグを付けることをお勧めします。イメージに git commit のタグを付けた場合、イメージが実行しているコードのバージョンをより迅速に見つけることができます。

また、Amazon Elastic Container Registry でイミュータブルなイメージタグをオンにすることをお勧めします。この設定では、タグがポイントするコンテナイメージを変更することはできません。代わりに、Amazon ECR は、新しいイメージを新しいタグにアップロードするよう強制します。詳細については、「Amazon ECR ユーザーガイド」の「イメージタグの変更可能性」を参照してください。

AWS Fargate で実行されるアプリケーションを構築する場合には、複数のコンテナを同一のタスク定義にデプロイするか、あるいは複数のタスク定義に個々のコンテナを別々にデプロイするかのいずれかを選択する必要があります。以下のような要件がある場合には、1 つのタスク定義にコンテナを配置することをお勧めします。

- 各コンテナが同じライフサイクルを共有している (つまり、起動と終了が同時に行われる)。
- 実行基盤となるホストが同じになるようにコンテナを実行する (つまり、あるコンテナが、localhost ポート上の別のコンテナを参照する) 必要がある。
- 各コンテナがリソースを共有している。
- コンテナでデータボリュームを共有している。

上記の要件がない場合は、複数のタスク定義でコンテナを個別にデプロイすることをお勧めします。これにより、各コンテナを個別にスケーリング、プロビジョニング、およびデプロビジョニングできます。

Amazon ECS タスクサイズのベストプラクティス

コンテナとタスクのサイズ決定は、スケーリングとキャパシティプランニングに不可欠な要素です。Amazon ECS では、CPU とメモリがキャパシティーに使用される 2 つのリソースメトリクスです。CPU 量 は、フル vCPU の 1024 分の 1 の単位で測定されます (1024 ユニットは 1 つの vCPU 全体に相当します)。メモリはメガバイト単位で測定されます。タスク定義では、リソースの予約と制限を設定できます。

予約を設定すると、タスクに最低限必要な量のリソースが設定されます。タスクは少なくとも要求された最低限の量のリソースを受け取ります。アプリケーションは、宣言された予約量よりも多くの CPU またはメモリを使用できる可能性があります。ただし、これには宣言した制限が適用されます。予約量を超えるリソースを使用することをバーストと呼びます。Amazon ECS では、予約量が保証されます。たとえば、Amazon EC2 インスタンスを使用してキャパシティを提供する場合、Amazon ECS は予約量を満足できないインスタンスにタスクを課しません。

制限は、コンテナまたはタスクが使用できる CPU ユニットまたはメモリの最大量です。この制限を超える CPU 量 を使用しようとすると、スロットリングが発生します。それ以上メモリを使おうとすると、コンテナは停止します。

これらの値の決定は簡単ではありません。これは、各アプリケーションに最も適した値は、そのアプリケーションのリソース要件に大きく依存するためです。適切にリソース要件を計画し、アプリケーション要件を正確に把握するには、アプリケーションの負荷テストを行うことが重要です。

ステートレスアプリケーション

ロードバランサーの背後にあるアプリケーションなど、水平スケーリングするタイプのステートレスアプリケーションでは、まずそのアプリケーションがリクエストを処理するときに消費するメモリの量を確認することをお勧めします。これは、`ps` や `top` などの従来のツール、あるいは CloudWatch Container Insights などのモニタリングソリューションを使用して実施できます。

CPU 予約を決定する際には、ビジネス要件を満たすにはアプリケーションをどのようにスケーリングすべきかを考慮すること。256 CPU ユニット (つまりフル vCPU の 4 分の 1) などの小さめの CPU 予約を行うことで、コストを最小限に抑えながらきめ細かくスケールアウトできます。ただしその場合、需要が急増した時にスケーリング速度が追い付かない可能性があります。CPU 予約量を増やすとより迅速にスケールイン/スケールアウトできるため、需要の急増にもスムーズに対応できます。ただし、CPU の予約量が多いほどコストが高くなりますのでご注意ください。

その他のアプリケーション

シングルトンワーカーやデータベースサーバーなど、水平スケーリングしないタイプのアプリケーションでは、利用可能な容量とコストが最も重要な考慮事項となります。サービスレベル目標達成のためのトラフィック処理にはどの程度のメモリと CPU 量が必要かを負荷テストで確認した上でメモリおよび CPU 量を決定する必要があります。Amazon ECS は、アプリケーションが十分な容量のあるホストに配置されるよう保証します。

EC2 起動タイプの Amazon ECS タスクネットワークオプション

Amazon EC2 インスタンスでホストされる Amazon ECS タスクのネットワーク動作は、タスク定義で定義されているネットワークモードに左右されます。Amazon ECS では、別のネットワークモードを使用する特別の必要性がある場合を除き、`awsvpc` ネットワークモードの使用を推奨します。

使用可能なネットワークモードは次のとおりです。

ネットワークモード	EC2 の Linux コンテナ	EC2 の Windows コンテナ	[Description] (説明)
`awsvpc`	あり	あり	このタスクには、独自の Elastic Network Interface (ENI) とプライマリプライベート IPv4 アドレスが割り当てられます。これにより、タスクに Amazon EC2 インスタンスと同じネットワークプロパティが与えられます。
`bridge`	あり	不可	タスクは、そのタスクをホストする各 Amazon EC2 インスタンス内で実行される、Linux 上の Docker の組み込み仮想ネットワークを使用します。Linux の組み込み仮想ネットワークでは、`bridge` Docker ネットワークドライバーが使用されます。これは、タスク定義でネットワークモードが指定されていない場合の、Linux のデフォルトのネットワークモードです。
`host`	あり	不可	タスクは、そのタスクをホストする Amazon EC2 インスタンスの ENI にコンテナポートを直接マッピングすることで Docker の組み込み仮想ネットワークをバイパスする、ホストのネットワークを使用します。ダイナミックポートマッピングは、このネットワークモードでは使用できません。このモードを使用するタスク定義内のコンテナには、特定の `hostPort` 番号を指定する必要があります。ホストのポート番号は、複数のタスクで使用できません。その結果として、1 つの Amazon EC2 インスタンスで同じタスク定義のタスクを複数実行することはできません。
`none`	あり	不可	このタスクには外部ネットワーク接続がありません。

ネットワークモード	EC2 の Linux コンテナ	EC2 の Windows コンテナ	[Description] (説明)
`default`	いいえ	あり	タスクは、そのタスクをホストする各 Amazon EC2 インスタンス内で実行される、Windows 上の Docker の組み込み仮想ネットワークを使用します。Windows の組み込み仮想ネットワークは `nat` Docker ネットワークドライバーを使用します。これは、タスク定義でネットワークモードが指定されていない場合の、Windows のデフォルトのネットワークモードです。

Linux の Docker ネットワークについて詳しくは、「Networking overview」(ネットワークの概要) および「Docker Documentation」(Docker ドキュメント) を参照してください。

Windows の Docker ネットワークについて詳しくは、Microsoft の「Containers on Windows Documentation」(Windows のコンテナドキュメント) の「Windows container networking」(Windows コンテナネットワーク) を参照してください。

Amazon ECS タスクにネットワークインターフェイスを割り当てる

`awsvpc` ネットワークモードで利用できるタスクネットワーキング機能により、Amazon EC2 インスタンスと同じネットワーキングプロパティが Amazon ECS タスクに提供されます。`awsvpc` ネットワークモードを使用すると、コンテナネットワークが簡素化されます。また、アプリケーション間およびそのアプリケーションと VPC 内の他のサービスとの相互通信をより強力にコントロールできます。`awsvpc` ネットワークモードによりコンテナのセキュリティも強化されます。これは、セキュリティグループやネットワークモニタリングツールを、タスク内でより詳細なレベルで利用できるためです。VPC フローログなどの各種 Amazon EC2 ネットワーキング機能により、タスクが送受信するトラフィックをモニタリングできます。さらに、同じタスクに属するコンテナが、`localhost` インターフェイス経由で通信できるようになります。

タスク向け Elastic Network Interface (ENI) は、Amazon ECS のフルマネージド型機能です。Amazon ECS により ENI が作成され、指定されたセキュリティグループが関連付けられているホスト Amazon EC2 インスタンスにアタッチされます。タスクは、Amazon EC2 インスタンスがプライマリネットワークインターフェイスで実行する場合と同じ方法で、ENI を介してネットワークト

ラフィックを送受信します。各タスクの ENI には、デフォルトでプライベート IPv4 アドレスが割り当てられます。VPC がデュアルスタックモードに対応していて、IPv6 CIDR ブロックを備えたサブネットを使用する場合、タスクの ENI も IPv6 アドレスを受け取ります。各タスクは、ENI を 1 つだけ持つことができます。

これらの ENI は、アカウントの Amazon EC2 コンソールに表示されます。アカウント側では ENI をデタッチしたり変更したりすることはできません。これは、実行中のタスクに関連付けられている ENI が誤って削除されないようにするためです。タスクの ENI のアタッチに関する情報は、Amazon ECS コンソールか、DescribeTasks API オペレーションで確認できます。タスクが停止した場合やサービスがスケールダウンした場合は、ENI がデタッチされて削除されます。

ENI 密度を上げる必要がある場合は、`awsvpcTrunking` アカウント設定を使用してください。また Amazon ECS は、コンテナインスタンスのトランクネットワークインターフェイスを作成およびアタッチします。トランクネットワークは Amazon ECS によって完全に管理されます。コンテナインスタンスを Amazon ECS クラスターから削除または登録解除するときに、トランク ENI は削除されます。`awsvpcTrunking` アカウント設定の詳細については、「前提条件」を参照してください。

タスク定義の `networkMode` パラメータで `awsvpc` を指定します。詳細については、「ネットワークモード」を参照してください。

次に、タスクの実行時またはサービスの作成時に、タスクを配置する 1 つ以上のサブネットと、ENI にアタッチする 1 つ以上のセキュリティグループを含む `networkConfiguration` パラメータを使用します。詳細については、「ネットワーク構成」を参照してください。タスクは、これらのサブネットとして、同じアベイラビリティーゾーン内の適切な Amazon EC2 インスタンスに配置されます。また、指定されたセキュリティグループが、タスク用にプロビジョニングされた ENI に関連付けられます。

Linux に関する考慮事項

Linux オペレーティングシステムを使用する場合は、以下の点を考慮してください。

- `awsvpc` モードで p5.48xlarge インスタンスを使用する場合、インスタンスで複数のタスクを実行することはできません。
- `awsvpc` ネットワークモード使用するタスクとサービスには、Amazon ECS サービスにリンクされたロールが必要です。このロールにより、ユーザーに代わってその他の AWS サービスを呼び出す許可を、Amazon ECS に付与できるようになります。このロールは、クラスターの作成、またはサービスの作成や更新を AWS Management Console から行う際に、自動的に作成されます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。サービスにリンクされたロールは、次の AWS CLI コマンドを使用して作成することもできます。

```
aws iam create-service-linked-role --aws-service-name ecs.amazonaws.com
```

- Amazon EC2 Linux インスタンスでは、awsvpc ネットワークモードを使用するタスクを実行するには、コンテナエージェントのバージョン 1.15.0 以降が必要です。Amazon ECS 最適化 AMI を使用している場合、インスタンスには、少なくとも ecs-init パッケージの 1.15.0-4 バージョン以降も必要です。
- enableDnsHostnames と enableDnsSupport オプションの両方が VPC で有効になっている場合、Amazon ECS は Amazon が提供する (内部) DNS ホスト名でタスクのホスト名を設定します。これらのオプションが有効でない場合、タスクの DNS ホスト名にはランダムな名前が付けられます。VPC の DNS 設定の詳細については、「Amazon VPC ユーザーガイド」の「VPC の DNS 属性を変更する」を参照してください。
- awsvpc ネットワークモードを使用する Amazon ECS タスクには、それぞれ独自の Elastic Network Interface (ENI) が提供されます。この ENI は、ENI をホストする Amazon EC2 インスタンスにアタッチされています。Amazon EC2 Linux インスタンスにアタッチできるネットワークインターフェイスの数には、デフォルトのクォータが設定されます。そのクォータに対して、プライマリネットワークインターフェイスは 1 個としてカウントされます。例えば、c5.large インスタンスのデフォルトでは、アタッチ可能な ENI の数は最大 3 個までです。このインスタンスのプライマリネットワークインターフェイスも、1 個としてカウントされます。さらに 2 つの ENI をインスタンスにアタッチできます。awsvpc ネットワークモードを使用する各タスクには ENI が必要なため、通常このインスタンスタイプでは、このようなタスクを 2 つのみ実行できます。各インスタンスタイプのデフォルトの ENI 制限については、「Amazon EC2 ユーザーガイド」の「インスタンスタイプのネットワークインターフェイスあたりの IP アドレス数」を参照してください。
- Amazon ECS では、高い ENI 密度がサポートされているインスタンスタイプを使用して、Amazon EC2 Linux インスタンスを起動します。awsvpcTrunking アカウント設定にオプトインし、これらのインスタンスタイプを使用して Amazon EC2 Linux インスタンスをクラスターに登録すると、対象のインスタンスで ENI のクオータが引き上げられます。これらの、クォータが引き上げられたインスタンスを使用することで、各 Amazon EC2 Linux インスタンスにさらに多くのタスクを配置できます。高い ENI 密度をトランキング機能で使用するには、Amazon EC2 インスタンスにコンテナエージェントのバージョン 1.28.1 以降が必要です。Amazon ECS 最適化 Linux AMI を使用している場合には、インスタンスに ecs-init パッケージの 1.28.1-2 バージョン以降も必要です。awsvpcTrunking アカウント設定のオプトインの詳細については、「アカウント設定による Amazon ECS 機能へのアクセス」を参照してください。ENI トランキングの詳細については、「Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす」を参照してください。

- Amazon EC2 Linux インスタンスで awsvpc ネットワークモードを使用するタスクをホストする場合、タスク ENI にはパブリック IP アドレスが付与されません。インターネットにアクセスするには、NAT ゲートウェイを使用するよう設定されたプライベートサブネットでタスクを起動する必要があります。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。インバウンドのネットワークアクセスは、プライベート IP アドレスを使用する VPC 内からのものか、その VPC からロードバランサーを経由させルーティングされたものである必要があります。パブリックサブネット内で起動されたタスクは、インターネットにアクセスできません。
- Amazon ECS は、ユーザーの Amazon EC2 Linux インスタンスにアタッチする ENI のみを認識します。ENI をインスタンスに手動でアタッチした場合は、十分なネットワークアダプタを持たないインスタンスに対しても、Amazon ECS がタスクの追加を試みる可能性があります。これはタスクでのタイムアウトを引き起こし、ステータスがプロビジョニング解除へ、さらに停止状態へと移行する可能性があります。インスタンスに対する ENI の手動によるアタッチは推奨されません。
- Amazon EC2 インスタンスは、awsvpc ネットワークモードでのタスク配置を検討する ecs.capability.task-eni 機能に登録する必要があります。ecs-init の 1.15.0-4 バージョン以降を実行するインスタンスは、自動的にこの属性に登録されます。
- Amazon EC2 Linux インスタンスに作成およびアタッチされた ENI は、手動でデタッチしたり、ユーザーのアカウントを使って変更したりすることはできません。これは、実行中のタスクに関連付けられている ENI が誤って削除されないようにするためです。タスクの ENI を解放するには、タスクを停止します。
- タスクを実行するときや、awsvpc ネットワークモードを使用するサービスを作成するときは、awsVpcConfiguration に指定できるサブネットには 16 個、セキュリティグループには 5 個という制限があります。詳細については、Amazon Elastic Container Service API リファレンスの「AwsVpcConfiguration」を参照してください。
- awsvpc ネットワークモードを使用してタスクが開始されると、タスク定義内のコンテナが開始される前に、各タスクに Amazon ECS コンテナエージェントによって追加の pause コンテナが作成されます。次に、amazon-ecs-cni-plugins CNI プラグインを実行して pause コンテナのネットワーク名前空間が設定されます。その後、エージェントによってタスク内の残りのコンテナが開始されます。こうすることで pause コンテナのネットワークスタックが共有されます。つまり、タスク内のすべてのコンテナは ENI の IP アドレスによってアドレス可能であり、localhost インターフェイス経由で相互に通信できます。
- サービスに含まれるタスクに、awsvpc ネットワークモードを使用するものがある場合は、Application Load Balancer と Network Load Balancer のみがサポートされます。このようなサービス用にターゲットグループを作成する場合は、ターゲットタイプとして ip を選択する必要があります。instance を使用しません。これは、awsvpc ネットワークモードを使用するタスク

は、Amazon EC2 Linux インスタンスではなく、ENI に関連付けられているためです。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。

- 使用中の DHCP オプション設定を変更するように VPC が更新された場合も、既存のタスクにこれらの変更を適用することはできません。これらのネットワーク設定を安全に変更するためには、変更内容を適用して新しいタスクを開始し、それらの動作が正常なことを確認した上で、既存のタスクを停止します。

Windows に関する考慮事項

Windows オペレーティングシステムを使用するときは、考慮事項を次に示します:

- Amazon ECS 最適化 Windows Server 2016 AMI を使用するコンテナインスタンスは、`awsvpc` ネットワークモードを使用するタスクをホストしません。Amazon ECS 最適化 Windows Server 2016 AMI、および `awsvpc` ネットワークネットワークモ ードをサポートする Windows AMI を含むクラスターを使用する場合、`awsvpc` ネットワークモードを使用するタスクは Windows 2016 Server インスタンスでは起動されません。代わりに、`awsvpc` ネットワークモードがサポートされるインスタンスで起動されます。
- Amazon EC2 Windows インスタンスでは、`awsvpc` ネットワークモードを使用する Windows コンテナに CloudWatch メトリクスを使用するには、バージョン `1.57.1` 以降のコンテナエージェントが必要です。
- `awsvpc` ネットワークモード使用するタスクとサービスには、Amazon ECS サービスにリンクされたロールが必要です。このロールにより、ユーザーに代わってその他の AWS サービスを呼び出す許可を、Amazon ECS に付与できるようになります。このロールは、クラスターを作成する際、または AWS Management Console でサービスを作成または更新すると、自動的に作成されます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。サービスにリンクされたロールは、次の AWS CLI コマンドを使用して作成することもできます。

```
aws iam create-service-linked-role --aws-service-name ecs.amazonaws.com
```

- Amazon EC2 Windows インスタンスでは、`awsvpc` ネットワークモードを使用するタスクを実行するには、コンテナエージェントのバージョン `1.54.0` 以降が必要です。インスタンスをブートストラップするときは、`awsvpc` ネットワークモードに必要なオプションを設定する必要があります。詳しくは、「the section called “コンテナインスタンスのブートストラップ”」を参照してください。
- VPC で `enableDnsHostnames` と `enableDnsSupport` オプションの両方が有効になっている場合、Amazon ECS は、Amazon が提供する (内部) DNS ホスト名を使用してタスクのホスト名を設

定します。これらのオプションが有効になっていない場合は、タスクの DNS ホスト名はランダムな名前に設定されます。VPC の DNS 設定の詳細については、「Amazon VPC ユーザーガイド」の「VPC の DNS 属性を変更する」を参照してください。

- awsvpc モードを使用する Amazon ECS タスクには、それぞれ独自の Elastic Network Interface (ENI) が提供されます。この ENI は、ENI をホストする Amazon EC2 Windows インスタンスにアタッチされています。Amazon EC2 Windows インスタンスへのアタッチが可能な、ネットワークインターフェイスの数には、デフォルトでクォータが設定されます。このクォータに対して、プライマリネットワークインターフェイスは 1 個としてカウントされます。例えば、 c5.large インスタンスのデフォルトでは、最大 3 個までの ENI がアタッチできます。このインスタンスのプライマリネットワークインターフェイスも、それら ENI の内の 1 個としてカウントされます。さらに 2 つの ENI をインスタンスにアタッチできます。awsvpc ネットワークモードを使用する各タスクには ENI が必要なため、通常、このインスタンスタイプでは、このようなタスクを 2 つのみ実行できます。各インスタンスタイプのデフォルトの ENI 制限については、「Amazon EC2 ユーザーガイド」の「インスタンスタイプのネットワークインターフェイスあたりの IP アドレス数」を参照してください。
- Amazon EC2 Windows インスタンスで awsvpc ネットワークモードを使用するタスクをホストする場合、タスク ENI にはパブリック IP アドレスが付与されません。インターネットにアクセスするには、NAT ゲートウェイを使用するよう設定されたプライベートサブネットで、タスクを起動します。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。インバウンドのネットワークアクセスは、プライベート IP アドレスを使用する VPC 内からのものか、VPC 内のロードバランサーを経由してルーティングされたものである必要があります。パブリックサブネット内で起動されたタスクは、インターネットにアクセスできません。
- Amazon ECS は、Amazon EC2 Windows インスタンスにアタッチした ENI だけを認識します。ENI をインスタンスに手動でアタッチした場合は、十分なネットワークアダプタを持たないインスタンスに対しても、Amazon ECS がタスクの追加を試みる可能性があります。これはタスクでのタイムアウトを引き起こし、ステータスがプロビジョニング解除へ、さらに停止状態へと移行する可能性があります。インスタンスに対する ENI の手動によるアタッチは推奨されません。
- Amazon EC2 Windows インスタンスは、awsvpc ネットワークモードでのタスク配置を検討する ecs.capability.task-eni 機能に登録する必要があります。
- Amazon EC2 Windows インスタンスに作成およびアタッチされた ENI は、手動で変更したり、デタッチしたりはできません。これは、実行中のタスクに関連付けられている ENI を、誤って削除してしまわないようにするためです。タスクの ENI を解放するには、タスクを停止します。
- awsvpc ネットワークモードを使用するタスクの実行時、もしくはサービスの作成時は、最大 16 個までのサブネットと 5 個までのセキュリティグループを awsVpcConfiguration 内

で指定できます。詳細については、Amazon Elastic Container Service API リファレンス の「AwsVpcConfiguration」を参照してください。

- awsvpc ネットワークモードを使用してタスクが開始されると、タスク定義内のコンテナが開始される前に、各タスクに Amazon ECS コンテナエージェントによって追加の pause コンテナが作成されます。次に、amazon-ecs-cni-plugins CNI プラグインを実行して pause コンテナのネットワーク名前空間が設定されます。その後、エージェントによってタスク内の残りのコンテナが開始されます。こうすることで pause コンテナのネットワークスタックが共有されます。つまり、タスク内のすべてのコンテナは ENI の IP アドレスによってアドレス可能であり、localhost インターフェイス経由で相互に通信できます。
- サービスに含まれるタスクに、awsvpc ネットワークモードを使用するものがある場合は、Application Load Balancer と Network Load Balancer のみがサポートされます。このようなサービス用にターゲットグループを作成する場合は、ターゲットタイプとして instance ではなく、ip を選択する必要があります。これは、awsvpc ネットワークモードを使用するタスクは、Amazon EC2 Windows インスタンスではなく、ENI に関連付けられているためです。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。
- 使用中の DHCP オプション設定を変更するように VPC が更新された場合も、既存のタスクにこれらの変更を適用することはできません。これらのネットワーク設定を安全に変更するためには、変更内容を適用して新しいタスクを開始し、それらの動作が正常なことを確認した上で、既存のタスクを停止します。
- EC2 Windows 構成で awsvpc ネットワークモードを使用する場合、以下はサポートされません。
  - デュアルスタック設定
  - IPv6
  - ENI トランキング

デュアルスタックモードでの VPC の使用

デュアルスタックモードで VPC を使用する場合、タスクは IPv4 または IPv6、あるいはその両方を経由して通信できます。IPv4 と IPv6 アドレスは、互いに独立しています。そのため、VPC 内で IPv4 と IPv6 のルーティングとセキュリティを別々に設定する必要があります。VPC をデュアルスタックモード用に設定する方法については、「Amazon VPC ユーザーガイド」の「既存の VPC を IPv4 から IPv6 に移行する」を参照してください。

VPC でインターネットゲートウェイまたは送信専用インターネットゲートウェイを設定した場合は、その VPC をデュアルスタックモードで使用できます。この設定により、IPv6 アドレスが割り当てられたタスクは、インターネットゲートウェイまたは送信専用インターネットゲートウェイを介し

て、インターネットへのアクセスが可能になります。NAT ゲートウェイはオプションです。詳細については、Amazon VPC ユーザーガイドの「インターネットゲートウェイ」および「Egress-only インターネットゲートウェイ」を参照してください。

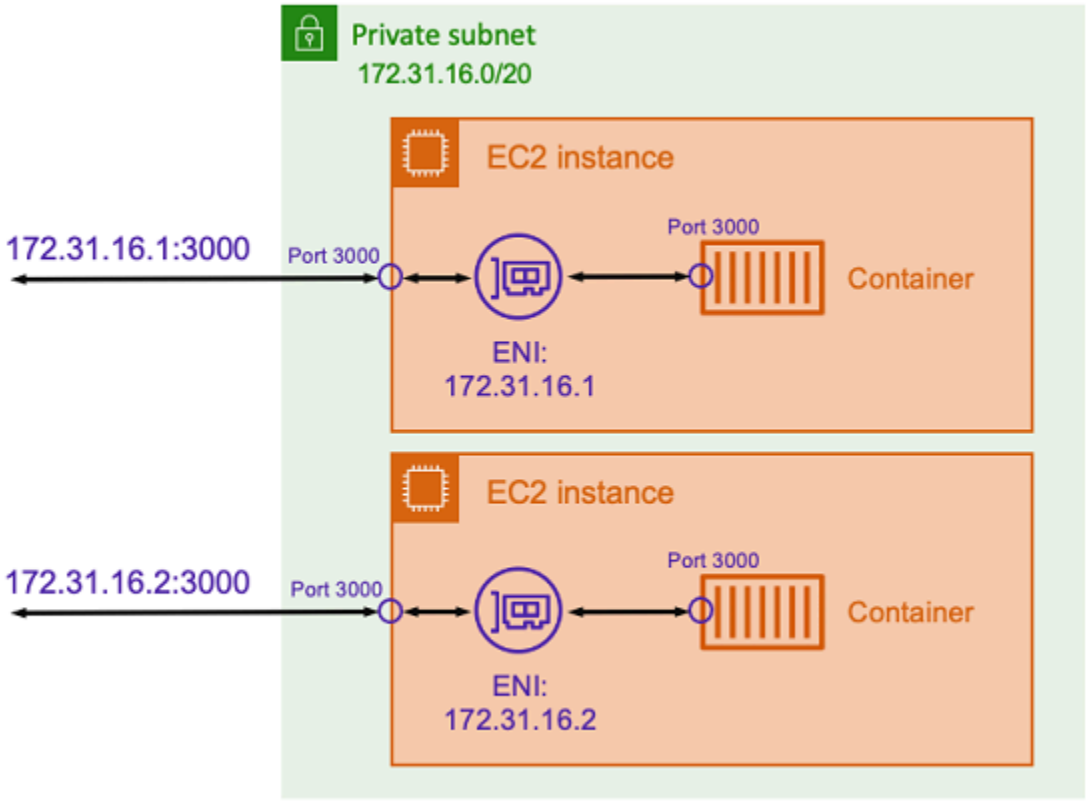
以下の条件が満たされた場合、Amazon ECS タスクには IPv6 アドレスが割り当てられます。

- タスクをホストしている Amazon EC2 インスタンスは、バージョン `1.45.0` 以降のコンテナエージェントを使用しています。インスタンスが使用しているエージェントのバージョンを確認し、必要に応じて更新する方法については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。
- `dualStackIPv6` アカウント設定が有効になります。詳細については、「アカウント設定による Amazon ECS 機能へのアクセス」を参照してください。
- タスクは `awsvpc` ネットワークモードを使用しています。
- VPC とサブネットは、IPv6 に対して有効になっています。この設定には、指定されたサブネットで作成されたネットワークインターフェイスが含まれます。VPC をデュアルスタックモードに設定する方法の詳細については、「Amazon VPC ユーザーガイド」 の「既存の VPC を IPv4 から IPv6 に移行する」および「Modify the IPv6 addressing attribute for your subnet」(サブネットの IPv6 アドレス属性を変更する) を参照してください。

Amazon ECS コンテナポートを EC2 インスタンスネットワークインターフェイスにマッピングする

`host` ネットワークモードは Amazon EC2 インスタンスでホストされている Amazon ECS タスクにのみサポートされています。Fargate で Amazon ECS を使用する場合はサポートされません。

`host` ネットワークモードは、Amazon ECS でサポートされている最も基本的なネットワークモードです。host モードでは、コンテナを稼働しているホストに直接関連付けられます。



上の図に示したようなポート `3000` でリッスンする Express アプリケーションで Node.js コンテナを実行していると仮定します。`host` ネットワークモードを使用すると、コンテナは基盤となるホストの Amazon EC2 インスタンスの IP アドレスを使用してポート 3000 でトラフィックを受信します。このモードを使用しないことをお勧めします。

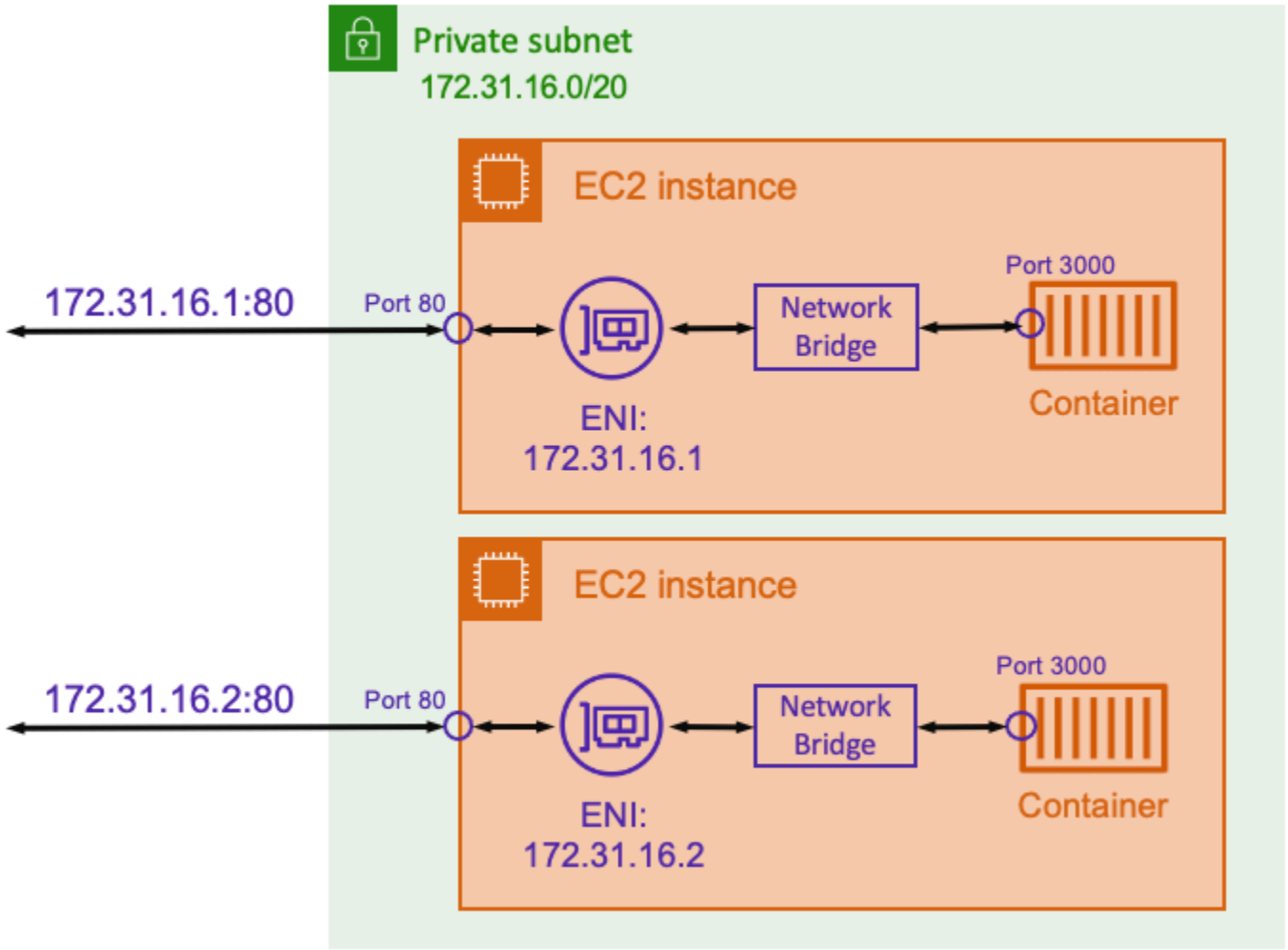
このネットワークモードを使用することには重大な欠点があります。各ホストで 1 つのタスクを複数インスタンス化することはできません。これは、Amazon EC2 インスタンスの必要なポートにバインドできるのは最初のタスクだけだからです。また、`host` ネットワークモードを使用している場合、コンテナポートを再マップする方法はありません。例えば、アプリケーションが特定のポート番号でリッスンする必要がある場合、ポート番号を直接再マップすることはできません。代わりに、アプリケーション構成を変更してポートの競合を管理する必要があります。

`host` ネットワークモードを使用する際には、セキュリティ上の問題もあります。このモードでは、コンテナがホストになりすますことができ、コンテナはホスト上のプライベートループバックネットワークサービスに接続できます。

Amazon ECS Linux タスクに Docker の仮想ネットワークを使用する

`bridge` ネットワークモードは Amazon EC2 インスタンスでホストされている Amazon ECS タスクにのみサポートされています。

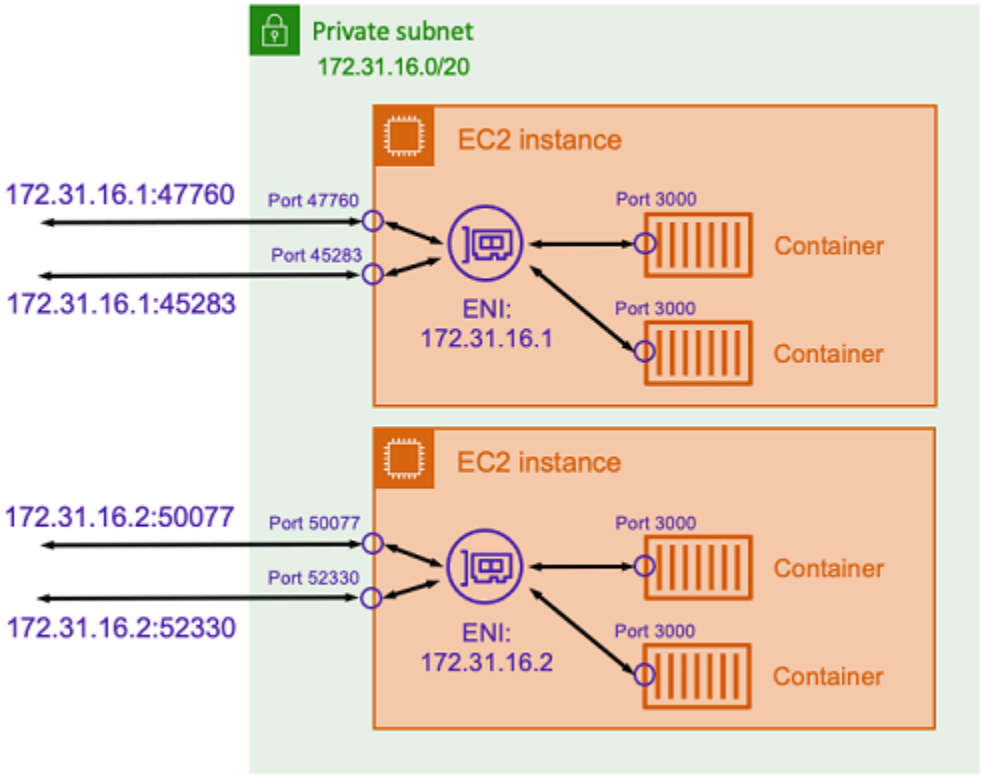
`bridge` モードでは、仮想ネットワークブリッジを使用してホストとコンテナのネットワーク間にレイヤーを作成します。これにより、ホストポートをコンテナポートに再マップするポートマッピングを作成できます。マッピングは静的または動的に実行することができます。



スタティックポートマッピングでは、どのホストポートをコンテナポートにマッピングするかを明示的に定義できます。上記の例を使用すると、ホスト上のポート `80` はコンテナのポート `3000` にマップされます。コンテナ化されたアプリケーションと通信するには、Amazon EC2 インスタンスの IP アドレスのポート `80` にトラフィックを送信します。コンテナ化されたアプリケーションの観点から見ると、ポート `3000` 上のインバウンドトラフィックがわかります。

トラフィックポートのみを変更する場合は、静的ポートマッピングが適しています。ただし、これには host ネットワークモードを使用する場合と同じ欠点があります。各ホストで 1 つのタスクを複数インスタンス化することはできません。これは、静的ポートマッピングでは、1 つのコンテナしかポート 80 にマッピングできないためです。

この問題を解決するには、次の図に示すように、bridge ネットワークモードと動的ポートマッピングを使用することを検討してください。



ポートマッピングでホストポートを指定しないことで、Docker にエフェメラルポート範囲から未使用のポートをランダムに選択させ、それをコンテナのパブリックホストポートとして割り当てることができます。例えば、コンテナのポート 3000 をリッスンしている Node.js アプリケーションには、Amazon EC2 ホスト上の 47760 のようにランダムに大きい番号のポートが割り当てられる場合があります。これにより、そのコンテナの複数のコピーをホスト上で実行できるようになります。さらに、各コンテナにはホスト上の独自のポートを割り当てることができます。コンテナの各コピーは、ポート 3000 でトラフィックを受信します。ただし、これらのコンテナにトラフィックを送信するクライアントは、ランダムに割り当てられたホストポートを使用します。

Amazon ECS は、各タスクにランダムに割り当てられたポートを追跡するのに役立ちます。これは、ロードバランサーのターゲットグループと AWS Cloud Map サービス検出を自動的に更新して、

タスクの IP アドレスとポートのリストを取得することによって行われます。このため、ダイナミックポートで bridge モードを使用するときのみにサポートされます。

ただし、bridge ネットワークモードを使用するデメリットの 1 つは、サービス間の通信をロックダウンするのが難しいことです。サービスはランダムで未使用のポートに割り当てられる可能性があるため、ホスト間で幅広いポート範囲を開く必要があります。ただし、特定のサービスが他の 1 つの特定のサービスとしか通信できないように特定のルールを作成するのは簡単ではありません。サービスには、セキュリティグループのネットワークルールに使用する特定のポートはありません。

Fargate 起動タイプの Amazon ECS タスクのネットワークオプション

デフォルトでは、Fargate 上のすべての Amazon ECS タスクには、プライマリプライベート IP アドレスを備えた Elastic Network Interface (ENI) が提供されます。パブリックサブネットを使用する際には、オプションで、タスクの ENI にパブリック IP アドレスを割り当てることができます。VPC がデュアルスタックモード向けに設定されていて、IPv6 CIDR ブロックを備えたサブネットを使用する場合、タスクの ENI にも IPv6 アドレスが割り当てられます。タスクには、一度に 1 つの ENI しか関連付けられません。また、同じタスクに属するコンテナでも、localhost インターフェイス経由での通信が可能になります。VPC とサブネットの詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC の仕組み」を参照してください。

Fargate のタスクがコンテナイメージをプルできるようにするには、そのタスクにインターネットへのルートが必要です。次に、タスクにインターネットへのルートがあるか検証する方法について説明します。

- パブリックサブネットを使用する場合、タスク ENI にパブリック IP アドレスを割り当てることができます。
- プライベートサブネットを使用する場合、サブネットに NAT ゲートウェイをアタッチできます。
- Amazon ECR でホストされるコンテナイメージを使用する場合、インターフェイスの VPC エンドポイントを使用するように Amazon ECR を設定でき、イメージのプルはタスクのプライベート IPv4 アドレス上で実行されます。詳細については、Amazon Elastic コンテナレジストリ ユーザーガイドの Amazon ECR Interface VPC エンドポイント(AWS PrivateLink)を参照してください。

各タスクにはそれぞれ独自の ENI が提供されるため、VPC フローログなどのネットワーキング機能を使用して、タスクとの間で送受信されるトラフィックをモニタリングできるようになります。詳細については、「Amazon VPC ユーザーガイド」の「VPC フローログを使用した IP トラフィックのログ記録」を参照してください。

AWS PrivateLink を活用することもできます。VPC インターフェースエンドポイントを設定することで、プライベート IP アドレスを通じて Amazon ECS の API にアクセスができます。AWS PrivateLink は、VPC と Amazon ECS 間のすべてのネットワークトラフィックを Amazon ネットワークに制限します。インターネットゲートウェイ、NAT デバイス、または仮想プライベートゲートウェイは必要ありません。詳細については、Amazon ECR インターフェイス VPC エンドポイント (AWS PrivateLink)をご参照ください。

AWS CloudFormation で `NetworkConfiguration` リソースを使用する方法の例については、「the section called “別のスタックを使用して Amazon ECS リソースを作成する”」を参照してください。

作成した ENI は、AWS Fargate によって完全に管理されます。加えて、Fargate へのアクセス許可を付与するために使用される IAM ポリシーが関連付けられます。Fargate プラットフォームバージョン `1.4.0` 以降を使用するタスクは、単一の ENI (タスク ENI と呼ばれる) を受け取ります。すべてのネットワークトラフィックは、VPC 内でこの ENI を通過します。このトラフィックは VPC フローログに記録されます。Fargate プラットフォームバージョン `1.3.0` 以前を使用するタスクには、タスク ENI に加えて Fargate が所有する ENI も別に割り当てられます。この ENI は、VPC フローログに表示されない一部のネットワークトラフィックに使用されます。次の表で、ネットワークトラフィックの動作と、プラットフォームバージョンごとに必要な IAM ポリシーについて説明します。

アクション	Linux プラットフォームバージョン **`1.3.0`** 以前でのトラフィックフロー	Linux プラットフォームバージョン **`1.4.0`** でのトラフィックフロー	Windows プラットフォームバージョン **`1.0.0`** でのトラフィックフロー	IAM アクセス許可
Amazon ECR ログイン認証情報の取得	Fargate が所有する ENI	タスク ENI	タスク ENI	タスク実行IAM ロール
イメージプル	タスク ENI	タスク ENI	タスク ENI	タスク実行IAM ロール
ログドライバーによるログの送信	タスク ENI	タスク ENI	タスク ENI	タスク実行IAM ロール

アクション	Linux プラットフォームバージョン **1.3.0** 以前でのトラフィックフロー	Linux プラットフォームバージョン **1.4.0** でのトラフィックフロー	Windows プラットフォームバージョン **1.0.0** でのトラフィックフロー	IAM アクセス許可
FireLens for Amazon ECS を介したログの送信	タスク ENI	タスク ENI	タスク ENI	タスク IAM ロール
Secrets Manager またはSystems Manager からシークレットの取得	Fargate が所有する ENI	タスク ENI	タスク ENI	タスク実行IAM ロール
Amazon EFS ファイルシステムトラフィック	利用不可	タスク ENI	タスク ENI	タスク IAM ロール
アプリケーションのトラフィック	タスク ENI	タスク ENI	タスク ENI	タスク IAM ロール

考慮事項

タスクネットワーキングを使用する際は、以下の点を考慮してください。

- Amazon ECS のサービスにリンクされたロールは、ユーザーの代わりにその他の AWS サービスを呼び出すアクセス許可 を Amazon ECS に付与します。このロールは、クラスターを作成する際、または AWS Management Console 内のサービスを作成または更新する際に自動的に作成されます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。サービスにリンクされたロールは、次の AWS CLI コマンドを使用して作成することもできます。

```
aws iam create-service-linked-role --aws-service-name ecs.amazonaws.com
```

- VPC で `enableDnsHostnames` と `enableDnsSupport` オプションの両方が有効になっている場合、Amazon ECS は、Amazon が提供する (内部) DNS ホスト名を使用してタスクのホスト名を設定します。これらのオプションが有効でない場合、タスクの DNS ホスト名にはランダムな名前が付けられます。VPC の DNS 設定の詳細については、「Amazon VPC ユーザーガイド」の「VPC の DNS 属性を変更する」を参照してください。
- `awsVpcConfiguration` には、最大 16 個のサブネットまでと、5 個のセキュリティグループまでが指定可能です。詳細については、Amazon Elastic Container Service API リファレンス の「AwsVpcConfiguration」を参照してください。
- Fargate によって作成およびアタッチされた ENI は、手動でデタッチしたり変更したりできません。これは、実行中のタスクに関連付けられている ENI が誤って削除されないようにするためです。タスクの ENI を解放するには、タスクを停止します。
- VPC サブネットが更新され、使用する DHCP オプションセットが変更された場合でも、VPC を使用する既存のタスクにこれらの変更を適用することはできません。新しい設定で新しいタスクを開始し、変更内容をテストしてロールバックの必要性がないことを確認した上で、古いタスクを停止しスムーズに移行を行います。
- 以下は、Linux の場合は Fargate プラットフォームバージョン `1.4.0` 以降、Windows の場合は `1.0.0` 以降で実行されるタスクに適用されます。デュアルスタックサブネットで起動されたタスクは、IPv4 アドレスおよび IPv6 アドレスを受け取ります。
- プラットフォームバージョン `1.4.0` 以降 (Linux の場合)、またはバージョン `1.0.0` (Windows の場合) を使用するタスクの場合、タスク ENI はジャンボフレームをサポートします。ネットワークインターフェイスは、最大転送単位 (MTU) で設定されます。MTU は、1 つのフレームに収まるペイロードの最大サイズです。MTU が大きいほど、1 つのフレーム内に収まるアプリケーションのペイロードが増えるため、フレームあたりのオーバーヘッドが減少し、効率が向上します。ジャンボフレームをサポートし、タスクと転送先とのネットワークパスでジャンボフレームをサポートすると、オーバーヘッドを削減できます。
- Fargate 起動タイプを使用するタスクのサービスは、Application Load Balancer と Network Load Balancer のみをサポートします。Classic Load Balancer はサポートされていません。ターゲットグループを作成する場合は、ターゲットタイプとして `instance` ではなく、`ip` を選択する必要があります。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。

デュアルスタックモードでの VPC の使用

デュアルスタックモードで VPC を使用する場合、タスクは IPv4 または IPv6、あるいはその両方を経由して通信できます。IPv4 アドレスと IPv6 アドレスは互いに独立しています。また VPC で IPv4

と IPv6 のルーティングとセキュリティを設定する必要があります。VPC をデュアルスタックモードに設定する方法の詳細については、Amazon VPC ユーザーガイドの「IPv6 への移行」を参照してください。

以下の条件が満たされた場合、Fargate の Amazon ECS タスクには IPv6 アドレスが割り当てられます。

- タスクを起動するリージョンで、タスクを起動する IAM プリンシパルの Amazon ECS `dualStackIPv6` アカウント設定がオン (`enabled`) になっていること。この設定は、API もしくは AWS CLI を使用してのみ変更できます。アカウントの特定の IAM プリンシパルに対してのみこの設定を有効にしてもよいし、あるいはアカウントのデフォルト設定を変更してアカウント全体に対して有効にすることもできます。詳細については、「アカウント設定による Amazon ECS 機能へのアクセス」を参照してください。
- VPC とサブネットが IPv6 に対して有効になっています。VPC をデュアルスタックモード用に設定する方法については、「Amazon VPC ユーザーガイド」の「既存の VPC を IPv4 から IPv6 に移行する」を参照してください。
- サブネットが、IPv6 アドレスの自動割り当てに有効になっています。サブネットの設定方法の詳細については、Amazon VPC ユーザーガイドの「サブネットの IPv6 アドレス属性を変更する」を参照してください。
- タスクまたはサービスは、Linux 用の Fargate プラットフォームバージョン `1.4.0` 以降を使用します。

VPC が、インターネットゲートウェイまたは出力専用インターネットゲートウェイを使用して設定されている場合には、IPv6 アドレスが割り当てられた Fargate の Amazon ECS タスクから、インターネットへのアクセスが可能になります。NAT ゲートウェイは必要ありません。詳細については、Amazon VPC ユーザーガイドの「インターネットゲートウェイ」および「Egress-only インターネットゲートウェイ」を参照してください。

Amazon ECS タスクのストレージオプション

Amazon ECS には、柔軟で使いやすく、コスト効率の良い各種データストレージオプションが用意されています。Amazon ECS は、以下のコンテナ向けデータボリュームオプションをサポートします。

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
Amazon Elastic Block Store (Amazon EBS)	Fargate、Amazon EC2	リナックス	スタンドアロンタスクにアタッチすることにより永続化できます。サービスが管理するタスクにアタッチすると一時的になります。	Amazon EBS ボリュームは、データ集約型のコンテナ化されたワークロード向けに、費用対効果と耐久性に優れた高性能なブロックストレージを提供します。一般的なユースケースには、データベース、仮想デスクトップ、ルートボリュームなどのトランザクションワークロード、またログ処理や ETL ワークロードなどのスループット集約型ワークロードがあります。詳細については、「Amazon ECS での Amazon EBS ボリュームの使用」を参照してください。

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
Amazon Elastic File System (Amazon EFS)	Fargate、Amazon EC2	リナックス	永続	Amazon EFS ボリュームは、Amazon ECS タスクで使用できるシンプルかつスケーラブルで永続的な共有ファイルストレージです。ファイルの追加および削除に合わせて自動的に拡大/縮小します。Amazon EFS ボリュームは同時実行をサポートするため、低レイテンシー、高スループット、書き込み後の読み取り整合性などのストレージ機能を必要とする水平スケーリングタイプのコンテナ化されたアプリケーションに適しています。一般的なユースケースには、データ分析、メディア

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
				処理、コンテンツ管理、ウェブサービスなどのワークロードが含まれます。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
Amazon FSx for Windows File Server	Amazon EC2	Windows	永続	FSx for Windows File Server ボリュームは、永続的、分散型、共有型、および静的なファイルストレージを必要とする Windows タスクのプロビジョニングに使用できる、フルマネージド型 Windows ファイルサーバー を提供します。一般的なユースケースには、アプリケーションの出力を保存するためにローカルフォルダーを永続ストレージとして必要とする.NET アプリケーションなどがあります。Amazon FSx for Windows File Server では、コンテナ内にローカルフォルダが用意され

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
				ており、SMB 共有によりバックアップされている同一のファイルシステム上で複数のコンテナが読み取り/書き込みを行うことができます。詳細については、「Amazon ECS での FSx for Windows File Server ボリュームの使用」を参照してください。

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
Docker ボリューム	Amazon EC2	Windows、Linux	永続	Docker ボリュームは Docker コンテナランタイムの機能の一つで、ホストのファイルシステムからディレクトリをマウントすることでコンテナにデータを保持することができます。Docker ボリュームドライバー (プラグインとも呼ばれる) は、コンテナボリュームを外部ストレージシステムと統合するのに使用されます。Docker ボリュームは、サードパーティードライバーまたは組み込みの `local` ドライバーで管理できます。Docker ボリュームの一般的なユースケースには、永

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
				続的データボリュームの提供や、同じコンテナインスタンスの異なるコンテナ上の別々の場所でのボリュームの共有などが含まれます。詳細については、「Amazon ECS での Docker ボリュームの使用」を参照してください。

データボリューム	サポートされている起動タイプ	サポートされるオペレーティングシステム	ストレージの永続化	ユースケース
バインドマウント	Fargate、Amazon EC2	Windows、Linux	一時的	バインドマウントは、コンテナにマウントされた Amazon EC2 インスタンスや AWS Fargate などのホスト上にあるファイルまたはディレクトリで構成されます。バインドマウントの一般的なユースケースには、ソースコンテナのボリュームを同じタスク内の他のコンテナと共有したり、あるいはホストボリュームや空のボリュームを 1 つもしくは複数のコンテナにマウントすることが含まれます。詳細については、「Amazon ECS でのバインドマウントの使用」を参照してください。

Amazon ECS での Amazon EBS ボリュームの使用

Amazon Elastic Block Store (Amazon EBS) ボリュームは、可用性、費用対効果と耐久性に優れた、データ集約型ワークロード向けの高性能ブロックストレージです。Amazon EBS ボリュームは、高スループットなトランザクション集約型アプリケーションの Amazon ECS タスクに使用できます。

スタンドアロンタスクの起動時に、1 つの EBS ボリュームをタスクにアタッチする設定を提供できます。サービスの作成または更新時に、Amazon ECS サービスが管理する各タスクについて、タスクごとに 1 つの EBS ボリュームをアタッチする設定を提供できます。

タスク定義ではなく起動時にボリューム設定を提供することで、特定のデータボリュームタイプや特定の EBS ボリューム設定に制限されないタスク定義を作成できます。その後、作成したタスク定義をさまざまなランタイム環境で再利用できます。たとえば、本番環境向けワークロードのデプロイ時には、本番前のテスト環境よりも高いスループットを提供できます。

Amazon ECS タスクにアタッチされた Amazon EBS ボリュームは、お客様に代わって Amazon ECS で管理します。データ保護のため、ボリュームは AWS Key Management Service (AWS KMS) キーで暗号化できます。新しい空のボリュームを設定してアタッチすることもできるし、あるいはスナップショットを使用して既存のボリュームからデータをロードすることもできます。

ボリュームのパフォーマンスのモニタリングには、Amazon CloudWatch メトリクスを使用できます。Amazon EBS ボリューム向け Amazon ECS メトリクスの詳細については、「Amazon ECS CloudWatch メトリクス」および「Amazon ECS Container Insights メトリクス」を参照してください。

Amazon EBS ボリュームのタスクへのアタッチは、Amazon ECS をサポートするすべての商用および中国 AWS リージョンでサポートされています。

Amazon EBS ボリュームのその他の詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS ボリューム」を参照してください。

サポートされているオペレーティングシステムと起動タイプ

次の表は、サポートされているオペレーティングシステムと起動タイプの設定を示しています。

起動タイプ	リナックス	Windows
Fargate	Amazon EBS ボリュームは、プラットフォームバージョン `1.4.0` 以降 (Linux) でサポートされます。詳細につい	サポートされていません

起動タイプ	リナックス	Windows
	ては、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。	
EC2	Amazon ECS に最適化された Amazon マシンイメージ (AMI) を使用して Nitro ベースの Linux インスタンスでホストされるタスク。インスタンスタイプの詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスタイプ」を参照してください。 Amazon EBS ボリュームは、ECS に最適化された AMI 20231219 以降でサポートされています。詳細については、「Amazon ECS に最適化された AMI メタデータを取得する」を参照してください。	Amazon ECS に最適化された Amazon マシンイメージ (AMI) を使用して Nitro ベースの Linux インスタンスでホストされるタスク。インスタンスタイプの詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスタイプ」を参照してください。 Amazon EBS ボリュームは、ECS に最適化された AMI 20241017 以降でサポートされています。詳細については、「Amazon ECS に最適化された Windows AMI メタデータを取得する」を参照してください。

考慮事項

Amazon EBS ボリュームを使用する場合には、以下の点を考慮してください。

- Amazon EBS ボリュームは、 `use1-az3` アベイラビリティーゾーン内の Fargate 起動タイプの Amazon ECS タスクへのアタッチメント向けに設定することはできません。
- マグネティックタイプ (`standard`) の Amazon EBS ボリュームは、Fargate でホストされるタスクではサポートされていません。Amazon EBS ボリュームタイプの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS ボリューム」を参照してください。
- Amazon ECS インフラストラクチャ IAM ロールは、デプロイ時にボリュームを設定するサービスまたはスタンドアロンタスクを作成するときに必要です。AWS マネージド型

`AmazonECSInfrastructureRolePolicyForVolumes` IAM ポリシーをロールにアタッチしてもよいし、あるいはマネージド型ポリシーをガイドとして使用して、所定のニーズを満たすアクセス許可を持つ独自のポリシーを作成してアタッチすることもできます。詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。

- 各 Amazon ECS タスクには最大 1 つの Amazon EBS ボリュームをアタッチできますが、新しいボリュームである必要があります。既存の Amazon EBS ボリュームをタスクにアタッチすることはできません。ただし、既存のボリュームのスナップショットを使用してデプロイ時に新しい Amazon EBS ボリュームを設定することはできます。
- デプロイ時に Amazon EBS ボリュームを設定できるのは、ローリングアップデートデプロイタイプとレプリカスケジュール戦略を使用するサービスのみです。
- マウントした Amazon EBS ボリュームにタスク内のコンテナから書き込みを行うには、コンテナをルートユーザーとして実行する必要があります。
- Amazon ECS は、アタッチされたボリュームにリザーブドタグ `AmazonECSCreated` および `AmazonECSManaged` を自動で追加します。これらのタグをボリュームから削除すると、Amazon ECS がユーザーに代わってボリュームを管理できなくなりますので注意してください。Amazon EBS ボリュームのタグ付けの詳細については、「Amazon EBS ボリュームのタグ付け」を参照してください。Amazon ECS リソースへのタグ付けの詳細については、「Amazon ECS リソースのタグ付け」を参照してください。
- パーティションを含む Amazon EBS ボリュームのスナップショットからのボリュームのプロビジョニングはサポートされていません。
- サービスによって管理されるタスクにアタッチされたボリュームは保存されず、タスクが終了すると必ず削除されます。
- AWS Outposts で実行される Amazon ECS タスクにアタッチするように Amazon EBS ボリュームを設定することはできません。

ボリューム設定を Amazon ECS のタスク定義の起動時刻まで延期する

Amazon EBS ボリュームを設定してタスクにアタッチするには、タスク定義でマウントポイント設定を指定して、ボリュームに名前を付ける必要があります。また、Amazon EBS ボリュームはタスク定義内でアタッチするようには設定ができないため、`configuredAtLaunch` を `true` に設定する必要があります。代わりに、Amazon EBS ボリュームはデプロイ時にアタッチするように設定します。

AWS Command Line Interface (AWS CLI) を使用してタスク定義を登録するには、テンプレートを JSON ファイルとして保存し、そのファイルを `register-task-definition` コマンドの入力として渡します。

AWS Management Consoleを使用してタスク定義を作成および登録するには、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

以下のタスク定義に、タスク定義内の mountPoints および volumes オブジェクト用構文を示します。タスク定義パラメータの詳細については、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」を参照してください。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

リナックス

```
{
    "family": "mytaskdef",
    "containerDefinitions": [
        {
            "name": "nginx",
            "image": "public.ecr.aws/nginx/nginx:latest",
            "networkMode": "awsvpc",
           "portMappings": [
                {
                    "name": "nginx-80-tcp",
                    "containerPort": 80,
                    "hostPort": 80,
                    "protocol": "tcp",
                    "appProtocol": "http"
                }
            ],
            "mountPoints": [
                {
                    "sourceVolume": "myEBSVolume",
                    "containerPath": "/mount/ebs",
                    "readOnly": true
                }
            ]
        }
    ],
    "volumes": [
        {
            "name": "myEBSVolume",
            "configuredAtLaunch": true
        }
    ],
    "requiresCompatibilities": [
        "FARGATE", "EC2"
```

```
    ],
    "cpu": "1024",
    "memory": "3072",
    "networkMode": "awsvpc"
}
```

Windows

```
{
    "family": "mytaskdef",
     "memory": "4096",
     "cpu": "2048",
    "family": "windows-simple-iis-2019-core",
    "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
    "runtimePlatform": {"operatingSystemFamily": "WINDOWS_SERVER_2019_CORE"},
    "requiresCompatibilities": ["EC2"]
    "containerDefinitions": [
        {
             "command": ["New-Item -Path C:\\inetpub\\wwwroot\\index.html -Type file
 -Value '<html> <head> <title>Amazon ECS Sample App</title> <style>body {margin-top:
 40px; background-color: #333;} </style> </head><body> <div style=color:white;text-
align:center> <h1>Amazon ECS Sample App</h1> <h2>Congratulations!</h2> <p>Your
 application is now running on a container in Amazon ECS.</p>'; C:\\ServiceMonitor.exe
 w3svc"],
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "essential": true,
            "cpu": 2048,
            "memory": 4096,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "name": "sample_windows_app",
            "portMappings": [
                {
                    "hostPort": 443,
                    "containerPort": 80,
                    "protocol": "tcp"
                }
            ],
            "mountPoints": [
                {
```

```
                    "sourceVolume": "myEBSVolume",
                    "containerPath": "drive:\ebs",
                    "readOnly": true
                }
            ]
        }
    ],
    "volumes": [
        {
            "name": "myEBSVolume",
            "configuredAtLaunch": true
        }
    ],
    "requiresCompatibilities": [
        "FARGATE", "EC2"
    ],
    "cpu": "1024",
    "memory": "3072",
    "networkMode": "awsvpc"
}
```

`mountPoints`

タイプ: オブジェクト配列

必須: いいえ

コンテナでのデータボリュームのマウントポイント。このパラメータは creat-container Docker API の `Volumes` にマッピングされ、docker run の `--volume` オプションにマッピングされます。

Windows コンテナは `$env:ProgramData` と同じドライブに全部のディレクトリをマウントできます。Windows コンテナは、別のドライブにディレクトリをマウントすることはできません。また、マウントポイントは複数のドライブにまたがることはできません。Amazon EBS ボリュームを Amazon ECS タスクに直接アタッチするには、マウントポイントを指定する必要があります。

`sourceVolume`

タイプ: 文字列

必須: はい (`mountPoints` を使用する場合)

マウントするボリュームの名前。

containerPath

型: 文字列

必須: はい (mountPoints を使用する場合)

ボリュームをマウントするコンテナ内のパス。

readOnly

型: ブール値

必須: いいえ

この値が true の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が false の場合、コンテナはボリュームに書き込むことができます。デフォルト値は false です。

Windows オペレーティングシステムを実行している EC2 インスタンスで実行されるタスクの場合、 値をデフォルト の false のままにします。

name

タイプ: 文字列

必須: いいえ

ボリュームの名前。最大 255 文字の英字 (大文字と小文字の区別あり)、数字、ハイフン (-)、アンダースコア (_) を使用できます。この名前は、コンテナ定義 mountPoints オブジェクトの sourceVolume パラメータで参照されます。

configuredAtLaunch

型: ブール値

必須: はい。EBS ボリュームをタスクに直接アタッチしたい場合には必須です。

起動時にボリュームを設定可能にするかどうかを指定します。true に設定すると、スタンドアロンタスクを実行するとき、またはサービスを作成または更新するときにボリュームを設定できます。false に設定すると、タスク定義内で別のボリューム設定を提供することはできません。タスクにアタッチする Amazon EBS ボリュームを設定するには、このパラメータを true に設定する必要があります。

Amazon ECS の Amazon EBS ボリュームに保存されているデータの暗号化

AWS Key Management Service (AWS KMS) を使用して、データを保護する暗号化キーを作成および管理できます。Amazon EBS ボリュームは、保管時には AWS KMS keys を使用して暗号化されます。以下の種類のデータが暗号化されます。

- ボリュームに保管されているデータ
- ディスク I/O
- ボリュームから作成されるスナップショット
- スナップショットから作成される新しいボリューム

Amazon EBS 暗号化をデフォルトで設定できます。これにより、作成されてタスクにアタッチされる新しいボリュームはすべて、アカウントに設定した KMS キーを使用して暗号化されます。Amazon EBS の暗号化およびデフォルトの暗号化については、「Amazon EC2 ユーザーガイド」の「Amazon EBS の暗号化」を参照してください。

タスクにアタッチされている Amazon EBS ボリュームは、エイリアス `alias/aws/ebs` の付いたデフォルトのAWS マネージドキーか、もしくはカスタマーマネージド型対称キーを使用して暗号化できます。デフォルトの AWS マネージドキー はそれぞれの AWS リージョン ごとの AWS アカウント に対して固有で、自動的に作成されます。カスタマーマネージド型対称キーを作成するには、「AWS KMS デベロッパーガイド」の「対称暗号化 KMS キーの作成」のステップに従います。

カスタマーマネージド型 KMS キーのポリシー

カスタマーマネージド型キーを使用してタスクにアタッチされている EBS ボリュームを暗号化するには、KMS キーポリシーを設定して、ボリューム設定に使用する IAM ロールにキーの使用に必要な権限を付与する必要があります。キーポリシーには、`kms:CreateGrant` と `kms:GenerateDataKey*` 両方のアクセス許可を含める必要があります。スナップショットを使用して作成されたボリュームを暗号化するには、`kms:ReEncryptTo` および `kms:ReEncryptFrom` のアクセス許可が必要です。アタッチする新しい空のボリュームのみを設定して暗号化する場合は、`kms:ReEncryptTo` および `kms:ReEncryptFrom` のアクセス許可は除外できます。

以下の JSON スニペットは、KMS キーポリシーにアタッチするキーポリシーステートメントを示します。これらのステートメントにより、Amazon ECS がキーを使用して EBS ボリュームを暗号化できるようになります。ここに挙げたポリシーステートメントを実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。他の場合と同様に、必要な権限のみを設定してください。

```
{
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::111122223333:role/ecsInfrastructureRole" },
      "Action": "kms:DescribeKey",
      "Resource":"*"
    },
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::111122223333:role/ecsInfrastructureRole" },
      "Action": [
      "kms:GenerateDataKey*",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom"
      ],
      "Resource":"*",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "aws_account_id",
          "kms:ViaService": "ec2.region.amazonaws.com"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": "aws:ebs:id"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": { "AWS": "arn:aws:iam::111122223333:role/ecsInfrastructureRole" },
      "Action": "kms:CreateGrant",
      "Resource":"*",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": "aws_account_id",
          "kms:ViaService": "ec2.region.amazonaws.com"
        },
        "ForAnyValue:StringEquals": {
          "kms:EncryptionContextKeys": "aws:ebs:id"
        },
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
```

キーポリシーとアクセス許可について詳しくは、「AWS KMS 開発者ガイド」の「AWS KMS のキーポリシー」と「AWS KMS アクセス許可」を参照してください。キーのアクセス許可に関連する EBS ボリュームアタッチメントのトラブルシューティングについては、「Amazon ECS タスクへの Amazon EBS ボリュームのアタッチに関するトラブルシューティング」を参照してください。

Amazon ECS のデプロイ時に Amazon EBS ボリューム設定を指定する

`configuredAtLaunch` パラメータを `true` に設定してタスク定義を登録すると、デプロイ時にスタンドアロンタスクを実行するとき、またはサービスを作成または更新するときに Amazon EBS ボリュームを設定できます。

ボリュームを設定するには、Amazon ECS API を使用するか、あるいは次の AWS CLI コマンドの入力として JSON ファイルを渡します。

- スタンドアロン ECS タスクを実行するための `run-task`。
- 特定のコンテナインスタンスでスタンドアロン ECS タスクを実行するための `start-task`。このコマンドは Fargate 起動タイプのタスクには適用されません。
- 新しい ECS サービスを作成するための `create-service`。
- 既存のサービスを更新するための `update-service`。

> **Note**
>
> マウントした Amazon EBS ボリュームにタスク内のコンテナから書き込みを行うには、コンテナをルートユーザーとして実行する必要があります。

あるいは、AWS Management Console を使用して Amazon EBS ボリュームを設定することもできます。詳細については Amazon ECS タスクとしてのアプリケーションの実行、コンソールを使用した Amazon ECS サービスの作成、および コンソールを使用した Amazon ECS サービスの更新 を参照してください。

以下の JSON スニペットは、デプロイ時に設定可能なすべての Amazon EBS ボリュームパラメータを示します。ボリューム設定でこれらのパラメータを使用するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。これらのパラメータの詳細については、「ボリュームの設定」を参照してください。

```
"volumeConfigurations": [
```

```
        {
            "name": "ebs-volume",
            "managedEBSVolume": {
                "encrypted": true,
                "kmsKeyId": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "volumeType": "gp3",
                "sizeInGiB": 10,
                "snapshotId": "snap-12345",
                "iops": 3000,
                "throughput": 125,
                "tagSpecifications": [
                    {
                        "resourceType": "volume",
                        "tags": [
                            {
                                "key": "key1",
                                "value": "value1"
                            }
                        ],
                        "propagateTags": "NONE"
                    }
                ],
                "roleArn": "arn:aws:iam:1111222333:role/ecsInfrastructureRole",
                 "terminationPolicy": {
                    "deleteOnTermination": true//can't be configured for service-
managed tasks, always true
                },
                "filesystemType": "ext4"
            }
        }
    ]
```

> **Important**
>
> 設定内で指定する volumeName は、タスク定義で指定する volumeName と同じであること。

ボリュームアタッチメントのステータスの確認については、「Amazon ECS タスクへの Amazon EBS ボリュームのアタッチに関するトラブルシューティング」を参照してください。EBS ボリュームのアタッチメントに必要な Amazon ECS インフラストラクチャ AWS Identity and Access

Management (IAM) ロールの詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。

Amazon EBS ボリュームの設定内容を示す JSON スニペットの例を以下に挙げます。これらの例は、スニペットを JSON ファイルに保存し、そのファイルを AWS CLI コマンドのパラメータ (`--cli-input-json file://filename` パラメータを使用) として渡すことで使用できます。*user input placeholders* を、ユーザー自身の情報に置き換えます。

スタンドアロンタスク向けボリュームの設定

以下のスニペットは、Amazon EBS ボリュームをスタンドアロンタスクにアタッチする設定の構文を示します。以下の JSON スニペットは、volumeType、sizeInGiB、encrypted、kmsKeyId の各設定を構成するための構文を示します。JSON ファイルに指定された設定を使用して EBS ボリュームを作成し、スタンドアロンタスクにアタッチします。

```
{
   "cluster": "mycluster",
   "taskDefinition": "mytaskdef",
   "volumeConfigurations": [
        {
            "name": "datadir",
            "managedEBSVolume": {
                "volumeType": "gp3",
                "sizeInGiB": 100,
                "roleArn":"arn:aws:iam:1111222333:role/ecsInfrastructureRole",
                "encrypted": true,
                "kmsKeyId":
 "arn:aws:kms:region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }
        }
   ]
}
```

サービス作成時のボリューム設定

以下のスニペットは、サービスで管理されるタスクにアタッチする Amazon EBS ボリュームを設定する構文を示します。ボリュームは、snapshotId を使用してスナップショットから取得します。JSON ファイルに指定された設定を使用して EBS ボリュームを作成し、サービスで管理される各タスクにアタッチします。

```
{
   "cluster": "mycluster",
```

```
    "taskDefinition": "mytaskdef",
    "serviceName": "mysvc",
    "desiredCount": 2,
    "volumeConfigurations": [
         {
             "name": "myEbsVolume",
             "managedEBSVolume": {
               "roleArn":"arn:aws:iam:1111222333:role/ecsInfrastructureRole",
               "snapshotId": "snap-12345"
             }
         }
    ]
}
```

サービス更新時のボリューム設定

以下の JSON スニペットは、これまでタスクへのアタッチ用に Amazon EBS ボリュームが設定されていなかったサービスを更新するための構文を示します。configuredAtLaunch を true に設定したタスク定義リビジョンの ARN を提供する必要があります。以下の JSON スニペットは、volumeType、sizeInGiB、throughput、iops、および filesystemType 設定を構成する構文を示します。これらの設定を使用して EBS ボリュームを作成し、サービスで管理される各タスクにアタッチします。

```
{
    "cluster": "mycluster",
    "taskDefinition": "mytaskdef",
    "serviceName": "mysvc",
    "desiredCount": 2,
   "volumeConfigurations": [
         {
             "name": "myEbsVolume",
             "managedEBSVolume": {
               "roleArn":"arn:aws:iam:1111222333:role/ecsInfrastructureRole",
                "volumeType": "gp3",
                 "sizeInGiB": 100,
                  "iops": 3000,
                 "throughput": 125,
                 "filesystemType": "ext4"
             }
         }
    ]
}
```

Amazon EBS ボリュームを使用しないようにサービスを設定する

以下の JSON スニペットは、Amazon EBS ボリュームをそれ以上使用しないようにサービスを更新するための構文を示します。`configuredAtLaunch` を `false` に設定したタスク定義の ARN 、または `configuredAtLaunch` パラメータのないタスク定義を提供する必要があります。空の `volumeConfigurations` オブジェクトも提供する必要があります。

```
{
   "cluster": "mycluster",
   "taskDefinition": "mytaskdef",
   "serviceName": "mysvc",
   "desiredCount": 2,
   "volumeConfigurations": []
}
```

Amazon EBS ボリュームの終了ポリシー

Amazon ECS タスクが終了すると、Amazon ECS は `deleteOnTermination` の値に基づいて、終了したタスクに関連付けられている Amazon EBS ボリュームを削除する必要があるかどうかを判断します。デフォルトでは、タスクにアタッチされている EBS ボリュームは、タスクが終了すると削除されます。スタンドアロンタスクの場合、タスク終了時にボリュームを保存するように設定を変更することができます。

> **Note**
>
> サービスにより管理されるタスクにアタッチされたボリュームは保存されず、タスク終了時に必ず削除されます。

Amazon EBS ボリュームのタグ付け

`tagSpecifications` オブジェクトを使用して Amazon EBS ボリュームにタグを付けることができます。このオブジェクトを使用すると、ボリュームがスタンドアロンタスクにアタッチされているか、あるいはサービス内のタスクにアタッチされているかに応じて、独自のタグを提供したり、あるいはタスク定義またはサービスからタグを伝播するよう設定することができます。1 つのボリュームにアタッチできるタグの最大数は 50 個です。

> **Important**
>
> Amazon ECS は、AmazonECSCreated および AmazonECSManaged のリザーブドタグを Amazon EBS ボリュームに自動的にアタッチするので、1 つのボリュームにユーザーが追加できるタグの最大数は 48 個になります。追加できるタグは、ユーザー定義タグ、ECS マネージド型タグ、または伝播されたタグのいずれです。

Amazon ECS マネージド型タグをボリュームに追加する場合は、UpdateService、CreateService、RunTask、StartTask の呼び出しの enableECSManagedTags を true に設定する必要があります。Amazon ECS マネージド型タグをオンにすると、Amazon ECS はボリュームにクラスターとサービスの情報 (aws:ecs:*clusterName* と aws:ecs:*serviceName*) を自動的にタグ付けします。Amazon ECS リソースへのタグ付けの詳細については、「Amazon ECS リソースのタグ付け」を参照してください。

以下の JSON スニペットは、サービス内の各タスクにアタッチされた Amazon EBS ボリュームにユーザー定義タグを付ける構文を示します。この例を使用してサービスを作成するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
   "cluster": "mycluster",
   "taskDefinition": "mytaskdef",
   "serviceName": "mysvc",
   "desiredCount": 2,
   "enableECSManagedTags": true,
   "volumeConfigurations": [
        {
            "name": "datadir",
            "managedEBSVolume": {
                "volumeType": "gp3",
                "sizeInGiB": 100,
                 "tagSpecifications": [
                    {
                        "resourceType": "volume",
                        "tags": [
                            {
                                "key": "key1",
                                "value": "value1"
                            }
                        ],
```

```
                        "propagateTags": "NONE"
                    }
                ]
                "roleArn":"arn:aws:iam:1111222333:role/ecsInfrastructureRole",
                "encrypted": true,
                "kmsKeyId":
 "arn:aws:kms:region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            }
        }
    ]
}
```

> **Important**
>
> Amazon EBS ボリュームにタグを付けるには、volume リソースタイプを指定する必要があります。

Fargate オンデマンドタスク向け Amazon EBS ボリュームのパフォーマンス

Fargate オンデマンドタスクで使用できる Amazon EBS ボリュームのベースライン IOPS とスループットは、タスクにリクエストする CPU ユニット数の合計によって異なります。Fargate タスクに 0.25 ユニット、0.5 ユニット、または 1 ユニットの仮想 CPU (vCPU) をリクエストする場合は、汎用 SSD ボリューム (gp2 または gp3) もしくはハードディスクドライブ (HDD) ボリューム (st1 または sc1) を設定することをお勧めします。Fargate タスク向けに 1 ユニットを超える vCPU をリクエストする場合、タスクにアタッチされる Amazon EBS ボリュームには以下のベースラインパフォーマンス制限が適用されます。EBS のパフォーマンスは、一時的には以下の制限値よりも高くなる場合がありますが、これらの制限値に基づいてワークロードを計画することをお勧めします。

リクエストされる CPU (vCPU) ユニット数	Amazon EBS のベースライン IOPS (16 KiB I/O)	Amazon EBS のベースラインスループット (MiBps、128 KiB I/O)	ベースライン帯域幅 (Mbps)
2	3,000	75	360
4	5,000	120	1,150
8	10,000	250	2,300

リクエストされる CPU (vCPU) ユニット数	Amazon EBS のベースライン IOPS (16 KiB I/O)	Amazon EBS のベースラインスループット (MiBps、128 KiB I/O)	ベースライン帯域幅 (Mbps)
16	15,000	500	4,500

> **Note**
>
> Fargate タスクにアタッチする Amazon EBS ボリュームを設定すると、その Fargate タスク向け Amazon EBS パフォーマンス制限は、タスクの一時ストレージとアタッチされたボリューム間で共有されます。

EC2 タスクの Amazon EBS ボリュームのパフォーマンス

Amazon EBS では以下のボリュームタイプを提供しており、これらはパフォーマンス特性と料金が異なるため、アプリケーションのニーズに応じてストレージのパフォーマンスとコストを調整できます。ボリュームあたりの IOPS やボリュームあたりのスループットなどのパフォーマンスの詳細については、「Amazon Elastic Block Store ユーザーガイド」の「Amazon EBS ボリュームタイプ」を参照してください。

Amazon ECS タスクへの Amazon EBS ボリュームのアタッチに関するトラブルシューティング

場合により、Amazon EBS ボリュームの Amazon ECS タスクへのアタッチをトラブルシューティングまたは検証しなければならない場合があります。

ボリュームのアタッチメントステータスを確認する

AWS Management Consoleを使用して、Amazon EBS ボリュームの Amazon ECS タスクへのアタッチのステータスを確認できます。タスクが開始されたがアタッチメントが機能しない場合は、表示されるステータス理由を確認してトラブルシューティングに活用してください。作成されたボリュームは削除され、タスクは停止します。ステータス理由の詳細については、「Amazon ECS タスクへの Amazon EBS ボリュームアタッチメントのステータス理由」を参照してください。

コンソール上でボリュームのアタッチステータスとステータス理由を確認するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。

2. [クラスター] ページで、タスクが実行されているクラスターを選択します。クラスターの詳細ページが表示されます。
3. クラスターの詳細ページで、[タスク] タブを選択します。
4. ボリュームアタッチメントステータスを確認したいタスクを選択します。確認したいタスクが停止している場合には、[表示するステータスを絞り込む] で [停止] を選択しなければならない場合があります。
5. タスクの詳細ページで、[ボリューム] タブを選択します。Amazon EBS ボリュームのアタッチメントステータスは、[アタッチメントステータス] で確認できます。ボリュームがタスクにアタッチされない場合は、[アタッチメントのステータス] でステータスを選択して、失敗の原因を表示できます。

または、DescribeTasks API を使用して、タスクのボリュームアタッチメントステータスおよび関連するステータス理由を確認することもできます。

サービスとタスクの失敗

Amazon EBS ボリュームに固有ではないサービスまたはタスクの失敗が発生して、ボリュームのアタッチメントに影響を及ぼす場合があります。詳細については「」を参照してください。

- サービスイベントメッセージ
- 停止したタスクのエラーコード
- API 失敗の理由

Amazon ECS タスクへの Amazon EBS ボリュームアタッチメントのステータス理由

Amazon ECS タスクにアタッチする Amazon EBS ボリュームを設定する際に AWS Management Console上にステータス理由として表示されるエラーを解決するには、以下の情報を参照してください。コンソール上でこれらのステータス理由を見つける方法については、「ボリュームのアタッチメントステータスを確認する」を参照してください。

ECS は、設定された ECS インフラストラクチャロール「arn:aws:iam::*111122223333*:role/*ecsInfrastructureRole*」を引き受けることができませんでした。渡されるロールが Amazon ECS と適切な信頼関係にあることを確認してください。

このステータス理由は以下のシナリオにおいて発生します。

- 必要な信頼ポリシーをアタッチせずに IAM ロールを提供した場合。ロールに必要な信頼ポリシーがない場合、Amazon ECS は提供された Amazon ECS インフラストラクチャ IAM ロール

にアクセスできません。タスクが DEPROVISIONING 状態でスタックすることがあります。必要な信頼ポリシーの詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。

- IAM ユーザーが、Amazon ECS インフラストラクチャロールを Amazon ECS に渡すアクセス許可を持っていません。タスクが DEPROVISIONING 状態でスタックすることがあります。この問題を回避するには、ユーザーに PassRole 許可を付与します。詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。
- IAM ロールが、Amazon EBS ボリュームのアタッチメントに必要なアクセス許可を持っていません。タスクが DEPROVISIONING 状態でスタックすることがあります。Amazon EBS ボリュームをタスクにアタッチするために必要なアクセス許可の詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。

> **Note**
>
> このエラーメッセージは、ロールの伝播が遅れている場合にも表示されることがあります。数分待ってからロールを使用しても問題が解決しない場合は、ロールの信頼ポリシーが誤って設定されている可能性があります。

ECS が EBS ボリュームを設定できません。「IdempotentParameterMismatch が発生しました」。「指定したクライアントトークンは、すでに削除されているリソースに関連付けられています。別のクライアントトークンを使用してください。」

以下のような AWS KMS キーシナリオでは、IdempotentParameterMismatch メッセージが表示されることがあります。

- 無効な KMS キー ARN、ID、またはエイリアスが指定されました。このシナリオでは、一見タスクが正常に起動したように見えますが、AWS は KMS キーを非同期で認証するため、タスクは最終的に失敗します。詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EBS の暗号化」を参照してください。
- Amazon ECS インフラストラクチャ IAM ロールがそのキーを暗号化に使用することを許可する権限を持たないカスタマーマネージド型キーが提供されました。キーポリシー権限に関する問題を回避するには、「Amazon EBS ボリュームのデータ暗号化」の AWS KMS キーポリシー例を参照してください。

Amazon EBS ボリュームイベントと Amazon ECS タスク状態変更イベントを Amazon CloudWatch グループなどのターゲットに送信するように Amazon EventBridge を設定できます。その後、これらのイベントを使用して、ボリュームアタッチメントに影響を及ぼしている力

スタマーマネージド型キーに関する問題を特定することができます。詳細については「」を参照してください。

- AWS re: Post 上の「EventBridge ルールのターゲットとして使用する CloudWatch ロググループをどのように作成できますか?」。
- タスク状態変更イベント。
- 「Amazon EBS ユーザーガイド」の Amazon EBS の Amazon EventBridge イベント。

タスクへの EBS ボリュームアタッチメントの設定中に ECS がタイムアウトしました。

このメッセージは、ファイルシステム形式に関する以下のシナリオにおいて発生します。

- 設定時に指定されたファイルシステム形式は、タスクのオペレーティングシステムと互換性がありません。
- Amazon EBS ボリュームをスナップショットから作成するように設定しましたが、スナップショットのファイルシステム形式にはタスクのオペレーティングシステムとの互換性がありません。スナップショットから作成されたボリュームでは、スナップショットの作成時にボリュームが使用していたのと同じファイルシステムタイプを指定する必要があります。

Amazon ECS コンテナエージェントのログを利用して、Amazon EC2 起動タイプのタスクに関するこのメッセージのトラブルシューティングを行うことができます。詳細については、「Amazon ECS ログファイルの場所」と「Amazon ECS ログコレクター」を参照してください。

Amazon ECS での Amazon EFS ボリュームの使用

Amazon Elastic File System (Amazon EFS) では、Amazon ECS タスクで使用するためのシンプルでスケーラブルなファイルストレージを提供します。Amazon EFSでは、ストレージ容量は伸縮性があります。この容量は、ファイルの追加や削除に伴い自動的に拡大および縮小されます。アプリケーションは、必要な時点で必要なストレージを確保できます。

Amazon EFS ファイルシステムを Amazon ECS で使用して、コンテナインスタンスのフリート全体のファイルシステムデータをエクスポートできます。これにより、タスクは、配置されているインスタンスにかかわらず、同じ永続的ストレージにアクセスできます。ファイルシステムを使用するには、タスク定義からコンテナインスタンスのボリュームマウントを参照する必要があります。

チュートリアルについては、「コンソールを使用した Amazon ECS での Amazon EFS ファイルシステムの設定」を参照してください。

考慮事項

Amazon EFS ボリュームを使用する場合には、以下の点を考慮してください。

- EC2 起動タイプを使用するタスク用として、Amazon ECS に最適化された AMI バージョン 20191212 でのコンテナエージェントバージョン 1.35.0 を使用する、Amazon EFS ファイルシステムのサポートが、パブリックプレビューとして追加されました。ただし、Amazon EFS ファイルシステムのサポートは、コンテナエージェントバージョンが 1.38.0 の Amazon ECS 最適化 AMI バージョン 20200319 (Amazon EFS アクセスポイントと IAM 認可機能が含まれるもの) で一般提供されています。これらの機能を使用する際には、Amazon ECS 最適化 AMI バージョン 20200319 以降の使用をお勧めします。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

  > **Note**
  >
  > 独自の AMI を作成する場合、コンテナエージェント 1.38.0 以降、`ecs-init` バージョン 1.38.0-1 以降を使用し、Amazon EC2 インスタンスで以下のコマンドを実行して、Amazon ECS ボリュームプラグインを有効にする必要があります。コマンドは、ベースイメージとして Amazon Linux 2 と Amazon Linux のどちらを使用しているかによって異なります。
  >
  > Amazon Linux 2
  >
  > ```
  > yum install amazon-efs-utils
  > systemctl enable --now amazon-ecs-volume-plugin
  > ```
  >
  > Amazon Linux
  >
  > ```
  > yum install amazon-efs-utils
  > sudo shutdown -r now
  > ```

- Fargate でホストされるタスクの場合、プラットフォームバージョン 1.4.0 以降 (Linux) で、Amazon EFS ファイルシステムがサポートされます。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。
- Fargate でホストされるタスクに Amazon EFS ボリュームを使用する場合、Fargate は Amazon EFS ボリュームの管理を担当するスーパーバイザーコンテナを作成します。スーパーバイザーコンテナは、タスクのメモリと CPU を少量使用します。スーパーバイザーコンテナは、タスクメタデータバージョン 4 エンドポイントにクエリを実行するときに表示されます。さらに、CloudWatch Container Insights では、コンテナ名 `aws-fargate-supervisor` として表示

されます。Amazon EC2 起動タイプを使用する場合の詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。Fargate 起動タイプを使用する場合の詳細については、「Fargate のタスク用の Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。

- Amazon EFS ボリュームの使用または `EFSVolumeConfiguration` の指定は、外部インスタンスではサポートされていません。
- エージェント設定ファイルの `ECS_ENGINE_TASK_CLEANUP_WAIT_DURATION` パラメータは、デフォルトよりも小さい値 (約 1 時間) に設定することをお勧めします。この変更は、EFS マウント認証情報の有効期限切れを防ぎ、使用されていないマウントをクリーンアップするのに役立ちます。 詳細については、Amazon ECS コンテナエージェントの設定 をご参照ください。

Amazon EFS アクセスポイントの使用

Amazon EFS アクセスポイントは、EFS ファイルシステムへのアプリケーション固有のエントリポイントです。これにより、共有データセットへのアプリケーションによるアクセスを管理します。Amazon EFS アクセスポイントの詳細およびアクセス制御方法については、Amazon Elastic File System ユーザーガイドの「Amazon EFS アクセスポイントの使用」を参照してください。

アクセスポイントを使用すると、アクセスポイントを介したすべてのファイルシステム要求に対してユーザーアイデンティティ (ユーザーの POSIX グループなど) を適用できます。また、アクセスポイントでは、ファイルシステムに対して別のルートディレクトリを適用することも可能です。クライアントは、指定したディレクトリまたはそのサブディレクトリ内のデータに対してのみアクセスが可能なためです。

> **Note**
>
> EFS アクセスポイントを作成する際は、ファイルシステム上でルートディレクトリとして機能するパスを指定します。Amazon ECS タスク定義内でアクセスポイント ID を持つ EFS ファイルシステムを参照する場合、ルートディレクトリは省略するか、EFS アクセスポイントに設定されたパスを適用するために `/` を設定する必要があります。

Amazon ECS タスクの IAM ロールを使用して、特定のアプリケーションで使用するアクセスポイントを限定できます。IAM ポリシーとアクセスポイントを組み合わせると、アプリケーションによる特定のデータセットへのアクセスを保護できます。タスクIAM ロールの使用方法については、「Amazon ECS タスクの IAM ロール」を参照してください。

Amazon ECS で Amazon EFS ボリュームを使用する場合のベストプラクティス

Amazon ECS で Amazon EFS を使用する場合は、以下のベストプラクティス推奨事項に留意すること。

Amazon EFS ボリュームのセキュリティとアクセスコントロール

Amazon EFS には、Amazon EFS ファイルシステムに保存されているデータのセキュリティを確保し、それを必要とするアプリケーションからのみアクセスを許可するためのアクセス制御機能があります。保管中と転送中両方の暗号化を有効にすることで、データのセキュリティを確保します。詳細については、Amazon Elastic File System ユーザーガイド の「Amazon EFS でのデータの暗号化」を参照してください。

データの暗号化に加えて、Amazon EFS を使用してファイルシステムへのアクセスを制限することもできます。EFS にアクセス制御を実装するには 3 つの方法があります。

- セキュリティグループ — Amazon EFS マウントターゲットでは、ネットワークトラフィックを許可または拒否するのに使用するセキュリティグループを設定できます。Amazon EFS にアタッチされるセキュリティグループを設定することにより、Amazon ECS インスタンス、もしくは `awsvpc` ネットワークモードを使用している場合は Amazon ECS タスクにアタッチされているセキュリティグループからの NFS トラフィック (ポート 2049) を許可できます。
- IAM — IAM を使用して Amazon EFS ファイルシステムへのアクセスを制限できます。Amazon ECS タスクを設定すると、EFS ファイルシステムをマウントするためにファイルシステムにアクセスする IAM ロールが必要になります。詳細については、「Amazon Elastic File System User Guide」の「Using IAM to control file system data access」を参照してください。

  IAM ポリシーでは、Amazon EFS ファイルシステムへの接続時に TLS の使用をクライアントに要求するなど、あらかじめ定義された条件を執行することもできます。詳細については、「Amazon Elastic File System ユーザーガイド」の「クライアント向け Amazon EFS 条件キー」を参照してください。
- Amazon EFS アクセスポイント — Amazon EFS アクセスポイントとは、アプリケーション固有の Amazon EFS ファイルシステムへのエントリポイントです。アクセスポイントを使用すると、そのアクセスポイントを介したすべてのファイルシステム要求に対してユーザーアイデンティティ (ユーザーの POSIX グループなど) を適用することができます。また、アクセスポイントでは、ファイルシステムに対して別のルートディレクトリを適用することも可能です。これは、クライアントは指定したディレクトリまたはそのサブディレクトリ内のデータにしかアクセスできないためです。

IAM ポリシー

IAM ポリシーを使用すると、Amazon EFS ファイルシステムへのアクセスを制御できます。

ファイルシステムポリシーを使用してファイルシステムにアクセスするクライアントに対して、以下のアクションを指定できます。

[アクション]	説明
`elasticfilesystem:ClientMount`	ファイルシステムへの読み取り専用アクセス許可を付与します。
`elasticfilesystem:ClientWrite`	ファイルシステムへの書き込みアクセス許可を付与します。
`elasticfilesystem:ClientRootAccess`	ファイルシステムへのアクセス時にルートユーザーの使用を許可します。

ポリシーで各アクションを指定する必要があります。ポリシーは次の方法で定義できます。

- クライアントベース – ポリシーをタスクロールにアタッチします

  タスク定義の作成時に [IAM 認可] オプションを設定します。
- リソースベース – Amazon EFS ファイルシステムにポリシーをアタッチします

  リソースベースのポリシーが存在しない場合、ファイルシステム作成時にデフォルトですべてのプリンシパル (*) にアクセス許可が付与されます。

[IAM 認可] オプションを設定すると、タスクロールに関連付けられたポリシーと Amazon EFS リソースベースのポリシーがマージされます。[IAM 認可] オプションは、このポリシーを持つタスクアイデンティティ (タスクロール) を Amazon EFS に渡します。この結果、Amazon EFS リソースベースのポリシーに、ポリシーで指定された IAM ユーザーまたはロールのコンテキストを入れることができます。このオプションを設定しない場合、Amazon EFS リソースレベルのポリシーは IAM ユーザーを「匿名」として識別します。

セキュリティを最大化するため、Amazon EFS ファイルシステムに 3 つのアクセス制御すべてを実装することを検討してください。たとえば、Amazon EFS マウントポイントにアタッチされるセキュリティグループを設定することで、コンテナインスタンスまたは Amazon ECS タスクに関連付

けられたセキュリティグループからの進入 NFS トラフィックのみを許可することができます。さらに、Amazon EFS の設定により、許可されたセキュリティグループからの接続であっても、ファイルシステムにアクセスするための IAM ロールを要求することができます。最後に、Amazon EFS アクセスポイントの使用により、POSIX ユーザー権限を執行してアプリケーション向けルートディレクトリを指定することができます。

以下のタスク定義スニペットは、アクセスポイントを使用して Amazon EFS ファイルシステムをマウントする方法を示します。

```
"volumes": [
    {
      "efsVolumeConfiguration": {
        "fileSystemId": "fs-1234",
        "authorizationConfig": {
          "accessPointId": "fsap-1234",
          "iam": "ENABLED"
        },
        "transitEncryption": "ENABLED",
        "rootDirectory": ""
      },
      "name": "my-filesystem"
    }
]
```

Amazon EFS ボリュームパフォーマンス

Amazon EFS には、汎用と Max I/O の 2 つのパフォーマンスモードがあり、汎用モードは、コンテンツ管理システムや CI/CD ツールなどのレイテンシーの影響を受けやすいアプリケーションに適しています。これとは対照的に、Max I/O ファイルシステムは、データ分析、メディア処理、機械学習などのワークロードに適しています。これらのワークロードは、数百または数千のコンテナからの並列演算を実行する必要があり、可能な限り高い総スループットと IOPS を必要とします。詳細については、「Amazon Elastic File System ユーザーガイド」の「Amazon EFS パフォーマンスモード」を参照してください。

レイテンシーの影響を受けやすいワークロードには、Max I/O パフォーマンスモードによる高い I/O レベルと、汎用パフォーマンスモードによる低レイテンシーの両方が必要です。このタイプのワークロードでは、複数の[General Purpose(汎用)]パフォーマンスモードファイルシステムを作成することをお勧めします。この場合、ワークロードとアプリケーションでサポート可能な限り、すべてのファイルシステム全体にアプリケーションのワークロードを分散することをお勧めします。

Amazon EFS ボリュームスループット

すべての Amazon EFS ファイルシステムには、プロビジョニングされたスループットを使用したファイルシステムのプロビジョニングされたスループットの量、またはバーストスループットを使用したファイルシステムの EFS 標準または One Zone ストレージクラスに保存されたデータの量のいずれかにより決定される、関連するメータリングスループットがあります。詳細については、「Amazon Elastic File System ユーザーガイド」の「メータリングスループットについて理解する」を参照してください。

Amazon EFS ファイルシステムのデフォルトのスループットモードはバーストモードです。バーストモードでは、ファイルシステムが利用できるスループットは、ファイルシステムの拡大に応じてスケールインまたはスケールアウトされます。ファイルベースのワークロードは通常スパイクが発生する、つまり、特定の時間のみ高レベルのスループットを必要とし、残りの時間は低レベルのスループットになることが多いため、Amazon EFS は一定期間高いスループットレベルにバーストできるように設計されています。さらに、多くのワークロードは読み取り負荷が高いため、読み取り操作は他の NFS 操作 (書き込みなど) と 1:3 の比率でメータリングされます。

Amazon EFS ファイルシステムは、すべての Amazon EFS 標準ストレージまたは Amazon EFS One Zone ストレージについて 1 TB ごとに 50 MB/秒という安定したベースラインパフォーマンスを提供します。サイズに関係なく、すべてのファイルシステムは 100 MB/秒までバーストできます。1 TB を超える EFS 標準ストレージまたは EFS One Zone ストレージを持つファイルシステムでは、1 TB ごとに 100 MB/秒までバーストできます。読み取り操作は 1:3 の比率でメータリングされるため、読み取りスループットは 1 TiB ごとに最大 300 MiB/秒を駆動できます。ファイルシステムにデータを追加すると、そのファイルシステムで使用できる最大スループットは、Amazon EFS 標準ストレージクラスのストレージに比例して自動的にスケーリングされます。保存されているデータ量で達成できる以上に高いスループットが必要な場合は、ワークロードが必要とする量に合わせてプロビジョンドスループットを設定できます。

ファイルシステムのスループットは、ファイルシステムに接続されたすべての Amazon EC2 インスタンス間で共有されます。たとえば、100 MB/秒のスループットまでバーストできる 1 TB のファイルシステムでは、1 つの Amazon EC2 インスタンスから 10 MB/秒を駆動できます。詳細については、Amazon Elastic File System ユーザーガイドの「Amazon EFS のパフォーマンス」を参照してください。

Amazon EFS ボリュームのコストの最適化

Amazon EFS はストレージのスケーリングを簡素化します。Amazon EFS ファイルシステムは、データを追加すると自動的に拡張されます。特に Amazon EFS のバーストスループットモードでは、Amazon EFS のスループットは、標準ストレージクラスのファイルシステムのサイズが大きく

なるにつれて拡大します。EFS ファイルシステムのプロビジョンドスループットに追加費用を支払わずにスループットを向上させるには、Amazon EFS ファイルシステムを複数のアプリケーション間で共有することができます。Amazon EFS アクセスポイントを使用して、共有 Amazon EFS ファイルシステムにストレージ分離を実装できます。そうすることで、アプリケーション間で同じファイルシステムを共有していても、ユーザーが許可しない限りデータにアクセスできなくなります。

データが大きくなると、Amazon EFS ではアクセス頻度の低いファイルを自動的に下位のストレージクラスに移動できます。Amazon EFS 標準の低頻度アクセス (IA) ストレージクラスは、毎日アクセスされないファイルのストレージコストを削減します。これにより、Amazon EFS が提供する高可用性、高耐久性、伸縮性、および POSIX ファイルシステムへのアクセス性が損なわれることはありません。詳細については、「Amazon Elastic File System ユーザーガイド」の「Amazon EFS ストレージクラス」を参照してください。

Amazon EFS ライフサイクルポリシーを使用してアクセス頻度の低いファイルを Amazon EFS IA ストレージに移動することで、自動的にコストを節約することを検討してください。詳細については、「Amazon Elastic File System User Guide」(Amazon Elastic File System ユーザーガイド) の「Amazon EFS のライフサイクル管理」を参照してください。

Amazon EFS ファイルシステムを作成する場合、Amazon EFS でデータを複数のアベイラビリティーゾーン (標準) に複製するか、あるいは単一のアベイラビリティーゾーン内でデータを冗長的に保存するかを選択できます。Amazon EFS One Zone ストレージクラスは、Amazon EFS 標準ストレージクラスと比較してストレージコストを大幅に削減できます。マルチ AZ の耐障害性を必要としないワークロードには Amazon EFS One Zone ストレージクラスの使用を検討してください。アクセス頻度の低いファイルを Amazon EFS One Zone の低頻度アクセスストレージに移動することで、Amazon EFS One Zone ストレージのコストをさらに削減できます。詳細については、「Amazon EFS 低頻度アクセス」を参照してください。

Amazon EFS ボリュームデータ保護

Amazon EFS は、標準ストレージクラスを使用するファイルシステムについては、複数のアベイラビリティーゾーン間でデータを冗長的に保存します。Amazon EFS One Zone ストレージクラスを選択した場合、単一のアベイラビリティーゾーン内でデータを冗長的に保存します。さらに、Amazon EFS は、1 年間に 99.999999999% (9 が 11 桁) の耐久性を保証するよう設計されています。

どの環境でもそうですが、データのバックアップを取り、誤って削除されないように保護することがベストプラクティスです。Amazon EFS データのベストプラクティスには、正常に機能し定期的にテストされている AWS Backup 型バックアップの使用が含まれます。Amazon EFS One Zone ストレージクラスを使用するファイルシステムは、意図的に無効にしない限り、ファイルシステムの作成時にデフォルトでファイルを自動的にバックアップするように設定されています。詳細については、

「Amazon Elastic File System ユーザーガイド」の「EFS ファイルシステムのバックアップ」を参照してください。

タスク定義内での Amazon EFS ファイルシステムの指定

コンテナに Amazon EFS ファイルシステムボリュームを使用するには、タスク定義でボリュームとマウントポイントの設定を指定する必要があります。次のスニペットの JSON によるタスク定義では、コンテナの volumes と mountPoints オブジェクトの構文を示しています。

```
{
    "containerDefinitions": [
        {
            "name": "container-using-efs",
            "image": "public.ecr.aws/amazonlinux/amazonlinux:latest",
            "entryPoint": [
                "sh",
                "-c"
            ],
            "command": [
                "ls -la /mount/efs"
            ],
            "mountPoints": [
                {
                    "sourceVolume": "myEfsVolume",
                    "containerPath": "/mount/efs",
                    "readOnly": true
                }
            ]
        }
    ],
    "volumes": [
        {
            "name": "myEfsVolume",
            "efsVolumeConfiguration": {
                "fileSystemId": "fs-1234",
                "rootDirectory": "/path/to/my/data",
                "transitEncryption": "ENABLED",
                "transitEncryptionPort": integer,
                "authorizationConfig": {
                    "accessPointId": "fsap-1234",
                    "iam": "ENABLED"
                }
            }
```

```
        }
    ]
}
```

`efsVolumeConfiguration`

タイプ: オブジェクト

必須: いいえ

このパラメータは、Amazon EFS ボリュームを使用する場合に指定します。

`fileSystemId`

型: 文字列

必須: はい

使用する Amazon EFS ファイルシステムの ID。

`rootDirectory`

型: 文字列

必須: いいえ

ホスト内にルートディレクトリとしてマウントする Amazon EFS ファイルシステム内のディレクトリ。このパラメータを省略すると、Amazon EFS ボリュームのルートが使用されます。/ を指定すると、このパラメータを省略した場合と同じ結果になります。

> **Important**
>
> `authorizationConfig` に EFS アクセスポイントを指定する場合は、ルートディレクトリパラメータを省略するか、または / に設定して EFS アクセスポイントにパスを設定する必要があります。

`transitEncryption`

型: 文字列

有効な値: `ENABLED` | `DISABLED`

必須: いいえ

Amazon ECS ホストと Amazon EFS サーバー間で、転送中の Amazon EFS データの暗号化を有効にするかどうかを指定します。Amazon EFS IAM 認可を使用する場合は、転送中の暗号化を有効にする必要があります。このパラメータを省略すると、DISABLED のデフォルト値が使用されます。詳細については、Amazon Elastic ファイルシステムユーザーガイドの「転送中データの暗号化」を参照してください。

`transitEncryptionPort`

タイプ: 整数

必須: いいえ

Amazon ECS ホストと Amazon EFS サーバーとの間で、暗号化されたデータを送信するときに使用するポート。転送中の暗号化ポートを指定しないと、Amazon EFS マウントヘルパーが使用するポート選択方式が使用されます。詳細については、[Amazon Elastic File System User Guide] (Amazon Elastic File System ユーザーガイド) の[EFS Mount Helper] (EFS マウントヘルパー) を参照してください。

`authorizationConfig`

タイプ: オブジェクト

必須: いいえ

Amazon EFS ファイルシステムに対する認可構成の詳細。

`accessPointId`

型: 文字列

必須: いいえ

使用するアクセスポイント ID。アクセスポイントを指定する場合は、efsVolumeConfiguration のルートディレクトリ値を省略するか、EFS アクセスポイントに設定されたパスを適用するために / を設定する必要があります。アクセスポイントを使用する場合は、EFSVolumeConfiguration で転送中の暗号化を有効にする必要があります。詳細については、Amazon Elastic ファイルシステムユーザーガイドのAmazon EFS アクセスポイントの使用を参照してください。

`iam`

型: 文字列

有効な値: ENABLED | DISABLED

必須: いいえ

タスク定義で定義した Amazon ECS タスクの IAM ロールを、Amazon EFS ファイルシステムのマウント時に使用するかどうかを指定します。使用する場合は、`EFSVolumeConfiguration` で転送中の暗号化を有効にする必要があります。このパラメータを省略すると、`DISABLED` のデフォルト値が使用されます。詳細については、「タスク用の IAM ロール」を参照してください。

コンソールを使用した Amazon ECS での Amazon EFS ファイルシステムの設定

Amazon ECS で Amazon Elastic File System (Amazon EFS) ファイルシステムを使用する方法について説明します。

ステップ 1: Amazon ECS クラスターを作成する

次の手順に従って Amazon ECS クラスターを作成します。

新しいクラスターを作成するには (Amazon ECS コンソール)

開始する前に、適切な IAM アクセス許可を割り当ててください。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [クラスター設定] の [クラスター名] に、名前として「`EFS-tutorial`」を入力します。
6. (オプション) タスクとサービスが起動する VPC とサブネットを変更するには、[Networking] (ネットワーク) で、次のいずれかのオペレーションを実行します。
   - サブネットを削除するには、[Subnets] (サブネット) で、削除するサブネットごとに [X] を選択します。
   - [default] (デフォルト) VPC 以外の VPC に変更するには、[VPC] で既存の [VPC] を選択し、[Subnets] (サブネット) で各サブネットを選択します。
7. クラスターに Amazon EC2 インスタンスを追加するには、[インフラストラクチャー] を展開して [Amazon EC2 インスタンス] を選択します。次に、キャパシティープロバイダーとして機能する Auto Scaling グループを設定します。

- Auto Scaling グループを作成するには、Auto Scaling group(ASG) (Auto Scaling グループ) から、[Create new group] (新しいグループの作成) を選択し、グループに関する以下の詳細情報を入力します。
  - [オペレーティングシステム/アーキテクチャ] で、[Amazon Linux 2] を選択します。
  - [EC2 instance type] で、[t2.micro] を選択します。

    [SSH key pair] (SSH キーペア) を使用する場合、インスタンスに接続する際に ID を証明するペアを選択してください。
  - [キャパシティ] に、「1」と入力します。

8. [Create] (作成) を選択します。

ステップ 2: Amazon EC2 インスタンスと Amazon EFS ファイルシステムのセキュリティグループを作成する

このステップでは、ポート 80 でのインバウンドネットワークトラフィックを許可する Amazon EC2 インスタンスと、コンテナインスタンスからのインバウンドアクセスを許可する Amazon EFS ファイルシステムのセキュリティグループを作成します。

以下のオプションを使用して Amazon EC2 インスタンスのセキュリティグループを作成します。

- [セキュリティグループ名] — セキュリティグループの名前を入力します。
- [VPC] - クラスター用に前に特定した VPC を選択します。
- インバウンドルール
  - タイプ - HTTP
  - ソース - 0.0.0.0/0

以下のオプションを使用して Amazon EFS ファイルシステムのセキュリティグループを作成します。

- [セキュリティグループ名] — セキュリティグループの名前を入力します。例えば、EFS-access-for-sg-*dc025fa2* と指定します。
- [VPC] - クラスター用に前に特定した VPC を選択します。
- インバウンドルール
  - [タイプ] – [NFS]

- ソース - [カスタム]で、インスタンス用に作成したセキュリティグループの ID を使用します。

セキュリティグループの作成方法については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 インスタンス用のセキュリティグループの作成」を参照してください。

ステップ 3:Amazon EFS ファイルシステムを作成する

このステップでは、Amazon EFS ファイルシステムを作成します。

Amazon ECS タスク用の Amazon EFS ファイルシステムを作成するには

1. Amazon Elastic File System コンソール (https://console.aws.amazon.com/efs/) を開きます。
2. [Create file system] を選択します。
3. ファイルシステムの名前を入力し、コンテナインスタンスをホストする VPC を選択します。デフォルトでは、指定した VPC の各サブネットに、その VPC のデフォルトセキュリティグループを使用するマウントターゲットが割り当てられます。次に [カスタマイズ] を選択します。

   > **Note**
   >
   > このチュートリアルでは、Amazon EFS ファイルシステム、Amazon ECS クラスター、コンテナインスタンス、およびタスクが同じ VPC 内に存在することを前提としています。別の VPC からファイルシステムをマウントする方法の詳細については、Amazon EFS ユーザーガイドの「チュートリアル: 別の VPC からファイルシステムをマウントする」を参照してください。

4. [ファイルシステムの設定] ページでオプション設定を行い、[パフォーマンス設定] でファイルシステムの[バースト] スループットモードを選択します。設定が完了したら、[次へ] を選択します。

   a. (オプション) ファイルシステムのタグを追加します。例えば、ファイルシステムの一意の名前を指定するには、[名前] キーの横にある [値] 列にその名前を入力します。

   b. (オプション) ライフサイクル管理を有効にして、アクセス頻度の低いストレージのコストを節約します。詳細については、Amazon Elastic File System User Guide の「EFS のライフサイクル管理」を参照してください。

   c. (オプション) 暗号化を有効にします。保管時の Amazon EFS ファイルシステムの暗号化を有効にするチェックボックスを選択します。

5. [ネットワークアクセス]ページの [マウントターゲット] で、各アベイラビリティーゾーンの既存のセキュリティグループ設定を、ステップ 2: Amazon EC2 インスタンスと Amazon EFS ファイルシステムのセキュリティグループを作成する でファイルシステム用に作成したセキュリティグループに置き換え、[次へ] を選択します。
6. このチュートリアルでは[ファイルシステムポリシー]を設定する必要はないので、[次へ] を選択すればセクションをスキップできます。
7. ファイルシステムのオプションを確認し、[作成] を選択してプロセスを完了します。
8. [ファイルシステム] 画面から、ファイルシステム ID を書き留めます。次のステップで、Amazon ECS タスク定義で、この値をリファレンスします。

ステップ 4: Amazon EFS ファイルシステムにコンテンツを追加する

このステップでは、Amazon EFS ファイルシステムを Amazon EC2 インスタンスにマウントし、コンテンツを追加します。これは、このチュートリアルでデータの永続的な性質を示すことを目的としたテストです。この機能を使用する場合は、通常、Amazon EFS ファイルシステムにデータを書き込むためのアプリケーションや別の方法があります。

Amazon EC2 インスタンスを作成し、Amazon EFS ファイルシステムをマウントします。

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. [Launch Instance] (インスタンスの起動) を選択します。
3. [アプリケーションおよび OS イメージ (Amazon マシンイメージ)] で、[Amazon Linux 2 AMI (HVM)] を選択します。
4. [インスタンス タイプ] で、デフォルトのインスタンスタイプ `t2.micro` をそのまま使用します。
5. [キーペア (ログイン)] で、インスタンスへの SSH アクセス用のキーペアを選択します。
6. [ネットワーク設定] で、Amazon EFS ファイルシステムおよび Amazon ECS クラスター用に指定した VPC を選択します。サブネットと、ステップ 2: Amazon EC2 インスタンスと Amazon EFS ファイルシステムのセキュリティグループを作成する で作成したインスタンスセキュリティグループを選択します。インスタンスのセキュリティグループを設定します。[パブリック IP の自動割り当て] が有効になっていることを確認します。
7. [ストレージの設定] で、ファイルシステムの [編集] ボタンを選択し、[EFS] を選択します。ステップ 3:Amazon EFS ファイルシステムを作成する で作成したファイルシステムを選択します。必要に応じて、マウントポイントを変更したり、デフォルト値をそのまま使用したりできます。

> **Important**
>
> インスタンスにファイルシステムを追加する前に、サブネットを選択する必要があります。

8. [セキュリティグループを自動的に作成してアタッチする] をオフにします。もう 1 つのチェックボックスはオンのままにしておきます。[Add shared file system] (共有ファイルシステムの追加) を選択します。
9. [Advanced Details] で、Amazon EFS ファイルシステムのマウント ステップを使用してユーザー データスクリプトが自動的に入力されていることを確認します。
10. [概要] で、[インスタンス数] が 1 であることを確認します。[Launch instance (インスタンスの起動)] を選択します。
11. [インスタンスを起動] ページで、[すべてのインスタンスを表示] を選択して、インスタンスのステータスを表示します。最初、[インスタンスの状態] ステータスは PENDING です。状態が RUNNING に変わり、インスタンスがすべてのステータスチェックに合格すると、インスタンスは使用可能になります。

次に、Amazon EC2 インスタンスに接続し、コンテンツを Amazon EFS ファイルシステムに追加します。

Amazon EC2 インスタンスに接続し、コンテンツを Amazon EFS ファイルシステムに追加するには

1. 作成した Amazon EC2 インスタンスに SSH 接続します。詳細については、「Amazon EC2 ユーザーガイド」の「SSH を使用した Linux インスタンスへの接続」を参照してください。
2. ターミナルウィンドウから、df -T コマンドを実行して、Amazon EFS ファイルシステムがマウントされていることを確認します。次の出力では、Amazon EFS ファイルシステムのマウントを強調表示しています。

```
$ df -T
Filesystem     Type            1K-blocks    Used        Available Use% Mounted on
devtmpfs       devtmpfs           485468       0           485468   0% /dev
tmpfs          tmpfs              503480       0           503480   0% /dev/shm
tmpfs          tmpfs              503480     424           503056   1% /run
tmpfs          tmpfs              503480       0           503480   0% /sys/fs/
cgroup
/dev/xvda1     xfs               8376300 1310952          7065348  16% /
127.0.0.1:/    nfs4     9007199254739968       0 9007199254739968   0% /mnt/efs/fs1
```

```
tmpfs           tmpfs               100700       0           100700    0% /run/
user/1000
```

3. Amazon EFS ファイルシステムのマウント先のディレクトリに移動します。上の例では `/mnt/efs/fs1` に移動します。
4. 以下の内容で `index.html` という名前のファイルを作成します。

```
<html>
    <body>
        <h1>It Works!</h1>
        <p>You are using an Amazon EFS file system for persistent container
 storage.</p>
    </body>
</html>
```

ステップ 5: タスク定義を作成する

次のタスク定義は、`efs-html` というデータボリュームを作成します。`nginx` コンテナは、ホストデータボリュームを NGINX ルート `/usr/share/nginx/html` にマウントします。

Amazon ECS コンソールを使用して新しいタスク定義を作成するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
4. JSON エディターボックスには、次の JSON テキストをコピーして貼り付けます。`fileSystemId` は、実際の Amazon EFS ファイルシステムの ID に置き換えます。

```
{
    "containerDefinitions": [
        {
            "memory": 128,
            "portMappings": [
                {
                    "hostPort": 80,
                    "containerPort": 80,
                    "protocol": "tcp"
                }
            ],
```

```
            "essential": true,
            "mountPoints": [
                {
                    "containerPath": "/usr/share/nginx/html",
                    "sourceVolume": "efs-html"
                }
            ],
            "name": "nginx",
            "image": "public.ecr.aws/docker/library/nginx:latest"
        }
    ],
    "volumes": [
        {
            "name": "efs-html",
            "efsVolumeConfiguration": {
                "fileSystemId": "fs-1324abcd",
                "transitEncryption": "ENABLED"
            }
        }
    ],
    "family": "efs-tutorial",
    "executionRoleArn":"arn:aws:iam::111122223333:role/ecsTaskExecutionRole"
}
```

> **Note**
>
> Amazon ECS タスク実行 IAM ロールに次のアクセス許可を追加すると、スタートアップ時に Amazon ECS エージェントが Amazon EFS ファイルシステムを検索してタスクにマウントできるようになります。
>
> - `elasticfilesystem:ClientMount`
> - `elasticfilesystem:ClientWrite`
> - `elasticfilesystem:DescribeMountTargets`
> - `elasticfilesystem:DescribeFileSystems`

5. [Create] (作成) を選択します。

ステップ 6: タスクを実行して結果を表示する

さて、Amazon EFS ファイルシステムが作成され、NGINX コンテナのウェブコンテンツが用意されたので、作成したタスク定義を使用してタスクを実行できます。NGINX ウェブサーバーは、シンプルな HTML ページを提供します。Amazon EFS ファイルシステムのコンテンツを更新した場合、それらの変更は、そのファイルシステムがマウントされているすべてのコンテナにも伝達されます。

タスクは、クラスターのために定義したサブネットで実行されます。

コンソールを使用してタスクを実行し結果を表示するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、スタンドアロンタスクを実行するクラスターを選択します。

   サービスを起動するリソースを決定します。

サービスの起動元	ステップ
クラスター	a. [Clusters] ページで、サービスを作成するクラスターを選択します。 b. Tasksタブで、Run new taskを選択します。
起動タイプ	a. [Task] (タスク) ページで、タスク定義を選択します。 b. リビジョンが複数ある場合は、リビジョンを選択します。 c. [Create] (作成)、[Run task] (タスクの実行) の順に選択します。

3. (オプション) スケジュールされたタスクをクラスターのインフラストラクチャ全体に分散する方法を選択します。[Compute configuration] (コンピュート設定) を展開し、以下の操作を実行します。

ディストリビューションの方法	ステップ
起動タイプ	a. [Compute options] (コンピューティングオプション) セクションで、[Launch type] (起動タイプ) を選択します。 b. [起動タイプ] で、[EC2] を選択します。

4. Application type(アプリケーションの種類)で、Task(タスク)を選択します。
5. [タスク定義] で、先に作成した `efs-tutorial` タスク定義を選択します。
6. [必要なタスク] に、「1」と入力します。
7. [Create] (作成) を選択します。
8. [クラスター] ページで、[インフラストラクチャ] を選択します。
9. [コンテナインスタンス] で、接続先となるコンテナインスタンスを選択します。
10. [コンテナインスタンス] ページの インスタンスの [ネットワーキング] で、インスタンスの [パブリック IP] を書き留めます。
11. ブラウザを開き、パブリック IP アドレスを入力します。次のメッセージが表示されます。

```
It works!
You are using an Amazon EFS file system for persistent container storage.
```

> **Note**
>
> メッセージが表示されない場合は、コンテナインスタンスのセキュリティグループがポート 80 でインバウンドネットワークトラフィックを許可しており、ファイルシステムのセキュリティグループがコンテナインスタンスからのインバウンドアクセスを許可していることを確認してください。

Amazon ECS での FSx for Windows File Server ボリュームの使用

FSx for Windows File Server は、Windows ファイルシステムによってバックアップされるフルマネージド型 Windows ファイルサーバーを提供します。ECS と共に FSx for Windows File Server を使用する場合、永続的、分散、共有、静的ファイルストレージで Windows タスクをプロビジョニングできます。詳細については、FSx for Windows File Serverとは？を参照してください。

> **Note**
>
> FSx for Windows File Server ECS のタスクボリュームは、Amazon ECS に最適化された Windows Server 2016 Full AMI を使用する EC2 インスタンスではサポートされていません。Fargate 設定上の Windows コンテナで、FSx for Windows File Server ボリュームを使用することはできません。代わりに、起動時にコンテナをマウントするように変更できます。

FSx for Windows File Server を使用すると、共有外部ストレージ、リージョン別の高可用ストレージ、または高スループットストレージへのアクセスを必要とする Windows ワークロードのデプロイが行えます。Amazon ECS Windows インスタンスで実行されている Amazon ECS コンテナには、1 つ以上の FSx for Windows File Server ファイルシステムボリュームをマウントできます。1 つの Amazon ECS タスク内の複数の Amazon ECS コンテナ間で、FSx for Windows File Server ファイルシステムボリュームを共有できます。

ECS で FSx for Windows File Server を使用できるようにするには、次のタスク定義 JSON スニペット例に示すように、タスク定義に FSx for Windows File Server ファイルシステム ID と関連情報を含める必要があります。この例を、次のタスク定義 JSON スニペットで示します。タスク定義を作成して実行する際には、以下を用意しておきます。

- 有効なドメインに参加している ECS Windows EC2 インスタンス。これは AWS Directory Service for Microsoft Active Directory や、オンプレミスまたは Amazon EC2 上でセルフホストされたアクティブディレクトリのいずれかで、ホストされます。
- Active Directory ドメインの接続と FSx for Windows File Server ファイルシステムのアタッチに使用される、認証情報を含む AWS Secrets Manager シークレットまたは Systems Manager パラメータ。認証情報値は、アクティブディレクトリの作成時に入力した名前とパスワードの認証情報です。

関連チュートリアルについては、「Amazon ECS 用の FSx for Windows File Server ファイルシステムを設定する方法について説明します。」を参照してください。

考慮事項

FSx for Windows File Server ボリュームを使用する際は、以下の点を考慮します。

- Amazon ECS FSx for Windows File Server は、Windows Amazon EC2 インスタンスのみをサポートします。Linux Amazon EC2 インスタンスはサポートされていません。
- Amazon ECS を使用した FSx for Windows File Server は AWS Fargate をサポートしません。
- `awsvpc` ネットワークモードで Amazon ECS を使用した FSx for Windows File Server はコンテナエージェントのバージョン `1.54.0` 以降が必要です。
- Amazon ECS タスクに使用できるドライブ文字の最大数は 23 です。FSx for Windows File Server ボリュームを持つ各タスクには、ドライブ文字が割り当てられます。
- デフォルトで、タスクのリソースのクリーンアップ時間は、タスク終了後の 3 時間後に設定されます。タスクによって作成されたファイルマッピングは、使用するタスクが存在しなくなっても 3 時間は保持されます。デフォルトのクリーンアップ時間は、Amazon ECS 環境変数を使用して、設定することができます。`ECS_ENGINE_TASK_CLEANUP_WAIT_DURATION`詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。
- 通常、タスクは FSx for Windows File Server ファイルシステムと同じ VPC でのみ実行されます。ただし、Amazon ECS クラスター VPC と FSx for Windows File Server ファイルシステムの間に VPC ピアリングを介してネットワーク接続が確立されている場合は、クロス VPC の実行がサポートされます。
- VPC セキュリティグループを設定することにより、ネットワークレベルで FSx for Windows File Server ファイルシステムへのアクセスを制御します。Active Directory セキュリティグループが正しく設定された Active Directory ドメインに参加している EC2 インスタンスでホストされているタスクのみが、FSx for Windows File Server ファイル共有にアクセスできます。セキュリティグループの設定が正確でない場合、Amazon ECS はタスクの起動に失敗し、次のエラーメッセージを表示します:「`unable to mount file system fs-id`」。
- FSx for Windows File Server は、AWS Identity and Access Management(IAM) を使用して、IAM ユーザーおよびグループが Windows ファイルサーバーリソースに対して特定の FSx で実行可能なアクションを制御します。クライアント認可を使用すると、ユーザーは、特定の FSx for Windows File Server ファイルシステムへのアクセスを許可または拒否する IAM ロールを定義できます。オプションとして、読み取り専用アクセスを必要とし、またクライアントからのファイルシステムへの root アクセスを許可または禁止することができます。詳細については、Amazon FSx Windows ユーザーガイドの「Security」を参照してください。

Amazon ECS での FSx for Windows File Server の使用に関するベストプラクティス

Amazon ECS で FSx for Windows File Server を使用する場合は以下のベストプラクティスに従うことをお勧めします。

FSx for Windows File Server のセキュリティとアクセス制御

FSx for Windows File Server には、FSx for Windows File Server ファイルシステムに保存されるデータのセキュリティを保証し、それを必要とするアプリケーションからのみアクセス可能とするために使用できる以下のアクセス制御機能があります。

FSx for Windows File Server ボリュームのデータ暗号化

FSx for Windows File Server は、2 つのファイルシステム向け暗号化形式をサポートしています。つまり、保管中および転送中のデータの暗号化です。転送中のデータの暗号化は、SMB プロトコル 3.0 以降をサポートするコンテナインスタンスにマップされたファイル共有でサポートされます。保管中のデータの暗号化は、Amazon FSx ファイルシステムの作成時に自動的に有効になります。Amazon FSx は、アプリケーションを変更することなくファイルシステムにアクセスする際に、SMB 暗号化を使用して転送中のデータを自動的に暗号化します。詳細については、「Amazon FSx for Windows File Server ユーザーガイド」の「Amazon FSx でのデータの暗号化」を参照してください。

フォルダレベルのアクセス制御に Windows ACL を使用する

Windows Amazon EC2 インスタンスは、Active Directory 認証情報を使用して Amazon FSx ファイル共有にアクセスします。きめ細かいファイルレベルおよびフォルダレベルのアクセス制御には、標準の Windows アクセス制御リスト (ACL) を使用します。複数の認証情報を作成でき、それぞれの認証情報は、特定のタスクに対応する共有内の特定のフォルダ向けとなります。

以下の例では、タスクは Secrets Manager に保存されている認証情報を使用してフォルダ `App01` にアクセスできます。Amazon リソースネーム (ARN) は `1234` です。

```
"rootDirectory": "\\path\\to\\my\\data\App01",
"credentialsParameter": "arn-1234",
"domain": "corp.fullyqualified.com",
```

別の例では、タスクは Secrets Manager に保存されている認証情報を使用してフォルダ `App02` にアクセスできます。その ARN は 6789 です。

```
"rootDirectory": "\\path\\to\\my\\data\App02",
"credentialsParameter": "arn-6789",
```

```
"domain": "corp.fullyqualified.com",
```

Amazon ECS タスク定義で FSx for Windows File Server ファイルシステムを指定する

コンテナに FSx for Windows File Server ファイルシステムボリュームを使用するには、タスク定義でボリュームとマウントポイントの設定を指定します。次のスニペットの JSON によるタスク定義では、コンテナの `volumes` と `mountPoints` オブジェクトの構文を示しています。

```
{
    "containerDefinitions": [
        {
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "portMappings": [],
            "command": ["New-Item -Path C:\\fsx-windows-dir\\index.html -ItemType file
 -Value '<html> <head> <title>Amazon ECS Sample App</title> <style>body {margin-top:
 40px; background-color: #333;} </style> </head><body> <div style=color:white;text-
align:center> <h1>Amazon ECS Sample App</h1> <h2>It Works!</h2> <p>You are using Amazon
 FSx for Windows File Server file system for persistent container storage.</p>' -
Force"],
            "cpu": 512,
            "memory": 256,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "essential": false,
            "name": "container1",
            "mountPoints": [
                {
                    "sourceVolume": "fsx-windows-dir",
                    "containerPath": "C:\\fsx-windows-dir",
                    "readOnly": false
                }
            ]
        },
        {
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "portMappings": [
                {
```

```
                    "hostPort": 443,
                    "protocol": "tcp",
                    "containerPort": 80
                }
            ],
            "command": ["Remove-Item -Recurse C:\\inetpub\\wwwroot\\* -Force; Start-
Sleep -Seconds 120; Move-Item -Path C:\\fsx-windows-dir\\index.html -Destination C:\
\inetpub\\wwwroot\\index.html -Force; C:\\ServiceMonitor.exe w3svc"],
            "mountPoints": [
                {
                    "sourceVolume": "fsx-windows-dir",
                    "containerPath": "C:\\fsx-windows-dir",
                    "readOnly": false
                }
            ],
            "cpu": 512,
            "memory": 256,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "essential": true,
            "name": "container2"
        }
    ],
    "family": "fsx-windows",
    "executionRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    "volumes": [
        {
            "name": "fsx-windows-dir",
            "fsxWindowsFileServerVolumeConfiguration": {
                "fileSystemId": "fs-0eeb5730b2EXAMPLE",
                "authorizationConfig": {
                    "domain": "example.com",
                    "credentialsParameter": "arn:arn-1234"
                },
                "rootDirectory": "share"
            }
        }
    ]
}
```

FSxWindowsFileServerVolumeConfiguration

タイプ: オブジェクト

必須: いいえ

このパラメータは、タスクストレージに FSx for Windows File Server ファイルシステムを使用する場合に指定します。

`fileSystemId`

タイプ: 文字列

必須: はい

使用する FSx for Windows File Server ファイルシステムID。

`rootDirectory`

型: 文字列

必須: はい

ホスト内にルートディレクトリとしてマウントする FSx for Windows File Server ファイルシステム内のディレクトリ。

`authorizationConfig`

`credentialsParameter`

型: 文字列

必須: はい

認可の認証情報オプション。

- Secrets Manager シークレットの Amazon リソースネーム (ARN)。
- 用の Amazon リソースネーム (ARN)Systems Managerパラメータ。

`domain`

型: 文字列

必須: はい

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) ディレクトリ、またはセルフホスト型 EC2 Active Directory によってホストされる完全修飾ドメイン名。

FSx for Windows File Server ボリューム認証情報を保存する方法

credentials パラメータで使用するために認証情報を格納するには、2 つの異なる方法があります。

- AWS Secrets Managerシークレット

  この認証情報は、[その他のタイプのシークレット] カテゴリを使用して AWS Secrets Manager コンソールで作成できます。キー/値のペア、ユーザー名/管理者、パスワード/#####ごとに行を追加します。

- Systems Manager パラメータ

  この認証情報は、次のコードスニペット例でのフォームにテキストを入力することで、Systems Manager パラメータコンソールで作成できます。

```
{
  "username": "admin",
  "password": "password"
}
```

タスク定義の `FSxWindowsFileServerVolumeConfiguration` パラメータにある `credentialsParameter` では、シークレット ARN または Systems Manager パラメータ ARN が保持されます 。詳細については、Secrets Manager ユーザーガイド の「AWSSecrets Manager とは？」およびSecrets Manager ユーザーガイド の「Systems Manager パラメータの保存」を参照してください。

Amazon ECS 用の FSx for Windows File Server ファイルシステムを設定する方法について説明します。

FSx for Windows File Server ファイルシステムと、ファイルシステムにアクセスできるコンテナをホストする Amazon ECS に最適化された Windows インスタンスを起動する方法について説明します。これを行うには、最初に AWS Directory Service AWS Managed Microsoft Active Directory を作成します。次に、Amazon EC2 インスタンスとタスク定義を使用して、FSx for Windows File Server ファイルシステムとクラスターを作成します。FSx for Windows File Server ファイルシステムを使用するために、コンテナのタスク定義を設定します。最後に、ファイルシステムをテストします。

アクティブディレクトリ または FSx for Windows File Server ファイルシステムのいずれかを起動または削除するのに、毎回 20～45 分かかります。90 分以上予約して、チュートリアルを完了するか、いくつかのセッションでチュートリアルを完了する準備をしてください。

チュートリアルの前提条件

- 管理ユーザー。「Amazon ECS を使用するようにセットアップする」を参照してください。
- (オプション) RDP アクセスを介して EC2 Windows インスタンスに接続するための PEM キーペア。キーペアの作成方法については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 のキーペアと Amazon EC2 インスタンス」を参照してください。
- 少なくとも 1 つのパブリックサブネットと 1 つのプライベートサブネット、および 1 つのセキュリティグループを持つ VPC。デフォルトの VPC を使用できます。NAT ゲートウェイやデバイスは必要ありません。AWS Directory Service は、Active Directory でのネットワークアドレス変換 (NAT) をサポートしていません。これを機能させるには、アクティブディレクトリ、FSx for Windows File Server ファイルシステム、ECS クラスター、および EC2 インスタンスが VPC 内に配置されている必要があります。VPC と Active Directory の詳細については、「VPC を作成する」および「AWS Managed Microsoft AD を作成するための前提条件」を参照してください。
- IAM ecsInstanceRole および ecsTaskExecutionRole アクセス許可は、お客様のアカウントに関連付けられています。このようなサービスリンクロールを使用すると、サービスが API 呼び出しを行い、ユーザーに代わってコンテナ、シークレット、ディレクトリ、ファイルサーバーにアクセスできます。

ステップ 1: IAM アクセスロールを作成する

AWS Management Console を使用してクラスターを作成します。

1. Amazon ECS コンテナインスタンスの IAM ロールを参照して ecsInstanceRole があるかどうかを確認し、持っていない場合はどのように作成できるかを確認してください。
2. 実際の本番環境では、ロールポリシーを最小限のアクセス許可に合わせてカスタマイズすることをお勧めします。このチュートリアルを通じて取り組むために、次の AWS マネージド ポリシーが ecsInstanceRole に添付されていることを確認します。ポリシーがまだアタッチされていない場合は、ポリシーをアタッチします。

   - AmazonEC2ContainerServiceforEC2Role
   - AmazonSSMManagedInstanceCore
   - AmazonSSMDirectoryServiceAccess

   AWS マネージド ポリシーをアタッチするには

   a. IAM コンソールを開きます。

b. ナビゲーションペインで [Roles (ロール)] を選択します。

c. [AWS 管理ロール] を選択します。

d. [アクセス許可]、[ポリシーのアタッチ] の順に選択します。

e. アタッチする利用可能なポリシーを絞り込むには、[Filter] を使用します。

f. 適切なポリシーを選択し、[Attach policy] を選択します。

3. Amazon ECS タスク実行IAM ロール を参照して ecsTaskExecutionRole があるかどうかを確認し、持っていない場合はどのように作成できるかを確認してください。

   実際の本番環境では、ロールポリシーを最小限のアクセス許可に合わせてカスタマイズすることをお勧めします。このチュートリアルを通じて取り組むために、次の AWSマネージド ポリシーが ecsTaskExecutionRole に添付されていることを確認します。ポリシーがまだアタッチされていない場合は、ポリシーをアタッチします。AWSマネージド ポリシーをアタッチするには、前のセクションで説明した手順を使用します。

   - SecretsManagerReadWrite
   - AmazonFSxReadOnlyAccess
   - AmazonSSMReadOnlyAccess
   - AmazonECSTaskExecutionRolePolicy

手順 2: Windows Active Directory (AD) を作成する

1. 「AWS Directory Service 管理ガイド」の「AWS マネージド AD の作成]で説明されている手順に従います。このチュートリアル用に指定した VPC を使用します。「AWS マネージド AD の作成」のステップ 3 で、次のステップで使用するためにユーザー名と管理者パスワードを保存します。また、今後の手順の完全修飾ディレクトリ DNS 名をメモしておきます。Active Directory の作成中に、次の手順を実行できます。
2. 次のステップで使用する AWS Secrets Manager のシークレットを作成します。詳細については、「AWS Secrets Manager ユーザーガイド」の「Secrets Manager の使用を開始する」を参照してください。

   a. Secrets Managerコンソール を開きます。

   b. [新しいシークレットを保存する] を選択します。

   c. [その他のシークレット] を選択します。

   d. [シークレットキー/値] では、最初の行に値 **admin** を含むキー **username** を作成します。[+ 行を追加] をクリックします。

e. 新しい行で、キー **password** を作成します。値には、AWSマネージド AD ディレクトリ の作成 の手順 3 で入力したパスワードを入力します。

f. [Next] ボタンをクリックします。

g. シークレットの名前と説明を入力します。[次へ] をクリックします。

h. [次へ] をクリックします。[保存] をクリックします。

i. [シークレット] ページのリストから、作成したシークレットをクリックします。

j. 次の手順で使用するために、新しいシークレットの ARN を保存します。

k. Active Directory の作成中に、次の手順に進むことができます。

ステップ 3: セキュリティグループを確認および更新する

このステップでは、使用しているセキュリティグループのルールを確認および更新します。このためには、VPC 用に作成されたデフォルトのセキュリティグループを使用できます。

セキュリティグループを確認および更新します。

ポートとの間でデータを送信するには、セキュリティグループを作成または編集する必要があります。これについては、[FSx for Windows File Server ユーザーガイド]の[Amazon VPC セキュリティグループ]で説明されています。これを行うには、インバウンドルールの次の表の最初の行に示されているセキュリティグループインバウンドルールを作成します。このルールでは、同じセキュリティグループに割り当てられているネットワークインターフェイス (および関連付けられているインスタンス) からのインバウンドトラフィックを使用できます。作成したクラウドリソースはすべて同じ VPC 内にあり、同じセキュリティグループにアタッチされます。したがって、このルールでは、必要に応じて、FSx for Windows File Server ファイルシステム、アクティブディレクトリ、ECSインスタンスとの間でトラフィックを送信することができます。その他のインバウンドルールでは、ウェブサイトでトラフィックを利用し、ECS インスタンスに接続するための RDP アクセスが行えます。

次の表に、このチュートリアルに必要なセキュリティグループのインバウンドルールを示します。

タイプ	プロトコル	ポート範囲	ソース
すべてのトラフィック	すべて	すべて	*sg-securitygroup*
HTTPS	TCP	443	0.0.0.0/0

タイプ	プロトコル	ポート範囲	ソース
RDP	TCP	3389	ラップトップの IP アドレス

次の表に、このチュートリアルに必要なセキュリティグループのアウトバウンドルールを示します。

タイプ	プロトコル	ポート範囲	デスティネーション
すべてのトラフィック	すべて	すべて	0.0.0.0/0

1. EC2 コンソールを開き、左側のメニューから [セキュリティグループ] を選択します。
2. 表示されるセキュリティグループのリストから、このチュートリアルで使用しているセキュリティグループの左側にあるチェックボックスをオンにします。

   セキュリティグループの詳細が表示されます。
3. [Inbound rules] (インバウンドルール) または [Outbound rules] (アウトバウンドルール) タブを選択して、[Edit inbound rules] (インバウンドルールの編集) または [Edit outbound rules] (アウトバウンドルールの編集) ボタンを選択して、インバウンドルールおよびアウトバウンドルールを編集します。前の表に表示されたルールと一致するようにルールを編集します。このチュートリアルの後半で EC2 インスタンスを作成した後、「Amazon EC2 ユーザーガイド」の「RDP を使用して Windows インスタンスに接続する」の説明に従って、EC2 インスタンスのパブリック IP アドレスを使用してインバウンドルールの RDP ソースを編集します。

ステップ 4: FSx for Windows File Server ファイルシステムを作成する

セキュリティグループが検証および更新され、アクティブディレクトリ が作成され、アクティブステータスになったら、Active Directory と同じ VPC に FSx for Windows File Server ファイルシステムを作成します。次のステップを使用して、Windows タスク用の FSx for Windows File Server ファイルシステムを作成します。

最初のファイルシステムを作成します。

1. [Amazon FSx コンソール] を開きます。

2. ダッシュボードで [Create file system] (ファイルシステムの作成) を選択して、ファイルシステム作成ウィザードをスタートします。
3. [Select file system type] (ファイルシステムのタイプを選択) のページで、[FSx for Windows File Server] (FSx for Windows ファイルサーバー) を選択し、[Next] (次へ) を選択します。[Create file system] (ファイルシステムを作成) ページが表示されます。
4. [File system details] (ファイルシステム詳細) セクションで、ファイルシステムの名前を入力します。ファイルシステムに名前を付けると、ファイルの検索と管理が容易になります。最大 256 文字の Unicode 文字を使用できます。使用できる文字は、文字、数字、スペース、および特殊文字のプラス記号 (+)、マイナス記号 (-)、等号 (=)、ピリオド (.)、アンダースコア (_)、コロン (:)、スラッシュ (/) です。
5. [Deployment type] で [Single-AZ] を選択して、1 つのアベイラビリティーゾーンにデプロイされたファイルシステムをデプロイします。[Single-AZ 2] (シングル AZ 2) は、最新世代の単一アベイラビリティーゾーンファイルシステムで、SSD および HDD ストレージをサポートします。
6. [Storage type] で、 [HDD] を選択します。
7. [Storage capacity] に、ストレージの最小容量を入力します。
8. [Throughput capacity] はデフォルト設定のままにします。
9. [ネットワーク & セキュリティ] セクションで、AWS Directory Service ディレクトリに対して選択したものと同じ Amazon VPC を選択します。
10. [VPC Security Groups] で、ステップ 3: セキュリティグループを確認および更新するで検証したセキュリティグループを選択します。
11. [Windows 認証] では、[AWSマネージド Microsoft アクティブディレクトリ] を選択し、リストからお使いの AWS Directory Service ディレクトリを選択します。
12. [Encryption] (暗号化) では、[aws / fsx (default)] (aws / fsx (デフォルト) の [Encryption key] (暗号化キー) 設定をデフォルトのままにします。
13. [Maintenance preferences] ではデフォルト設定のままにします。
14. [Next] ボタンをクリックします。
15. [Create file system] (ファイルシステムの作成) ページで表示されるファイルシステム設定を確認します。参照のために、ファイルシステム作成後に変更できるファイルシステム設定を書き留めます。[Create file system] (ファイルシステムの作成) を選択します。
16. ファイルシステム ID をメモします。ID は後の手順で使用する必要があります。

    FSx for Windows File Server ファイルシステムの作成中に、クラスターと EC2 インスタンスを作成するには、次のステップに進みます。

ステップ 5: Amazon ECS クラスターを作成する

Amazon ECS コンソールを使用してクラスターを作成する

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [クラスター設定] の [クラスター名] に「windows-fsx-cluster」と入力します。
6. [インフラストラクチャ] を展開し、[AWS Fargate (サーバーレス)] をクリアして、[Amazon EC2 インスタンス] を選択します。
   - Auto Scaling グループを作成するには、Auto Scaling group(ASG) (Auto Scaling グループ) から、[Create new group] (新しいグループの作成) を選択し、グループに関する以下の詳細情報を入力します。
     - [オペレーティングシステム/アーキテクチャ] で [Windows Server 2019 Core] を選択します。
     - [EC2 インスタンスタイプ] で [t2.medium] または [t2.micro] を選択します。
7. [Create] (作成) を選択します。

ステップ 6: Amazon ECS に最適化された Amazon EC2 インスタンスを作成する

Amazon ECS Windows コンテナインスタンスを作成します。

Amazon ECS インスタンスを作成するには

1. `aws ssm get-parameters` コマンドを使用して、VPC をホストするリージョン用の AMI 名を取得します。詳細については、「Amazon ECS に最適化された AMI メタデータを取得する」を参照してください。
2. Amazon EC2 コンソールを使用して、インスタンスを起動します。
   a. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
   b. ナビゲーションバーから、使用するリージョンを選択します。
   c. EC2 ダッシュボードから、[Launch Instance] を選択します。
   d. [Name (名前)] に一意の名前を入力します。

e. [アプリケーションと OS イメージ (Amazon マシンイメージ)] の [検索] フィールドに、取得した AMI 名を入力します。

f. [インスタンスタイプ] で [t2.medium] または [t2.micro] を選択します。

g. [Key pair (login)] (キーペア (ログイン)) には、キーペアを選択します。キーペアを指定しない場合、

h. [ネットワーク設定] の [VPC] と [サブネット]で VPC とパブリックサブネットを選択します。

i. [Network settings] (ネットワーク設定) にある [Security group] (セキュリティグループ) には、既存のセキュリティグループを選択することも、新しいセキュリティグループを作成することもできます。選択したセキュリティグループに チュートリアルの前提条件 で定義されたインバウンドルールとアウトバウンドルールがあることを確認してください。

j. [Network settings] (ネットワーク設定) の [Auto-assign Public IP] (パブリック IP の自動割り当て) で、[Enable] (有効にする) を選択します。

k. [高度な詳細] を展開し、作成した Active Directory の ID を [ドメイン結合ディレクトリ] で選択します。このオプションドメインは、EC2 インスタンスの起動時に AD に参加します。

l. [Advanced details] (高度な詳細) で、[IAM instance profile] (IAM インスタンスプロファイル) として [ecsInstanceRole] を選択します。

m. 次のユーザーデータを使用して、Amazon ECS コンテナインスタンスを設定します。[Advanced Details] (詳細情報) にある [User data] (ユーザーデータ) フィールドに以下のスクリプトを貼り付け、*cluster_name* をクラスターの名前に置き換えます。

```
<powershell>
Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
</powershell>
```

n. 準備ができたら、確認フィールドを選択してから、[Launch Instances] を選択します。

o. 確認ページは、インスタンスが起動中であることを通知します。[View Instances] (インスタンスを表示) を選択して確認ページを閉じ、コンソールに戻ります。

3. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。

4. ナビゲーションペインで、[クラスター] を選択し、[windows-fsx-cluster] を選択します。

5. [インフラストラクチャ] タブを選択し、インスタンスが windows-fsx-cluster クラスターに登録されていることを確認します。

ステップ 7: Windows タスク定義を登録する

Amazon ECS クラスターで Windows コンテナを実行する前に、タスク定義を登録する必要があります。次のタスク定義の例では、シンプルなウェブページを表示します。このタスクは、FSx ファイルシステムにアクセスできる 2 つのコンテナを起動します。最初のコンテナは HTML ファイルをファイルシステムに書き込みます。2 番目のコンテナは、ファイルシステムから HTML ファイルをダウンロードし、ウェブページを提供します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
4. JSON エディタボックスで、タスク実行ロールの値と FSx ファイルシステムの詳細を置き換えてから [保存] を選択します。

```
{
    "containerDefinitions": [
        {
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "portMappings": [],
            "command": ["New-Item -Path C:\\fsx-windows-dir\\index.html -ItemType
 file -Value '<html> <head> <title>Amazon ECS Sample App</title> <style>body
 {margin-top: 40px; background-color: #333;} </style> </head><body> <div
 style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1> <h2>It
 Works!</h2> <p>You are using Amazon FSx for Windows File Server file system for
 persistent container storage.</p>' -Force"],
            "cpu": 512,
            "memory": 256,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "essential": false,
            "name": "container1",
            "mountPoints": [
                {
                    "sourceVolume": "fsx-windows-dir",
                    "containerPath": "C:\\fsx-windows-dir",
                    "readOnly": false
                }
```

```
            ]
        },
        {
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "portMappings": [
                {
                    "hostPort": 443,
                    "protocol": "tcp",
                    "containerPort": 80
                }
            ],
            "command": ["Remove-Item -Recurse C:\\inetpub\\wwwroot\\* -Force;
 Start-Sleep -Seconds 120; Move-Item -Path C:\\fsx-windows-dir\\index.html -
Destination C:\\inetpub\\wwwroot\\index.html -Force; C:\\ServiceMonitor.exe
 w3svc"],
            "mountPoints": [
                {
                    "sourceVolume": "fsx-windows-dir",
                    "containerPath": "C:\\fsx-windows-dir",
                    "readOnly": false
                }
            ],
            "cpu": 512,
            "memory": 256,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "essential": true,
            "name": "container2"
        }
    ],
    "family": "fsx-windows",
    "executionRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
    "volumes": [
        {
            "name": "fsx-windows-dir",
            "fsxWindowsFileServerVolumeConfiguration": {
                "fileSystemId": "fs-0eeb5730b2EXAMPLE",
                "authorizationConfig": {
                    "domain": "example.com",
                    "credentialsParameter": "arn:arn-1234"
                },
```

```
                "rootDirectory": "share"
            }
        }
    ]
}
```

ステップ 8: タスクを実行して結果を表示する

タスクを実行する前に、FSx for Windows File Server ファイルシステムのステータスが [Available] であることを確認します。利用可能になったら、作成したタスク定義を使用してタスクを実行できます。タスクはコンテナを作成することから始まります。コンテナはファイルシステムを使用してコンテナ間で HTML ファイルをシャッフルします。シャッフル後、ウェブサーバーは単純な HTML ページを提供します。

> **Note**
>
> VPN 内からそのウェブサイトに接続できない場合があります。

Amazon ECS コンソールを使用して、タスクを実行して結果を表示します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、[クラスター] を選択し、[windows-fsx-cluster] を選択します。
3. [タスク] タブを選択し、[新しいタスクを実行] を選択します。
4. [起動タイプ] で、[EC2] を選択します。
5. デプロイ設定の [タスク定義] で [fsx-windows] を選択し、[作成] を選択します。
6. タスクのステータスが [実行中] の場合は、タスク ID を選択します。
7. [コンテナ] で container1 のステータスが [停止] の場合、 container2 を選択してコンテナの詳細を表示します。
8. [container2 のコンテナの詳細] で [ネットワークバインディング] を選択し、コンテナに関連付けられている外部 IP アドレスをクリックします。ブラウザが開き、次のメッセージが表示されます。

```
Amazon ECS Sample App
It Works!
You are using Amazon FSx for Windows File Server file system for persistent
 container storage.
```

> **Note**
>
> メッセージが表示されるまでに数分かかることがあります。このメッセージが数分経っても表示されない場合は、VPN で実行していないことを確認し、コンテナインスタンスのセキュリティグループがポート 443 でのインバウンドネットワーク HTTP トラフィックを許可していることを確認します。

ステップ 9: クリーンアップする。

> **Note**
>
> FSx for Windows File Server ファイルシステムまたは AD の削除には、20～45分かかります。AD の削除操作を開始する前に、FSx for Windows File Server ファイルシステムの削除操作が完了するまで待たなければなりません。

FSx for Windows File Server ファイルシステムを削除します。

1. [Amazon FSxコンソール] を開きます。
2. 作成した FSx for Windows File Server ファイルシステムの左側にあるラジオボタンを選択します。
3. [アクション] を選択します。
4. [Delete file system] をクリックします。

AD を削除します。

1. AWS Directory Service コンソールを開きます。
2. 作成した AD の左側にあるラジオボタンを選択します。
3. [アクション] を選択します。
4. [Delete directory] を選択します。

クラスターを削除します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。

2. ナビゲーションペインで、[クラスター] を選択し、[fsx-windows-cluster] を選択します。
3. [クラスターの削除] を選択してください。
4. フレーズを入力し、[削除] を選択します。

EC2 インスタンスを終了します。

1. Amazon EC2 コンソールを開きます。
2. 左側のメニューから、[Instances] を選択します。
3. 作成した EC2 インスタンスの左側にあるボックスをチェックします。
4. [インスタンス状態]、[インスタンスを終了] の順にクリックします。

シークレットを削除します。

1. Secrets Managerコンソール を開きます。
2. このチュートリアル用に作成したシークレットを選択します。
3. [Actions] をクリックします。
4. [Delete secret] を選択します。

Amazon ECS での Docker ボリュームの使用

Docker ボリュームを使用している場合は、組み込みの `local` ドライバーまたはサードパーティーのボリュームドライバーを使用できます。Docker ボリュームは Docker で管理され、ディレクトリはボリュームデータを含むコンテナインスタンスの `/var/lib/docker/volumes` に作成されます。

Docker ボリュームを使用するには、タスク定義で `dockerVolumeConfiguration` を指定します。詳細については、Docker ドキュメントの「Volumes」を参照してください。

Docker ボリュームの一般的ユースケースは以下のとおりです。

- コンテナで使用する永続データボリュームを提供する
- 定義したデータボリュームを同じコンテナインスタンス上の異なるコンテナにある別々の場所で共有する
- 空の非永続データボリュームを定義し、同じタスク内の複数のコンテナにマウントする
- サードパーティー製ドライバーによって管理されるタスクに、データボリュームを提供する

Docker ボリュームの使用に関する考慮事項

Docker ボリュームを使用する際は、以下の点を考慮します。

- Docker ボリュームは、EC2 起動タイプ、または外部インスタンスを使用する場合にのみサポートされます。
- Windows コンテナでは、`local` ドライバーの使用のみサポートされます。
- サードパーティー製ドライバーを使用する場合は、コンテナエージェントを起動する前に、必ずドライバーをコンテナインスタンスにインストールしアクティブ化しておきます。エージェントを開始する前にサードパーティー製ドライバーがアクティブ化されていない場合は、以下のいずれかのコマンドを使用してコンテナエージェントを再起動することが可能です。
  - Amazon ECS に最適化された Amazon Linux 2 AMI の場合:

    ```
    sudo systemctl restart ecs
    ```

  - Amazon ECS に最適化された Amazon Linux AMI の場合:

    ```
    sudo stop ecs && sudo start ecs
    ```

Amazon ECS タスク定義で Docker ボリュームを指定する

コンテナでデータボリュームを使用するには、ボリュームを指定し、タスク定義でポイント設定をマウントする必要があります。このセクションでは、コンテナのボリューム設定について説明します。Docker ボリュームを使用する`dockerVolumeConfiguration` を指定します。バインドマウントのホストボリュームを使用するタスクで、`host` とオプションの `sourcePath` を指定します。

次のタスク定義の JSON スニペットに、コンテナの `volumes` と `mountPoints` オブジェクト用の構文を示します。

```
{
    "containerDefinitions": [
        {
            "mountPoints": [
                {
                    "sourceVolume": "string",
                    "containerPath": "/path/to/mount_volume",
                    "readOnly": boolean
                }
            ]
```

```
        }
    ],
    "volumes": [
        {
            "name": "string",
            "dockerVolumeConfiguration": {
                "scope": "string",
                "autoprovision": boolean,
                "driver": "string",
                "driverOpts": {
                    "key": "value"
                },
                "labels": {
                    "key": "value"
                }
            }
        }
    ]
}
```

name

タイプ: 文字列

必須: いいえ

ボリュームの名前。最大 255 文字の英字 (大文字と小文字の区別あり)、数字、ハイフン (-)、アンダースコア (_) を使用できます。この名前は、コンテナ定義 mountPoints オブジェクトの sourceVolume パラメータで参照されます。

dockerVolumeConfiguration

タイプ: DockerVolumeConfiguration オブジェクト

必須: いいえ

このパラメータは、Docker ボリュームを使用する場合に指定します。Docker ボリュームは、EC2 インスタンスでタスクを実行する場合にのみサポートされます。Windows コンテナでは、local ドライバーの使用のみがサポートされます。バインドマウントを使用するには、代わりに host を指定します。

scope

型: 文字列

有効な値: task | shared

必須: いいえ

Docker ボリュームのスコープ。これにより、ボリュームのライフサイクルが決定されます。Docker ボリュームの範囲が task の場合は、タスクが開始すると自動的にプロビジョンされ、タスクが停止すると破棄されます。Docker ボリュームの範囲が shared の場合は、タスクの停止後も保持されます。

autoprovision

タイプ: ブール値

デフォルト値: false

必須: いいえ

この値が true の場合、既に存在していない場合は Docker ボリュームが作成されます。このフィールドは、scope が shared の場合にのみ使用されます。scope が task の場合、このパラメータは省略する必要があります。

driver

タイプ: 文字列

必須: いいえ

使用する Docker ボリュームドライバー。この名前はタスク配置に使用されるため、ドライバー値は Docker で提供されているドライバー名と一致する必要があります。ドライバーが Docker プラグイン CLI を使用してインストールされた場合は、docker plugin ls を使用してコンテナインスタンスからドライバー名を取得します。ドライバーが別の方法でインストール済みである場合は、Docker プラグイン検出を使用してドライバー名を取得します。

driverOpts

タイプ: 文字列

必須: いいえ

パススルーする Docker ドライバー固有のオプションのマップ。このパラメータは、Docker の「Create a volume」セクションの DriverOpts にマッピングされます。

labels

タイプ: 文字列

必須: いいえ

Docker ボリュームに追加するカスタムメタデータ。

`mountPoints`

タイプ: オブジェクト配列

必須: いいえ

コンテナでのデータボリュームのマウントポイント。このパラメータは creat-container Docker API の `Volumes` にマッピングされ、docker run の `--volume` オプションにマッピングされます。

Windows コンテナは `$env:ProgramData` と同じドライブに全部のディレクトリをマウントできます。Windows コンテナは、別のドライブにディレクトリをマウントすることはできません。また、マウントポイントは複数のドライブにまたがることはできません。Amazon EBS ボリュームを Amazon ECS タスクに直接アタッチするには、マウントポイントを指定する必要があります。

`sourceVolume`

タイプ: 文字列

必須: はい (`mountPoints` を使用する場合)

マウントするボリュームの名前。

`containerPath`

型: 文字列

必須: はい (`mountPoints` を使用する場合)

ボリュームをマウントするコンテナ内のパス。

`readOnly`

型: ブール値

必須: いいえ

この値が `true` の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が `false` の場合、コンテナはボリュームに書き込むことができます。デフォルト値は `false` です。

Windows オペレーティングシステムを実行している EC2 インスタンスで実行されるタスクの場合、 値をデフォルト の `false` のままにします。

Docker ボリュームの例

Docker ボリュームを使用してコンテナの一時ストレージを提供する

この例では、コンテナは空のデータボリュームを使用しており、これはタスクが完了した後に破棄されます。ユースケースの一例としては、タスクの実行中に一部のスクラッチファイルストレージにアクセスする必要のあるコンテナが考えられます。このタスクは、Docker ボリュームを使用して行うことができます。

1. タスク定義の `volumes` セクションで、`name` および `DockerVolumeConfiguration` 値を使用して、データボリュームを定義します。この例では、タスクが停止した後にボリュームが削除されるように、範囲に `task` を指定して、組み込みの `local` ドライバーを使用します。

```
"volumes": [
    {
        "name": "scratch",
        "dockerVolumeConfiguration" : {
            "scope": "task",
            "driver": "local",
            "labels": {
                "scratch": "space"
            }
        }
    }
]
```

2. `containerDefinitions` セクションで、定義したボリュームの名前を参照する `mountPoints` 値と、コンテナにボリュームをマウントするための `containerPath` 値を使用して、コンテナを定義します。

```
"containerDefinitions": [
    {
        "name": "container-1",
        "mountPoints": [
            {
              "sourceVolume": "scratch",
              "containerPath": "/var/scratch"
            }
```

```
        ]
    }
]
```

Docker ボリュームを使用してコンテナの永続的ストレージを提供する

この例では、複数のコンテナで使用する共有ボリュームが必要で、また、使用するタスクの内の 1 つが停止した後も、このボリュームを維持する必要があります。組み込みの `local` ドライバーは使用中です。このためボリュームは、コンテナインスタンスのライフサイクルに紐付けられたままです。

1. タスク定義の `volumes` セクションで、`name` および `DockerVolumeConfiguration` 値を使用して、データボリュームを定義します。この例では、`shared` スコープをボリュームが維持されるように指定し、自動プロビジョニングを `true` に設定します。これは、使用するためのボリュームが作成されるようにするためです。また、組み込みの `local` ドライバーも使用します。

```
"volumes": [
    {
        "name": "database",
        "dockerVolumeConfiguration" : {
            "scope": "shared",
            "autoprovision": true,
            "driver": "local",
            "labels": {
                "database": "database_name"
            }
        }
    }
]
```

2. `containerDefinitions` セクションで、定義したボリュームの名前を参照する `mountPoints` 値と、コンテナにボリュームをマウントするための `containerPath` 値を使用して、コンテナを定義します。

```
"containerDefinitions": [
    {
        "name": "container-1",
        "mountPoints": [
        {
```

```
          "sourceVolume": "database",
          "containerPath": "/var/database"
        }
      ]
    },
    {
      "name": "container-2",
      "mountPoints": [
        {
          "sourceVolume": "database",
          "containerPath": "/var/database"
        }
      ]
    }
  ]
```

Docker ボリュームを使用してコンテナの NFS 永続的ストレージを提供する

この例では、コンテナはタスクの開始時に自動的にマウントされ、タスクの停止時にアンマウントされる NFS データボリュームを使用します。これは Docker ビルトイン `local` ドライバーを使用します。ユースケースの一例としては、ローカル NFS ストレージがあり、ECS Anywhere タスクからアクセスする必要がある場合があります。これは、NFS ドライバーオプションの Docker ボリュームを使用して実現できます。

1. タスク定義の `volumes` セクションで、`name` および `DockerVolumeConfiguration` 値を使用して、データボリュームを定義します。この例では、タスクが停止した後にボリュームがアンマウントされるように `task` のスコープを指定してください。`local` ドライバーを使用し、`type`、`device`、および `o` オプションを適宜使用して `driverOpts` を設定します。NFS_SERVER は NFS サーバーエンドポイントに置き換えます。

```
"volumes": [
       {
           "name": "NFS",
           "dockerVolumeConfiguration" : {
               "scope": "task",
               "driver": "local",
               "driverOpts": {
                   "type": "nfs",
                   "device": "$NFS_SERVER:/mnt/nfs",
                   "o": "addr=$NFS_SERVER"
               }
```

```
            }
        }
    ]
```

2. containerDefinitions セクションで、定義したボリュームの名前を参照する mountPoints 値と、コンテナにボリュームをマウントするための containerPath 値を使用して、コンテナを定義します。

```
"containerDefinitions": [
        {
            "name": "container-1",
            "mountPoints": [
                {
                  "sourceVolume": "NFS",
                  "containerPath": "/var/nfsmount"
                }
            ]
        }
    ]
```

Amazon ECS でのバインドマウントの使用

バインドマウントでは、ホスト (Amazon EC2 インスタンスなど) 上のファイルまたはディレクトリがコンテナにマウントされます。バインドマウントは、Fargate インスタンスと Amazon EC2 インスタンスの両方でホストされているタスクでサポートされています。バインドマウントは、それらを使用するコンテナのライフサイクルに紐付けられています。タスクが停止するなど、バインドマウントを使用するすべてのコンテナが停止すると、データが削除されます。Amazon EC2 インスタンスでホストされているタスクの場合、タスク定義で host とオプションの sourcePath 値を指定することにより、ホスト側 Amazon EC2 インスタンスのライフサイクルにデータを紐付けすることができます。詳細については、Docker ドキュメントの「Bind mounts」を参照してください。

バインドマウントの一般的なユースケースは以下のとおりです。

- 1 つ以上のコンテナにマウントするための空のデータボリュームを提供する。
- 1 つ以上のコンテナにホストデータボリュームをマウントする。
- ソースコンテナのデータボリュームを、同じタスク内の他のコンテナと共有する。
- Dockerfile から 1 つ以上のコンテナにパスとその内容を公開する。

バインドマウントを使用するときの考慮事項

バインドマウントを使用する際には、以下の点を考慮してください。

- プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) を使用して AWS Fargate でホストされているタスクの場合、デフォルトでは、バインドマウント用に最低 20 GiB の一時ストレージが割り当てられます。タスク定義で `ephemeralStorage` パラメータを指定することによって、一時ストレージの総量を最大 200 GiB まで増やすことができます。
- タスクの実行時に Dockerfile のファイルをデータボリュームに公開するために、Amazon ECS データプレーンが `VOLUME` ディレクティブを探します。`VOLUME` ディレクティブで指定された絶対パスが、タスク定義で指定された `containerPath` と同じである場合、`VOLUME` ディレクティブパス内のデータがデータボリュームにコピーされます。次の Dockerfile の例では、`/var/log/exported` ディレクトリにある `examplefile` という名前のファイルがホストに書き込まれ、その後でコンテナ内にマウントされます。

  ```
  FROM public.ecr.aws/amazonlinux/amazonlinux:latest
  RUN mkdir -p /var/log/exported
  RUN touch /var/log/exported/examplefile
  VOLUME ["/var/log/exported"]
  ```

  デフォルトでは、ボリューム許可は `0755` に設定され、所有者は `root` に設定されます。これらのアクセス許可は Dockerfile でカスタマイズできます。次の例では、ディレクトリの所有者を node として定義しています。

  ```
  FROM public.ecr.aws/amazonlinux/amazonlinux:latest
  RUN yum install -y shadow-utils && yum clean all
  RUN useradd node
  RUN mkdir -p /var/log/exported && chown node:node /var/log/exported
  RUN touch /var/log/exported/examplefile
  USER node
  VOLUME ["/var/log/exported"]
  ```

- Amazon EC2 インスタンスでホストされているタスクで、`host` 値と `sourcePath` 値が指定されていない場合には、Docker デーモンがバインドマウントを自動的に管理します。このバインドマウントを参照するコンテナが存在しない場合、このマウントは、Amazon ECS コンテナエージェントのタスククリーンアップサービスによって最終的に削除されます。デフォルトでは、この処理はコンテナが終了してから 3 時間後に実行されま。また、この期間は `ECS_ENGINE_TASK_CLEANUP_WAIT_DURATION` エージェント変数により設定することも可能です。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。コン

テナのライフサイクルを通じてこのデータを永続化する必要がある場合は、バインドマウントの sourcePath 値を指定します。

Amazon ECS タスク定義でバインドマウントを指定する

Fargate または Amazon EC2 インスタンスでホストされている Amazon ECS タスクについて、以下のタスク定義 JSON スニペットにタスク定義向け volumes、mountPoints、ephemeralStorage オブジェクトの構文を示します。

```
{
   "family": "",
   ...
   "containerDefinitions" : [
      {
         "mountPoints" : [
            {
               "containerPath" : "/path/to/mount_volume",
               "sourceVolume" : "string"
            }
          ],
          "name" : "string"
       }
    ],
    ...
    "volumes" : [
       {
          "name" : "string"
       }
    ],
    "ephemeralStorage": {
    "sizeInGiB": integer
    }
}
```

Amazon EC2 インスタンスでホストされる Amazon ECS タスクで、タスクボリュームの詳細を指定する場合は、オプションの host パラメータおよび sourcePath を使用できます。これを指定すると、バインドマウントはコンテナではなくタスクのライフサイクルに紐付けされます。

```
"volumes" : [
    {
        "host" : {
```

```
            "sourcePath" : "string"
        },
        "name" : "string"
    }
]
```

以下では、各タスク定義パラメータについて詳しく説明します。

name

型: 文字列

必須: いいえ

ボリュームの名前。最大 255 文字の英字 (大文字と小文字の区別あり)、数字、ハイフン (-)、アンダースコア (_) を使用できます。この名前は、コンテナ定義 mountPoints オブジェクトの sourceVolume パラメータで参照されます。

host

必須: いいえ

host パラメーターは、バインドマウントのライフサイクルを、タスクではなくホスト Amazon EC2 インスタンスと、それが格納されている場所に関連付けるために使用されます。host パラメーターが空の場合、Docker デーモンはデータボリュームのホストパスを割り当てますが、関連付けられたコンテナの実行が停止した後にデータが保持されるとは限りません。

Windows コンテナは $env:ProgramData と同じドライブに全部のディレクトリをマウントできます。

> **Note**
>
> sourcePath パラメータは、Amazon EC2 インスタンスでホストされているタスクを使用する場合にのみサポートされます。

sourcePath

タイプ: 文字列

必須: いいえ

host パラメータを使用する場合は、sourcePath を指定して、コンテナに表示されるホスト Amazon EC2 インスタンスのパスを宣言します。このパラメータが空の場合は、Docker デーモンによってホストパスが割り当てられます。host パラメータに sourcePath の場所が含まれている場合、データボリュームは手動で削除するまでホスト Amazon EC2 インスタンスの指定された場所に保持されます。sourcePath の値がホスト Amazon EC2 インスタンスに存在しない場合は、Docker デーモンによって作成されます。その場所が存在する場合は、ソースパスフォルダの内容がエクスポートされます。

mountPoints

タイプ: オブジェクト配列

必須: いいえ

コンテナでのデータボリュームのマウントポイント。このパラメータは creat-container Docker API の Volumes にマッピングされ、docker run の --volume オプションにマッピングされます。

Windows コンテナは $env:ProgramData と同じドライブに全部のディレクトリをマウントできます。Windows コンテナは、別のドライブにディレクトリをマウントすることはできません。また、マウントポイントは複数のドライブにまたがることはできません。Amazon EBS ボリュームを Amazon ECS タスクに直接アタッチするには、マウントポイントを指定する必要があります。

sourceVolume

タイプ: 文字列

必須: はい (mountPoints を使用する場合)

マウントするボリュームの名前。

containerPath

型: 文字列

必須: はい (mountPoints を使用する場合)

ボリュームをマウントするコンテナ内のパス。

readOnly

型: ブール値

必須: いいえ

この値が `true` の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が `false` の場合、コンテナはボリュームに書き込むことができます。デフォルト値は `false` です。

Windows オペレーティングシステムを実行している EC2 インスタンスで実行されるタスクの場合、 値をデフォルト の `false` のままにします。

`ephemeralStorage`

タイプ: オブジェクト

必須: いいえ

タスクに割り当てるエフェメラルストレージの容量(GB)。このパラメータは、AWS Fargate プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) を使用してホストされているタスクの場合、利用可能なエフェメラルストレージの総量をデフォルト容量を超えて拡張するために使用されます。

コパイロットCLI、CloudFormation、AWSSDK または CLI を使用して、バインドマウントのエフェメラルストレージを指定します。

バインドマウントの例

以下の例では、コンテナにバインドマウントを使用する場合の一般的なユースケースについて説明します。

Fargate タスク用の一時ストレージ容量の増加を割り当てるには

プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` (Windows) を使用して Fargate でホストされる Amazon ECS タスクの場合、使用するタスク内のコンテナに対して、デフォルト容量を超えるエフェメラルストレージを割り当てることができます。この例は、他の例に組み込むことで、Fargate タスクに一時ストレージを割り当てることができます。

- タスク定義で、`ephemeralStorage`オブジェクトを定義します。`sizeInGiB` は `21`および`200` の値の間にある整数である必要があり、GiB に表されます。

```
"ephemeralStorage": {
    "sizeInGiB": integer
}
```

1 つまたは複数のコンテナに空のデータボリュームを提供する

場合によっては、タスク内のコンテナにスクラッチスペースを提供することがあります。例えば、タスクの実行中に同じスクラッチファイルの保存場所にアクセスする必要のある、2 つのデータベースコンテナがあるとします。これは、バインドマウントを使用して実現できます。

1. タスク定義の volumes セクションで、名前を database_scratch としてバインドマウントを定義します。

```
  "volumes": [
    {
      "name": "database_scratch"
    }
  ]
```

2. containerDefinitions セクションで、データベースのコンテナ定義を作成します。これにより、ボリュームがマウントされます。

```
"containerDefinitions": [
    {
      "name": "database1",
      "image": "my-repo/database",
      "cpu": 100,
      "memory": 100,
      "essential": true,
      "mountPoints": [
        {
          "sourceVolume": "database_scratch",
          "containerPath": "/var/scratch"
        }
      ]
    },
    {
      "name": "database2",
      "image": "my-repo/database",
      "cpu": 100,
      "memory": 100,
      "essential": true,
      "mountPoints": [
        {
          "sourceVolume": "database_scratch",
          "containerPath": "/var/scratch"
        }
```

```
      ]
    }
  ]
```

Dockerfile 内のパスとその内容をコンテナに公開する

この例には、コンテナ内にマウントするデータを書き込む Dockerfile があります。この例は、Fargate または Amazon EC2 インスタンスでホストされているタスクで機能します。

1. Dockerfile を作成します。次の例では、パブリックな Amazon Linux 2 コンテナイメージを使用して、コンテナ内にマウントする /var/log/exported ディレクトリに examplefile という名前のファイルを作成します。VOLUME ディレクティブは絶対パスを指定する必要があります。

   ```
   FROM public.ecr.aws/amazonlinux/amazonlinux:latest
   RUN mkdir -p /var/log/exported
   RUN touch /var/log/exported/examplefile
   VOLUME ["/var/log/exported"]
   ```

   デフォルトでは、ボリューム許可は 0755 に設定され、所有者は root に設定されます。これらのアクセス許可は Dockerfile で変更できます。以下の例では、/var/log/exported ディレクトリの所有者が node に設定されています。

   ```
   FROM public.ecr.aws/amazonlinux/amazonlinux:latest
   RUN yum install -y shadow-utils && yum clean all
   RUN useradd node
   RUN mkdir -p /var/log/exported && chown node:node /var/log/exported
   USER node
   RUN touch /var/log/exported/examplefile
   VOLUME ["/var/log/exported"]
   ```

2. タスク定義の volumes セクションで、名前を application_logs としてボリュームを定義します。

   ```
   "volumes": [
     {
       "name": "application_logs"
     }
   ]
   ```

3. containerDefinitions セクションで、アプリケーションのコンテナ定義を作成します。これにより、ストレージがマウントされます。containerPath 値は、Dockerfile の VOLUME ディレクティブで指定された絶対パスと一致する必要があります。

```
"containerDefinitions": [
  {
    "name": "application1",
    "image": "my-repo/application",
    "cpu": 100,
    "memory": 100,
    "essential": true,
    "mountPoints": [
      {
        "sourceVolume": "application_logs",
        "containerPath": "/var/log/exported"
      }
    ]
  },
  {
    "name": "application2",
    "image": "my-repo/application",
    "cpu": 100,
    "memory": 100,
    "essential": true,
    "mountPoints": [
      {
        "sourceVolume": "application_logs",
        "containerPath": "/var/log/exported"
      }
    ]
  }
]
```

ホスト Amazon EC2 インスタンスのライフサイクルに紐付けされているコンテナに、空のデータボリュームを提供するには

Amazon EC2 インスタンスでホストされているタスクの場合、バインドマウントを使用して、ホスト Amazon EC2 インスタンスのライフサイクルにデータを紐付けすることができます。これは、host パラメータを使用して sourcePath 値を指定することで設定できます。sourcePath に存在するファイルはすべて、containerPath の値でコンテナに表示されます。containerPath

に書き込まれたファイルは、ホストの Amazon EC2 インスタンス上の sourcePath 値に書き込まれます。

> **Important**
>
> Amazon ECS は、Amazon EC2 インスタンス間でストレージを同期しません。永続的ストレージを使用するタスクは、使用可能なキャパシティーのあるクラスター内の Amazon EC2 インスタンスに配置できます。タスクを停止して再び開始した後に永続的ストレージが必要な場合は、タスクの開始時に毎回 AWS CLI の start-task コマンドを使用して、同一の Amazon EC2 インスタンスを指定し直す必要があります。永続ストレージに Amazon EFS ボリュームを使用することもできます。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。

1. タスク定義の volumes セクションで、name および sourcePath 値を使用して、バインドマウントを定義します。次の例では、ホスト Amazon EC2 インスタンスはコンテナ内にマウントしたい /ecs/webdata のデータを含めます。

```
"volumes": [
  {
    "name": "webdata",
    "host": {
      "sourcePath": "/ecs/webdata"
    }
  }
]
```

2. containerDefinitions セクションで、定義したバインドマウントの名前を参照する mountPoints 値と、コンテナにバインドマウントをマウントするための containerPath 値を使用して、コンテナを定義します。

```
"containerDefinitions": [
  {
    "name": "web",
    "image": "public.ecr.aws/docker/library/nginx:latest",
    "cpu": 99,
    "memory": 100,
    "portMappings": [
      {
        "containerPort": 80,
```

```
          "hostPort": 80
        }
      ],
      "essential": true,
      "mountPoints": [
        {
          "sourceVolume": "webdata",
          "containerPath": "/usr/share/nginx/html"
        }
      ]
    }
  ]
```

定義したボリュームを異なる場所にある複数のコンテナにマウントする

タスク定義でデータボリュームを定義し、そのボリュームをさまざまなコンテナのさまざまな場所にマウントできます。例えば、ホストコンテナの /data/webroot に、ウェブサイトのデータフォルダがあるとします。そのデータボリュームを、異なるドキュメントルートを持つ 2 つの異なる Web サーバーに、読み取り専用としてマウントしたい場合があります。

1. タスク定義の volumes セクションで、名前を webroot、ソースパスを /data/webroot としてデータボリュームを定義します。

```
"volumes": [
  {
    "name": "webroot",
    "host": {
      "sourcePath": "/data/webroot"
    }
  }
]
```

2. containerDefinitions セクションで、各ウェブサーバーのコンテナを定義しています。各コンテナの mountPoints で、webroot ボリュームを、そのコンテナのドキュメントルートを参照する containerPath 値に関連付けます。

```
"containerDefinitions": [
  {
    "name": "web-server-1",
    "image": "my-repo/ubuntu-apache",
    "cpu": 100,
```

```
      "memory": 100,
      "portMappings": [
        {
          "containerPort": 80,
          "hostPort": 80
        }
      ],
      "essential": true,
      "mountPoints": [
        {
          "sourceVolume": "webroot",
          "containerPath": "/var/www/html",
          "readOnly": true
        }
      ]
    },
    {
      "name": "web-server-2",
      "image": "my-repo/sles11-apache",
      "cpu": 100,
      "memory": 100,
      "portMappings": [
        {
          "containerPort": 8080,
          "hostPort": 8080
        }
      ],
      "essential": true,
      "mountPoints": [
        {
          "sourceVolume": "webroot",
          "containerPath": "/srv/www/htdocs",
          "readOnly": true
        }
      ]
    }
  ]
```

volumesFrom を使用して別のコンテナからボリュームをマウントするには

Amazon EC2 インスタンスでホストされているタスクの場合、あるコンテナに 1 つ以上のボリュームを定義し、(同じタスクの) 異なるコンテナ定義で volumesFrom パラメータを使用し

て、sourceContainer のすべてのボリュームを、最初に定義されていたマウントポイントにマウントできます。volumesFrom パラメータは、タスク定義で定義されたボリューム、および Dockerfile でイメージに組み込まれたボリュームに適用されます。

1. (オプション) イメージに組み込まれているボリュームを共有するには、Dockerfile の VOLUME 命令を使用します。次の Dockerfile の例では、httpd イメージを使用しボリュームを追加して、それを Apache ドキュメントルートの dockerfile_volume にマウントしています。これは、httpd ウェブサーバーが使用するフォルダーです。

   ```
   FROM httpd
   VOLUME ["/usr/local/apache2/htdocs/dockerfile_volume"]
   ```

   この Dockerfile を使用してイメージを構築し、Docker ハブなどのレポジトリにプッシュして、タスク定義で使用できます。以下のステップで使用する my-repo/httpd_dockerfile_volume イメージ例は、上記の Dockerfile から構築したものです。

2. コンテナの他のボリュームとマウントポイントを定義するタスク定義を作成します。この例の volumes セクションでは、Docker デーモンによって管理される空のボリューム empty を作成します。また、host_etc と呼ばれるホストボリュームも定義されています。これは、ホストコンテナインスタンス上の /etc フォルダをエクスポートします。

   ```
   {
     "family": "test-volumes-from",
     "volumes": [
       {
         "name": "empty",
         "host": {}
       },
       {
         "name": "host_etc",
         "host": {
           "sourcePath": "/etc"
         }
       }
     ],
   ```

   コンテナ定義セクションで、先ほど定義したボリュームをマウントするコンテナを作成します。この例では、web コンテナが empty および host_etc ボリュームをマウントします。このコンテナは、Dockerfile 内のボリュームでビルドされたイメージを使用しています。

```
"containerDefinitions": [
    {
      "name": "web",
      "image": "my-repo/httpd_dockerfile_volume",
      "cpu": 100,
      "memory": 500,
      "portMappings": [
        {
          "containerPort": 80,
          "hostPort": 80
        }
      ],
      "mountPoints": [
        {
          "sourceVolume": "empty",
          "containerPath": "/usr/local/apache2/htdocs/empty_volume"
        },
        {
          "sourceVolume": "host_etc",
          "containerPath": "/usr/local/apache2/htdocs/host_etc"
        }
      ],
      "essential": true
    },
```

volumesFrom を使用して、web コンテナに関連付けられているすべてのボリュームをマウントする、別のコンテナを作成します。web コンテナ上にあるすべてのボリュームは、同様に busybox コンテナにもマウントされます。これには、my-repo/httpd_dockerfile_volume イメージのビルドに使用された Dockerfile で指定されたボリュームも含まれます。

```
    {
      "name": "busybox",
      "image": "busybox",
      "volumesFrom": [
        {
          "sourceContainer": "web"
        }
      ],
      "cpu": 100,
      "memory": 500,
```

```
      "entryPoint": [
        "sh",
        "-c"
      ],
      "command": [
        "echo $(date) > /usr/local/apache2/htdocs/empty_volume/date && echo $(date)
 > /usr/local/apache2/htdocs/host_etc/date && echo $(date) > /usr/local/apache2/
htdocs/dockerfile_volume/date"
      ],
      "essential": false
    }
  ]
}
```

このタスクが実行されると、2 つのコンテナでボリュームがマウントされ、busybox コンテナの command がファイルに日付と時刻を書き込みます。このファイルは、各ボリュームフォルダに date の名前で保存されています。その後、フォルダは web コンテナによって表示されるウェブサイトで見ることができます。

> **Note**
>
> busybox コンテナはクイックコマンドを実行して終了するため、コンテナ定義で "essential": false として設定する必要があります。そうしなければ、終了時にタスク全体が停止します。

Amazon ECS のコンテナスワップメモリ空間の管理

Amazon ECS を使用すると、Linux ベースの Amazon EC2 インスタンスで、スワップメモリ空間の使用状況をコンテナレベルで制御できるようになります。コンテナ単位のスワップ設定を使用すると、タスク定義内で各コンテナについて、スワップを有効または無効にできます。これが有効化されたコンテナでは、使用されるスワップ領域の最大量を制限できます。例えば、レイテンシーが厳しいコンテナでは、スワップを無効にすることができます。一方で、メモリ需要が一時的に高くなるコンテナでは、スワップを有効にすることで、コンテナのロード時にメモリ不足エラーが発生する可能性を減らすことができます。

コンテナのスワップ設定は、以下のコンテナ定義パラメータによって管理されます。

maxSwap

コンテナが使用できるスワップメモリの合計 (MiB 単位)。このパラメータは、docker run の --memory-swap オプションに変換されます。値はコンテナメモリの合計に maxSwap の値を加えた値です。

0 の maxSwap 値を指定した場合、コンテナはスワップを使用しません。許容値は、0 または任意の正の整数です。maxSwap パラメータを省略すると、コンテナは実行中のコンテナインスタンスのスワップ設定を使用します。swappiness パラメータを使用するには、maxSwap 値を設定する必要があります。

swappiness

これにより、コンテナのメモリスワップ動作を調整できます。swappiness の値が 0 であると、必要な場合を除きスワップは発生しません。swappiness の値が 100 の場合は、ページが積極的にスワップされます。使用できる値は、0 と 100 の間の整数です。swappiness パラメータを指定しない場合、デフォルト値の 60 が使用されます。maxSwap の値が指定されていない場合、このパラメータは無視されます。このパラメータは、docker run の --memory-swappiness オプションにマッピングされます。

次の例に、JSON での構文を示します。

```
"containerDefinitions": [{
        ...
        "linuxParameters": {
            "maxSwap": integer,
            "swappiness": integer
        },
        ...
}]
```

考慮事項

コンテナごとのスワップ構成を使用する場合は、次の点を考慮してください。

- スワップ領域は有効化され、使用するコンテナ向けのタスクをホストする、Amazon EC2 インスタンスに割り当てられる必要があります。Amazon ECS 最適化 AMI のデフォルトでは、スワップは有効になっていません。この機能を使用するには、インスタンスでスワップを有効にする必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスストアス

ワップボリューム」または「How do I allocate memory to work as swap space in an Amazon EC2 instance?」を参照してください。

- スワップスペースのコンテナ定義パラメータは、EC2 起動タイプを指定したタスク定義でのみサポートされます。これらのパラメータは、Fargate の Amazon ECS での使用のみを目的としたタスク定義ではサポートされていません。
- この機能は Linux コンテナでのみサポートされています。現在、Windows コンテナはサポートされていません。
- コンテナ定義の `maxSwap` および `swappiness` パラメータがタスク定義から省略されている場合、各コンテナの `swappiness` には、デフォルト値の `60` が設定されます。さらに、スワップの合計使用量は、コンテナのメモリ量の 2 倍に制限されます。
- Amazon Linux 2023 でタスクを使用している場合、`swappiness` パラメータはサポートされていません。

Fargate 起動タイプでの Amazon ECS タスク定義の違い

Fargate を使用するには、Fargate 起動タイプを使用するようにタスク定義を設定する必要があります。Fargate の使用については他にもいくつかの考慮事項があります。

タスク定義パラメータ

Fargate 起動タイプを使用するタスクは利用可能な Amazon ECS タスク定義パラメータのすべてをサポートするわけではありません。一部のパラメータはサポートされていません。また、Fargate タスクでは動作が異なるパラメータがあります。

次のタスク定義パラメータは Fargateタスクでは無効です:

- `disableNetworking`
- `dnsSearchDomains`
- `dnsServers`
- `dockerSecurityOptions`
- `extraHosts`
- `gpu`
- `ipcMode`
- `links`
- `placementConstraints`

- privileged
- maxSwap
- swappiness

以下のタスク定義パラメータはFargateタスクで有効ですが、注意すべき制限があります:

- linuxParameters – コンテナに適用される Linux 固有のオプションを指定する場合、capabilities に追加できる機能は CAP_SYS_PTRACE のみです。devices、sharedMemorySize、および tmpfs パラメータはサポートされません。詳細については、「Linux パラメータ」を参照してください。
- volumes – Fargateタスクはバインドマウントのホストボリュームのみをサポートするため、dockerVolumeConfiguration パラメータはサポートされません。詳細については、「ボリューム」を参照してください。
- cpu - AWS Fargate での Windows コンテナの場合、値は 1 vCPU 未満にすることはできません。
- networkConfiguration – Fargate タスクは、常に awsvpc ネットワークモードを使用します。

タスク定義が Fargateでの使用が有効であることを確認するために、タスク定義を登録する際に以下を指定できます:

- AWS Management Console の [Requires Compatibilities (互換性が必要)] フィールドで、FARGATE を指定します。
- AWS CLI で、--requires-compatibilities オプションを指定します。
- Amazon ECS API で、requiresCompatibilities フラグを指定します。

オペレーティングシステムとアーキテクチャ

AWS Fargate のタスク定義とコンテナの定義を構成する場合、コンテナが実行するオペレーティングシステムを指定する必要があります。以下のオペレーティングシステムが AWS Fargate でサポートされています。

- Amazon Linux 2

> **Note**
>
> Linux コンテナは、ホストオペレーティングシステムのカーネルおよびカーネル設定のみを使用することに留意してください。例えば、カーネル構成には sysctl システムコント

ロールが含まれます。Linux コンテナイメージは、任意の Linux ディストリビューションのファイルとプログラムを含むベースイメージから作成できます。CPU アーキテクチャが一致すると、どの OS 上で実行しているどの Linux コンテナイメージからでもコンテナを実行できます。

- Windows Server 2019 Full
- Windows Server 2019 Core
- Windows Server 2022 Full
- Windows Server 2022 Core

AWS Fargate で Windows コンテナを実行する場合、X86_64 CPU アーキテクチャを備えている必要があります。

AWS Fargate で Linux コンテナを実行する場合、ARM ベースのアプリケーションに X86_64 CPU アーキテクチャ、または ARM64 アーキテクチャを使用できます。詳細については、「the section called “64 ビット ARM ワークロードでのタスク定義”」を参照してください。

タスク CPU とメモリ

AWS Fargate の Amazon ECS タスク定義では、CPU とメモリをタスクレベルで指定する必要があります。Fargateタスクのコンテナレベルで CPU とメモリを指定することもできますが、これはオプションです。ほとんどのユースケースでは、タスクレベルでこれらのリソースを指定するだけで十分です。以下の表に、タスクレベル CPU とメモリの有効な組み合わせを示します。タスク定義では、メモリの値を MiB または GB の文字列として指定できます。例えば、メモリの値を `3072` (MiB) または `3 GB` (GB) のいずれかで指定できます。JSON ファイルでは、CPU 値を CPU ユニットまたは仮想 CPU (vCPU) の文字列として指定できます。例えば、CPU 値を `1 vCPU` (CPU ユニット) または `1024` (vCPU) として指定できます。

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
256 (.25 vCPU)	512 MiB、1 GB、2 GB	リナックス
512 (.5 vCPU)	1 GB、2 GB、3 GB、4 GB	リナックス
1,024 (1 vCPU)	2 GB、3 GB、4 GB、5 GB、6 GB、7 GB、8 GB	Linux、Windows

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
2,048 (2 vCPU)	4 GB ～ 16 GB (1 GB のインクリメント)	Linux、Windows
4,096 (4 vCPU)	8 GB ～ 30 GB (1 GB のインクリメント)	Linux、Windows
8192 (8 vCPU) **Note** このオプションには Linux プラットフォーム 1.4.0 以降が必要です。	16 GB ~ 60 GB (4 GB のインクリメント)	リナックス
16384 (16vCPU) **Note** このオプションには Linux プラットフォーム 1.4.0 以降が必要です。	32 GB ~ 120 GB (8 GB のインクリメント)	リナックス

タスクネットワーク

AWS Fargate の Amazon ECS を使用するタスクでは、awsvpc ネットワークモードが必要です。これは各タスクに Elastic Network Interface を提供します。このネットワークモードを使用したタスクの実行またはサービスの作成時に、ネットワークインターフェイスにアタッチするサブネットを 1 つ以上、またはネットワークインターフェイスに適用するセキュリティグループを 1 つ以上、指定する必要があります。

パブリックサブネットを使用している場合は、ネットワークインターフェイスにパブリック IP アドレスを指定するかどうかを決定します。パブリックサブネットの Fargate タスクを使用してコンテナ

イメージをプルするには、タスクの Elastic Network Interface に、インターネットへのルートまたはリクエストをインターネットにルーティングできる NAT ゲートウェイを持つパブリック IP アドレスが割り当てられている必要があります。　　プライベートサブネットのFargateタスクでコンテナイメージをプルするには、リクエストをインターネットにルーティングするためのNATゲートウェイがサブネットに必要です。Amazon ECR でコンテナイメージをホストする場合、 Amazon ECR を設定してインターフェイス VPC エンドポイントを使用するようにできます。この場合、タスクのプライベート IPv4 アドレスがイメージのプルに使用されます。Amazon ECRインターフェイスエンドポイントの詳細については、Amazon Elastic Container Registry ユーザーガイドの Amazon ECR Interface VPC エンドポイント (AWS PrivateLink)を参照してください。

Fargate サービス向け `networkConfiguration` セクションの例を以下に示します。

```
"networkConfiguration": {
   "awsvpcConfiguration": {
      "assignPublicIp": "ENABLED",
      "securityGroups": [ "sg-12345678" ],
      "subnets": [ "subnet-12345678" ]
   }
}
```

タスクリソースの制限

AWS Fargate での Linux コンテナのAmazon ECS タスク定義では、コンテナに設定するリソース制限を定義するための `ulimits` パラメータがサポートされます。

AWS Fargate での Windows の Amazon ECS タスク定義では、コンテナに設定するリソース制限を定義するための `ulimits` パラメータがサポートされます。

Fargate でホストされる Amazon ECS タスクは、オペレーションシステムで設定されたデフォルトのリソース制限値を使用します。ただし、`nofile` リソース制限パラメータを除きます。`nofile` リソース制限は、コンテナが使用できるオープンファイルの数の制限を設定します。Fargate では、デフォルトの `nofile` ソフト制限は　65535 で、ハード制限は 65535 です。両方の制限の値を設定できます (最大 1048576)。

以下は、2 倍になったカスタム `nofile` 制限を定義する方法を示すタスク定義スニペットの例です。

```
"ulimits": [
    {
       "name": "nofile",
       "softLimit": 2048,
       "hardLimit": 8192
```

```
    }
]
```

調整可能なその他のリソース制限の詳細については、リソースの制限 を参照してください。

ロギング

イベントログ

Amazon ECS は、実行したアクションを EventBridge にログ記録します。Amazon ECS の Eventbridge イベントを使用して、Amazon ECS クラスター、サービスおよびタスクの現在の状態に関するほぼリアルタイムの通知を受け取れます。さらに、これらのイベントに対応するアクションを自動化できます。詳細については、「EventBridge を使用して Amazon ECS エラーへの対応を自動化する」を参照してください。

タスクライフサイクルログ

Fargate で実行されるタスクは、タイムスタンプを公開してタスクライフサイクルの状態を追跡します。AWS CLI および SDK でタスクを説明することにより、AWS Management Console のタスク詳細でタイムスタンプを確認できます。例えば、タイムスタンプを使用して、タスクがコンテナイメージのダウンロードに費やした時間を評価し、コンテナイメージのサイズを最適化するか、Seekable OCI インデックスを使用するかを判断できます。コンテナイメージのプラクティスに関する詳細については、「Amazon ECS コンテナイメージのベストプラクティス」を参照してください。

アプリケーションログ

AWS Fargate の Amazon ECS タスク定義はログ設定の `awslogs`、`splunk`、および `awsfirelens` ログドライバーをサポートします。

この`awslogs`ログドライバーは、Amazon CloudWatch Logs にログ情報を送信するように Fargate タスクを設定します。以下に、`awslogs` ログドライバーが設定されているタスク定義のスニペットを示します。

```
"logConfiguration": {
   "logDriver": "awslogs",
   "options": {
      "awslogs-group" : "/ecs/fargate-task-definition",
      "awslogs-region": "us-east-1",
      "awslogs-stream-prefix": "ecs"
   }
}
```

タスク定義で `awslogs` ログドライバーを使用してコンテナログをCloudWatch Logs に送信する方法の詳細については、Amazon ECS ログを CloudWatch に送信する を参照してください。

タスク定義での `awsfirelens` ログドライバーの詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。

タスク定義での `splunk` ログドライバーの使用の詳細については、「splunk ログドライバー」を参照してください。

タスクストレージ

Fargate でホストされた Amazon ECS タスクでは、次のストレージタイプがサポートされています:

- Amazon EBS ボリュームは、データ集約型のコンテナ化されたワークロード向けに、費用対効果と耐久性に優れた高性能なブロックストレージを提供します。詳細については、「Amazon ECS での Amazon EBS ボリュームの使用」を参照してください。
- 永続的ストレージ用のAmazon EFS ボリューム。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。
- エフェメラルストレージ用のバインドマウント。詳細については、「Amazon ECS でのバインドマウントの使用」を参照してください。

Seekable OCI (SOCI) を使ったコンテナイメージの遅延読み込み

Linux プラットフォーム バージョン `1.4.0` を使用する Fargate 上の Amazon ECS タスクは、Seekable OCI (SOCI) を使用してタスクをより速く開始できます。SOCI では、コンテナは起動前にイメージプルに数秒しかかからないため、イメージがバックグラウンドでダウンロードされている間、環境のセットアップとアプリケーションのインスタンス化に時間を割けます。これは遅延読み込みと呼ばれています。Fargate が Amazon ECS タスクを開始すると、Fargate はタスク内のイメージに SOCI インデックスが存在するかどうかを自動的に検出し、イメージ全体がダウンロードされるのを待たずにコンテナを起動します。

SOCI インデックスなしで実行されるコンテナの場合、コンテナイメージはコンテナを起動する前に完全にダウンロードされます。この動作は、Fargate の他のすべてのプラットフォームバージョンと Amazon EC2 インスタンス上の Amazon ECS 最適化された AMI でも同じです。

Seekable OCI インデックス

Seekable OCI (SOCI) は AWS によって開発されたオープンソースのテクノロジーであり、コンテナイメージを遅延読み込みすることでコンテナをより速く起動できます。SOCI は、既存のコンテナイ

メージ内のファイルのインデックス (SOCI インデックス) を作成することで機能します。このインデックスは、イメージ全体をダウンロードする前にコンテナイメージから個々のファイルを抽出できるため、コンテナをより速く起動するのに役立ちます。SOCI インデックスは、コンテナレジストリ内のイメージと同じリポジトリにアーティファクトとして保存する必要があります。インデックスはイメージのコンテンツの信頼できるソースなので、信頼できるソースからの SOCI インデックスのみを使用してください。詳細については、「コンテナイメージを遅延ロードするためのSeekable OCIの導入」を参照してください。

考慮事項

Fargate に SOCI インデックスを使用してコンテナイメージをタスクに遅延読み込ませる場合は、次の点を考慮してください。

- Linux プラットフォームバージョン `1.4.0` で実行されるタスクのみ SOCI インデックスを使用できます。Fargate で Windows コンテナを実行するタスクはサポートされていません。
- X86_64 または ARM64 CPU アーキテクチャ上で実行されるタスクがサポートされています。
- タスク定義内のコンテナイメージには、イメージと同じコンテナレジストリに SOCI インデックスが必要です。
- タスク定義内のコンテナイメージは、互換性のあるイメージレジストリに保存する必要があります。以下に互換性のあるレジストリを示します。
  - Amazon ECR プライベートレジストリ
- gzip 圧縮を使用する、または圧縮されていないコンテナイメージのみがサポートされます。zstd 圧縮を使用するコンテナイメージはサポートされていません。
- 圧縮サイズが 250 MiB より大きいコンテナイメージを使用して遅延読み込みを試すことをお勧めします。小さいイメージを読み込む時間が短くなる可能性は低くなります。
- 遅延読み込みによってタスクの開始にかかる時間が変わる可能性があるため、Elastic Load Balancing のヘルスチェック猶予期間など、さまざまなタイムアウトを変更する必要がある場合があります。
- コンテナイメージが遅延読み込みされないようにするには、コンテナレジストリーから SOCI インデックスを削除します。タスク内のコンテナイメージが考慮事項のいずれかを満たさない場合、そのコンテナイメージはデフォルトの方法でダウンロードされます。

Seekable OCI インデックスの作成

コンテナイメージを遅延ロードするには、SOCI インデックス (メタデータファイル) を作成し、コンテナイメージと共にコンテナイメージリポジトリに保存する必要があります。SOCI インデックスを

作成しプッシュするには、GitHub にあるオープンソースの soci-snapshotter CLI ツールを使用できます。または、CloudFormation AWS SOCI Index Builder をデプロイすることもできます。これは、コンテナイメージが Amazon ECR にプッシュされるときに SOCI インデックスを自動的に作成してプッシュするサーバーレスソリューションです。ソリューションとインストール手順の詳細については、GitHub の「CloudFormation AWS SOCI Index Builder」を参照してください。CloudFormation AWS SOCI Index Builder は SOCI の導入を自動化できる手段ですが、オープンソースの SOCI ツールの方がインデックス生成に関してはより柔軟性があり、継続的インテグレーションと継続的デリバリー (CI/CD) パイプラインにインデックス生成を統合できます。

> **Note**
>
> イメージの SOCI インデックスを作成するには、そのイメージが `soci-snapshotter` を実行しているコンピュータ上の containerd イメージストアに存在する必要があります。イメージが Docker イメージストアにある場合、イメージは見つかりません。

タスクが遅延読み込みを使用したことの検証

SOCI を使用してタスクが遅延読み込みされたことを確認するには、タスク内部からタスクメタデータエンドポイントを確認します。タスクメタデータエンドポイントバージョン 4 をクエリすると、クエリ元のコンテナのデフォルトパスに `Snapshotter` フィールドが存在します。さらに、`/task` パス内のコンテナごとに `Snapshotter` フィールドがあります。このフィールドのデフォルト値は `overlayfs` であり、SOCI が使用されている場合、このフィールドは `soci` に設定されます。

Windows を実行している EC2 インスタンスでの Amazon ECS タスク定義の違い

EC2 Windows インスタンスで実行されるタスクは、使用可能なすべての Amazon ECS タスク定義パラメータをサポートしているわけではありません。サポートされていないパラメータもあり、また一部のパラメータでは動作が異なることがあります。

以下のタスク定義パラメータは、Amazon EC2 Windows タスク定義ではサポートされていません。

- `containerDefinitions`
  - `disableNetworking`
  - `dnsServers`
  - `dnsSearchDomains`

  - extraHosts
  - links
  - linuxParameters
  - privileged
  - readonlyRootFilesystem
  - user
  - ulimits
- volumes
  - dockerVolumeConfiguration
- cpu

  Windows コンテナではコンテナレベル CPU を指定することをお勧めします。
- memory

  Windows コンテナではコンテナレベルメモリを指定することをお勧めします。
- proxyConfiguration
- ipcMode
- pidMode
- taskRoleArn

  EC2 Windows インスタンス上のタスク向け IAM ロールには追加の設定が必要ですが、それらの設定の多くは Linux コンテナインスタンス上のタスクの IAM ロールの設定と類似しています。詳細については、「the section called “ Amazon EC2 Windows インスタンスの追加設定”」を参照してください。

コンソールを使用した Amazon ECS タスク定義の作成

タスクまたはサービスとして実行するアプリケーションを定義できるように、タスク定義を作成します。

外部起動タイプのタスク定義を作成するときは、JSON エディタを使用してタスク定義を作成し、requireCapabilities パラメータを EXTERNAL に設定する必要があります。

タスク定義は、コンソールエクスペリエンスを使用するか、JSON ファイルを指定して作成できます。

JSON 検証

Amazon ECS コンソールの JSON エディタは、JSON ファイル内で以下を検証します。

- ファイルが有効な JSON ファイルであること。
- ファイルに外部キーが含まれていないこと。
- ファイルに `familyName` パラメータが含まれていること。
- `containerDefinitions` の下に少なくとも 1 つのエントリがあること。

AWS CloudFormation スタック

次の動作は、2023 年 1 月 12 日以前に新しい Amazon ECS コンソールで作成されたタスク定義に適用されます。

タスク定義の作成時、Amazon ECS コンソールは、名前が `ECS-Console-V2-TaskDefinition-` で始まる CloudFormation スタックを自動的に作成します。AWS CLI または AWS SDK を使用してタスク定義を登録解除した場合は、手動でタスク定義スタックを削除する必要があります。詳細については、「AWS CloudFormation ユーザーガイド」の「スタックの削除」を参照してください。

2023 年 1 月 12 日以降に作成されたタスク定義では、CloudFormation スタックの自動的な作成は行われません。

手順

Amazon ECS console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [新しいタスク定義の作成] メニューで、[新しいタスク定義を作成する] を選択します。
4. [Task definition family] (タスク定義ファミリー) を使用する場合、タスク定義ファミリーには、タスク定義に一意の名前を指定します。
5. [起動タイプ] で、アプリケーション環境を選択します。コンソールのデフォルトは、AWS Fargate (サーバーレス) です。Amazon ECS は、この値を使用して検証を実行し、タスク定義パラメータがインフラストラクチャタイプに対して有効であることを確認します。
6. [Operating system/Architecture] (オペレーティングシステム/アーキテクチャ) を使用する場合、タスクのオペレーティングシステムと CPU アーキテクチャを選択します。

タスクを 64 ビット ARM アーキテクチャで実行するには、[Linux/ARM64] を選択します。詳細については、「the section called “ランタイムプラットフォーム”」を参照してください。

Windows コンテナで AWS Fargate タスクを実行するには、サポートされている Windows オペレーティングシステムを選択します。詳細については、「the section called “オペレーティングシステムとアーキテクチャ”」を参照してください。

7. [Task size] (タスクサイズ) では、タスク用に予約する CPU とメモリの値を選択します。CPU 値は vCPUs として指定され、メモリは GB として指定されます。

   Fargate でホストされるタスクの場合、次の表に有効な CPU とメモリの組み合わせを示します。

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
256 (.25 vCPU)	512 MiB、1 GB、2 GB	リナックス
512 (.5 vCPU)	1 GB、2 GB、3 GB、4 GB	リナックス
1,024 (1 vCPU)	2 GB、3 GB、4 GB、5 GB、6 GB、7 GB、8 GB	Linux、Windows
2,048 (2 vCPU)	4 GB ~ 16 GB (1 GB のインクリメント)	Linux、Windows
4,096 (4 vCPU)	8 GB ~ 30 GB (1 GB のインクリメント)	Linux、Windows
8192 (8 vCPU) **Note** このオプションには Linux プラットフォーム `1.4.0` 以降が必要です。	16 GB ~ 60 GB (4 GB のインクリメント)	リナックス

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
16384 (16vCPU) **Note** このオプションには Linux プラットフォーム `1.4.0` 以降が必要です。	32 GB ~ 120 GB (8 GB のインクリメント)	リナックス

EC2 または外部起動タイプを使用するタスクの場合、サポートされるタスク CPU 値は 128 CPU ユニット (0.125 vCPUs) から 196608 CPU ユニット (192 vCPU) の範囲です。

メモリ値を GB 単位で指定するには、数字に続けて [GB] と入力します。たとえば、[メモリ値] を 3 GB に設定するには、[3GB] と入力します。

> **Note**
> タスクレベル CPU およびメモリのパラメータは Windows コンテナでは無視されます。

8. [Network mode] (ネットワークモード) の場合、使用するネットワークモードを選択します。デフォルトは、awsvpc モードです。詳細については、Amazon ECS タスクネットワーキングを参照してください。

   [ポートマッピング] で、[ホストポート] に [ブリッジ] を選択した場合は、コンテナ用に予約するコンテナインスタンスのポート番号を入力します。

9. (オプション) [タスクロール] セクションを展開してタスク向け AWS Identity and Access Management (IAM) ロールを設定できます。

   a. [Task role] (タスクロール) では、タスクに割り当てる IAM ロールを選択します。タスク IAM ロールは、タスク内のコンテナが AWS API 操作を呼び出すアクセス許可を提供します。

b. [タスク実行ロール] で、ロールを選択します。

タスク実行ロールをいつ使用するかの詳細については、「the section called “タスク実行 IAM ロール”」を参照してください。ロールが不要な場合は、[なし] を選択します。

10. (オプション) タスク配置 セクションを展開して、配置の制約を追加します。タスク配置の制約により、組み込み属性またはカスタム属性を使用して、タスクの配置に使用されるコンテナインスタンスをフィルタリングできます。
11. (オプション) フォールトインジェクション セクションを展開して、フォールトインジェクションを有効にします。フォールトインジェクションを使用すると、特定の障害シナリオに対するアプリケーションの反応をテストできます。
12. タスク定義で定義するコンテナごとに、以下のステップを実行します。

a. [Name] (名前) に、コンテナの名前を入力します。

b. [Image URI] (イメージ URI) には、コンテナの開始に使用するイメージを指定します。Amazon ECR Public Gallery レジストリ内のイメージは、Amazon ECR Public レジストリ名の使用でのみ指定することができます。例えば、`public.ecr.aws/ecs/amazon-ecs-agent:latest` が指定されている場合は、Amazon ECR Public Gallery でホストされている Amazon Linux コンテナが使用されます。他のすべてのリポジトリの場合は、`repository-url/image:tag` または `repository-url/image@digest` の形式を使用してリポジトリを指定します。

c. イメージが Amazon ECR の外部のプライベートレジストリにある場合は、[プライベートレジストリ] で [プライベートレジストリ認証] をオンにします。その後、[Secrets Manager ARN または名前] で、シークレットの Amazon リソースネーム (ARN) を入力します。

d. [基本コンテナ] の場合、もしタスク定義に 2 つ以上のコンテナが定義されていれば、そのコンテナを基本と見なすかどうかを指定できます。コンテナが [基本] とマークされている場合は、そのコンテナが停止するとタスクは停止します。各タスク定義には、少なくとも 1 つの基本コンテナを含む必要があります。

e. ポートマッピングにより、コンテナはホスト上のポートにアクセスしてトラフィックを送受信できるようになります。[Port mappings] (ポートマッピング) で、次のいずれかを実行]ます。

- [awsvpc] ネットワークモードを使用する場合、[Container port] (コンテナポート) と [Protocol] (プロトコル) で、コンテナに使用するポートマッピングを選択します。
- [bridge] ネットワークモードを使用する場合、[Container port] (コンテナポート) と [Protocol] (プロトコル) で、コンテナに使用するポートマッピングを選択します。

追加のコンテナポートマッピングを指定するには、[Add more port mappings] (ポートマッピングを追加) を選択します。

f. コンテナにルート ファイル システムへの読み取り専用アクセスを付与するには、[読み取り専用ルートファイルシステム] で [読み取り専用] を選択します。

g. (オプション) [リソース割り当て制限] のタスクレベルの値とは異なるコンテナ レベルの CPU、GPU、およびメモリの制限を定義するには、次の手順を実行します。

- [CPU] には、Amazon ECS コンテナエージェントがそのコンテナ用に予約している CPU ユニット数を入力します。
- [GPU] では、コンテナインスタンス用の GPU ユニット数を入力します。

  GPU サポートを使用する Amazon EC2 インスタンスには、各 GPU について 1 つの GPU ユニットが装備されます。詳細については、「the section called “GPU ワークロード向けのタスク定義”」を参照してください。
- [メモリのハード制限] には、コンテナに提供するメモリの量を GB 単位で入力します。コンテナがハード制限を超えようとすると、コンテナは停止します。
- Docker 20.10.0 以降のデーモンではコンテナ用に最低 6 MiB のメモリを予約するため、コンテナ用に 6 MiB 未満のメモリを指定しないでください。

  Docker 19.03.13-ce 以前のデーモンではコンテナ用に最低 4 MiB のメモリを予約するため、コンテナ用に 4 MiB 未満のメモリを指定しないでください。
- [メモリのソフト制限] に、コンテナに予約するメモリのソフト制限 (GB 単位) を入力します。

  システムメモリに競合がある場合、Docker はコンテナのメモリ量をこのソフト制限値内に維持しようとします。タスクレベルのメモリを指定しない場合は、[メモリのハード制限] と [メモリのソフト制限] の一方または両方にゼロ以外の整数を指定する必要があります。両方を指定する場合は、[メモリのハード制限] がメモリの [ソフト制限] より大きい必要があります。

  この機能は Windows コンテナではサポートされません。

h. (オプション) [環境変数] セクションを展開し、コンテナに挿入する環境変数を指定します。環境変数は、キー値ペアを使用して個別に指定するか、Amazon S3 バケットでホストされている環境変数ファイルを指定して一括で指定できます。環境変数ファイルの

フォーマット方法については、「個々の環境変数を Amazon ECS コンテナに渡す」を参照してください。

シークレットストレージの環境変数を指定するときは、[キー] にシークレット名を入力します。次に、[ValueFrom] に、Systems Manager パラメータストアシークレットまたは Secrets Manager シークレットの完全な ARN を入力します。

i. (オプション) [Use log collection] (ログコレクションを使用) を選択し、ログ構成を指定します。使用可能なログドライバーごとに、指定するログドライバーオプションがあります。デフォルトのオプションでは、コンテナログを Amazon CloudWatch Logs に送信します。その他のログドライバーオプションは、AWS FireLens を使用して設定されます。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。

以下では、各コンテナログの送信先について詳しく説明します。

- Amazon CloudWatch — コンテナログを CloudWatch Logs に送信するようにタスクを設定します。デフォルトのログドライバーオプションが提供され、ユーザーに代わり CloudWatch ロググループを作成します。別のロググループ名を指定するには、ドライバーオプションの値を変更します。
- Splunk へのログのエクスポート — リモートサービスにログを送信する Splunk ドライバーにコンテナログを送信するタスクを設定します。Splunk Web サービスの URL を入力する必要があります。Splunk トークンは機密データとして扱われる可能性があるため、シークレットのオプションとして指定します。
- [Amazon Data Firehose へのログのエクスポート] — Firehose にコンテナログを送信するようタスクを設定します。Firehose 配信ストリームにログを送信するデフォルトのログドライバーオプションが提供されています。別の配信ストリーム名を指定するには、ドライバーオプションの値を変更します。
- Amazon Kinesis Data Streams へのログのエクスポート — Kinesis Data Streams にコンテナログを送信するようタスクを設定します。Kinesis Data Streams のストリームにログを送信するデフォルトのログドライバーオプションが提供されています。別のストリーム名を指定するには、ドライバーオプションの値を変更します。
- Amazon OpenSearch Service へのログのエクスポート — コンテナログを OpenSearch Service ドメインに送信するようタスクを設定します。ログドライバーオプションを提供する必要があります。

- Amazon S3 へのログのエクスポート — Amazon S3 バケットにコンテナログを送信するようタスクを設定します。デフォルトのログドライバーオプションが提供されていますが、有効な Amazon S3 バケット名を指定する必要があります。

j. (オプション) コンテナの追加パラメータを設定します。

このオプションを設定するには	この操作を行います	
再起動ポリシー これらのオプションは、コンテナの終了時にコンテナを再起動する再起動ポリシーを定義します。	[再起動ポリシー] を展開して以下の項目を設定します。 • コンテナの再起動ポリシーを有効にするには、[再起動ポリシーを有効にする] をオンにします。 • [無視された終了コード] には、整数コンテナの終了コードのカンマ区切りリストを指定します。指定された終了コードのいずれかでコンテナが終了した場合、Amazon ECS はコンテナの再起動を試みません。何も指定しない場合、Amazon ECS はいずれの終了コードも無視しません。 • [試行リセット期間] には、終了した際に再起動を試みる前にコンテナが実行する必要がある期間を整数 (秒) で指定します。Amazon ECS は、[試行リセット期間] で指定した秒ごと	

このオプションを設定するには	この操作を行います	
	にコンテナの再起動を 1 回だけ試みることができます。何も指定しない場合、再起動を試みる前にコンテナは 300 秒間実行する必要があります。	

このオプションを設定するには	この操作を行います	
HealthCheck これらはコンテナが正常かどうかを判断するコマンドです。詳細については、「コンテナのヘルスチェックを使用して Amazon ECS タスク状態を判定する」を参照してください。	HealthCheck を展開し、次の項目を設定します。 • [Command] (コマンド) には、カンマで区切られたコマンドのリストを入力します。コマンド引数を直接実行するための CMD、またはコンテナのデフォルトシェルでコマンドを実行するための CMD-SHELL を使用してコマンドを実行できます。これらのいずれも指定しない場合は CMD が使用されます。 • [Interval] (間隔) に、各ヘルスチェックの間隔を秒数で入力します。有効な値は 5～30 です。 • [Timeout] (タイムアウト) には、成功まで待機しているヘルスチェックが、失敗したと見なされるまでの期間 (秒単位) を入力します。有効な値は 2～60 です。 •	

このオプションを設定するには	この操作を行います	
	[Start period] (開始時期) には、ヘルスチェックコマンドを実行する前にコンテナがブートストラップするのを待つ期間 (秒単位) を入力します。有効な値は 0～300 です。 • [Retries] (再試行) には、障害発生時にヘルスチェックコマンドを再試行する回数を入力します。有効な値の範囲は 1～10 です。	
[起動の依存関係の順序] このオプションは、コンテナの起動と停止の依存関係を定義します。コンテナには複数の依存関係を含めることができます。	[起動時の依存関係の順序] を展開し、次の項目を設定します。 a. [コンテナ依存関係を追加] を選択します。 b. [コンテナ] で、対象のコンテナを選択します。 c. [条件]で、起動時の依存条件を選択します。 依存関係を追加するには、[コンテナ依存関係を追加]を選択します。	

このオプションを設定するには	この操作を行います	
[コンテナのタイムアウト] これらのオプションは、コンテナをいつ起動および停止するかを決定します。	[コンテナタイムアウト] を展開し、次の項目を設定します。 • コンテナの依存関係を解決するための再試行を止めるまでの待機時間を設定するには、[タイムアウト開始時間] (秒) を入力します。 • コンテナが正常に終了しなかった場合にコンテナが停止されるまでの [タイムアウト停止時間] (秒) を指定します。	

このオプションを設定するには	この操作を行います
コンテナネットワーク設定 これらのオプションはコンテナ内でネットワークを使用するかどうかを決定します。	[コンテナネットワーク設定] を展開し、以下を設定します。 • コンテナネットワーキングを無効にするには、[ネットワーキングをオフにする] を選択します。 • コンテナに提供する DNS サーバー IP アドレスを設定するには、[DNS サーバー] に各サーバーの IP アドレスを個々の行に入力します。 • コンテナに提示された完全修飾されていないホスト名を検索するように DNS ドメインを設定するには、[DNS 検索ドメイン] で各ドメインを別々の行に入力します。 パターンは **^[a-zA-Z0-9-.]{0,253}[a-zA-Z0-9]$** です。 • コンテナのホスト名を設定するには、[ホスト

このオプションを設定するには	この操作を行います	
	名] にコンテナのホスト名を入力します。 • コンテナの /etc/hosts ファイルに追加するホスト名と IP アドレスマッピングを追加するには、[追加のホストを追加] を選択し、[ホスト名] と [IP アドレス] にホスト名と IP アドレスを入力します。	

このオプションを設定するには	この操作を行います	
Docker 設定 これらは Dockerfile 内の値を上書きします。	[Docker 設定] を展開して以下の項目を設定します。 • [コマンド] には、コンテナに対する実行可能なコマンドを入力します。 このパラメータは、Docker Remote API の [コンテナの作成] セクションにある `Cmd` にマッピングされ、`COMMAND` オプションは `docker run` にマッピングされます。このパラメータは、Dockerfile 内の `CMD` 命令よりも優先されます。 • [エントリポイント] で、コンテナに渡される Docker エントリポイントを入力します。 このパラメータは、Docker Remote API の [コンテナの作成] セクションにある `Entrypoint` にマッピングされ、`--`	

このオプションを設定するには	この操作を行います	
	`entrypoint` オプションは `docker run` にマッピングされます。このパラメータは、Dockerfile 内の `ENTRYPOINT` 命令よりも優先されます。 • [作業ディレクトリ] には、エントリポイントと提供されたコマンド命令をコンテナが実行するための、ディレクトリを入力します。 このパラメータは、Docker Remote API の [コンテナの作成] セクションにある `WorkingDir` にマッピングされ、`--workdir` オプションは `docker run` にマッピングされます。このパラメータは、Dockerfile 内の `WORKDIR` 命令よりも優先されます。	

このオプションを設定するには	この操作を行います	
[リソースの制限 (Ulimits)] この値は、オペレーティングシステムのデフォルトのリソースクォータ設定を上書きします。 このパラメータは、Docker Remote API の「Create a container (コンテナを作成する)」セクションの `Ulimits` にマップされ、`--ulimit` オプションは docker run にマップされます。	[リソース制限 (ulimits)] を展開し、[ulimit の追加] を選択します。[制限名] で制限を選択します。次に、[ソフトリミット] と [ハードリミット] に値を入力します。 さらに ulimits を追加するには、[ulimit の追加] を選択します。	
Docker ラベル このオプションは、コンテナにメタデータを追加します。 このパラメータは、Docker Remote API の「Create a container (コンテナを作成する)」セクションの `Labels` にマップされ、`--label` オプションは docker run にマップされます。	[Docker ラベル]を展開し、[キー値ペアを追加] を選択して、[キー] と [値] を入力します。 Docker ラベルをさらに追加するには、[キー値ペアを追加] を選択します。	

k. (オプション) [コンテナを追加する]をクリックして、タスク定義にコンテナを追加します。

13. (オプション) [ストレージ] セクションを使用して、Fargate でホストされるタスクの一時ストレージ量を拡張することができます。またこのセクションを使用して、タスクのデータボリューム設定を追加することもできます。

    - Fargate タスクに使用可能なエフェメラルストレージをデフォルト値の 20 gibibytes (GiB) を超えて拡張するには、[Amount] (量) に最大で 200 GiB までの値を入力します。

14. (オプション) タスク定義のデータ ボリューム構成を追加するには、[ボリュームの追加] を選択し、以下のステップを実行します。

    a. [Volume name] (ボリューム名) には、データボリュームの名前を入力します。データボリューム名は、コンテナマウントポイントを作成するときに使用されます。

    b. [ボリューム設定] では、ボリュームをタスク定義の作成時に設定するのか、デプロイ時に設定するのかを選択します。

    > **Note**
    >
    > タスク定義の作成時に設定できるボリュームには、バインドマウント、Docker、Amazon EFS、Amazon FSx for Windows File Server などがあります。デプロイ時にタスクを実行するとき、またはサービスを作成または更新するときに設定できるボリュームには Amazon EBS が含まれます。

    c. [ボリュームタイプ]では、選択した設定タイプと互換性のあるボリュームタイプを選択し、ボリュームタイプを設定します。

ボリュームタイプ	ステップ	
[バインドマウント]	a. [Add mount point] (マウントポイントの追加) を選択し、次の設定を行います。 • [Container] (コンテナ) には、マウントポイントのコンテナを選択します。	

ボリュームタイプ	ステップ	
	• [Source volume] (ソースボリューム) を使用する場合、コンテナにマウントするデータボリュームを選択します。 • [Container path] (コンテナパス) に、ボリュームをマウントするコンテナのパスを指定します。 • [読み取り専用] では、コンテナがボリュームに対して読み取り専用アクセスを持つかどうかを選択します。 b. マウントポイントを追加するには、[Add mount point] (マウントポイントの追加)。	

ボリュームタイプ	ステップ	
EFS	a. [File system ID] (ファイルシステム ID) で、Amazon EFS のファイルシステム ID を選択します。 b. (オプション) [Root directory] (ルートディレクトリ) には、ホスト内にルートディレクトリとしてマウントする Amazon EFS ファイルシステム内のディレクトリを入力します。このパラメータを省略すると、Amazon EFS ボリュームのルートが使用されます。 EFS アクセスポイントを使用する予定の場合は、このフィールドを空白のままにします。 c. (オプション) [Access point] (アクセスポイント) で、使用するアクセスポイント ID を選択します。 d. (オプション) Amazon EFS ファイルシステムと Amazon ECS ホスト間のデータを暗号化する	

ボリュームタイプ	ステップ	
	場合、または、ボリュームをマウントするときにタスク実行ロールを使用する場合は、[Advanced configurations] (詳細設定) を選択し、以下を設定します。 • Amazon EFS ファイルシステムと Amazon ECS ホスト間のデータを暗号化するには、[Transit encryption] (トランジットの暗号化) を選択し、[Port] (ポート) に、Amazon ECS ホストと Amazon EFS サーバーの間で暗号化されたデータを送信する際に使用するポートを入力します。転送中の暗号化ポートを指定しないと、Amazon EFS マウントヘルパーが使用するポート選択方式が使用されます。詳細については、[Amazon Elastic File System User Guide] (Amazon Elastic File System ユーザーガイド) の[EFS Mount Helper] (EFS マウント	

ボリュームタイプ	ステップ	
	ヘルパー) を参照してください。 • Amazon EFS ファイルシステムをマウントするときにタスク定義で定義された Amazon ECS タスク IAM ロールを使用するには、[IAM 認可] を選択します。 e. [Add mount point] (マウントポイントの追加) を選択し、次の設定を行います。 • [Container] (コンテナ) には、マウントポイントのコンテナを選択します。 • [Source volume] (ソースボリューム) を使用する場合、コンテナにマウントするデータボリュームを選択します。 • [Container path] (コンテナパス) に、ボリュームをマウントするコンテナのパスを指定します。 •	

ボリュームタイプ	ステップ	
	[読み取り専用] では、コンテナがボリュームに対して読み取り専用アクセスを持つかどうかを選択します。 f. マウントポイントを追加するには、[Add mount point] (マウントポイントの追加)。	

ボリュームタイプ	ステップ	
Docker	a. [ドライバー] に、Docker ボリュームの設定を入力します。Windows コンテナでは、[ローカル] ドライバーの使用のみがサポートされます。バインドマウントを使用するには、host を指定します。 b. [Scope] (スコープ) で、ボリュームのライフサイクルを選択します。 • タスクの開始時と停止時にライフサイクルが続くようにするには、[Task] (タスク) を選択します。 • タスクが停止した後もボリュームを維持するには、[Shared] (共有) を選択します。 c. [Add mount point] (マウントポイントの追加) を選択し、次の設定を行います。 • [Container] (コンテナ) には、マウントポイントのコンテナを選択します。 •	

ボリュームタイプ	ステップ	
	[Source volume] (ソースボリューム) を使用する場合、コンテナにマウントするデータボリュームを選択します。 • [Container path] (コンテナパス) に、ボリュームをマウントするコンテナのパスを指定します。 • [読み取り専用] では、コンテナがボリュームに対して読み取り専用アクセスを持つかどうかを選択します。 d. マウントポイントを追加するには、[Add mount point] (マウントポイントの追加)。	

ボリュームタイプ	ステップ	
FSx for Windows File Server	a. [ファイルシステム ID] で、FSx for Windows File Server システムの ID を選択します。 b. [ルートディレクトリ] で、ホスト内にルートディレクトリとしてマウントするための、FSx for Windows File Server ファイルシステム内のディレクトリを入力します。 c. [認証情報パラメータ] で、認証情報の保存方法を選択します。 • AWS Secrets Manager を使用するには、Secrets Manager シークレットの Amazon リソースネーム (ARN) を入力します。 • AWS Systems Manager を使用するには、Systems Manager パラメータの Amazon リソースネーム (ARN) を入力します。 d. [ドメイン] に、AWS Directory Service	

ボリュームタイプ	ステップ	
	for Microsoft Active Directory (AWS Managed Microsoft AD) ディレクトリまたはセルフホスト型 EC2 Active Directory によってホストされる完全修飾ドメイン名を入力します。 e. [Add mount point] (マウントポイントの追加) を選択し、次の設定を行います。 • [Container] (コンテナ) には、マウントポイントのコンテナを選択します。 • [Source volume] (ソースボリューム) を使用する場合、コンテナにマウントするデータボリュームを選択します。 • [Container path] (コンテナパス) に、ボリュームをマウントするコンテナのパスを指定します。 • [読み取り専用] では、コンテナがボリュームに対して読み取り専用	

ボリュームタイプ	ステップ	
	アクセスを持つかどうかを選択します。 f. マウントポイントを追加するには、[Add mount point] (マウントポイントの追加)。	

ボリュームタイプ	ステップ	
Amazon EBS	a. [Add mount point] (マウントポイントの追加) を選択し、次の設定を行います。 • [Container] (コンテナ) には、マウントポイントのコンテナを選択します。 • [Source volume] (ソースボリューム) を使用する場合、コンテナにマウントするデータボリュームを選択します。 • [Container path] (コンテナパス) に、ボリュームをマウントするコンテナのパスを指定します。 • [読み取り専用] では、コンテナがボリュームに対して読み取り専用アクセスを持つかどうかを選択します。 b. マウントポイントを追加するには、[Add mount point] (マウントポイントの追加)。	

ボリュームタイプ	ステップ	

15. 別のコンテナからボリュームを追加するには、[以下からボリュームを追加:] を選択し、次のように構成します。

    - [コンテナ] で、対象のコンテナを選択します。
    - [ソース] で、マウントするボリュームが含まれるコンテナを選択します。
    - [読み取り専用] では、コンテナがボリュームに対して読み取り専用アクセスを持つかどうかを選択します。

16. (オプション) AWS Distro for OpenTelemetry 統合を使用してアプリケーショントレースとメトリクス収集設定を構成するには、[モニタリング] を展開し、[メトリクス収集を使用] を選択してタスクのメトリクスを収集し、Amazon CloudWatch または Amazon Managed Service for Prometheus に送信します。このオプションを選択すると、Amazon ECS はアプリケーションメトリクスの送信向けに事前設定された AWS Distro for OpenTelemetry コンテナサイドカーを作成します。詳細については、「アプリケーションメトリクスを使用して Amazon ECS アプリケーションのパフォーマンスを相関させる」を参照してください。

    a. [Amazon CloudWatch] を選択した場合、カスタムアプリケーションメトリクスはカスタムメトリクスとして CloudWatch にルーティングされます。詳細については、「アプリケーションメトリクスを Amazon CloudWatch にエクスポートする」を参照してください。

    > **Important**
    >
    > Amazon CloudWatch にアプリケーションメトリクスをエクスポートする場合、タスク定義には、必要なアクセス権限を持つタスク IAM ロールが必要です。詳しくは、「OpenTelemetry 用 AWS Distro と Amazon CloudWatch の統合に必要な IAM 許可」を参照してください。

    b. [Amazon Managed Service for Prometheus (Prometheus libraries instrumentation)] (Prometheus 向け Amazon マネージドサービス (Prometheus ライブラリ計測)) を選択した場合、タスクレベルの CPU、メモリ、ネットワーク、ストレージのメトリクスとカスタムアプリケーションメトリクスが Amazon Managed Service for Prometheus にルーティングされます。[Workspace のリモート書き込み用エンドポイント] には、Prometheus ワークスペースのリモート書き込みエンドポイント URL を入力し

ます。[スクレイピングターゲット] には、AWS Distro for OpenTelemetry コレクターがメトリクスデータをスクレイプするために使用できるホストとポートを入力します。詳細については、「アプリケーションメトリクスを Amazon Managed Service for Prometheus にエクスポートする」を参照してください。

> **Important**
>
> Amazon Managed Service for Prometheus にアプリケーションメトリクスをエクスポートする場合、タスク定義には、必要なアクセス権限を持つタスク IAM ロールが必要です。詳細については、「OpenTelemetry 用 AWS Distro と Amazon Managed Service for Prometheus の統合に必要な IAM 許可」を参照してください。

c. [Amazon Managed Service for Prometheus (OpenTelemetry 計測)] を選択した場合、タスクレベルの CPU、メモリ、ネットワーク、ストレージのメトリクスとカスタムアプリケーションメトリクスが Amazon Managed Service for Prometheus にルーティングされます。[Workspace のリモート書き込み用エンドポイント] には、Prometheus ワークスペースのリモート書き込みエンドポイント URL を入力します。詳細については、「アプリケーションメトリクスを Amazon Managed Service for Prometheus にエクスポートする」を参照してください。

> **Important**
>
> Amazon Managed Service for Prometheus にアプリケーションメトリクスをエクスポートする場合、タスク定義には、必要なアクセス権限を持つタスク IAM ロールが必要です。詳細については、「OpenTelemetry 用 AWS Distro と Amazon Managed Service for Prometheus の統合に必要な IAM 許可」を参照してください。

17. (オプション) [Tags] (タグ) を展開します。タグをキーバリューペアとしてタスク定義に追加します。

    - [タグを追加] [Add tag] (タグを追加) を選択し、以下を実行します。
      - [キー] にはキー名を入力します。
      - [値] にキー値を入力します。
    - [タグの削除] タグの横にある [タグの削除] を選択します。

18. [作成] を選択してタスク定義を登録します。

Amazon ECS console JSON editor

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [新しいタスク定義の作成] メニューで、[JSON で新しいタスク定義を作成する] を選択します。
4. JSON エディタボックスで、JSON ファイルを編集し、

   JSON は、the section called “JSON 検証” で指定された検証チェックに合格する必要があります。
5. [Create] (作成) を選択します。

コンソールを使用した Amazon ECS タスク定義の更新

あるタスク定義リビジョンは、現在のタスク定義のコピーであり、新しいパラメータ値が既存のパラメータ値に置き換えられます。変更しないパラメータはすべて新しいリビジョンにあります。

タスク定義を更新するには、タスク定義リビジョンを作成します。サービスでタスク定義を使用する場合、更新されたタスク定義を使用するようサービスを更新する必要があります。

リビジョンを作成するときに、次のコンテナプロパティと環境プロパティを変更できます。

- コンテナイメージ URI
- ポートマッピング
- 環境変数
- タスクサイズ
- コンテナサイズ
- タスクロール
- タスク実行ロール
- ボリュームとコンテナマウントポイント
- プライベートレジストリ

JSON 検証

Amazon ECS コンソールの JSON エディタは、JSON ファイル内で以下を検証します。

- このJSON ファイルは有効です
- ファイルに外部キーは含まれていません
- ファイルに `familyName` パラメータが含まれています
- `containerDefinitions` の下に少なくとも 1 つのエントリがあります

手順

Amazon ECS console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、タスク定義を含むリージョンを選択します。
3. ナビゲーションペインで、[Task Definitions] を選択します。
4. タスク定義を選択します。
5. タスク定義リビジョンを選択し、[新しいリビジョンを作成]、[新しいリビジョンを作成] を選択します。
6. [Create new task definition revision (タスク定義の新しいリビジョンの作成) ページで変更を加えます。例えば、既存のコンテナの定義 (コンテナイメージ、メモリ制限、ポートマッピングなど) を変更する場合は、コンテナを選択して変更を加えます。
7. 情報を確認し、[更新] を選択します。
8. サービスでタスク定義を使用する場合、更新されたタスク定義でサービスを更新します。詳細については、「コンソールを使用した Amazon ECS サービスの更新」を参照してください。

Amazon ECS console JSON editor

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [Create new revision] (新しいリビジョンの作成)、[Create new revision with JSON] (JSON で新しいリビジョンを作成) の順に選択します。
4. JSON エディタボックスで、JSON ファイルを編集し、

   JSON は、the section called “JSON 検証” で指定された検証チェックに合格する必要があります。

5. [Create] (作成) を選択します。

新しいコンソールを使用した Amazon ECS タスク定義リビジョンの登録解除

そのタスク定義リビジョンを登録解除することで、タスクの実行やサービスの更新時、そのタスク定義リビジョンが ListTaskDefinition API コールにもコンソールにも表示されなくなります。

タスク定義リビジョンは登録解除されると、すぐに INACTIVE とマークされます。INACTIVE タスク定義リビジョンを参照する既存のタスクおよびサービスは、中断することなく引き続き実行されます。INACTIVE タスク定義のリビジョンを参照する既存のサービスは、希望するサービスの数を変更することでスケールアップまたはスケールダウンできます。

INACTIVE タスク定義のリビジョンを使用して、新しいタスクを実行したり、新しいサービスを作成したりすることはできません。また、INACTIVE タスク定義のリビジョンを参照するように既存のサービスを更新することはできません (登録解除後 10 分経過するまでは、これらの制限が有効にならないことがあります)。

> **Note**
>
> タスクファミリーのすべてのリビジョンを登録解除すると、タスク定義ファミリーが INACTIVE リストに移動されます。INACTIVE タスク定義の新しいリビジョンを追加すると、タスク定義ファミリーが ACTIVE リストに戻ります。
> 現時点では、INACTIVE タスク定義のリビジョンはアカウントで無期限に検出可能です。ただし、この動作は、今後変更される可能性があります。したがって、関連するタスクおよびサービスのライフサイクルを超えて持続する INACTIVE タスク定義のリビジョンに依存しないでください。

AWS CloudFormation スタック

次の動作は、2023 年 1 月 12 日以前に新しい Amazon ECS コンソールで作成されたタスク定義に適用されます。

タスク定義の作成時、Amazon ECS コンソールは、名前が ECS-Console-V2-TaskDefinition- で始まる CloudFormation スタックを自動的に作成します。AWS CLI または AWS SDK を使用してタスク定義を登録解除した場合は、手動でタスク定義スタックを削除する必要があります。詳細については、「AWS CloudFormation ユーザーガイド」の「スタックの削除」を参照してください。

2023 年 1 月 12 日以降に作成されたタスク定義では、CloudFormation スタックの自動的な作成は行われません。

手順

新しいタスク定義を登録解除するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、タスク定義を含むリージョンを選択します。
3. ナビゲーションペインで、[Task Definitions] を選択します。
4. [Task Definitions] (タスク定義) ページで、登録解除する 1 つ以上のタスク定義リビジョンを含むタスク定義ファミリーを選択します。
5. [タスク定義名] ページで、削除するリビジョンを選択し、次に [アクション]、[登録解除] の順に選択します。
6. [Deregister] (登録解除) ウィンドウの情報を確認し、[Deregister] (登録解除) を選択して終了します。

コンソールを使用した Amazon ECS タスク定義リビジョンの削除

Amazon ECS で特定のタスク定義リビジョンが不要になったら、そのタスク定義リビジョンを削除することができます。

削除されたタスク定義リビジョンは、その後すぐに INACTIVE から DELETE_IN_PROGRESS に遷移します。状態が DELETE_IN_PROGRESS のタスク定義リビジョンを参照している既存のタスクおよびサービスは、中断することなく引き続き実行されます。

状態が DELETE_IN_PROGRESS のタスク定義リビジョンは、新しいタスクの実行や、新しいサービスの作成のために使用することはできません。また、DELETE_IN_PROGRESS 状態にあるタスク定義リビジョンを参照するように、既存のサービスを更新することもできません。

すべての INACTIVE タスク定義リビジョンを削除すると、タスク定義名はコンソールで表示されず、API でも返されません。タスク定義リビジョンが DELETE_IN_PROGRESS 状態にある場合、タスク定義名はコンソールに表示され、API で返されます。タスク定義名は Amazon ECS によって保持され、次回その名前を使用してタスク定義を作成するときにリビジョンがインクリメントされます。

削除をブロックできる Amazon ECS リソース

タスク定義リビジョンに依存する Amazon ECS リソースがある場合、タスク定義の削除リクエストは完了しません。次のリソースが原因で、タスク定義が削除されない場合があります。

- Amazon ECS スタンドアロンタスク – タスクを正常に動作させるには、タスク定義が必要です。
- Amazon ECS サービスタスク - タスクを正常に動作させるには、タスク定義が必要です。
- Amazon ECS サービスのデプロイとタスクセット - Amazon ECS のデプロイまたはタスクセットのスケーリングイベントが開始される場合は、タスク定義が必要です。

タスク定義が `DELETE_IN_PROGRESS` の状態のままである場合は、コンソールまたは AWS CLI を使用して、タスク定義の削除をブロックしているリソースを特定し、停止できます。

ブロックされたリソースが削除された後のタスク定義の削除

タスク定義の削除をブロックするリソースを削除すると、次のルールが適用されます。

- Amazon ECS タスク - タスク定義の削除は、タスクが停止されてから完了するまでに最大 1 時間かかる場合があります。
- Amazon ECS サービスのデプロイとタスクセット - タスク定義の削除は、デプロイまたはタスクセットが削除されてから完了するまでに最大 24 時間かかる場合があります。

手順

タスク定義を登録解除するには (Amazon ECS コンソール)

タスク定義リビジョンは、削除する前に登録解除する必要があります。詳細については、「the section called “新しいコンソールを使用したタスク定義リビジョンの登録解除”」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、タスク定義を含むリージョンを選択します。
3. ナビゲーションペインで、[Task Definitions] を選択します。
4. [タスク定義] ページで、登録解除する 1 つ以上のタスク定義リビジョンを含むタスク定義ファミリーを選択します。
5. [タスク定義名] ページで、削除するリビジョンを選択し、次に [アクション]、[削除] の順に選択します。

[削除] が使用できない場合は、タスク定義の登録を解除する必要があります。

6. [削除] 確認ボックス内の情報を確認し、[削除する] を選択して終了します。

Amazon ECS タスク定義のユースケース

さまざまな AWS のサービスや機能のタスク定義を作成する方法を説明します。

ワークロードによっては、設定を要するいくつかのタスク定義パラメータがあります。また、EC2 起動タイプでは、そのワークロード用に設計された特定のインスタンスを選択する必要があります。

トピック

- GPU ワークロード向けの Amazon ECS タスク定義
- 動画トランスコーディングワークロードでの Amazon ECS タスク定義
- AWS Neuron 機械学習ワークロードでの Amazon ECS タスク定義
- 深層学習インスタンスでの Amazon ECS タスク定義
- 64 ビット ARM ワークロードでの Amazon ECS タスク定義
- Amazon ECS ログを CloudWatch に送信する
- Amazon ECS ログを AWS サービスまたは AWS Partner に送信する
- Amazon ECS での AWS 以外のコンテナイメージの使用
- コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する
- Amazon ECS コンテナに機密データを渡す

GPU ワークロード向けの Amazon ECS タスク定義

GPU 対応コンテナインスタンスを使用してクラスターを作成することで、GPU を使用するワークロードが Amazon ECS でサポートされます。p2、p3、p5、g3、g4、g5 のインスタンスタイプを使用する、Amazon EC2 GPU ベースのコンテナインスタンスでは、NVIDIA GPU へのアクセスが可能です。詳細については、「Amazon EC2 インスタンスタイプガイド」の「Linux Accelerated Computing Instances」を参照してください。

Amazon ECS には、事前設定された NVIDIA カーネルドライバーと Docker GPU ランタイムが付属する、GPU 最適化 AMI が用意されています。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

コンテナレベルのタスク配置のために、タスク定義でいくつかの GPU を指定できます。Amazon ECS は、使用が可能で GPU をサポートしているコンテナインスタンスをスケジュールし、物理的 GPU を適切なコンテナに固定して最適なパフォーマンスを実現します。

以下の Amazon EC2 GPU ベースのインスタンスタイプがサポートされています。詳細については、「Amazon EC2 P2 インスタンス」、「Amazon EC2 P3 インスタンス」、「Amazon EC2 P4d インスタンス」、「Amazon EC2 P5 インスタンス」、「Amazon EC2 G3 インスタンス」、「Amazon EC2 G4 インスタンス」、「Amazon EC2 G5 インスタンス」、「Amazon EC2 G6 インスタンス」、「Amazon EC2 G6e Instances」を参照してください。

インスタンスタイプ	GPU	GPU メモリ (GiB)	vCPUs	メモリ (GiB)
p3.2xlarge	1	16	8	61
p3.8xlarge	4	64	32	244
p3.16xlarge	8	128	64	488
p3dn.24xlarge	8	256	96	768
p4d.24xlarge	8	320	96	1152
p5.48xlarge	8	640	192	2048
g3s.xlarge	1	8	4	30.5
g3.4xlarge	1	8	16	122
g3.8xlarge	2	16	32	244
g3.16xlarge	4	32	64	488
g4dn.xlarge	1	16	4	16
g4dn.2xlarge	1	16	8	32
g4dn.4xlarge	1	16	16	64
g4dn.8xlarge	1	16	32	128

インスタンスタイプ	GPU	GPU メモリ (GiB)	vCPUs	メモリ (GiB)
g4dn.12xlarge	4	64	48	192
g4dn.16xlarge	1	16	64	256
g5.xlarge	1	24	4	16
g5.2xlarge	1	24	8	32
g5.4xlarge	1	24	16	64
g5.8xlarge	1	24	32	128
g5.16xlarge	1	24	64	256
g5.12xlarge	4	96	48	192
g5.24xlarge	4	96	96	384
g5.48xlarge	8	192	192	768
g6.xlarge	1	24	4	16
g6.2xlarge	1	24	8	32
g6.4xlarge	1	24	16	64
g6.8xlarge	1	24	32	128
g6.16.xlarge	1	24	64	256
g6.12xlarge	4	96	48	192
g6.24xlarge	4	96	96	384
g6.48xlarge	8	192	192	768
g6.metal	8	192	192	768
gr6.4xlarge	1	24	16	128

インスタンスタイプ	GPU	GPU メモリ (GiB)	vCPUs	メモリ (GiB)
gr6e.xlarge	1	48	4	32
g6e.2xlarge	1	48	8	64
g6e.4xlarge	1	48	16	128
g6e.8xlarge	1	48	32	256
g6e16.xlarge	1	48	64	512
g6e12.xlarge	4	192	48	384
g6e24.xlarge	4	192	96	768
g6e48.xlarge	8	384	192	1536
gr6.8xlarge	1	24	32	256

AWS Systems Manager パラメータストア API をクエリすることで、Amazon ECS に最適化された AMI の Amazon マシンイメージ (AMI) ID を取得できます。このパラメータを使用することで、Amazon ECS 最適化 AMI ID を手動で検索する必要がなくなります。Systems Manager Parameter Store API の詳細については、GetParameter を参照してください。使用するユーザーには、Amazon ECS 最適化 AMI メタデータを取得するための `ssm:GetParameter` IAM 許可が必要です。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/gpu/
recommended --region us-east-1
```

考慮事項

> **Note**
>
> g2 インスタンスファミリータイプのサポートは廃止されました。
> p2 インスタンスファミリータイプは、バージョン `20230912` より前の Amazon ECS GPU 最適化 AMI でのみサポートされています。引き続き p2 インスタンスを使用する必要がある場合は、P2 インスタンスが必要な場合の対処方法 を参照してください。

これら両方のインスタンスファミリータイプで NVIDIA/CUDA ドライバーをインプレース更新すると、GPU ワークロードに障害が発生する可能性があります。

Amazon ECS で GPU の使用を開始する前に、以下について検討することをお勧めします。

- クラスターには、GPU 対応コンテナインスタンスと GPU 非対応コンテナインスタンスを混在させることができます。
- GPU ワークロードは外部インスタンスでの実行が可能です。外部インスタンスをクラスターに登録するときは、`--enable-gpu` フラグがインストールスクリプトに含まれていることを確認してください。詳細については、「Amazon ECS クラスターに外部インスタンスを登録する」を参照してください。
- エージェント設定ファイルで `ECS_ENABLE_GPU_SUPPORT` を `true` に設定する必要があります。詳細については、「the section called “コンテナエージェントの設定”」を参照してください。
- タスクの実行時またはサービスの作成時に、インスタンスタイプ属性を使用してタスク配置制約を設定することで、タスクが起動されるコンテナインスタンスを指定できます。これにより、リソースをより効果的に使用できます。詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

  以下の例では、デフォルトクラスター内の `g4dn.xlarge` コンテナインスタンスでタスクを起動しています。

  ```
  aws ecs run-task --cluster default --task-definition ecs-gpu-task-def \
       --placement-constraints type=memberOf,expression="attribute:ecs.instance-type ==
    g4dn.xlarge" --region us-east-2
  ```

- Amazon ECS は、コンテナ定義で指定された GPU リソース要件が適用されるコンテナごとに、コンテナランタイムとして NVIDIA のコンテナランタイムが使用されるように設定します。
- NVIDIA コンテナランタイムが適切に機能するためには、コンテナにいくつかの環境変数を設定する必要があります。これらの環境変数のリストについては、「Docker を使用した特殊設定」を参照してください。Amazon ECS は、`NVIDIA_VISIBLE_DEVICES`環境変数の値を Amazon ECS がコンテナに割り当てる GPU デバイス ID のリストに設定します。Amazon ECS は、これら以外の必須環境変数の設定は行いません。そのため、これらの必須変数がコンテナイメージで設定されていること、あるいはコンテナ定義内で設定されていることを確認する必要があります。
- p5 インスタンスタイプファミリーは、バージョン `20230929` 以降の Amazon ECS GPU 最適化 AMI でサポートされています。

- g4 インスタンスタイプファミリーは、バージョン 20230913 以降の Amazon ECS GPU 最適化 AMI でサポートされています。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。Amazon ECS コンソールのクラスター作成ワークフローではサポートされていません。これらのインスタンスタイプを使用するには、Amazon EC2 コンソール、AWS CLI、または API を使用して、手動でインスタンスをクラスターに登録する必要があります。
- p4d.24xlarge インスタンスタイプは、CUDA 11 以降でのみ動作します。
- Amazon ECS GPU 最適化 AMI は IPv6 が有効になっているため、yum を使用するとき問題が生じます。これは、以下のコマンドで IPv4 を使用するように yum を構成することで解決できます。

```
echo "ip_resolve=4" >> /etc/yum.conf
```

- NVIDIA/CUDA ベースのイメージを使用しないコンテナイメージをビルドする場合は、NVIDIA_DRIVER_CAPABILITIES コンテナランタイム変数に以下のいずれかの値を設定します。
  - utility,compute
  - all

  変数の設定方法については、NVIDIA の Web サイトの「NVIDIA コンテナランタイムの制御」を参照してください。
- Windows コンテナでは、GPU はサポートされません。

Amazon ECS 向け GPU コンテナインスタンスの起動

Amazon ECS で GPU インスタンスを使用するには、起動テンプレートとユーザーデータファイルを作成し、インスタンスを起動する必要があります。

これにより、GPU 用に設定されたタスク定義を使用するタスクを実行できます。

起動テンプレートを使用する

起動テンプレートを作成します。

- Amazon ECS に最適化された AMI 用の GPU AMI ID を使用する起動テンプレートを作成してください。起動テンプレートの作成方法については、「Amazon EC2 ユーザーガイド」の「Create a new launch template using parameters you define」を参照してください。

[Amazon マシンイメージ] には、前のステップの AMI ID を使用します。Systems Manager パラメータで AMI ID を指定する方法については、「Amazon EC2 ユーザーガイド」の「Specify a Systems Manager parameter in a launch template」を参照してください。

起動テンプレートの [ユーザーデータ] に以下を追加します。*cluster-name* をクラスターの名前に置き換えます。

```
#!/bin/bash
echo ECS_CLUSTER=cluster-name >> /etc/ecs/ecs.config;
echo ECS_ENABLE_GPU_SUPPORT=true >> /etc/ecs/ecs.config
```

AWS CLI を使用する

AWS CLI を使用して、コンテナインスタンスを起動できます。

1. userdata.toml というファイルを作成します。このファイルは、インスタンスのユーザーデータに使用されます。*cluster-name* をクラスターの名前に置き換えます。

```
#!/bin/bash
echo ECS_CLUSTER=cluster-name >> /etc/ecs/ecs.config;
echo ECS_ENABLE_GPU_SUPPORT=true >> /etc/ecs/ecs.config
```

2. 次のコマンドを実行して、GPU AMI ID を取得します。これは次のステップで使用します。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/gpu/
recommended --region us-east-1
```

3. 次のコマンドを実行して、GPU インスタンスを起動します。次のパラメータを必ず置き換えてください。

   - *subnet* を、インスタンスを起動するプライベートまたはパブリックサブネットの ID に置き換えます。
   - *gpu_ami* を、前のステップの AMI ID に置き換えます。
   - *t3.large* を、使用するインスタンスタイプに置き換えます。
   - *region* を、リージョンコードに置き換えます。

```
aws ec2 run-instances --key-name ecs-gpu-example \
```

```
    --subnet-id subnet \
    --image-id gpu_ami \
    --instance-type t3.large \
    --region region \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=GPU,Value=example}]' \
    --user-data file://userdata.toml \
    --iam-instance-profile Name=ecsInstanceRole
```

4. 次のコマンドを実行して、コンテナインスタンスがクラスターに登録されていることを検証します。このコマンドを実行するときは、次のパラメータを必ず置き換えてください。

   - *cluster* を、自分のクラスター名に置き換えます。
   - *region* を、リージョンコードに置き換えます。

```
aws ecs list-container-instances --cluster cluster-name --region region
```

Amazon ECS タスク定義での GPU の指定

コンテナインスタンス上の GPU と Docker GPU ランタイムを利用するには、コンテナに必要な GPU の数をタスク定義内で必ず指定します。GPU をサポートするコンテナが配置されると、Amazon ECS コンテナエージェントは必要な数の物理 GPU を適切なコンテナに固定します。タスク内でコンテナ用に予約されている、すべての GPU の数は、タスクが起動されたコンテナインスタンスで使用できる GPU の数を超えることはできません。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

> **Important**
>
> GPU 要件をタスク定義で指定していない場合、タスクではデフォルトの Docker ランタイムが使用されます。

タスク定義での GPU 要件の JSON 形式は以下のとおりです。

```
{
  "containerDefinitions": [
     {
        ...
        "resourceRequirements" : [
            {
```

```
                "type" : "GPU",
                "value" : "2"
             }
          ],
      },
...
}
```

以下の例では、GPU 要件を指定する Docker コンテナの構文を示しています。このコンテナは 2 つの GPU を使用しており、nvidia-smi ユーティリティを実行した後に終了します。

```
{
  "containerDefinitions": [
    {
      "memory": 80,
      "essential": true,
      "name": "gpu",
      "image": "nvidia/cuda:11.0.3-base",
      "resourceRequirements": [
         {
           "type":"GPU",
           "value": "2"
         }
      ],
      "command": [
        "sh",
        "-c",
        "nvidia-smi"
      ],
      "cpu": 100
    }
  ],
  "family": "example-ecs-gpu"
}
```

GPU の共有

複数のコンテナで 1 つの GPU を共有する場合は、次のユーザーデータをインスタンスに追加します。詳細については、「Amazon EC2 ユーザーガイド」の「ユーザーデータ入力を使用して EC2 インスタンスを起動するときにコマンドを実行する」を参照してください。

サポートされている最新の GPU 最適化 AMI を使用する

GPU に最適化された AMI の 20230906 バージョンを使用して、インスタンスのユーザーデータに以下を追加できます。

cluster-name をクラスターの名前に置き換えます。

```
const userData = ec2.UserData.forLinux();
 userData.addCommands(
 'sudo rm /etc/sysconfig/docker',
 'echo DAEMON_MAXFILES=1048576 | sudo tee -a /etc/sysconfig/docker',
 'echo OPTIONS="--default-ulimit nofile=32768:65536 --default-runtime nvidia" | sudo
 tee -a /etc/sysconfig/docker',
 'echo DAEMON_PIDFILE_TIMEOUT=10 | sudo tee -a /etc/sysconfig/docker',
 'sudo systemctl restart docker',
);
```

P2 インスタンスが必要な場合の対処方法

P2 インスタンスを使用する必要がある場合、次のいずれかのオプションを使用してインスタンスを使用し続けることができます。

どちらのオプションでも、インスタンスユーザーデータを変更する必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「ユーザーデータ入力を使用して EC2 インスタンスを起動するときにコマンドを実行する」を参照してください。

サポートされている最新の GPU 最適化 AMI を使用する

GPU に最適化された AMI の 20230906 バージョンを使用して、インスタンスのユーザーデータに以下を追加できます。

cluster-name をクラスターの名前に置き換えます。

```
#!/bin/bash
echo "exclude=*nvidia* *cuda*" >> /etc/yum.conf
echo "ECS_CLUSTER=cluster-name" >> /etc/ecs/ecs.config
```

GPU に最適化された最新の AMI を使用し、ユーザーデータを更新する

以下をインスタンスのユーザーデータに追加します。これにより Nvidia 535/Cuda12.2 ドライバーがアンインストールされ、次に Nvidia 470/Cuda11.4 ドライバーがインストールされ、バージョンが修正されます。

```
#!/bin/bash
yum remove -y cuda-toolkit* nvidia-driver-latest-dkms*
tmpfile=$(mktemp)
cat >$tmpfile <<EOF
[amzn2-nvidia]
name=Amazon Linux 2 Nvidia repository
mirrorlist=\$awsproto://\$amazonlinux.\$awsregion.\$awsdomain/\$releasever/amzn2-
nvidia/latest/\$basearch/mirror.list
priority=20
gpgcheck=1
gpgkey=https://developer.download.nvidia.com/compute/cuda/repos/rhel7/
x86_64/7fa2af80.pub
enabled=1
exclude=libglvnd-*
EOF

mv $tmpfile /etc/yum.repos.d/amzn2-nvidia-tmp.repo
yum install -y system-release-nvidia cuda-toolkit-11-4 nvidia-driver-latest-
dkms-470.182.03
yum install -y libnvidia-container-1.4.0 libnvidia-container-tools-1.4.0 nvidia-
container-runtime-hook-1.4.0 docker-runtime-nvidia-1

echo "exclude=*nvidia* *cuda*" >> /etc/yum.conf
nvidia-smi
```

P2 と互換性のある GPU に最適化された独自の AMI を作成する

P2 インスタンスと互換性のある独自の Amazon ECS GPU 最適化 AMI を作成し、その AMI を使用して P2 インスタンスを起動できます。

1. 次のコマンドを実行して `amazon-ecs-ami repo` をクローンします。

   ```
   git clone https://github.com/aws/amazon-ecs-ami
   ```

2. 必要な Amazon ECS エージェントとソースの Amazon Linux AMI バージョンを `release.auto.pkrvars.hcl` または `overrides.auto.pkrvars.hcl` に設定します。
3. P2 と互換性のあるプライベート EC2 AMI を構築するには、次のコマンドを実行します。

   リージョンをインスタンスリージョンがあるリージョンに置き換えます。

   ```
   REGION=region make al2keplergpu
   ```

4. 以下のインスタンスユーザーデータを含む AMI を使用して Amazon ECS クラスターに接続します。

   cluster-name をクラスターの名前に置き換えます。

```
#!/bin/bash
echo "ECS_CLUSTER=cluster-name" >> /etc/ecs/ecs.config
```

動画トランスコーディングワークロードでの Amazon ECS タスク定義

Amazon ECS で動画トランスコーディングワークロードを使用するには、Amazon EC2 VT1 インスタンスを登録します。これらのインスタンスを登録した後は、事前レンダリングされたライブ動画のトランスコーディングワークロードを、Amazon ECS タスクとして実行できます。Amazon EC2 VT1 インスタンスは、Xilinx U30 メディアトランスコーディングカードを使用して、事前レンダリングされたライブ動画のトランスコーディングワークロードを高速化します。

> **Note**
>
> Amazon ECS 以外のコンテナで動画トランスコーディングワークロードを実行する方法については、Xilinx のドキュメントを参照してください。

考慮事項

Amazon ECS で VT1 のデプロイを開始する前に、以下の点を考慮してください。

- クラスターには、VT1 コンテナインスタンスと VT1 以外のインスタンスを混在させることができます。
- アクセラレータ付きの AVC (H.264) および HEVC (H.265) コーデックを備えた、Xilinx U30 メディアトランスコーディングカードを使用する Linux アプリケーションが必要です。

> **Important**
>
> 他のコーデックを使用するアプリケーションでは、VT1 インスタンスのパフォーマンスが強化されていない場合があります。

- U30 カードでは、トランスコーディングタスクを 1 つのみ実行できます。各カードには、2 つのデバイスが関連付けられています。VT1 インスタンスごとに、使用しているカードの数だけのトランスコーディングタスクを実行できます。
- サービスの作成時、またはスタンドアロンタスクの実行時に、インスタンスタイプ属性を使用してタスク配置制約を設定することができます。これにより、指定したコンテナインスタンスでタスクが起動されることを保証します。また、リソースを効果的に使用し、動画トランスコーディングワークロードのタスクが VT1 インスタンスに配置されるようにすることができます。詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

  次の例では、タスクが`default` クラスターの `vt1.3xlarge` インスタンス上で実行されます。

```
aws ecs run-task \
     --cluster default \
     --task-definition vt1-3xlarge-xffmpeg-processor \
     --placement-constraints type=memberOf,expression="attribute:ecs.instance-type ==
 vt1.3xlarge"
```

- ホストコンテナインスタンス向けに用意された、特定の U30 カードを使用するようにコンテナを設定します。これを行うには、`linuxParameters` パラメータによりデバイスの詳細を指定します。詳細については、「タスク定義の要件」を参照してください。

VT1 AMI の使用

Amazon ECS コンテナインスタンス用 Amazon EC2 上で AMI を実行するには、2 つのオプションがあります。1 番目のオプションは、AWS Marketplace にある Xilinx 公式 AMI を使用することです。2 番目のオプションは、サンプルのリポジトリを利用して、独自の AMI を構築することです。

- Xilinx は、AWS Marketplace に AMI を提供しています。
- Amazon ECS は、動画トランスコーディングワークロード用の AMI を構築するために使用できる、サンプルのリポジトリを提供しています。この AMI には Xilinx U30 ドライバー備わります。GitHub で、Packer スクリプトを含むリポジトリを入手できます。Packer の詳細については、「Packer documentation」(Packer ドキュメント) を参照してください。

タスク定義の要件

Amazon ECS で動画トランスコーディングコンテナを実行するには、アクセラレータ付きの H.264/AVC および H.265/HEVC コーデックを使用する動画トランスコーディングアプリケーションが、タ

スク定義に含まれている必要があります。Xilinx GitHub の手順に従うことで、コンテナイメージを構築できます。

タスク定義は、インスタンスタイプに固有である必要があります。これらのインスタンスタイプは、3xlarge、6xlarge、および 24xlarge です。コンテナでは、ホストコンテナインスタンス向けに用意された、特定の Xilinx U30 デバイスの使用を設定する必要があります。これは、`linuxParameters` パラメータを使用して設定します。次の表に、各インスタンスタイプに固有のカードとデバイス SoC の詳細を示します。

インスタンスタイプ	vCPUs	RAM (GiB)	U30 アクセラレータカード	アドレス可能な XCU30 SoC デバイス	デバイスへのパス
vt1.3xlarge	12	24	1	2	`/dev/dri/renderD128 ,/dev/dri/renderD129`
vt1.6xlarge	24	48	2	4	`/dev/dri/renderD128 ,/dev/dri/renderD129 ,/dev/dri/renderD130 ,/dev/dri/renderD131`
vt1.24xlarge	96	182	8	16	`/dev/dri/renderD128 ,/dev/dri/`

インスタンスタイプ	vCPUs	RAM (GiB)	U30 アクセラレータカード	アドレス可能な XCU30 SoC デバイス	デバイスへのパス
					renderD129 ,/dev/dri/renderD130 ,/dev/dri/renderD131 ,/dev/dri/renderD132 ,/dev/dri/renderD133 ,/dev/dri/renderD134 ,/dev/dri/renderD135 ,/dev/dri/renderD136 ,/dev/dri/renderD137 ,/dev/dri/renderD138 ,/dev/dri/renderD139 ,/dev/

インスタンスタイプ	vCPUs	RAM (GiB)	U30 アクセラレータカード	アドレス可能な XCU30 SoC デバイス	デバイスへのパス
					dri/renderD140 ,/dev/dri/renderD141 ,/dev/dri/renderD142 ,/dev/dri/renderD143

> **Important**
>
> タスク定義に EC2 インスタンスにないデバイスがリストされている場合、タスクの実行は失敗します。タスクが失敗した場合は、stoppedReason にエラーメッセージ CannotStartContainerError: Error response from daemon: error gathering device information while adding custom device "/dev/dri/renderD*130*": no such file or directory が表示されます。

Amazon ECS タスク定義での動画トランスコーディングの指定

次の例に、Amazon EC2 の Linux コンテナのタスク定義に使用される構文を示します。このタスク定義は、「Xilinx documentation」(Xilinx のドキュメント) で説明されている手順により構築されるコンテナイメージ用です。この例を使用する場合は、image を独自のイメージで置き換え、/home/ec2-user ディレクトリにあるインスタンスにビデオファイルをコピーします。

vt1.3xlarge

1. vt1-3xlarge-ffmpeg-linux.json と言う名前で、以下の内容が記述されたテキストファイルを作成します。

```
{
    "family": "vt1-3xlarge-xffmpeg-processor",
    "requiresCompatibilities": ["EC2"],
    "placementConstraints": [
        {
            "type": "memberOf",
            "expression": "attribute:ecs.os-type == linux"
        },
        {
            "type": "memberOf",
            "expression": "attribute:ecs.instance-type == vt1.3xlarge"
        }
    ],
    "containerDefinitions": [
        {
            "entryPoint": [
                "/bin/bash",
                "-c"
            ],
            "command": ["/video/ecs_ffmpeg_wrapper.sh"],
            "linuxParameters": {
                "devices": [
                    {
                        "containerPath": "/dev/dri/renderD128",
                        "hostPath": "/dev/dri/renderD128",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD129",
                        "hostPath": "/dev/dri/renderD129",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    }
```

```
                ]
            },
            "mountPoints": [
                {
                    "containerPath": "/video",
                    "sourceVolume": "video_file"
                }
            ],
            "cpu": 0,
            "memory": 12000,
            "image": "0123456789012.dkr.ecr.us-west-2.amazonaws.com/aws/xilinx-
xffmpeg",
            "essential": true,
            "name": "xilinix-xffmpeg"
        }
    ],
    "volumes": [
        {
            "name": "video_file",
            "host": {"sourcePath": "/home/ec2-user"}
        }
    ]
}
```

2. タスク定義を登録します。

```
aws ecs register-task-definition --family vt1-3xlarge-xffmpeg-processor --cli-
input-json file://vt1-3xlarge-xffmpeg-linux.json --region us-east-1
```

vt1.6xlarge

1. vt1-6xlarge-ffmpeg-linux.json と言う名前で、以下の内容が記述されたテキストファイルを作成します。

```
{
    "family": "vt1-6xlarge-xffmpeg-processor",
    "requiresCompatibilities": ["EC2"],
    "placementConstraints": [
        {
            "type": "memberOf",
            "expression": "attribute:ecs.os-type == linux"
        },
```

```
        {
            "type": "memberOf",
            "expression": "attribute:ecs.instance-type == vt1.6xlarge"
        }
    ],
    "containerDefinitions": [
        {
            "entryPoint": [
                "/bin/bash",
                "-c"
            ],
            "command": ["/video/ecs_ffmpeg_wrapper.sh"],
            "linuxParameters": {
                "devices": [
                    {
                        "containerPath": "/dev/dri/renderD128",
                        "hostPath": "/dev/dri/renderD128",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD129",
                        "hostPath": "/dev/dri/renderD129",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD130",
                        "hostPath": "/dev/dri/renderD130",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD131",
                        "hostPath": "/dev/dri/renderD131",
                        "permissions": [
                            "read",
                            "write"
```

```
                        ]
                    }
                ]
            },
            "mountPoints": [
                {
                    "containerPath": "/video",
                    "sourceVolume": "video_file"
                }
            ],
            "cpu": 0,
            "memory": 12000,
            "image": "0123456789012.dkr.ecr.us-west-2.amazonaws.com/aws/xilinx-
xffmpeg",
            "essential": true,
            "name": "xilinix-xffmpeg"
        }
    ],
    "volumes": [
        {
            "name": "video_file",
            "host": {"sourcePath": "/home/ec2-user"}
        }
    ]
}
```

2. タスク定義を登録します。

```
aws ecs register-task-definition --family vt1-6xlarge-xffmpeg-processor --cli-
input-json file://vt1-6xlarge-xffmpeg-linux.json --region us-east-1
```

vt1.24xlarge

1. vt1-24xlarge-ffmpeg-linux.json と言う名前で、以下の内容が記述されたテキストファイルを作成します。

```
{
    "family": "vt1-24xlarge-xffmpeg-processor",
    "requiresCompatibilities": ["EC2"],
    "placementConstraints": [
        {
            "type": "memberOf",
```

```
            "expression": "attribute:ecs.os-type == linux"
        },
        {
            "type": "memberOf",
            "expression": "attribute:ecs.instance-type == vt1.24xlarge"
        }
    ],
    "containerDefinitions": [
        {
            "entryPoint": [
                "/bin/bash",
                "-c"
            ],
            "command": ["/video/ecs_ffmpeg_wrapper.sh"],
            "linuxParameters": {
                "devices": [
                    {
                        "containerPath": "/dev/dri/renderD128",
                        "hostPath": "/dev/dri/renderD128",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD129",
                        "hostPath": "/dev/dri/renderD129",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD130",
                        "hostPath": "/dev/dri/renderD130",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD131",
                        "hostPath": "/dev/dri/renderD131",
                        "permissions": [
```

```
                        "read",
                        "write"
                    ]
                },
                {
                    "containerPath": "/dev/dri/renderD132",
                    "hostPath": "/dev/dri/renderD132",
                    "permissions": [
                        "read",
                        "write"
                    ]
                },
                {
                    "containerPath": "/dev/dri/renderD133",
                    "hostPath": "/dev/dri/renderD133",
                    "permissions": [
                        "read",
                        "write"
                    ]
                },
                {
                    "containerPath": "/dev/dri/renderD134",
                    "hostPath": "/dev/dri/renderD134",
                    "permissions": [
                        "read",
                        "write"
                    ]
                },
                {
                    "containerPath": "/dev/dri/renderD135",
                    "hostPath": "/dev/dri/renderD135",
                    "permissions": [
                        "read",
                        "write"
                    ]
                },
                {
                    "containerPath": "/dev/dri/renderD136",
                    "hostPath": "/dev/dri/renderD136",
                    "permissions": [
                        "read",
                        "write"
                    ]
                },
```

```
                    {
                        "containerPath": "/dev/dri/renderD137",
                        "hostPath": "/dev/dri/renderD137",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD138",
                        "hostPath": "/dev/dri/renderD138",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD139",
                        "hostPath": "/dev/dri/renderD139",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD140",
                        "hostPath": "/dev/dri/renderD140",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD141",
                        "hostPath": "/dev/dri/renderD141",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD142",
                        "hostPath": "/dev/dri/renderD142",
                        "permissions": [
```

```
                            "read",
                            "write"
                        ]
                    },
                    {
                        "containerPath": "/dev/dri/renderD143",
                        "hostPath": "/dev/dri/renderD143",
                        "permissions": [
                            "read",
                            "write"
                        ]
                    }
                ]
            },
            "mountPoints": [
                {
                    "containerPath": "/video",
                    "sourceVolume": "video_file"
                }
            ],
            "cpu": 0,
            "memory": 12000,
            "image": "0123456789012.dkr.ecr.us-west-2.amazonaws.com/aws/xilinx-
xffmpeg",
            "essential": true,
            "name": "xilinix-xffmpeg"
        }
    ],
    "volumes": [
        {
            "name": "video_file",
            "host": {"sourcePath": "/home/ec2-user"}
        }
    ]
}
```

2. タスク定義を登録します。

```
aws ecs register-task-definition --family vt1-24xlarge-xffmpeg-processor --cli-
input-json file://vt1-24xlarge-xffmpeg-linux.json --region us-east-1
```

AWS Neuron 機械学習ワークロードでの Amazon ECS タスク定義

機械学習のワークロード用に、Amazon EC2 Trn1、Amazon EC2 Inf1、Amazon EC2 Inf2 インスタンスをクラスターに登録できます。

Amazon EC2 Trn1 インスタンスは、AWS Trainium チップを搭載しています。これらのインスタンスは、クラウドでの機械学習用に高性能で低コストのトレーニングを提供します。Trn1 インスタンスで AWS Neuron を使用した機械学習フレームワークを使用して、機械学習推論モデルをトレーニングできます。その後、Inf1 インスタンスまたは Inf2 インスタンスでモデルを実行して、AWS Inferentia チップのアクセラレーションを使用できます。

Amazon EC2 Inf1 インスタンスと Inf2 インスタンスは、AWS Inferentia チップを搭載しています。これらは、クラウドで高性能かつ最低レベルのコストの推論を提供します。

機械学習モデルは、専用の Software Developer Kit (SDK) である AWS Neuron を使用してコンテナにデプロイされます。この SDK は、AWS 機械学習チップの機械学習パフォーマンスを最適化するコンパイラ、ランタイム、およびプロファイリングツールからなります。 AWSNeuron は、TensorFlow、PyTorch、Apache MXNet などの一般的な機械学習フレームワークをサポートしています。

考慮事項

Amazon ECS での Neuron のデプロイを開始する前に、以下の点を考慮してください。

- クラスターには、Trn1、Inf1、Inf2、およびその他のインスタンスを混在させることができます。
- AWS Neuron をサポートする機械学習フレームワークを使用するコンテナ内に、Linux アプリケーションが必要です。

> **Important**
>
> 他のフレームワークを使用するアプリケーションでは、Trn1、Inf1、Inf2 インスタンスのパフォーマンスが強化されていない場合があります。

- 各 AWS Trainium または AWS Inferentia チップで実行できる推論または推論トレーニングのタスクは 1 つだけです。Inf1 の場合、各チップには 4 つの NeuronCore があります。Trn1 と Inf2 の場合、各チップには 2 つの NeuronCore があります。Trn1、Inf1、Inf2 インスタンスごとに、使用しているチップの数だけのタスクを実行できます。
- サービスの作成時、またはスタンドアロンタスクの実行時にタスク配置制約を設定する場合は、インスタンスタイプ属性を使用します。これにより、指定したコンテナインスタンスでタスクが起動

されることを保証します。そうすることで、全体的なリソース使用率を最適化し、推論ワークロードのタスクを確実に Trn1、Inf1、Inf2 インスタンスに配置できます。詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

次の例では、`default` クラスターの `Inf1.xlarge` インスタンスでタスクが実行されます。

```
aws ecs run-task \
     --cluster default \
     --task-definition ecs-inference-task-def \
     --placement-constraints type=memberOf,expression="attribute:ecs.instance-type ==
 Inf1.xlarge"
```

- Neuron リソース要件はタスク定義で定義できません。代わりに、ホストコンテナインスタンス向けに用意された、特定の AWS Trainium または AWS Inferentia チップを使用するようコンテナを設定します。これを行うには、`linuxParameters` パラメータを使用してデバイスの詳細を指定します。詳細については、「タスク定義の要件」を参照してください。

Amazon ECS に最適化された Amazon Linux 2023 (Neuron) AMI の使用

Amazon ECS では、Amazon Linux 2023 ベースの Amazon ECS 最適化 AMI が、AWS Trainium および AWS Inferentia のワークロード用に用意されています。これには、Docker 用の AWS Neuron ドライバーとランタイムが付属しています。この AMI により、Amazon ECS 上で機械学習推論ワークロードの実行が容易になります。

Amazon EC2 の Trn1、Inf1、Inf2 インスタンスを起動する際は、Amazon ECS に最適化された Amazon Linux 2023 (Neuron) AMI を使用することをお勧めします。

現在の Amazon ECS に最適化された Amazon Linux 2023 (Neuron) AMI を取得するには、AWS CLI で次のコマンドを使用します。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2023/neuron/
recommended
```

Amazon ECS に最適化された Amazon Linux 2023 (Neuron) AMI は、以下のリージョンでサポートされています。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)

- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)
- アジアパシフィック (東京)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 南米 (サンパウロ)

Amazon ECS に最適化された Amazon Linux 2 (Neuron) AMI の使用

Amazon ECS では、Amazon Linux 2 ベースの Amazon ECS 最適化 AMI が、AWS Trainium および AWS Inferentia のワークロード用に用意されています。これには、Docker 用の AWS Neuron ドライバーとランタイムが付属しています。この AMI により、Amazon ECS 上で機械学習推論ワークロードの実行が容易になります。

Amazon EC2 の Trn1、Inf1、Inf2 インスタンスを起動する際は、Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI を使用することをお勧めします。

現在の Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI を取得するには、AWS CLI で次のコマンドを使用します。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/inf/
recommended
```

Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI は、以下のリージョンでサポートされています。

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)
- アジアパシフィック (東京)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 南米 (サンパウロ)

タスク定義の要件

Amazon ECS 上に Neuron をデプロイするには、TensorFlow の推論モデルを提供するビルド済みコンテナのコンテナ定義が、タスク定義の中に含まれている必要があります。この定義は、AWS Deep Learning Containers によって提供されます。このコンテナには、AWS Neuron ランタイムと TensorFlow Serving アプリケーションが含まれています。起動時に、このコンテナは Amazon S3 からモデルを取得し、保存されたモデルを使用して Neuron TensorFlow Serving を起動した後、予測リクエストのために待機します。次の例でのコンテナイメージでは、 TensorFlow 1.15 と Ubuntu 18.04 を使用しています。Neuron 用に最適化された事前構築済みの Deep Learning Containers の完全なリストは、GitHub に保持されます。詳細については、「AWS Neuron TensorFlow Serving の使用」を参照してください。

```
763104351884.dkr.ecr.us-east-1.amazonaws.com/tensorflow-inference-neuron:1.15.4-neuron-py37-ubuntu18.04
```

または、独自の Neuron サイドカーコンテナイメージを構築することもできます。詳細については、「AWS Deep Learning AMIs デベロッパーガイド」の「チュートリアル: Neuron TensorFlow Serving」を参照してください。

タスク定義は、1 つのインスタンスタイプに固有である必要があります。コンテナでは、ホストコンテナインスタンス向けに用意された、固有の AWS Trainium または AWS Inferentia デバイスを使用するよう設定する必要があります。これは、`linuxParameters` パラメータを使用して設定します。次の表に、各インスタンスタイプに固有のチップの詳細を示します。

インスタンスタイプ	vCPUs	RAM (GiB)	AWS ML アクセラレーターチップ	デバイスへのパス
trn1.2xlarge	8	32	1	`/dev/neuron0`
trn1.32xlarge	128	512	16	`/dev/neuron0 ,/dev/neuron1 ,/dev/neuron2 ,/dev/neuron3 ,/dev/neuron4 ,/dev/neuron5 ,/dev/neuron6 ,/dev/neuron7 ,/dev/neuron8 ,/dev/neuron9 ,/dev/neuron10 ,/dev/neuron11 ,/dev/neuron12 ,/dev/neuron13 ,/dev/neuron14 ,`

インスタンスタイプ	vCPUs	RAM (GiB)	AWS ML アクセラレーターチップ	デバイスへのパス
				/dev/neuron15
inf1.xlarge	4	8	1	/dev/neuron0
inf1.2xlarge	8	16	1	/dev/neuron0
inf1.6xlarge	24	48	4	/dev/neuron0 ,/dev/neuron1 ,/dev/neuron2 ,/dev/neuron3

インスタンスタイプ	vCPUs	RAM (GiB)	AWS ML アクセラレーターチップ	デバイスへのパス
inf1.24xlarge	96	192	16	/dev/neuron0 ,/dev/neuron1 ,/dev/neuron2 ,/dev/neuron3 ,/dev/neuron4 ,/dev/neuron5 ,/dev/neuron6 ,/dev/neuron7 ,/dev/neuron8 ,/dev/neuron9 ,/dev/neuron10 ,/dev/neuron11 ,/dev/neuron12 ,/dev/neuron13 ,/dev/neuron14 ,/dev/neuron15
inf2.xlarge	8	16	1	/dev/neuron0
inf2.8xlarge	32	64	1	/dev/neuron0

インスタンスタイプ	vCPUs	RAM (GiB)	AWS ML アクセラレーターチップ	デバイスへのパス
inf2.24xlarge	96	384	6	/dev/neuron0 , /dev/neuron1 , /dev/neuron2 , /dev/neuron3 , /dev/neuron4 , /dev/neuron5 ,
inf2.48xlarge	192	768	12	/dev/neuron0 , /dev/neuron1 , /dev/neuron2 , /dev/neuron3 , /dev/neuron4 , /dev/neuron5 , /dev/neuron6 , /dev/neuron7 , /dev/neuron8 , /dev/neuron9 , /dev/neuron10 , /dev/neuron11

Amazon ECS タスク定義での AWS Neuron 機械学習の指定

次に、使用する構文を表示する `inf1.xlarge` 用の Linux タスク定義の例を示します。

```
{
    "family": "ecs-neuron",
```

```
    "requiresCompatibilities": ["EC2"],
    "placementConstraints": [
        {
            "type": "memberOf",
            "expression": "attribute:ecs.os-type == linux"
        },
        {
            "type": "memberOf",
            "expression": "attribute:ecs.instance-type == inf1.xlarge"
        }
    ],
    "executionRoleArn": "${YOUR_EXECUTION_ROLE}",
    "containerDefinitions": [
        {
            "entryPoint": [
                "/usr/local/bin/entrypoint.sh",
                "--port=8500",
                "--rest_api_port=9000",
                "--model_name=resnet50_neuron",
                "--model_base_path=s3://amzn-s3-demo-bucket/resnet50_neuron/"
            ],
            "portMappings": [
                {
                    "hostPort": 8500,
                    "protocol": "tcp",
                    "containerPort": 8500
                },
                {
                    "hostPort": 8501,
                    "protocol": "tcp",
                    "containerPort": 8501
                },
                {
                    "hostPort": 0,
                    "protocol": "tcp",
                    "containerPort": 80
                }
            ],
            "linuxParameters": {
                "devices": [
                    {
                        "containerPath": "/dev/neuron0",
                        "hostPath": "/dev/neuron0",
                        "permissions": [
```

```
                            "read",
                            "write"
                        ]
                    }
                ],
                "capabilities": {
                    "add": [
                        "IPC_LOCK"
                    ]
                }
            },
            "cpu": 0,
            "memoryReservation": 1000,
            "image": "763104351884.dkr.ecr.us-east-1.amazonaws.com/tensorflow-
inference-neuron:1.15.4-neuron-py37-ubuntu18.04",
            "essential": true,
            "name": "resnet50"
        }
    ]
}
```

深層学習インスタンスでの Amazon ECS タスク定義

Amazon ECS で深層学習ワークロードを使用するには、Amazon EC2 DL1インスタンスをクラスターに登録します。Amazon EC2 DL1 インスタンスには、Habana Labs (インテル子会社) の Gaudi アクセラレータを搭載しています。Habana Gaudiアクセラレータには、Habana SynapseAI SDK を使用して接続します。この SDK は、TensorFlow および PyTorch による、一般的な機械学習フレームワークをサポートしています。

考慮事項

Amazon ECS 上で DL1 のデプロイを開始する前に、以下の点を考慮してください。

- クラスターには、DL1 コンテナインスタンスと DL1 以外のインスタンスを混在させることができます。
- サービスの作成時、またはスタンドアロンタスクの実行時、特にタスク配置制約を設定する場合には、インスタンスタイプ属性を使用して、タスクが起動されるコンテナインスタンスを確定できます。これにより、リソースが効果的に使用され、深層学習ワークロードのタスクが DL1 インスタンス上に配置されることが保証されます。詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

次の例では、default クラスターの dl1.24xlarge インスタンスでタスクを実行します。

```
aws ecs run-task \
     --cluster default \
     --task-definition ecs-dl1-task-def \
     --placement-constraints type=memberOf,expression="attribute:ecs.instance-type ==
 dl1.24xlarge"
```

DL1 AMI の使用

Amazon ECS 向けの Amazon EC2 DL1 インスタンス上で AMI を実行するためには、以下の 3 つのオプションがあります。

- Habana がここで提供している AWS Marketplace AMI。
- Amazon Web Services によって提供される Habana 深層学習 AMI。これには、Amazon ECS コンテナエージェントは含まれないため、このエージェントを個別にインストールする必要があります。
- GitHub リポジトリを通じて提供されるカスタム AMI をビルドするには、Packer を使用します。詳細については、「the Packer documentation」(Packer ドキュメント) を参照してください。

Amazon ECS タスク定義での深層学習の指定

Habana Gaudi アクセラレータ付きの深層学習コンテナを Amazon ECS で実行するには、AWS Deep Learning Containers が提供する Habana SynapseAI を使用して TensorFlow または PyTorch 向けに深層学習モデルを提供する、ビルド済みコンテナのコンテナ定義が、対象のタスク定義内に含まれている必要があります。

次のコンテナイメージには TensorFlow 2.7.0 と Ubuntu 20.04 が含まれています。Neuron 用に最適化された事前構築済みの深層学習コンテナの完全なリストは、GitHub で確認できます。詳細については、「Habana Training Containers」(Habana トレーニングコンテナ) を参照してください。

```
763104351884.dkr.ecr.us-east-1.amazonaws.com/tensorflow-training-habana:2.7.0-hpu-py38-
synapseai1.2.0-ubuntu20.04
```

以下の例で、Amazon EC2 の Linux コンテナのタスク定義で使用する構文を示します。この例で使用するイメージには、vault.habana.ai/gaudi-docker/1.1.0/ubuntu20.04/habanalabs/

tensorflow-installer-tf-cpu-2.6.0:1.1.0-614 から入手が可能な Habana Labs のシステム管理インターフェイスツール (HL-SMI) が含まれています。

```
{
    "family": "dl-test",
    "requiresCompatibilities": ["EC2"],
    "placementConstraints": [
        {
            "type": "memberOf",
            "expression": "attribute:ecs.os-type == linux"
        },
        {
            "type": "memberOf",
            "expression": "attribute:ecs.instance-type == dl1.24xlarge"
        }
    ],
    "networkMode": "host",
    "cpu": "10240",
    "memory": "1024",
    "containerDefinitions": [
        {
            "entryPoint": [
                "sh",
                "-c"
            ],
            "command": ["hl-smi"],
            "cpu": 8192,
            "environment": [
                {
                    "name": "HABANA_VISIBLE_DEVICES",
                    "value": "all"
                }
            ],
            "image": "vault.habana.ai/gaudi-docker/1.1.0/ubuntu20.04/habanalabs/
tensorflow-installer-tf-cpu-2.6.0:1.1.0-614",
            "essential": true,
            "name": "tensorflow-installer-tf-hpu"
        }
    ]
}
```

64 ビット ARM ワークロードでの Amazon ECS タスク定義

Amazon ECS は 64 ビット ARM アプリケーションの使用をサポートしています。アプリケーションは、AWS Graviton プロセッサ搭載のプラットフォーム上で実行できます。この構成、さまざまなワークロードに適しています。対象となるのは、アプリケーションサーバー、マイクロサービス、ハイパフォーマンスコンピューティング、CPU ベースの機械学習推論、ビデオエンコーディング、電子回路設計オートメーション、ゲーム配信、オープンソースデータベース、インメモリーキャッシュなどのワークロードです。

考慮事項

64 ビット ARM アーキテクチャを使用するタスク定義のデプロイを開始する前に、次の点を考慮してください。

- アプリケーションは、Fargate 起動タイプ、または EC2 起動タイプを使用できます。
- アプリケーションは Linux オペレーティングシステムのみで使用できます。
- Fargate タイプの場合、アプリケーションは Fargate プラットフォームバージョン `1.4.0` 以降を使用する必要があります。
- アプリケーションは、モニタリングに Fluent Bit または CloudWatch を使用できます。
- Fargate 起動タイプの場合、次の AWS リージョン では 64 ビット ARM ワークロードがサポートされません。
  - 米国東部 (バージニア北部)、`use1-az3` アベイラビリティーゾーン
- Amazon EC2 起動タイプの場合、以下を参照して、使用したいインスタンスタイプが自分のリージョンでサポートされていることを確認してください。
  - Amazon EC2 M6g インスタンス
  - Amazon EC2 T4g インスタンス
  - Amazon EC2 C6g インスタンス
  - Amazon EC2 R6gd インスタンス
  - Amazon EC2 X2gd インスタンス

  フィルターで Amazon EC2 の `describe-instance-type-offerings` コマンドを使用して、リージョンのインスタンスオファリングを表示することもできます。

```
aws ec2 describe-instance-type-offerings --filters Name=instance-
type,Values=instance-type --region region
```

次の例では、米国東部 (バージニア北部) (us-east-1) リージョンで M6 インスタンスタイプが使用可能かどうかを確認します。

```
aws ec2 describe-instance-type-offerings --filters "Name=instance-type,Values=m6*" --region us-east-1
```

詳細については、「Amazon EC2 コマンドラインリファレンス」の「インスタンスタイプオファリングの説明」を参照してください。

Amazon ECS タスク定義での ARM アーキテクチャの指定

ARM アーキテクチャを使用するには、cpuArchitecture タスク定義パラメータに ARM64 を指定します。

次の例では、タスク定義で ARM アーキテクチャが指定されています。JSON 形式にあります。

```
{
    "runtimePlatform": {
        "operatingSystemFamily": "LINUX",
        "cpuArchitecture": "ARM64"
    },
...
}
```

次の例に、「hello world」を表示する ARM アーキテクチャのタスク定義を示します。

```
{
 "family": "arm64-testapp",
 "networkMode": "awsvpc",
 "containerDefinitions": [
    {
        "name": "arm-container",
        "image": "public.ecr.aws/docker/library/busybox:latest",
        "cpu": 100,
        "memory": 100,
        "essential": true,
        "command": [ "echo hello world" ],
        "entryPoint": [ "sh", "-c" ]
    }
 ],
```

```
 "requiresCompatibilities": [ "EC2" ],
 "cpu": "256",
 "memory": "512",
 "runtimePlatform": {
        "operatingSystemFamily": "LINUX",
        "cpuArchitecture": "ARM64"
  },
 "executionRoleArn": "arn:aws:iam::123456789012:role/ecsTaskExecutionRole"
}
```

Amazon ECS ログを CloudWatch に送信する

タスクのコンテナを設定して CloudWatch Logs にログ情報を送信できます。タスクで Fargate 起動タイプを使用すると、コンテナからログを表示できます。EC2 起動タイプを使用すると、コンテナからの異なるログを 1 か所で便利に表示できます。また、コンテナインスタンスのディスク容量をコンテナログが占有してしまうことも防止できます。

> **Note**
>
> タスクのコンテナによってログ記録される情報のタイプは、ENTRYPOINT コマンドによって大きく異なります。デフォルトでは、キャプチャされるログには、コンテナをローカルに実行した場合に通常はインタラクティブターミナルに表示されるコマンド出力 (STDOUT および STDERR I/O ストリーム) が表示されます。awslogs ログドライバーは、これらのログを Docker から CloudWatch Logs に渡します。Docker ログの処理方法 (ファイルデータやストリームをキャプチャする別の方法) の詳細については、Docker ドキュメントのコンテナまたはサービスのログを表示するを参照してください。

your Amazon ECS コンテナインスタンスから CloudWatch Logs にシステムログを送信するには、Amazon CloudWatch Logs ユーザーガイドの「ログファイルをモニタリングする」と「CloudWatch Logs クォータ」を参照してください。

Fargate 起動タイプ

タスクで Fargate 起動タイプを使用する場合、awslogs ログドライバーを有効化するには、必要な logConfiguration パラメータをタスク定義に追加する必要があります。詳細については、「Amazon ECS タスク定義の例: CloudWatch にログをルーティングする」を参照してください。

Fargate の Windows コンテナでは、タスク定義パラメータに & \ < > ^ | などの特殊文字が含まれている場合は、次のいずれかのオプションを実行します。

- パラメータ文字列全体を二重引用符で囲んだエスケープ (\) を追加する

  例

  ```
  "awslogs-multiline-pattern": "\"^[|DEBUG|INFO|WARNING|ERROR\"",
  ```

- 各特殊文字の周囲にエスケープ (^) 文字を追加する

  例

  ```
  "awslogs-multiline-pattern": "^^[^|DEBUG^|INFO^|WARNING^|ERROR",
  ```

EC2 起動タイプ

タスクで EC2 起動タイプを使用する場合、awslogs ログドライバーをオンにするには、Amazon ECS コンテナインスタンスに、コンテナエージェントのバージョン 1.9.0 以降が必要です。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

> **Note**
>
> Amazon ECS に最適化された AMI か、もしくは少なくともバージョン 1.9.0-1 の ecs-init パッケージを含むカスタム AMI を使用する必要があります。カスタム AMI を使用する場合、docker run ステートメント内で以下の環境変数を使用するか、または環境変数ファイルを使用することにより、エージェントの起動時に Amazon EC2 インスタンス上で awslogs ロギングドライバーが使用可能となることを指定する必要があります。
>
> ```
> ECS_AVAILABLE_LOGGING_DRIVERS=["json-file","awslogs"]
> ```

Amazon ECS コンテナインスタンスでは、コンテナインスタンスで起動する IAM ロールに logs:CreateLogStream および logs:PutLogEvents アクセス許可も必要になります。Amazon ECS で awslogs ログドライバーのサポートを有効にする前に Amazon ECS コンテナインスタンスを作成した場合は、このアクセス許可の追加が必要となる場合があります。ecsTaskExecutionRole はタスクに割り当てられた時点で使用され、また、正しいアクセス許可が含まれている必要があります。タスクの実行ロールの詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。コンテナインスタンスでコンテナインスタンス用の管理 IAM ポリシーを使用している場合、通常そのコンテナインスタンスには、適切なアクセス許可が付

与されています。コンテナインスタンスのマネージド IAM ポリシーについては、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

Amazon ECS タスク定義の例: CloudWatch にログをルーティングする

コンテナがログを CloudWatch に送信する前に、タスク定義でコンテナの awslogs ログドライバーを指定する必要があります。ログパラメータの詳細については、「ストレージとログ記録」を参照してください

下にあるタスク定義 JSON には、各コンテナに指定された logConfiguration オブジェクトが含まれています。その 1 つは、awslogs-wordpress というロググループにログを送信する WordPress コンテナ用です。もう 1 つは、awslogs-mysql というロググループにログを送信する MySQL コンテナ用です。どちらのコンテナも awslogs-example ログストリームプレフィックスを使用します。

```
{
    "containerDefinitions": [
        {
            "name": "wordpress",
            "links": [
                "mysql"
            ],
            "image": "public.ecr.aws/docker/library/wordpress:latest",
            "essential": true,
            "portMappings": [
                {
                    "containerPort": 80,
                    "hostPort": 80
                }
            ],
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-create-group": "true",
                    "awslogs-group": "awslogs-wordpress",
                    "awslogs-region": "us-west-2",
                    "awslogs-stream-prefix": "awslogs-example"
                }
            },
            "memory": 500,
            "cpu": 10
        },
```

```
        {
            "environment": [
                {
                    "name": "MYSQL_ROOT_PASSWORD",
                    "value": "password"
                }
            ],
            "name": "mysql",
            "image": "public.ecr.aws/docker/library/mysql:latest",
            "cpu": 10,
            "memory": 500,
            "essential": true,
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-create-group": "true",
                    "awslogs-group": "awslogs-mysql",
                    "awslogs-region": "us-west-2",
                    "awslogs-stream-prefix": "awslogs-example",
                    "mode": "non-blocking",
                    "max-buffer-size": "25m"
                }
            }
        }
    ],
    "family": "awslogs-example"
}
```

次のステップ

- CloudWatch AWS CLI または API を使用してロググループの保持ポリシーを設定できます (オプション)。詳細については、AWS Command Line Interface コマンドリファレンスの「put-retention-policy」を参照してください。
- awslogs ログドライバーを使用するタスク定義をコンテナ定義ログ設定に登録すると、タスク定義を使用してタスクを実行またはサービスを作成し、CloudWatch Logs へのログの送信を開始できます。詳細については、Amazon ECS タスクとしてのアプリケーションの実行およびコンソールを使用した Amazon ECS サービスの作成を参照してください。

Amazon ECS ログを AWS サービスまたは AWS Partner に送信する

FireLens for Amazon ECS では、タスク定義パラメータを使用してログを AWS サービスや AWS Partner Network (APN) の宛先にルーティングし、ログを保存および分析できます。AWS Partner Network は、プログラム、専門知識、リソースを活用して顧客向けサービスの構築、マーケティング、販売を行うパートナーのグローバルコミュニティです。詳細については、「AWS Partner」を参照してください。FireLens は Fluentd および Fluent Bit と連携しています。Fluent Bit イメージ用に AWS を提供していますが、Fluentd や Fluent Bit のイメージはご用意いただいたものを使用することもできます。

デフォルトでは、Amazon ECS は、Firelens コンテナを使用するコンテナより前に Firelens コンテナを起動するようにコンテナの依存関係を設定します。また Firelens コンテナは、それを使用するすべてのコンテナが停止した後で停止します。

FireLens for Amazon ECS を使用する際は、以下の点を考慮してください。

- コンソール上でコンテナ名を簡単に区別できるよう、`my_service_` をログコンテナ名に追加することをおすすめします。
- Amazon ECS はデフォルトで、アプリケーションコンテナと FireLens コンテナの間に開始コンテナ順序依存関係を追加します。アプリケーションコンテナと FireLens コンテナ間でコンテナ順序を指定すると、デフォルトの開始コンテナ順序が上書きされます。
- FireLens for Amazon ECS は、Linux の AWS Fargate と Linux の Amazon EC2 の両方でホストされたタスクでサポートされます。Windows コンテナは FireLens をサポートしていません。

  Windows コンテナの集中ロギングを設定する方法については、「Centralized logging for Windows containers on Amazon ECS using Fluent Bit」(Fluent Bit を使用した Amazon ECS での Windows コンテナの集中ロギング) を参照してください。
- Amazon ECS の FireLens は、AWS CloudFormation テンプレートを使用して設定できます。詳細については、AWS CloudFormation ユーザーガイドの「AWS::ECS::TaskDefinition FirelensConfiguration」を参照してください。
- FireLens はポート `24224` でリッスンするため、FireLens ログルーターがタスク外に到達できないようにするには、タスクが使用するセキュリティグループでポート `24224` でのインバウンドトラフィックを許可してはなりません。`awsvpc` ネットワークモードを使用するタスクの場合、これは、そのタスクに関連付けられたセキュリティグループです。`host` ネットワークモードを使用するタスクでは、そのタスクをホストする Amazon EC2 インスタンスに関連付けられているセキュリティグループです。`bridge` ネットワークモードを使用するタスクの場合、ポート `24224` を使用するポートマッピングを作成しないでください。

- bridge ネットワークモードを使用するタスクの場合、FireLens 設定のコンテナは、それに依存するアプリケーションコンテナが開始する前に開始する必要があります。コンテナの開始順序を制御するには、タスク定義の依存関係条件を使用します。詳細については、「コンテナの依存関係」を参照してください。

  > **Note**
  >
  > FireLens 設定のコンテナ定義で依存関係条件パラメータを使用する場合は、各コンテナに START または HEALTHY 条件要件があることを確認してください。

- デフォルトでは、FireLens はクラスターとタスクの定義名、およびクラスターの Amazon リソースネーム (ARN) をメタデータキーとして stdout/stderr コンテナログに追加します。メタデータ形式の例を次に示します。

  ```
  "ecs_cluster": "cluster-name",
  "ecs_task_arn": "arn:aws:ecs:region:111122223333:task/cluster-
  name/f2ad7dba413f45ddb4EXAMPLE",
  "ecs_task_definition": "task-def-name:revision",
  ```

  ログにメタデータを含めたくない場合は、タスク定義の「firelensConfiguration」セクションで enable-ecs-log-metadata を false に設定します。

  ```
  "firelensConfiguration":{
     "type":"fluentbit",
     "options":{
        "enable-ecs-log-metadata":"false",
        "config-file-type":"file",
        "config-file-value":"/extra.conf"
  }
  ```

この機能を使用するには、タスク用の IAM ロールを作成し、AWS のサービスを使用するために必要なアクセス許可をタスクに付与する必要があります。例えば、コンテナから Firehose にログをルーティングする場合、タスクには firehose:PutRecordBatch API を呼び出すためのアクセス許可が必要です。詳細については、IAM ユーザーガイドの「IAM ID アクセス許可の追加と削除」を参照してください。

以下の場合は、タスクに Amazon ECS タスク実行ロールが必要になることもあります。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

- タスクが Fargate でホストされていて、Amazon ECR からコンテナイメージをプルしたり、ログ設定で AWS Secrets Manager の機密データを参照したりする場合は、タスク実行 IAM ロールを含める必要があります。
- Amazon S3 でホストされているカスタム設定ファイルを使用する場合は、タスク実行 IAM ロールに `s3:GetObject` アクセス許可が含まれている必要があります。

Amazon S3 でホストするファイルや Amazon S3 内のファイルなど、Amazon ECS で複数の設定ファイルを使用する方法については、「Init process for Fluent Bit on ECS, multi-config support」を参照してください。

高スループットの Amazon ECS ログの設定

タスク定義を作成する際は、値 (`log-driver-buffer-limit`) を指定することで、メモリにバッファリングされるログの行数を指定できます。詳細については、Docker ドキュメントの「Fluentd ロギングドライバー」を参照してください。

このオプションは、スループットが高いために Docker がバッファメモリを使い果たし、新しいメッセージを追加するためにバッファメッセージを破棄する可能性がある場合に使用します。

バッファ制限オプションを指定して FireLens for Amazon ECS を使用する場合は、以下の点を考慮してください。

- このオプションは、Amazon EC2 起動タイプおよび プラットフォームバージョン `1.4.0` 以降の Fargate 起動タイプでサポートされています。
- このオプションは、`logDriver` が `awsfirelens` に設定されている場合にのみ有効です。
- デフォルトのバッファ制限は `1048576` (ログの行数) です。
- バッファ制限は、`0` ログ行以上、`536870912` ログ行未満である必要があります。
- このバッファに使用されるメモリの最大量は、各ログ行のサイズとバッファのサイズ積です。例えば、アプリケーションのログ行が平均 2 KiB の場合、4096 のバッファ制限では最大 8 MiB を使用します。タスクレベルで割り当てられるメモリの合計量は、ログドライバーのメモリバッファに加えて、すべてのコンテナに割り当てられたメモリ量よりも大きくなければなりません。

`awsfirelens` ログドライバーがタスク定義で指定されている場合、Amazon ECS コンテナエージェントは次の環境変数をコンテナに挿入します。

`FLUENT_HOST`

FireLens コンテナに割り当てられた IP アドレス。

> **Note**
>
> bridge ネットワークモードの EC2 起動タイプを使用している場合、FireLens ログルーターコンテナ (コンテナ定義に firelensConfiguration オブジェクトがあるコンテナ) を再起動した後で、アプリケーションコンテナの FLUENT_HOST 環境変数が不正確になる可能性があります。これは、FLUENT_HOST が動的 IP アドレスであり、再起動後に変更される場合があるためです。アプリケーションコンテナから FLUENT_HOST IP アドレスへの直接的なロギングは、アドレスの変更後に失敗することがあります。個々のコンテナの再起動に関する詳細については、「コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する」を参照してください。

FLUENT_PORT

Fluent Forward プロトコルがリッスンしているポート。

FLUENT_HOST 環境変数および FLUENT_PORT 環境変数を使用すると、stdout を介することなく、コードからログルーターに直接ログを記録できます。詳細については、GitHub の「fluent-logger-golang」 を参照してください。

以下に、log-driver-buffer-limit を指定するための構文を示します。my_service_ をユーザー自身のサービス名に置き換えます。

```
{
    "containerDefinitions": [
        {
            "name": "my_service_log_router",
            "image": "public.ecr.aws/aws-observability/aws-for-fluent-bit:stable",
            "cpu": 0,
            "memoryReservation": 51,
            "portMappings": [],
            "essential": true,
            "environment": [],
            "mountPoints": [],
            "volumesFrom": [],
            "user": "0",
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-group": "/ecs/ecs-aws-firelens-sidecar-container",
```

```
                    "mode": "non-blocking",
                    "awslogs-create-group": "true",
                    "max-buffer-size": "25m",
                    "awslogs-region": "us-east-1",
                    "awslogs-stream-prefix": "firelens"
                },
                "secretOptions": []
            },
            "systemControls": [],
            "firelensConfiguration": {
                "type": "fluentbit"
            }
        },
        {
            "essential": true,
            "image": "public.ecr.aws/docker/library/httpd:latest",
            "name": "app",
            "logConfiguration": {
                "logDriver": "awsfirelens",
                "options": {
                    "Name": "firehose",
                    "region": "us-west-2",
                    "delivery_stream": "my-stream",
                    "log-driver-buffer-limit": "51200"
                }
            },
            "dependsOn": [
                {
                    "containerName": "log_router",
                    "condition": "START"
                }
            ],
            "memoryReservation": 100
        }
    ]
}
```

Amazon ECS の Fluent Bit イメージリポジトリの AWS

AWS は、CloudWatch Logs と Firehose の両方のプラグインに Fluent Bit イメージを提供します。Fluent Bit は、リソース使用率が Fluentd よりも低いため、ログルーターとして使用することをお勧めします。詳細については、「CloudWatch Logs for Fluent Bit」および「Amazon Kinesis Firehose for Fluent Bit」を参照してください。

AWS for Fluent Bit イメージは、高可用性を実現するために、ほとんどの AWS リージョンで、Amazon ECR Public Gallery と Amazon ECR リポジトリの両方の Amazon ECR で利用が可能です。

Amazon ECR Public Gallery

AWS for Fluent Bit イメージは Amazon ECR Public Gallery で利用できます。これはパブリックリポジトリであり、すべての AWS リージョン リージョンから使用できるため、AWS for Fluent Bit イメージのダウンロード先として推奨されます 詳細については、Amazon ECR Public Gallery の「AWS for Fluent Bit」を参照してください。

リナックス

Amazon ECR Public Gallery の AWS for Fluent Bit イメージは、ARM 64 または x86-64 アーキテクチャの Amazon Linux オペレーティングシステムをサポートしています。

目的のイメージタグを使用してリポジトリ URL を指定することにより、Amazon ECR Public Gallery からAWS for Fluent Bit イメージをプルできます。利用可能な画像タグは、Amazon ECR Public Gallery の [Image tags (画像タグ)] タブにあります。

Docker CLI で使用する構文を以下に示します。

```
docker pull public.ecr.aws/aws-observability/aws-for-fluent-bit:tag
```

例えば、次の Docker CLI コマンドを使用して、AWS for Fluent Bit イメージの最新安定版をプルできます。

```
docker pull public.ecr.aws/aws-observability/aws-for-fluent-bit:stable
```

> **Note**
>
> 認証されていないプルは許可されますが、認証されたプルよりもレート制限が低くなります。プルする前に、次のコマンドを使用して AWS アカウントの使用を認証します。
>
> ```
> aws ecr-public get-login-password --region us-east-1 | docker login --username
>  AWS --password-stdin public.ecr.aws
> ```

Windows

Amazon ECR Public Gallery の AWS for Fluent Bit イメージは、次のオペレーティングシステムを備えた AMD64 アーキテクチャをサポートしています。

- Windows Server 2022 Full
- Windows Server 2022 Core
- Windows Server 2019 Full
- Windows Server 2019 Core

AWS Fargate の Windows コンテナは FireLens をサポートしません。

目的のイメージタグを使用してリポジトリ URL を指定することにより、Amazon ECR Public Gallery からAWS for Fluent Bit イメージをプルできます。利用可能な画像タグは、Amazon ECR Public Gallery の [Image tags (画像タグ)] タブにあります。

Docker CLI で使用する構文を以下に示します。

```
docker pull public.ecr.aws/aws-observability/aws-for-fluent-bit:tag
```

例えば、次の Docker CLI コマンドを使用して、AWS for Fluent Bit イメージの最新安定版をプルできます。

```
docker pull public.ecr.aws/aws-observability/aws-for-fluent-bit:windowsservercore-
stable
```

> **Note**
>
> 認証されていないプルは許可されますが、認証されたプルよりもレート制限が低くなります。プルする前に、次のコマンドを使用して AWS アカウントの使用を認証します。
>
> ```
> aws ecr-public get-login-password --region us-east-1 | docker login --username
>  AWS --password-stdin public.ecr.aws
> ```

Amazon ECR

AWS for Fluent Bit イメージは、Amazon ECR で高可用性を活用できます。これらのイメージは、AWS GovCloud (US) を含むほとんどの AWS リージョン で利用できます。

リナックス

最新の安定している AWS for Fluent Bit イメージの URI は、次のコマンドを使用して取得できます。

```
aws ssm get-parameters \
      --names /aws/service/aws-for-fluent-bit/stable \
      --region us-east-1
```

次のコマンドを使用して Systems Manager パラメータストアのパラメータをクエリすると、AWS for Fluent Bit イメージのすべてのバージョンを一覧表示できます。

```
aws ssm get-parameters-by-path \
      --path /aws/service/aws-for-fluent-bit \
      --region us-east-1
```

AWS for Fluent Bit イメージの最新安定版は、Systems Manager パラメータストア名を参照することにより、AWS CloudFormation テンプレート内に見つかります。次にの例を示します。

```
Parameters:
  FireLensImage:
    Description: Fluent Bit image for the FireLens Container
    Type: AWS::SSM::Parameter::Value<String>
    Default: /aws/service/aws-for-fluent-bit/stable
```

Windows

最新の安定している AWS for Fluent Bit イメージの URI は、次のコマンドを使用して取得できます。

```
aws ssm get-parameters \
      --names /aws/service/aws-for-fluent-bit/windowsservercore-stable \
      --region us-east-1
```

次のコマンドを使用して Systems Manager パラメータストアのパラメータをクエリすると、AWS for Fluent Bit イメージのすべてのバージョンを一覧表示できます。

```
aws ssm get-parameters-by-path \
      --path /aws/service/aws-for-fluent-bit/windowsservercore \
      --region us-east-1
```

最新の安定している AWS for Fluent Bit イメージは、Systems Manager パラメータストア名を参照することにより、AWS CloudFormation テンプレートで参照できます。次にの例を示します。

```
Parameters:
  FireLensImage:
    Description: Fluent Bit image for the FireLens Container
    Type: AWS::SSM::Parameter::Value<String>
    Default: /aws/service/aws-for-fluent-bit/windowsservercore-stable
```

Amazon ECS タスク定義の例: FireLens にログをルーティングする

FireLens でカスタムログルーティングを使用するには、タスク定義で以下を指定する必要があります。

- FireLens 設定を含むログルーターコンテナ。コンテナは `essential` とマークすることが推奨されます。
- `awsfirelens` ログドライバーを指定するログ設定を含む 1 つ以上のアプリケーションコンテナ。
- タスクでログをルーティングするために必要なアクセス許可を含むタスク IAM ロールの、Amazon リソースネーム (ARN)。

AWS Management Console を使用して新しいタスク定義を作成する場合、ログルーターコンテナを簡単に追加できる FireLens 統合セクションがあります。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

Amazon ECS はログ設定を変換し、Fluentd または Fluent Bit 出力設定を生成します。出力設定は、`/fluent-bit/etc/fluent-bit.conf` (Fluent Bit) および `/fluentd/etc/fluent.conf` (Fluentd) のログルーティングコンテナにマウントされます。

> **Important**
>
> FireLens は、ポート 24224 でリッスンします。したがって、FireLens ログルーターがタスクの外に到達できないようにするには、タスクが使用するセキュリティグループで、ポート 24224 での入力トラフィックを許可してはなりません。`awsvpc` ネットワークモードを使用する場合、このセキュリティグループは、タスクに関連付けられたセキュリティグループで

す。host ネットワークモードを使用する場合、これはタスクをホストする Amazon EC2 インスタンスに関連付けられているセキュリティグループです。bridge ネットワークモードを使用するタスクの場合、ポート 24224 を使用するポートマッピングを作成しないでください。

デフォルトでは、Amazon ECS は、ログのソースを識別するのに役立つ追加のフィールドをログエントリに追加します。

- ecs_cluster - タスクが所属するクラスターの名前。
- ecs_task_arn – コンテナが属しているタスクの完全な Amazon リソースネーム (ARN)。
- ecs_task_definition - タスクが使用しているタスク定義名とリビジョン。
- ec2_instance_id - コンテナがホストされている Amazon EC2 インスタンス ID。このフィールドは、EC2 起動タイプを使用するタスクでのみ有効です。

メタデータが必要ない場合は、enable-ecs-log-metadata を false に設定できます。

以下のタスク定義の例では、Fluent Bit を使用してログを CloudWatch Logs にルーティングするログルーターコンテナを定義しています。また、これによりアプリケーションコンテナを定義します。このコンテナでは、ログ設定を使用してログを Amazon Data Firehose にルーティングし、イベントのバッファリングに使用されるメモリを 2MiB に設定します。

> **Note**
>
> タスク定義のその他の例については、GitHub の Amazon ECS FireLens の例を参照してください。

```
{
  "family": "firelens-example-firehose",
  "taskRoleArn": "arn:aws:iam::123456789012:role/ecs_task_iam_role",
  "containerDefinitions": [
    {
            "name": "log_router",
            "image": "public.ecr.aws/aws-observability/aws-for-fluent-bit:stable",
            "cpu": 0,
            "memoryReservation": 51,
            "portMappings": [],
```

```
            "essential": true,
            "environment": [],
            "mountPoints": [],
            "volumesFrom": [],
            "user": "0",
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-group": "/ecs/ecs-aws-firelens-sidecar-container",
                    "mode": "non-blocking",
                    "awslogs-create-group": "true",
                    "max-buffer-size": "25m",
                    "awslogs-region": "us-east-1",
                    "awslogs-stream-prefix": "firelens"
                },
                "secretOptions": []
            },
            "systemControls": [],
            "firelensConfiguration": {
                "type": "fluentbit"
            }
        },
    {
      "essential": true,
      "image": "public.ecr.aws/docker/library/httpd:latest",
      "name": "app",
      "logConfiguration": {
        "logDriver": "awsfirelens",
        "options": {
          "Name": "firehose",
          "region": "us-west-2",
          "delivery_stream": "my-stream",
          "log-driver-buffer-limit": "2097152"
        }
      },
      "memoryReservation": 100
    }
  ]
}
```

logConfiguration オブジェクトのオプションとして指定されたキーバリューペアは、Fluentd または Fluent Bit 出力設定の生成に使用されます。Fluent Bit 出力定義のコード例は次のとおりです。

```
[OUTPUT]
    Name   firehose
    Match  app-firelens*
    region us-west-2
    delivery_stream my-stream
```

> **Note**
>
> FireLens は `match` 設定を管理します。タスク定義では `match` 設定を指定しません。

カスタム設定ファイルを使用する

カスタム設定ファイルを指定できます。設定ファイルの形式は、使用しているログルーターでネイティブな形式を使用します。詳細については、「Fluentd 設定ファイルの構文」および「YAML 設定」を参照してください。

カスタム設定ファイルでは、`bridge` または `awsvpc` ネットワークモードを使用するタスクについて、TCP 経由で Fluentd または Fluent Bit の転送入力を設定しないでください。入力設定は FireLens により追加されています。

カスタム設定ファイルを指定するには、FireLens 設定に次のオプションを含める必要があります。

`config-file-type`

カスタム設定ファイルのソースの場所。使用できるオプションは、`s3` または `file` です。

> **Note**
>
> AWS Fargate でホストされるタスクは、`file` 設定ファイルタイプのみをサポートします。

`config-file-value`

カスタム設定ファイルのソース。`s3` 設定ファイルタイプを使用する場合、設定ファイルの値は Amazon S3 バケットとファイルの完全な ARN です。`file` 設定ファイルタイプを使用する場合、設定ファイルのこの値は、コンテナイメージ内、またはそのコンテナにマウントされているボリューム上に存在する設定ファイルへの完全パスです。

> **Important**
>
> カスタム設定ファイルを使用する場合、FireLens が使用するパスとは異なるパスを指定する必要があります。Amazon ECS は Fluent Bit に `/fluent-bit/etc/fluent-bit.conf` ファイルパスと Fluentd に `/fluentd/etc/fluent.conf` を指定します。

次の例は、カスタム設定を指定するときに必要な構文を示しています。

> **Important**
>
> Amazon S3 でホストされるカスタム設定ファイルを指定するには、適切なアクセス許可を持つタスク実行 IAM ロールが作成されている必要があります。

次に、カスタム設定を指定する際に必要な構文を示します。

```
{
  "containerDefinitions": [
    {
      "essential": true,
      "image": "906394416424.dkr.ecr.us-west-2.amazonaws.com/aws-for-fluent-
bit:stable",
      "name": "log_router",
      "firelensConfiguration": {
        "type": "fluentbit",
        "options": {
          "config-file-type": "s3 | file",
          "config-file-value": "arn:aws:s3:::amzn-s3-demo-bucket/fluent.conf
 | filepath"
        }
      }
    }
  ]
}
```

> **Note**
>
> AWS Fargate でホストされるタスクは、`file` 設定ファイルタイプのみをサポートします。

Amazon ECS での AWS 以外のコンテナイメージの使用

プライベートレジストリを使用して認証情報を AWS Secrets Manager に保存し、タスク定義内で参照します。これは、タスク定義で認証が必要な AWS の外部にあるプライベートレジストリーに存在するコンテナイメージを参照できます。この機能は、Amazon ECS Anywhere を使用して Fargate、Amazon EC2 インスタンス、および外部インスタンスでホストされるタスクでサポートされています。

> **Important**
>
> タスク定義で、Amazon ECR に保存されたイメージを参照している場合、このトピックは適用されません。詳細については、Amazon Elastic Container Registry ユーザーガイドの「Amazon ECS で Amazon ECR イメージを使用する」を参照してください。

Amazon EC2 インスタンスでホストされるタスクの場合は、この機能のためにコンテナエージェントのバージョン `1.19.0` 以降が必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認方法と最新バージョンへの更新方法については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

Fargate でホストされているタスクの場合、この機能にはプラットフォームバージョン `1.2.0` 以降が必要です。詳細については、Amazon ECS 向け Fargate プラットフォームバージョン を参照してください。

コンテナの定義内で、作成したシークレットの詳細 で `repositoryCredentials` オブジェクトを指定します。参照されるシークレットは、タスクが使用するものと異なる AWS リージョン、または異なるアカウントに置くことができます。

> **Note**
>
> Amazon ECS API、AWS CLI、または AWS SDK を使用しており、起動するタスクと同じ AWS リージョン にシークレットが存在する場合は、シークレットの完全な ARN または名前のどちらも使用可能です。シークレットが別のアカウントに存在する場合は、シークレットの完全な ARN を指定する必要があります。AWS Management Console を使用する場合は、シークレットの完全な ARN を常に指定する必要があります。

必要なパラメータが含まれるタスク定義のスニペットを、以下に示します。

次のパラメータを置き換えます。

- *private-repo* をプライベートリポジトリのホスト名に
- *private-image* をイメージ名に
- *arn:aws:secretsmanager:region:aws_account_id:secret:secret_name* をシークレット Amazon リソースネーム (ARN) に

```
"containerDefinitions": [
    {
        "image": "private-repo/private-image",
        "repositoryCredentials": {
            "credentialsParameter":
 "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name"
        }
    }
]
```

> **Note**
>
> プライベートレジストリ認証を有効にするもうひとつの方法として、Amazon ECS コンテナエージェントの環境変数を使用してプライベートレジストリを認証する方法があります。このメソッドは、Amazon EC2 インスタンスでホストされるタスクでのみサポートされています。詳細については、「プライベート Docker イメージ用の Amazon ECS コンテナインスタンスを設定する 」を参照してください。

プライベートレジストリを使用するには

1. タスク定義にはタスク実行ロールが必要です。このロールを使用して、コンテナエージェントでコンテナイメージをプルできます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

   作成したシークレットにアクセスできるようにするには、以下のアクセス許可を、インラインポリシーとしてタスクの実行ロール追加します。詳細については、「IAM ポリシーの追加と削除」を参照してください。

   - `secretsmanager:GetSecretValue`

- `kms:Decrypt` - カスタムの KMS キーを使用するが、デフォルトのキーは使用しない場合にのみ必須。カスタムキーの Amazon リソースネーム (ARN) は、リソースとして追加する必要があります。

次の例では、インラインポリシーによりアクセス許可を追加しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [

 "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
                "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
            ]
        }
    ]
}
```

2. プライベートレジストリ認証情報のシークレットを作成するには、AWS Secrets Manager を使用します。シークレットの作成方法の詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットを作成する」を参照してください。

   以下の形式でプライベートレジストリの認証情報を入力します。

```
{
  "username" : "privateRegistryUsername",
  "password" : "privateRegistryPassword"
}
```

3. タスク定義を登録する 詳細については、「the section called “コンソールを使用したタスク定義の作成”」を参照してください。

コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する

タスク定義で定義されている必須のコンテナと必須ではないコンテナそれぞれに再起動ポリシーを有効にして、一時的な障害をより迅速に克服し、タスクの可用性を維持することができます。コンテナの再起動ポリシーを有効にすると、コンテナが終了した場合、Amazon ECS はタスクを置き換えることなくコンテナを再起動できます。

再起動ポリシーは、デフォルトではコンテナに対して有効になっていません。コンテナの再起動ポリシーを有効にすると、コンテナを再起動しない終了コードを指定できます。これらは、終了コード `0` のように再起動を必要としない成功を示す終了コードである可能性があります。再起動を試みる前に、コンテナが正常に実行する必要のある時間を指定することもできます。これらのパラメータの詳細については、「再起動ポリシー」を参照してください。これらの値を指定するタスク定義の例については、「Amazon ECS タスク定義でコンテナ再起動ポリシーを指定する」を参照してください。

Amazon ECS タスクメタデータエンドポイントまたは CloudWatch Container Insights を使用して、コンテナが再起動した回数をモニタリングできます。タスクメタデータエンドポイントの詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」および「Fargate のタスク用の Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。Amazon ECS Container Insights メトリクスの一覧については、「Amazon CloudWatch ユーザーガイド」の「Amazon ECS Container Insights メトリクス」を参照してください。

コンテナ再起動ポリシーは、Fargate、Amazon EC2 インスタンスに加えて、Amazon ECS Anywhere を使用する外部インスタンスでホストされるタスクでサポートされています。

考慮事項

コンテナの再起動ポリシーを有効にする前に、次の点を考慮してください。

- Fargate の Windows コンテナでは、再起動ポリシーはサポートされません。
- Amazon EC2 インスタンスでホストされるタスクの場合は、この機能のためにコンテナエージェントのバージョン `1.86.0` 以降が必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認方法と最新バージョンへの更新方法については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。
- Fargate でホストされているタスクの場合、この機能にはプラットフォームバージョン `1.4.0` 以降が必要です。詳細については、Amazon ECS 向け Fargate プラットフォームバージョン を参照してください。

- bridge ネットワークモードの EC2 起動タイプを使用している場合、FireLens ログルーターコンテナ (コンテナ定義に firelensConfiguration オブジェクトがあるコンテナ) を再起動した後で、アプリケーションコンテナの FLUENT_HOST 環境変数が不正確になる可能性があります。これは、FLUENT_HOST が動的 IP アドレスであり、再起動後に変更される場合があるためです。アプリケーションコンテナから FLUENT_HOST IP アドレスへの直接的なロギングは、アドレスの変更後に失敗することがあります。FLUENT_HOST の詳細については、「高スループットの Amazon ECS ログの設定」を参照してください。
- Amazon ECS エージェントは、コンテナの再起動ポリシーを処理します。予期しない理由で Amazon ECS エージェントが失敗するか実行されなくなったりすると、コンテナは再起動されません。
- ポリシーで定義された再起動試行期間は、Amazon ECS がコンテナを再起動するまでにコンテナが実行される必要のある期間 (秒単位) を決定します。

Amazon ECS タスク定義でコンテナ再起動ポリシーを指定する

タスク定義でコンテナの再起動ポリシーを指定するには、コンテナ定義内で restartPolicy オブジェクトを指定します。restartPolicy オブジェクトの詳細については、「再起動ポリシー」を参照してください。

以下は、Web サーバーをセットアップするために、Fargate 起動タイプで Linux コンテナを使用するタスク定義です。コンテナ定義には、コンテナの再起動ポリシーを有効にするために enabled が true に設定された restartPolicy オブジェクトが含まれています。コンテナは再起動する前に 180 秒間実行する必要があります。成功を示す終了コード 0 で終了した場合、コンテナは再起動しません。

```
{
  "containerDefinitions": [
    {
      "command": [
        "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample App</title>
 <style>body {margin-top: 40px; background-color: #333;} </style> </head><body>
 <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
 <h2>Congratulations!</h2> <p>Your application is now running on a container in Amazon
 ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html && httpd-
foreground\""
      ],
      "entryPoint": ["sh", "-c"],
      "essential": true,
      "image": "public.ecr.aws/docker/library/httpd:2.4",
```

```
      "logConfiguration": {
        "logDriver": "awslogs",
        "options": {
          "awslogs-group": "/ecs/fargate-task-definition",
          "awslogs-region": "us-east-1",
          "awslogs-stream-prefix": "ecs"
        }
      },
      "name": "sample-fargate-app",
      "portMappings": [
        {
          "containerPort": 80,
          "hostPort": 80,
          "protocol": "tcp"
        }
      ],
      "restartPolicy": {
        "enabled": true,
        "ignoredExitCodes": [0],
        "restartAttemptPeriod": 180
      }
    }
  ],
  "cpu": "256",
  "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
  "family": "fargate-task-definition",
  "memory": "512",
  "networkMode": "awsvpc",
  "runtimePlatform": {
    "operatingSystemFamily": "LINUX"
  },
  "requiresCompatibilities": ["FARGATE"]
}
```

コンテナ定義で `restartPolicy` オブジェクトを含むタスク定義を登録した後、そのタスク定義でタスクを実行するか、サービスを作成することができます。詳細については、Amazon ECS タスクとしてのアプリケーションの実行およびコンソールを使用した Amazon ECS サービスの作成を参照してください。

Amazon ECS コンテナに機密データを渡す

認証情報などの機密データを、コンテナ内のデータベースなどに安全に渡すことができます。

API キーやデータベース認証情報などのシークレットは、アプリケーションが他のシステムにアクセスするためによく使用されます。多くの場合、ユーザー名とパスワード、証明書、または API キーで構成されます。これらのシークレットへのアクセスは、IAM を使用する特定の IAM プリンシパルに限定され、またランタイムにコンテナに挿入される必要があります。

シークレットは、AWS Secrets Manager または Amazon EC2 Systems Manager Parameter Store からコンテナにシームレスに挿入できます。これらのシークレットは、タスク内で以下のいずれかとして参照できます。

1. `secrets` コンテナ定義パラメータを使用する環境変数として参照されます。
2. ロギングプラットフォームが認証を必要とする場合、`secretOptions` として参照されます。詳細については、「ログの設定オプション」を参照してください。
3. コンテナの取得元のレジストリーが認証を必要とする場合、これらは、`repositoryCredentials` コンテナ定義パラメータを使用するイメージによって取得されるシークレットとして参照されます。Amazon ECR Public Gallery からイメージを取得するときは、この方法を使用してください。詳細については、「タスクのプライベートレジストリの認証」を参照してください。

シークレットの管理を設定するときは、次を行うことをお勧めします。

シークレットマテリアルの保存に AWS Secrets Manager または AWS Systems Manager Parameter Store を使用する

API キー、データベース認証情報、およびその他のシークレットマテリアルは、Secrets Manager または暗号化されたパラメータとして Systems Manager Parameter Store に安全に保存する必要があります。これらのサービスは、どちらも AWS KMS を使用して機密データを暗号化する管理されたキー値ストアである点で似ています。ただし、Secrets Manager には、シークレットを自動的にローテーションし、ランダムなシークレットを生成し、アカウント間でシークレットを共有する機能も含まれています。これらの重要な機能がある場合は Secrets Manager を使用し、それ以外の場合は暗号化されたパラメータを使用してください。

> **Important**
>
> シークレットが変更された場合は、新しいデプロイを強制するか、新しいタスクを起動して最新のシークレット値を取得する必要があります。詳細については、以下の各トピックを参照してください。

- タスク - タスクを停止してから開始します。詳細については、Amazon ECS タスクの停止およびAmazon ECS タスクとしてのアプリケーションの実行を参照してください。
- サービス - サービスを更新し、[新しいデプロイの強制] オプションを使用します。詳細については、「コンソールを使用した Amazon ECS サービスの更新」を参照してください。

暗号化された Amazon S3 バケットからデータを取得する

暗号化された Amazon S3 バケットにシークレットを保存し、タスクロールを使用してそのシークレットへのアクセスを制限する必要があります。こうすることで、`docker inspect` の実行時に環境変数の値が誤ってログに漏れて公開されるのを防ぐことができます。これを行う場合、Amazon S3 バケットからシークレットを読み取るようにアプリケーションを作成する必要があります。手順については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。

サイドカーコンテナを使用してシークレットをボリュームにマウントする

環境変数はデータ漏えいのリスクが高いため、AWS Secrets Manager からシークレットを読みとり、共有ボリュームに書き込むサイドカーコンテナを実行する必要があります。このコンテナは、Amazon ECS コンテナの順序付けを使用することでアプリケーションコンテナより先に実行して終了できます。これを行うと、アプリケーションコンテナでシークレットが書き込まれたボリュームが後からマウントされます。Amazon S3 バケットメソッドと同様に、共有ボリュームからシークレットを読み取るようにアプリケーションを作成する必要があります。ボリュームの範囲はタスクに限定されるため、タスクが停止するとボリュームは自動的に削除されます。例については、「secrets-store-csi-driver-provider-aws」プロジェクトを参照してください。

Amazon EC2 では、シークレットが書き込まれるボリュームは、AWS KMS カスタマーマネージドキーで暗号化できます。AWS Fargate では、ボリュームストレージはサービスマネージドキーを使用して自動的に暗号化されます。

個々の環境変数を Amazon ECS コンテナに渡す

> **Important**
>
> 機密データは、AWS Secrets Manager secrets または AWS Systems Manager Parameter Store のパラメータに保存することをお勧めします。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

タスク定義で指定された環境変数は、許可されたすべてのユーザーとロールが、タスク定義の DescribeTaskDefinition アクションを読み取ることができます。

環境変数は、以下の方法でコンテナに渡すことができます。

- environment コンテナ定義パラメータを個別に使用します。これは、docker container run の --env オプションにマッピングされます。
- environmentFiles コンテナ定義パラメータを使用して、環境変数を含む 1 つ以上のファイルを一括で一覧表示します。ファイルは、Amazon S3 でホストされている必要があります。これは、docker run の --env-file オプションにマッピングされます。

以下は、個々の環境変数の指定方法を示すタスク定義のスニペットです。

```
{
    "family": "",
    "containerDefinitions": [
        {
            "name": "",
            "image": "",
            ...
            "environment": [
                {
                    "name": "variable",
                    "value": "value"
                }
            ],
            ...
        }
    ],
    ...
}
```

環境変数を Amazon ECS コンテナに渡す

Important

機密データは、AWS Secrets Manager secrets または AWS Systems Manager Parameter Store のパラメータに保存することをお勧めします。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

環境変数ファイルは Amazon S3 のオブジェクトのため、Amazon S3 のセキュリティに関するすべての考慮事項が適用されます。
Fargate の Windows コンテナと Windows コンテナでは、`environmentFiles` パラメータを使用できません。

環境変数ファイルを作成して Amazon S3 に保存し、環境変数をコンテナに渡すことができます。

ファイルに環境変数を指定することで、環境変数を一括で挿入できます。コンテナ定義内で、環境変数ファイルを含む `environmentFiles` バケットのリストを使用して Amazon S3 オブジェクトを指定します。

Amazon ECS は環境変数にサイズ制限を適用しませんが、環境変数ファイルが大きいとディスク容量が一杯になってしまう可能性があります。環境変数ファイルを使用する各タスクは、ファイルのコピーをディスクにダウンロードします。Amazon ECS は、タスクのクリーンアップの一環としてファイルを削除します。

サポートされている環境変数については、「高度なコンテナ定義パラメータ - 環境」を参照してください。

コンテナ定義で環境変数ファイルを指定する際には、以下の点を考慮してください。

- Amazon EC2 上の Amazon ECS タスクでこの機能を使用するには、コンテナインスタンスにバージョン `1.39.0` 以降のコンテナエージェントが必要です。エージェントのバージョンの確認方法と最新バージョンへの更新方法については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。
- AWS Fargate 上のAmazon ECS タスクでは、この機能を使用するには、タスクでプラットフォームバージョン `1.4.0` 以降 (Linux) を使用する必要があります。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。

  変数がオペレーティングシステムプラットフォームでサポートされていることを確認します。詳細については、the section called “コンテナ定義”およびthe section called “その他のタスク定義パラメータ”を参照してください。
- ファイルには、ファイル拡張子 `.env` と UTF-8 エンコーディングを使用する必要があります。
- タスク実行ロールは、Amazon S3 の追加アクセス許可でこの機能を使用するのに必要です。これにより、コンテナエージェントは Amazon S3 から環境変数ファイルをプルできます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。
- 1 つのタスク定義につき 10 ファイルという制限があります。

- 環境ファイルの各行には、VARIABLE=VALUE 形式で環境変数を含む必要があります。スペースまたは引用符は、Amazon ECS ファイルの値の一部として含まれます。# で始まる行はコメントとして扱われ、無視されます。環境変数ファイルの構文の詳細については、Docker ドキュメントの「Set environment variables (-e, --env, --env-file)」を参照してください。

  次に、適切な構文を示します。

  ```
  #This is a comment and will be ignored
  VARIABLE=VALUE
  ENVIRONMENT=PRODUCTION
  ```

- コンテナ定義に environment パラメータを使用して環境変数が指定されている場合は、環境ファイルに含まれる変数よりも優先されます。
- 同じ変数を含む複数の環境ファイルが指定されている場合、それらのファイルは入力順に処理されます。これは、変数の最初の値が使用され、重複する変数の後続の値は無視されることを意味します。一意の変数名を使用することをお勧めします。
- 環境ファイルがコンテナをオーバーライドするように指定されている場合、そのファイルが適用されます。さらに、コンテナ定義で指定されているその他の環境ファイルは、すべて無視されます。
- Fargate 起動タイプには次のルールが適用されます。
  - このファイルはネイティブの Docker env ファイルと同様に処理されます。
  - 空白で Amazon S3 に保存されている環境変数を参照するコンテナ定義は、コンテナに表示されません。
  - シェルエスケープ処理はサポートされていません。
  - コンテナのエントリポイントが VARIABLE 値を解釈します。

例

以下は、環境変数ファイルの指定方法を示すタスク定義のスニペットを示します。

```
{
    "family": "",
    "containerDefinitions": [
        {
            "name": "",
            "image": "",
            ...
            "environmentFiles": [
                {
```

```
                    "value": "arn:aws:s3:::amzn-s3-demo-
bucket/envfile_object_name.env",
                    "type": "s3"
                }
            ],
            ...
        }
    ],
    ...
}
```

Amazon ECS で Secrets Manager シークレットをプログラムで伝達する

アプリケーション内でプレーンテキストの機密情報をハードコーディングする代わりに、Secrets Manager を使用して機密データを保存することができます。

機密データの取得にはこの方法が推奨されます。これにより、以後、Secrets Manager のシークレットが更新された場合には、アプリケーションが自動的に最新バージョンのシークレットを取得するようになります。

Secrets Manager でシークレットを作成します。Secrets Manager シークレットの作成後、アプリケーションコードを更新して、そのシークレットを取得します。

Secrets Manager で機密データの保護を行う前に、以下の考慮事項を確認してください。

- CreateSecret API の `SecretString` パラメータで作成されたシークレットであるテキストデータを格納するシークレット のみがサポートされます。CreateSecret API の `SecretBinary` パラメータで作成されたシークレットであるバイナリデータを格納するシークレットはサポートされていません。
- セキュリティ制御を強化するために、インターフェイス VPC エンドポイントを使用します。Secrets Manager 用に、インターフェイス VPC エンドポイントを作成する必要があります。VPC エンドポイントの詳細については、「AWS Secrets Manager ユーザーガイド」の「VPC エンドポイントの作成」を参照してください。
- タスクで使用する VPC は、DNS 解決を使用している必要があります。
- タスク定義では、Secrets Manager の追加アクセス許可を持つタスク ロールを使用する必要があります。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

Secrets Manager シークレットを作成する

Secrets Manager コンソールを使用して、機密データ用のシークレットを作成できます。シークレットの作成方法の詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットを作成する」を参照してください。

Secrets Manager シークレットをプログラムにより取得するようにアプリケーションを更新する

アプリケーションから直接 Secrets Manager API を呼び出し、シークレットを取得することができます。詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager からのシークレットの取得」を参照してください。

AWS Secrets Manager に保存されている機密データを取得するには、「AWS SDK コードサンプルコードライブラリ」の「AWS SDK を使用する AWS Secrets Manager のコードサンプル」を参照してください。

Amazon ECS で Systems Manager Parameter Store シークレットをプログラムで伝達する

Systems Manager Parameter Store により、シークレットの安全な保管および管理ができます。パスワード、データベース文字列、EC2 インスタンス ID、AMI ID、ライセンスコードなどのデータをアプリケーションにハードコートする代わりに、パラメータ値として保存できます。値はプレーンテキストまたは暗号化されたデータとして保存できます。

機密データの取得にはこの方法が推奨されます。これにより、以後、Secrets Manager Parameter Store のパラメータが更新された場合にアプリケーションが自動的に最新バージョンを取得するようになります。

Systems Manager Parameter Store で機密データの保護を行う前に、以下の考慮事項を確認してください。

- テキストデータを格納するシークレットのみがサポートされます。バイナリデータを格納するシークレットはサポートされません。
- セキュリティ制御を強化するために、インターフェイス VPC エンドポイントを使用します。
- タスクで使用する VPC は、DNS 解決を使用している必要があります。
- EC2 起動タイプを使用するタスクでは、この機能を使用するのに Amazon ECS エージェント設定変数 `ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE=true` を使用する必要があります。コンテナインスタンスの作成時に `/etc/ecs/ecs.config` ファイルに追加するか、既存のインスタンスに追加して ECS エージェントを再起動できます。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

- タスク定義では、Systems Manager パラメーター ストアに対する追加のアクセス許可を持つタスク ロールを使用する必要があります。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

パラメータを作成する

Systems Manager コンソールを使用すると、機密データ用に Systems Manager Parameter Store のパラメータを作成できます。詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager パラメータを作成する (コンソール)」または「Systems Manager パラメータを作成する (AWS CLI)」を参照してください。

Systems Manager Parameter Store のシークレットをプログラムで取得するようにアプリケーションを更新する

Systems Manager Parameter Store のパラメータに保存されている機密データを取得するには、「AWS SDK コードサンプルコードライブラリ」の「AWS SDK を使用した Systems Manager のコードサンプル」を参照してください。

Amazon ECS 環境変数経由で Secrets Manager シークレットを伝達する

シークレットを環境変数として挿入する場合、シークレットの内容全体、シークレット内の特定の JSON キー、挿入するシークレットの特定のバージョンを指定できます。これは、コンテナに公開される機密データの制御に役立ちます。シークレットのバージョン管理の詳細については、「AWS Secrets Manager ユーザーガイド」の「Secrets Manager シークレットの内容」を参照してください。

環境変数を使用して Secrets Manager シークレットをコンテナに挿入する場合は、以下を考慮する必要があります。

- 重要なデータは、コンテナが最初に開始されたときにコンテナに挿入されます。シークレットを後で更新またはローテーションすると、コンテナには更新された値が自動的に送信されなくなります。この場合は、新しいタスクを起動する必要があります。または、タスクがサービスの一部である場合は、サービスを更新し、[Force new deployment] (新しいデプロイの強制) オプションを使用して、新しいタスクの起動をサービスに強制できます。
- AWS Fargate 上の Amazon ECS タスクでは、以下の点を考慮してください。
  - シークレットの内容全体を環境変数として挿入したり、ログ設定にシークレットを挿入したりするには、プラットフォームバージョン `1.3.0` 以降を使用する必要があります。詳細については、Amazon ECS 向け Fargate プラットフォームバージョン を参照してください。

  - 特定の JSON キーまたはシークレットのバージョンを環境変数または ログ設定に挿入するには、プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` (Windows) を使用する必要があります。詳細については、Amazon ECS 向け Fargate プラットフォームバージョン を参照してください。
- EC2 上の Amazon ECS タスクでは、以下の点を考慮する必要があります。
  - シークレットの特定の JSON キーやバージョンを使用してシークレットを挿入するには、コンテナインスタンスにバージョン `1.37.0` 以降のコンテナエージェントが必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

    シークレットの内容全体を環境変数として挿入したり、ログ設定にシークレットを挿入したりするには、コンテナインスタンスにバージョン `1.22.0` 以降のコンテナエージェントが必要です。
- インターフェイス VPC エンドポイントを使用してセキュリティコントロールを強化し、プライベートサブネットを介して Secrets Manager に接続します。Secrets Manager 用に、インターフェイス VPC エンドポイントを作成する必要があります。VPC エンドポイントの詳細については、「AWS Secrets Manager ユーザーガイド」の「VPC エンドポイントの作成」を参照してください。Secrets Manager と Amazon VPC の使用の詳細については、「How to connect to Secrets Manager service within a Amazon VPC」を参照してください。
- `awslogs` ログドライバーを使用するように設定された Windows タスクの場合は、コンテナインスタンスで `ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE` 環境変数も設定する必要があります。次の構文を使用します。

```
<powershell>
[Environment]::SetEnvironmentVariable("ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE",
 $TRUE, "Machine")
Initialize-ECSAgent -Cluster <cluster name> -EnableTaskIAMRole -LoggingDrivers
 '["json-file","awslogs"]'
</powershell>
```

- タスク定義では、Secrets Manager の追加アクセス許可を持つタスク実行ロールを使用する必要があります。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

AWS Secrets Manager シークレットを作成する

Secrets Manager コンソールを使用して、機密データ用のシークレットを作成できます。詳細については、「AWS Secrets Manager ユーザーガイド」の「AWS Secrets Manager シークレットを作成する」を参照してください。

コンテナ定義に環境変数を追加します。

コンテナの定義内では、以下を指定できます。

- コンテナに設定する環境変数の名前が含まれている `secrets` オブジェクト
- Secrets Manager シークレットの Amazon リソースネーム (ARN)。
- コンテナに渡す機密データが含まれている追加のパラメータ

次の例は、Secrets Manager シークレットに指定する必要がある完全な構文を示しています。

```
arn:aws:secretsmanager:region:aws_account_id:secret:secret-name:json-key:version-stage:version-id
```

次のセクションでは、追加のパラメータについて説明します。追加のパラメータはオプションですが、これらを使用しないでデフォルト値を使用する場合は、コロン : を含める必要があります。以下の例でより詳細なコンテキストを示します。

`json-key`

キーと値のペアのキーの名前を指定します。値は設定する環境変数の値です。JSON 形式の値のみがサポートされます。JSON キーを指定しないと、シークレットの内容全体が使用されます。

`version-stage`

使用するシークレットのバージョンのステージングラベルを指定します。バージョンのステージングラベルを指定した場合、バージョン ID は指定できません。バージョンのステージを指定しないと、デフォルトの動作として、`AWSCURRENT` ステージングラベルのシークレットが取得されます。

ステージングラベルは、シークレットが更新またはローテーションされたときに、シークレットのさまざまなバージョンを追跡するために使用します。シークレットの各バージョンには、1 つ以上のステージングラベルと 1 つの ID があります。詳細については、AWS Secrets Manager ユーザーガイドの「AWS Secrets Managerの主な用語と概念」を参照してください。

`version-id`

使用するシークレットのバージョンの固有 ID を指定します。バージョン ID を指定した場合、バージョンのステージングラベルは指定できません。バージョン ID を指定しないと、デフォルトの動作として、AWSCURRENT ステージングラベルのシークレットが取得されます。

バージョン ID は、シークレットが更新またはローテーションされたときに、シークレットのさまざまなバージョンを追跡するために使用します。シークレットの各バージョンには ID があります。詳細については、AWS Secrets Managerユーザーガイドの「AWS Secrets Managerの主な用語と概念」を参照してください。

コンテナの定義の例

以下の例では、コンテナの定義で Secrets Manager シークレットを参照する方法を示します。

Example シークレット全体を参照する

次に示すのは、Secrets Manager シークレットのテキスト全体を参照するときの形式を示すタスク定義のス二ペットです。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name-
AbCdEf"
    }]
  }]
}
```

コンテナ内から、このシークレットの値にアクセスするには、$environment_variable_name を呼び出します。

Example シークレット内の特定のキーを参照する

次に示すのは、シークレットの内容と、シークレットに関連付けられているバージョンのステージングラベルおよびバージョン ID を表示する get-secret-value コマンドの出力例です。

```
{
    "ARN": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-AbCdEf",
    "Name": "appauthexample",
    "VersionId": "871d9eca-18aa-46a9-8785-981ddEXAMPLE",
```

```
    "SecretString": "{\"username1\":\"password1\",\"username2\":\"password2\",
\"username3\":\"password3\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1581968848.921
}
```

前のコンテナの定義の出力で特定のキーを参照するには、ARN の最後にキー名を指定します。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-
AbCdEf:username1::"
    }]
  }]
}
```

Example 特定のシークレットバージョンを参照する

次に示すのは、シークレットの暗号化されていない内容と、シークレットのすべてのバージョンのメタデータを表示する describe-secret コマンドの出力例です。

```
{
    "ARN": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-AbCdEf",
    "Name": "appauthexample",
    "Description": "Example of a secret containing application authorization data.",
    "RotationEnabled": false,
    "LastChangedDate": 1581968848.926,
    "LastAccessedDate": 1581897600.0,
    "Tags": [],
    "VersionIdsToStages": {
        "871d9eca-18aa-46a9-8785-981ddEXAMPLE": [
            "AWSCURRENT"
        ],
        "9d4cb84b-ad69-40c0-a0ab-cead3EXAMPLE": [
            "AWSPREVIOUS"
        ]
    }
}
```

前のコンテナの定義の出力で特定のバージョンのステージングラベルを参照するには、ARN の最後にキー名を指定します。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-AbCdEf::AWSPREVIOUS:"
    }]
  }]
}
```

前のコンテナの定義の出力で特定のバージョン ID を参照するには、ARN の最後にキー名を指定します。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-AbCdEf:::9d4cb84b-ad69-40c0-a0ab-cead3EXAMPLE"
    }]
  }]
}
```

Example シークレットの特定のキーおよびバージョンのステージングラベルを参照する

シークレット内の特定のキーと特定のバージョンのステージングラベルの両方を参照する方法は次のとおりです。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-AbCdEf:username1:AWSPREVIOUS:"
    }]
  }]
}
```

特定のキーとバージョン ID を指定するには、次の構文を使用します。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:appauthexample-
AbCdEf:username1::9d4cb84b-ad69-40c0-a0ab-cead3EXAMPLE"
    }]
  }]
}
```

環境変数で指定されたシークレットを使用してタスク定義を作成する方法については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

Amazon ECS 環境変数を使用して Systems Manager パラメータを伝達する

Amazon ECS を使用すると、AWS Systems Manager Parameter Store のパラメータに機密データを保存した上で、コンテナの定義からそれを参照することによって、コンテナに機密データを取り込むことができます。

環境変数を使用して、コンテナに Systems Manager シークレットを注入する場合は、以下を考慮する必要があります。

- 重要なデータは、コンテナが最初に開始されたときにコンテナに挿入されます。シークレットを後で更新またはローテーションすると、コンテナには更新された値が自動的に送信されなくなります。この場合は、新しいタスクを起動する必要があります。または、タスクがサービスの一部である場合は、サービスを更新し、[Force new deployment] (新しいデプロイの強制) オプションを使用して、新しいタスクの起動をサービスに強制できます。
- AWS Fargate 上の Amazon ECS タスクでは、以下の点を考慮する必要があります。
  - シークレットの内容全体を環境変数として挿入したり、ログ設定にシークレットを挿入したりするには、プラットフォームバージョン `1.3.0` 以降を使用する必要があります。詳細については、Amazon ECS 向け Fargate プラットフォームバージョン を参照してください。
  - 特定の JSON キーまたはシークレットのバージョンを環境変数または log 設定に挿入するには、プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` (Windows) を使用する必要があります。詳細については、Amazon ECS 向け Fargate プラットフォームバージョン を参照してください。
- EC2 上の Amazon ECS タスクでは、以下の点を考慮する必要があります。
  - シークレットの特定の JSON キーやバージョンを使用してシークレットを挿入するには、コンテナインスタンスにバージョン `1.37.0` 以降のコンテナエージェントが必要です。ただし、最

新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

シークレットの内容全体を環境変数として挿入したり、ログ設定にシークレットを挿入したりするには、コンテナインスタンスにバージョン `1.22.0` 以降のコンテナエージェントが必要です。

- セキュリティ制御を強化するために、インターフェイス VPC エンドポイントを使用します。Systems Manager 用に、インターフェイス VPC エンドポイントを作成する必要があります。VPC エンドポイントについては、「AWS Systems Manager ユーザーガイド」の「Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する」を参照してください。
- タスク定義では、Secrets Manager の追加アクセス許可を持つタスク実行ロールを使用する必要があります。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。
- `awslogs` ログドライバーを使用するように設定された Windows タスクの場合は、コンテナインスタンスで `ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE` 環境変数も設定する必要があります。次の構文を使用します。

```
<powershell>
[Environment]::SetEnvironmentVariable("ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE",
 $TRUE, "Machine")
Initialize-ECSAgent -Cluster <cluster name> -EnableTaskIAMRole -LoggingDrivers
 '["json-file","awslogs"]'
</powershell>
```

Systems Manager パラメータを作成する

Systems Manager コンソールを使用すると、機密データ用に Systems Manager Parameter Store のパラメータを作成できます。詳細については、「AWS Systems Manager ユーザーガイド」の「Systems Manager パラメータを作成する (コンソール)」または「Systems Manager パラメータを作成する (AWS CLI)」を参照してください。

コンテナ定義に環境変数を追加します。

タスク定義でのコンテナ定義内では、コンテナに設定する環境変数の名前と、コンテナに渡す機密データが含まれている Systems Manager Parameter Store パラメータの ARN 全体を使用して `secrets` を指定します。詳細については、「`secrets`」を参照してください。

以下に示すのは、Systems Manager パラメータストアのパラメータを参照するときの形式を示すタスク定義のスニペットです。起動するタスクと同じリージョンに Systems Manager パラメータストアのパラメータが存在する場合は、パラメータの完全な ARN または名前のどちらも使用できます。パラメータが別のリージョンに存在する場合は、完全な ARN を指定する必要があります。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter/parameter_name"
    }]
  }]
}
```

環境変数で指定されたシークレットを使用してタスク定義を作成する方法については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

Systems Manager Parameter Store のシークレットをプログラムで取得するようにアプリケーションを更新する

Systems Manager Parameter Store のパラメータに保存されている機密データを取得するには、「AWS SDK コードサンプルコードライブラリ」の「AWS SDK を使用した Systems Manager のコードサンプル」を参照してください。

Amazon ECS ログ記録設定のシークレットを伝達する

`logConfiguration` に `secretOptions` パラメータを使用することで、ロギングに使用される機密データを渡すことができます。

シークレットは Secrets Manager または Systems Manager に保存できます。

Secrets Manager を使用する

コンテナの定義内で `logConfiguration` を指定するときに、コンテナに設定するログドライバーオプションの名前と、コンテナに渡す機密データが含まれている Secrets Manager シークレットの ARN 全体を使用して `secretOptions` を指定できます。

以下に示すのは、Secrets Manager シークレットを参照するときの形式を示すタスク定義のスニペットです。

```
{
```

```
  "containerDefinitions": [{
    "logConfiguration": [{
      "logDriver": "splunk",
      "options": {
        "splunk-url": "https://your_splunk_instance:8088"
      },
      "secretOptions": [{
        "name": "splunk-token",
        "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name-
AbCdEf"
      }]
    }]
  }]
}
```

コンテナ定義に環境変数を追加します。

コンテナの定義内で、コンテナに設定する環境変数の名前と、コンテナに渡す機密データが含まれている Systems Manager パラメータストアのパラメータの ARN 全体を使用して secrets を指定できます。詳細については、「secrets」を参照してください。

以下に示すのは、Systems Manager パラメータストアのパラメータを参照するときの形式を示すタスク定義のスニペットです。起動するタスクと同じリージョンに Systems Manager パラメータストアのパラメータが存在する場合は、パラメータの完全な ARN または名前のどちらも使用できます。パラメータが別のリージョンに存在する場合は、完全な ARN を指定する必要があります。

```
{
  "containerDefinitions": [{
    "secrets": [{
      "name": "environment_variable_name",
      "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter/parameter_name"
    }]
  }]
}
```

環境変数で指定されたシークレットを使用してタスク定義を作成する方法については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

使用アイテム Systems Manager

ログ設定には機密データを注入できます。コンテナの定義内で logConfiguration を指定するときに、コンテナに設定するログドライバーオプションの名前と、コンテナに渡す機密データが含まれ

ている Systems Manager パラメータストアのパラメータの ARN 全体を使用して `secretOptions` を指定できます。

> **Important**
>
> 起動するタスクと同じリージョンに Systems Manager パラメータストアのパラメータが存在する場合は、パラメータの完全な ARN または名前のどちらも使用できます。パラメータが別のリージョンに存在する場合は、完全な ARN を指定する必要があります。

以下に示すのは、Systems Manager パラメータストアのパラメータを参照するときの形式を示すタスク定義のスニペットです。

```
{
  "containerDefinitions": [{
    "logConfiguration": [{
      "logDriver": "fluentd",
      "options": {
        "tag": "fluentd demo"
      },
      "secretOptions": [{
        "name": "fluentd-address",
        "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter:/parameter_name"
      }]
    }]
  }]
}
```

Amazon ECS の Secrets Manager シークレットを使用した機密データの指定

Amazon ECS では、機密データを AWS Secrets Manager シークレットに保存し、コンテナ定義でそれを参照することで、機密データをコンテナに挿入することができます。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

Secrets Manager シークレットを作成して、Amazon ECS タスク定義でシークレットを参照し、コンテナ内の環境変数をクエリすることでシークレットの内容を表示して正しく動作したことを確認する方法について説明します。

前提条件

このチュートリアルでは、以下の前提条件が完了済みであることを前提としています。

- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- ユーザーに、Secrets Manager および Amazon ECS リソースを作成するのに必要な IAM アクセス許可があります。

ステップ 1:Secrets Manager シークレットを作成する

Secrets Manager コンソールを使用して、機密データ用のシークレットを作成できます。このチュートリアルでは、後にコンテナで参照するユーザー名とパスワードを保存するための基本的なシークレットを作成します。詳細については、AWS Secrets Manager ユーザーガイドの「Create an AWS Secrets Manager secret」を参照してください。

[key/value pairs to be stored in this secret] (このシークレットに格納されたキーおよび値のペア) は、チュートリアルの最後にコンテナに存在する環境変数の値です。

[Secret ARN] (シークレット ARN) を保存し、後のステップのタスク実行 IAM ポリシーとタスク定義で参照できるようにします。

ステップ 2: タスク実行ロールにシークレットアクセス許可を追加する

Amazon ECS で Secrets Manager シークレットから機密データを取得するには、タスク実行ロールにシークレットアクセス許可が必要です。詳細については、「Secrets Manager または Systems Manager のアクセス許可」を参照してください。

ステップ 3: タスク定義を作成する

Amazon ECS コンソールを使用して、Secrets Manager シークレットを参照するタスク定義を作成します。

シークレットを指定するタスク定義を作成するには

IAM コンソールを使用して、必要なアクセス許可を持つタスク実行ロールを更新します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
4. JSON エディタボックスで、以下のタスク定義 JSON テキストを入力して、ステップ 1 で作成した Secrets Manager シークレットの完全な ARN と、ステップ 2 で更新したタスク定義ロールを指定します。[Save] を選択します。

5.

```
{
    "executionRoleArn": "arn:aws:iam::aws_account_id:role/ecsTaskExecutionRole",
    "containerDefinitions": [
        {
            "entryPoint": [
                "sh",
                "-c"
            ],
            "portMappings": [
                {
                    "hostPort": 80,
                    "protocol": "tcp",
                    "containerPort": 80
                }
            ],
            "command": [
                "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample
 App</title> <style>body {margin-top: 40px; background-color: #333;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</
h1> <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html &&
 httpd-foreground\""
            ],
            "cpu": 10,
            "secrets": [
                {
                    "valueFrom":
 "arn:aws:secretsmanager:region:aws_account_id:secret:username_value",
                    "name": "username_value"
                }
            ],
            "memory": 300,
            "image": "public.ecr.aws/docker/library/httpd:2.4",
            "essential": true,
            "name": "ecs-secrets-container"
        }
    ],
    "family": "ecs-secrets-tutorial"
}
```

6. [Create] (作成) を選択します。

ステップ 4: クラスターを作成する

Amazon ECS コンソールを使用してコンテナインスタンスを含むクラスターを作成し、タスクを実行します。利用可能なリソースを使用して登録された少なくとも 1 つのコンテナインスタンスを持つ既存のクラスターがあり、このチュートリアル用に作成されたタスク定義の 1 つのインスタンスを実行できる場合は、次のステップに進みます。

このチュートリアルでは、Amazon ECS最適化Amazon Linux 2 AMIを使用して、1つの`t2.micro`コンテナ・インスタンスでクラスタを作成します。

EC2 起動タイプ用にクラスターを作成する方法については、「the section called “Amazon EC2 起動タイプ用のクラスターを作成する”」を参照してください。

ステップ 5: タスクを実行する

Amazon ECS コンソールを使用し、作成したタスク定義を使用してタスクを実行できます。このチュートリアルでは、前のステップで作成したクラスターを使用し、EC2 起動タイプを使用してタスクを実行します。

タスクを実行する方法については、「the section called “タスクとしてのアプリケーションの実行”」を参照してください。

ステップ 6: 確認する

以下のステップを使用して、すべてのステップが正常に完了し、コンテナに環境変数が適切に作成されたことを確認できます。

環境変数が作成されたことを確認するには

1. コンテナインスタンスのパブリック IP アドレスまたは DNS アドレスを見つけます。
   a. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
   b. ナビゲーションペインで [クラスター] を選択した後、作成してあるクラスターを選択します。
   c. [インフラストラクチャ] を選択した後、コンテナインスタンスを選択します。
   d. インスタンスの [パブリック IP] または [パブリック DNS] を記録します。
2. macOS または Linux コンピュータを使用している場合は、以下のコマンドでインスタンスに接続します (パスとアドレスはプライベートキーへのパスとインスタンスのパブリックアドレスに置き換えます)。

```
$ ssh -i /path/to/my-key-pair.pem ec2-user@ec2-198-51-100-1.compute-1.amazonaws.com
```

Windows コンピュータを使用している場合は、「Amazon EC2 ユーザーガイド」の「PuTTY を使用して Linux インスタンスに接続する」を参照してください。

> **Important**
>
> インスタンス接続時の問題の詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスへの接続に関するトラブルシューティング」を参照してください。

3. インスタンスで実行するコンテナを一覧表示します。`ecs-secrets-tutorial` コンテナのコンテナ ID をメモしておきます。

```
docker ps
```

4. 前のステップの出力のコンテナ ID を使用して `ecs-secrets-tutorial` コンテナに接続します。

```
docker exec -it container_ID /bin/bash
```

5. `echo` コマンドを使用して環境変数の値を出力します。

```
echo $username_value
```

このチュートリアルが成功すると、次のような出力が表示されます。

```
password_value
```

> **Note**
>
> あるいは、`env` (または `printenv`) コマンドを使用して、コンテナ内の環境変数をすべて一覧表示できます。

ステップ 7: クリーンアップする

このチュートリアルが終了したら、未使用のリソースに対する料金が発生しないように、それに関連付けられたリソースをクリーンアップする必要があります。

リソースをクリーンアップするには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [Delete Cluster] を選択します。
5. 確認ボックスで、delete ***cluster name*** と入力し、[削除] を選択します。
6. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
7. ナビゲーションペインで [Roles] (ロール) を選択します。
8. ロールの一覧で `ecsTaskExecutionRole` を探し、選択します。
9. [アクセス許可] を選択した後、[ECSSecrets チュートリアル] の横にある [X] を選択します。[削除] を選択してください。
10. [https://console.aws.amazon.com/secretsmanager/]で、Secrets Manager コンソール を開きます。
11. 作成した [username_value] シークレットを選択し、[Actions (アクション)]、[Delete secret (シークレットの削除)] の順に選択します。

Fargate 起動タイプでの Amazon ECS タスク定義パラメータ

タスク定義は、タスクファミリー、AWS Identity and Access Management (IAM) タスクロール、ネットワークモード、コンテナ定義、ボリューム、および起動タイプという各部分に分かれています。ファミリとコンテナの定義は、タスク定義の必須項目です。これに対して、タスクロール、ネットワークモード、ボリューム、および起動タイプは省略することができます。

これらのパラメータを JSON ファイルで使用し、タスク定義を設定できます。

以下に示すのは、Fargate 起動タイプの各タスク定義パラメータのより詳細な説明です。

ファミリー

`family`

タイプ: 文字列

必須: はい

タスク定義を登録するときに、ファミリー (複数バージョンのタスク定義の名前のようなもの) を指定する必要があります。登録したタスク定義には、リビジョン番号が与えられます。特定のファミリーに登録した最初のタスク定義には、リビジョン 1 が与えられます。その後に登録したタスク定義には、連番でリビジョン番号が与えられます。

起動タイプ

タスク定義の登録時、Amazon ECS がタスク定義の検証基準となる起動タイプを指定できます。タスク定義が指定された互換性を検証しない場合、クライアント例外が返されます。詳しくは、「Amazon ECS 起動タイプ」を参照してください。

タスク定義では、以下のパラメータが使用できます。

`requiresCompatibilities`

タイプ: 文字列配列

必須: いいえ

有効な値: `FARGATE`

タスク定義が検証された起動タイプ。これにより、タスク定義で使用されているすべてのパラメータが、起動タイプの要件を満たしていることの確認処理が開始されます。

タスクロール

`taskRoleArn`

タイプ: 文字列

必須: いいえ

タスク定義を登録するときに、IAM ロールのタスクロールを割り当てて、タスクのコンテナに、関連するポリシーに指定された AWS API を呼び出すためのアクセス権限を付与できます。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

タスク実行ロール

`executionRoleArn`

タイプ: 文字列

必須: 条件による

ユーザーに代わって AWS API コールを実行するアクセス許可を Amazon ECS コンテナエージェントに付与するタスク実行ロールの Amazon リソースネーム (ARN)。

> **Note**
>
> タスク実行 IAM ロールは、タスクの要件に応じて必要です。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

ネットワークモード

`networkMode`

タイプ: 文字列

必須: はい

タスクのコンテナで使用する Docker ネットワークモード。Fargate でホストされている Amazon ECS タスクでは、`awsvpc` ネットワークモードが必要です。

ネットワークモードに none を設定した場合、タスクのコンテナは外部への接続を持たないため、コンテナ定義でポートマッピングを指定することはできません。

ネットワークモードが `awsvpc` の場合は、タスクに Elastic Network Interface が割り当てられるため、タスク定義を使用したサービスの作成時またはタスクの実行時に `NetworkConfiguration` を指定する必要があります。詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。`awsvpc` ネットワー

クモードでは、コンテナのネットワークパフォーマンスは最大限になります。Amazon EC2 ネットワークスタックを使用するためです。公開されたコンテナのポートは、アタッチされた Elastic Network Interface ポートに直接マッピングされます。このため、動的ホストポートマッピングは使用できません。

awsvpc ネットワークモードでは、コンテナのネットワークパフォーマンスは最大限になります。Amazon EC2 ネットワークスタックを使用するためです。awsvpc ネットワークモードでは、公開されたコンテナのポートは、アタッチされた Elastic Network Interface ポートに直接マッピングされます。

このため、動的ホストポートマッピングは使用できません。

awsvpc ネットワークモードが必要です。

ランタイムプラットフォーム

`operatingSystemFamily`

タイプ: 文字列

必須: 条件による

デフォルト: LINUX

Fargate でホストされる Amazon ECS タスクでは、このパラメータは必須です。

タスク定義を登録する際、オペレーティングシステムファミリを指定します。

有効な値
は、LINUX、WINDOWS_SERVER_2019_FULL、WINDOWS_SERVER_2019_CORE、WINDOWS_SERVER_2
および WINDOWS_SERVER_2022_CORE です。

サービスで使用されるすべてのタスク定義は、このパラメータに対して同じ値を設定する必要があります。

タスク定義がサービスの一部である場合、この値はサービスの platformFamily 値と一致する必要があります。

`cpuArchitecture`

タイプ: 文字列

必須: 条件による

デフォルト: X86_64

パラメータを null のままにすると、Fargate でホストされているタスクの開始したときにデフォルト値が自動的に割り当てられます。

タスク定義を登録する際は、CPU アーキテクチャを指定します。有効な値は X86_64 および ARM64 です。

サービスで使用されるすべてのタスク定義は、このパラメータに対して同じ値を設定する必要があります。

Linux タスクがある場合は、値を ARM64 に設定できます。詳細については、「the section called "64 ビット ARM ワークロードでのタスク定義"」を参照してください。

タスクサイズ

タスク定義の登録時に、そのタスクが使用する CPU とメモリの合計量を指定できます。これは、コンテナ定義レベルの cpu および memory の値とは異なります。Fargate (Linux 向けと Windows 向けの両方) でホストされるタスクの場合、これらのフィールドは必須です。また、cpu および memory の両方について、特定の値がサポートされています。

> **Note**
> タスクレベル CPU およびメモリのパラメータは Windows コンテナでは無視されます。Windows コンテナではコンテナレベルリソースを指定することをお勧めします。

以下のパラメータをタスク定義で使用できます。

cpu

タイプ: 文字列

必須: 条件による

> **Note**
> このパラメータは Windows コンテナではサポートされません。

タスクに適用される CPU ユニットのハード制限。JSON ファイルでは、CPU 値を CPU ユニットまたは仮想 CPU (vCPU) の文字列として指定できます。例えば、CPU 値を 1 vCPU (CPU ユニット) または 1024 (vCPU) として指定できます。タスク定義が登録されると、vCPU 値は、CPU ユニットを示す整数に変換されます。

このフィールドは必須であり、次のいずれかの値を使用する必要があります。この値により memory パラメータでサポートされる値の範囲が決まります。以下の表に、タスクレベル CPU とメモリの有効な組み合わせを示します。

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
256 (.25 vCPU)	512 MiB、1 GB、2 GB	リナックス
512 (.5 vCPU)	1 GB、2 GB、3 GB、4 GB	リナックス
1,024 (1 vCPU)	2 GB、3 GB、4 GB、5 GB、6 GB、7 GB、8 GB	Linux、Windows
2,048 (2 vCPU)	4 GB ~ 16 GB (1 GB のインクリメント)	Linux、Windows
4,096 (4 vCPU)	8 GB ~ 30 GB (1 GB のインクリメント)	Linux、Windows
8192 (8 vCPU) **Note** このオプションには Linux プラットフォーム 1.4.0 以降が必要です。	16 GB ~ 60 GB (4 GB のインクリメント)	リナックス
16384 (16vCPU)	32 GB ~ 120 GB (8 GB のインクリメント)	リナックス

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
Note このオプションには Linux プラットフォーム 1.4.0 以降が必要です。		

`memory`

タイプ: 文字列

必須: 条件による

Note

このパラメータは Windows コンテナではサポートされません。

タスクに適用されるメモリのハード制限です。タスク定義のメモリの値は、メビバイト (MiB) またはギガバイト (GB) の文字列として指定できます。例えば、メモリの値を 3072 (MiB) または 3 GB (GB) のいずれかで指定できます。タスク定義が登録されると、GB 値は、MiB を示す整数に変換されます。

このフィールドは必須であり、次のいずれかの値を使用する必要があります。この値により cpu パラメータでサポートされる値の範囲が決まります。

メモリ値 (単位 MiB、ほぼ同等の GB での値を付記)	CPU の値	Fargate でサポートされるオペレーティングシステム
512 (0.5 GB)、1024 (1 GB)、2048 (2 GB)	256 (.25 vCPU)	リナックス

メモリ値 (単位 MiB、ほぼ同等の GB での値を付記)	CPU の値	Fargate でサポートされるオペレーティングシステム
1024 (1 GB)、2048 (2 GB)、3072 (3 GB)、4096 (4 GB)	512 (.5 vCPU)	リナックス
2048 (2 GB)、3072 (3 GB)、4096 (4 GB)、5120 (5 GB)、6144 (6 GB)、7168 (7 GB)、8192 (8 GB)	1,024 (1 vCPU)	Linux、Windows
4,096 (4 GB) ~ 16,384 (16 GB) (1,024 (1 GB) 単位の増加)	2,048 (2 vCPU)	Linux、Windows
8,192 (8 GB) ~ 30,720 (30 GB) (1,024 (1 GB) 単位の増加)	4,096 (4 vCPU)	Linux、Windows
16 GB ~ 60 GB (4 GB のインクリメント) **Note** このオプションには Linux プラットフォーム `1.4.0` 以降が必要です。	8192 (8 vCPU)	リナックス

メモリ値 (単位 MiB、ほぼ同等の GB での値を付記)	CPU の値	Fargate でサポートされるオペレーティングシステム
32 GB ~ 120 GB (8 GB のインクリメント) **Note** このオプションには Linux プラットフォーム 1.4.0 以降が必要です。	16384 (16vCPU)	リナックス

コンテナ定義

タスク定義を登録するときは、コンテナインスタンスの Docker デーモンに渡されるコンテナ定義のリストを指定する必要があります。以下のパラメータをコンテナ定義で使用できます。

トピック

- 標準のコンテナ定義のパラメータ
- 詳細コンテナ定義パラメータ
- その他のコンテナ定義のパラメータ

標準のコンテナ定義のパラメータ

以下のタスク定義のパラメータは必須であるか、ほとんどのコンテナ定義で使用されます。

トピック

- 名前
- イメージ
- 「メモリ」
- ポートマッピング
- プライベートリポジトリの認証情報

名前

name

タイプ: 文字列

必須: はい

コンテナの名前。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコアを使用できます。タスク定義で複数のコンテナをリンクしている場合、あるコンテナの name を別のコンテナの links に入力できます。これにより、コンテナ同士を接続します。

イメージ

image

タイプ: 文字列

必須: はい

コンテナの開始に使用するイメージ。この文字列は Docker デーモンに直接渡されます。デフォルトでは、Docker Hub レジストリのイメージを使用できます。*repository-url*/*image*:*tag* または *repository-url*/*image*@*digest* で他のリポジトリを指定することもできます。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコア、コロン、ピリオド、スラッシュ、シャープ記号を使用できます。このパラメータは、docker create-container コマンドの Image と docker run コマンドの IMAGE パラメータにマッピングされます。

- 新しいタスクが開始されると、Amazon ECS コンテナエージェントは、指定されたイメージおよびタグの最新バージョンをプルしてコンテナで使用します。ただし、リポジトリイメージの後続の更新がすでに実行されているタスクに反映されることはありません。
- タスク定義のイメージパスでタグまたはダイジェストを指定しない場合、Amazon ECS コンテナエージェントは指定されたイメージの最新バージョンを取り込みます。
- ただし、リポジトリイメージの後続の更新がすでに実行されているタスクに反映されることはありません。
- プライベートレジストリのイメージがサポートされています。詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。
- Amazon ECR リポジトリのイメージは、registry/repository:tag または registry/repository@digest の完全な命名規則 (例えば、*aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-web-*

app:*latest* や、*aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-web-app*@*sha256:94afd1f2e64d908bc90dbca0035a5b567EXAMPLE*) を使用して指定します。

- Docker Hub の公式リポジトリのイメージでは、1 つの名前 (例: ubuntu または mongo) を使用します。
- Docker Hub の他のリポジトリのイメージは、組織名で修飾されます (例: amazon/amazon-ecs-agent)。
- 他のオンラインリポジトリのイメージは、さらにドメイン名で修飾されます (例: quay.io/assemblyline/ubuntu)。

`versionConsistency`

タイプ: 文字列

有効な値: `enabled|disabled`

必須: いいえ

コンテナ定義で指定されたコンテナイメージタグを Amazon ECS がイメージダイジェストに解決するかどうかを指定します。デフォルトでは、この動作は `enabled` です。コンテナの値を `disabled` として設定した場合、Amazon ECS はコンテナイメージタグをダイジェストに解決せず、コンテナ定義で指定された元のイメージ URI をデプロイ用に使用します。コンテナイメージの解決の詳細については、「コンテナイメージの解決」を参照してください。

「メモリ」

`memory`

タイプ: 整数

必須: いいえ

コンテナに適用されるメモリの量 (MiB 単位)。コンテナは、ここで指定したメモリを超えようとすると、強制終了されます。タスク内のすべてのコンテナ用に予約されるメモリの合計量は、タスクの `memory` 値より小さくする必要があります (指定されている場合)。このパラメータは docker create-container コマンドの `Memory` にマッピングされ、`--memory` オプションは docker run にマッピングされます。

Docker デーモン 20.10.0 以降によって、コンテナ用として 6 MiB 以上のメモリが予約されます。従って、このコンテナに対しては 6 MiB 未満のメモリは指定しないようにします。

Docker デーモン 19.03.13-ce 以降では、コンテナ用として 4 MiB 以上のメモリが予約されます。このため、このコンテナ用には 4 MiB 未満のメモリを指定しないようにします。

> **Note**
>
> リソースの使用率を最大化することを目的に、特定のインスタンスタイプにおいて、タスクにできるだけ多くのメモリを提供する場合には、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

`memoryReservation`

タイプ: 整数

必須: いいえ

コンテナ用に予約するメモリのソフト制限 (MiB 単位)。システムメモリに競合がある場合、Docker はコンテナのメモリ量をこのソフト制限値内に維持しようとします。ただし、コンテナは必要に応じてより多くのメモリを使用することができます。コンテナは、`memory` パラメーターで指定されたハード制限 (該当する場合) またはコンテナインスタンス上の利用可能なすべてのメモリのいずれか早く達する方まで使用できます。このパラメータは docker create-container コマンドの `MemoryReservation` にマッピングされ、`--memory-reservation` オプションは docker run にマッピングされます。

タスクレベルでメモリ値を指定しない場合、コンテナ定義で `memory` または `memoryReservation` の一方または両方に 0 以外の整数を指定する必要があります。両方を指定する場合、`memory` は `memoryReservation` より大きいことが必要です。`memoryReservation` を指定する場合、コンテナが配置されているコンテナインスタンスで使用可能なメモリリソース量から、上記の値が減算されます。それ以外の場合は、`memory` の値が使用されます。

例えば、コンテナが通常 128 MiB のメモリを使用しているが、短期間にメモリが 256 MiB にバーストする場合があるとします。128 MiB の `memoryReservation` と 300 MiB の `memory` ハード制限を設定できます。この設定では、コンテナが、コンテナインスタンスの残りのリソースから 128 MiB のメモリのみを予約できます。同時に、この構成により、コンテナは必要に応じてより多くのメモリ リソースを使用できるようになります。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

Docker デーモン 20.10.0 以降によって、コンテナ用として 6 MiB 以上のメモリが予約されます。従って、このコンテナに対しては 6 MiB 未満のメモリは指定しないようにします。

Docker デーモン 19.03.13-ce 以降では、コンテナ用として 4 MiB 以上のメモリが予約されます。このため、このコンテナ用には 4 MiB 未満のメモリを指定しないようにします。

> **Note**
>
> リソースの使用率を最大化することを目的に、特定のインスタンスタイプにおいて、タスクにできるだけ多くのメモリを提供する場合には、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

ポートマッピング

`portMappings`

タイプ: オブジェクト配列

必須: いいえ

ポートマッピングは、コンテナのネットワークポートを外部に公開します。これは、クライアントがアプリケーションにアクセスすることを可能にします。これは、同じタスク内にあるコンテナ間の通信にも使用されます。

`awsvpc` ネットワークモードを使用するタスク定義では、`containerPort` のみを指定します。`hostPort` は常に無視され、コンテナポートはホスト上の番号が大きいランダムなポートに自動的にマップされます。

Windows のポートマッピングでは、`localhost` の代わりに `NetNAT` ゲートウェイを使用します。Windows のポートマッピングにはループバックが存在しないため、ホスト自体からコンテナのマッピングされたポートにアクセスはできません。

このパラメータのほとんどのフィールド (`containerPort`、`hostPort`、`protocol` を含む) は docker create-container コマンドの `PortBindings` にマッピングされ、`--publish` オプション

は docker run にマッピングされます。タスク定義でネットワークモードを host に設定している場合、ホストポートは未定義とするか、ポートマッピングのコンテナポートと一致させる必要があります。

> **Note**
>
> タスクが RUNNING ステータスに達すると、手動および自動で割り当てられたホストとコンテナポートが次の場所で表示されます:
>
> - コンソール: 指定されたタスクのコンテナ詳細の [Network Bindings] セクション。
> - AWS CLI: networkBindings コマンド出力の describe-tasks セクション。
> - API: DescribeTasks レスポンス。
> - メタデータ: タスクメタデータのエンドポイント。

`appProtocol`

タイプ: 文字列

必須: いいえ

ポートマッピングに使用されるアプリケーションプロトコル。このパラメータは Service Connect にのみ適用されます。アプリケーションが使用するプロトコルと一貫性を持つように、このパラメータを設定することをお勧めします。このパラメータを設定すると、Amazon ECS はサーバー コネクト プロキシにプロトコル固有の接続処理を追加します。このパラメータを設定すると、Amazon ECS は Amazon ECS コンソールと CloudWatch にプロトコル固有のテレメトリを追加します。

このパラメータ値を設定しないと、TCP が使用されます。ただし、Amazon ECS では、TCP 用のプロトコル固有のテレメトリーは追加されません。

詳細については、「the section called “ Service Connect”」を参照してください。

有効なプロトコル値: `"HTTP" | "HTTP2" | "GRPC"`

`containerPort`

タイプ: 整数

必須: はい (`portMappings` を使用する場合)

ユーザーが指定したホストポートまたは自動的に割り当てられたホストポートにバインドされるコンテナポートの番号。

awsvpc ネットワークモードを使用するタスクの場合は、containerPort を使用して公開ポートを指定します。

Fargate 上の Windows コンテナの場合、containerPort にポート 3150 は使用できません。このポートは予約済みです。

containerPortRange

タイプ: 文字列

必須: いいえ

動的にマッピングされたホストポート範囲にバインドされるコンテナのポート番号の範囲。

このパラメータは、register-task-definition API を使用してのみ設定できます。このオプションは、portMappings パラメータで使用できます。詳細については、「AWS Command Line Interface リファレンス」の「register-task-definition」を参照してください。

containerPortRange を指定するときは、以下のルールが適用されます。

- awsvpc ネットワークモードを使用する必要があります。
- このパラメータは、Linux と Windows の両オペレーティングシステムで使用できます。
- コンテナインスタンスには、少なくともコンテナエージェントのバージョン 1.67.0 と ecs-init パッケージのバージョン 1.67.0-1 が必要です。
- 各コンテナにつき、最大 100 のポートレンジを指定できます。
- hostPortRange は指定しません。hostPortRange の値は次のように設定されます。
  - awsvpc ネットワークモードのタスク内のコンテナでは、hostPort は containerPort と同じ値に設定されます。これは静的マッピング戦略です。
- containerPortRange の有効な値は 1 ~ 65535 です。
- 1 つのポートは、コンテナごとに 1 つのポートマッピングにのみ含められます。
- 重複するポート範囲は指定できません。
- 範囲内の最初のポートは、最後のポートよりも小さくなければなりません。
- Docker では、ポートの数が多い場合は、Docker デーモン設定ファイルの docker-proxy をオフにすることをお勧めします。

  詳細については、GitHub の Issue #11185 を参照してください。

Docker デーモン設定ファイルの docker-proxy をオフにする方法については、Amazon ECS 開発者ガイドの「Docker デーモン」を参照してください。

DescribeTasks を呼び出すと、コンテナポートにバインドされているホストポートである hostPortRange を表示できます。

ポート範囲は、EventBridge に送信される Amazon ECS タスクイベントに含まれません。詳細については、「the section called “EventBridge を使用して Amazon ECS エラーへの対応を自動化する”」を参照してください。

`hostPortRange`

型: 文字列

必須: いいえ

ネットワークバインディングで使用されるホストのポート番号範囲。これは Docker によって割り当てられ、Amazon ECS エージェントによって配信されます。

`hostPort`

タイプ: 整数

必須: いいえ

コンテナ用に予約するコンテナインスタンスのポート番号。

`hostPort` は、空白のままにするか、`containerPort` と同じ値にできます。

Docker バージョン 1.6.0 以降のデフォルトの一時ポート範囲は、インスタンスの `/proc/sys/net/ipv4/ip_local_port_range` にリストされています。このカーネルパラメータが使用できない場合、`49153-65535` から始まるデフォルトのエフェメラルポート範囲が使用されます。エフェメラルポート範囲では、ホストポートを指定しないでください。これらの範囲は自動割り当て用に予約済みです。一般的に、32768 より小さい番号のポートは一時ポート範囲に含まれません。

デフォルトの予約済みポートは、SSH 用の 22、Docker ポートの 2375 および 2376、Amazon ECS コンテナエージェントポートの `51678-51680` です。実行中のタスクに対して以前にユーザーが指定したホストポートも、タスクの実行中に予約されます。タスクが停止すると、ホストポートはリリースされます。現在の予約済みポートは、describe-container-instances 出力の `remainingResources` に表示されます。コンテナインスタンスには、デフォルトの予約済みポートを含めて、一度に最大 100 個の予約済みポートを割り当

てられます。自動的に割り当てられるポートは、この 100 個の予約済みポートクォータにはカウントされません。

`name`

タイプ: 文字列

必須: いいえ。サービスに Service Connect および VPC Lattice を設定する場合は必要です。

ポートマッピングに使用される名前。このパラメータは Service Connect および VPC Lattice にのみ適用されます。このパラメータは、サービスの Service Connect および VPC Lattice 設定で使用する名前です。

詳細については、「Service Connect を使用して Amazon ECS サービスを短縮名で接続する」を参照してください。

次の例では、Service Connect および VPC Lattice の 2 つの必須フィールドが使用されています。

```
"portMappings": [
    {
        "name": string,
        "containerPort": integer
    }
]
```

`protocol`

タイプ: 文字列

必須: いいえ

ポートマッピングに使用されるプロトコル。有効な値は、`tcp` および `udp` です。デフォルト: `tcp`。

> **Important**
>
> `tcp` は Service Connect でのみサポートされます。このフィールドが設定されていない場合は、`tcp` が暗示されることに注意してください。

ホストポートを指定する際は、以下の構文を使用します。

```
"portMappings": [
    {
        "containerPort": integer,
        "hostPort": integer
    }
    ...
]
```

自動割り当てのホストポートが必要な場合は、以下の構文を使用します。

```
"portMappings": [
    {
        "containerPort": integer
    }
    ...
]
```

プライベートリポジトリの認証情報

`repositoryCredentials`

タイプ: RepositoryCredentials オブジェクト

必須: いいえ

プライベートレジストリ認証用のリポジトリ認証情報。

詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

`credentialsParameter`

タイプ: 文字列

必須: はい (`repositoryCredentials` を使用する場合)

プライベートリポジトリの認証情報が含まれているシークレットの Amazon リソースネーム (ARN)。

詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

> **Note**
>
> Amazon ECS API、AWS CLI、または AWS SDK を使用する場合、起動するタスクと同じリージョンにシークレットが存在する場合は、シークレットの完全な ARN または名前のどちらも使用できます。AWS Management Console を使用する場合は、シークレットの完全な ARN を指定する必要があります。

必要なパラメータが含まれるタスク定義のスニペットを、以下に示します。

```
"containerDefinitions": [
    {
        "image": "private-repo/private-image",
        "repositoryCredentials": {
            "credentialsParameter":
 "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name"
        }
    }
]
```

詳細コンテナ定義パラメータ

以下のコンテナ定義用の詳細パラメータは、Amazon ECS コンテナインスタンスでのコンテナの起動に使用する docker run コマンドの拡張機能を追加します。

トピック

- 再起動ポリシー
- ヘルスチェック
- 環境
- ネットワーク設定
- ストレージとログ記録
- セキュリティ
- リソースの制限
- Docker のラベル

再起動ポリシー

`restartPolicy`

コンテナ再起動ポリシーと関連する設定パラメータ。コンテナの再起動ポリシーを設定すると、Amazon ECS はタスクを置き換えることなくコンテナを再起動できます。詳細については、「コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する」を参照してください。

`enabled`

型: ブール値

必須: はい

コンテナに対して再起動ポリシーを有効にするかどうかを指定します。

`ignoredExitCodes`

タイプ: 整数配列

必須: いいえ

Amazon ECS が無視し、再起動を試みない終了コードのリスト。最大 50 個のコンテナ終了コードを指定できます。デフォルトでは、Amazon ECS はいずれの終了コードも無視しません。

`restartAttemptPeriod`

タイプ: 整数

必須: いいえ

再起動を試みる前にコンテナが実行する必要がある時間 (秒単位) 。コンテナを再起動できるのは、`restartAttemptPeriod` 秒に 1 回のみです。コンテナがこの期間実行できずに早く終了した場合、コンテナは再起動されません。最小の `restartAttemptPeriod` は 60 秒、最大の `restartAttemptPeriod` は 604,800 秒 (7 日間) を指定できます。デフォルトでは、コンテナは再起動の前に 300 秒間実行する必要があります。

ヘルスチェック

`healthCheck`

コンテナに対するヘルスチェックのコマンドと、コンテナのための関連する設定パラメータです。詳細については、「コンテナのヘルスチェックを使用して Amazon ECS タスク状態を判定する」を参照してください。

`command`

正常状態かどうかを決定するために、コンテナが実行するコマンドが格納された文字列配列。この文字列配列の先頭には、コマンド引数を直接実行するための CMD、またはコンテナのデフォルトシェルでコマンドを実行するための CMD-SHELL を付加できます。これらのいずれも指定しない場合は CMD が使用されます。

AWS Management Console にタスク定義を登録する場合は、カンマで区切ったコマンドリストを使用してください。これらのコマンドは、タスク定義が作成された後に文字列に変換されます。ヘルスチェックに対する入力の例を次に示します。

```
CMD-SHELL, curl -f http://localhost/ || exit 1
```

AWS Management Console JSON パネル、AWS CLI、または API を使用してタスク定義を登録するときは、コマンドのリストを角かっこで囲みます。ヘルスチェックに対する入力の例を次に示します。

```
[ "CMD-SHELL", "curl -f http://localhost/ || exit 1" ]
```

stderr が出力されない終了コード 0 は成功を示し、0 以外の終了コードは失敗を示します。

`interval`

各ヘルスチェック間の時間間隔 (秒単位)。5 ～ 300 秒を指定できます。デフォルトの値は 30 秒です。

`timeout`

成功まで待機しているヘルスチェックが、失敗したと見なされるまでの期間 (秒単位) です。2 ～ 60 秒を指定できます。デフォルト値は 5 秒です。

`retries`

コンテナが異常と見なされるまでに、失敗したヘルスチェックを再試行する回数です。1～10 回を指定できます。デフォルト値は 3 回の再試行です。

`startPeriod`

失敗したヘルスチェックの再試行が最大回数に達する前に、コンテナにブートストラップための時間を提供するオプションの猶予期間です。0 ~ 100 秒の値を指定できます。デフォルトでは、`startPeriod` は無効となっています。

ヘルスチェックが `startPeriod` 内で成功した場合、コンテナは正常であるとみなされ、その後の失敗は最大再試行回数にカウントされます。

環境

`cpu`

タイプ: 整数

必須: いいえ

Amazon ECS コンテナエージェントがコンテナ用に予約した `cpu` ユニットの数。Linux では、このパラメータは「Create a container」セクションの `CpuShares` にマッピングされます。

Fargate 起動タイプを使用するタスクでは、このフィールドは省略可能です。タスク内のすべてのコンテナのために予約されている CPU の合計量は、タスクレベルの `cpu` 値以上にはできません。

Linux コンテナは、割り当てられた CPU ユニットと同じ比率を使用して、割り当てられていない CPU ユニットをコンテナインスタンス上の他コンテナと共有します。例えば、そのコンテナ用に 512 個の CPU ユニットが指定された単一コアインスタンスタイプで、唯一のコンテナタスクを実行するとします。さらに、そのタスクはコンテナインスタンスで実行される唯一のタスクです。この場合のコンテナは、1,024 個の CPU ユニット配分を任意のタイミングで使用できます。一方、そのコンテナインスタンスで同じタスクのコピーを別途起動したと仮定します。各タスクには、必要に応じて少なくとも 512 個の CPU ユニットが保証されます。同様に、その他のコンテナが残りの CPU を使用していない場合、各コンテナは CPU 使用率を高められます。ただし、両方のタスクが常に 100% アクティブである場合、使用できるのは 512 CPU ユニットに制限されます。

Linux コンテナインスタンスでは、コンテナインスタンス上の Docker デーモンは、CPU 値を使用して、実行中のコンテナに対する相対 CPU 配分比率を計算します。Linux カーネルが許可する最小の有効な CPU 共有値は 2 で、Linux カーネルが許可する最大の有効な CPU 共有値は 262,144 です。ただし、CPU のパラメータは必須ではなく、コンテナ定義では 2 未満の CPU

値および 262144 より大きな CPU 値を使用できます。CPU 値が 2 未満 (null を含む) および 262144 より大きな値である場合、動作は Amazon ECS コンテナエージェントのバージョンによって異なります。

Windows コンテナインスタンスでは、CPU クォータは絶対クォータとして適用されます。Windows コンテナは、タスク定義で定義されている指定された量の CPU にのみアクセスできます。null またはゼロの CPU 値が `0` として Docker に渡されます。次に Windows はこの値を 1 つの CPU の 1% として解釈します。

その他の例については、「Amazon ECS で CPU およびメモリリソースの管理方法」を参照してください。

`gpu`

このパラメータは、Fargate でホストされているコンテナではサポートされていません。

タイプ: ResourceRequirement オブジェクト

必須: いいえ

Amazon ECS コンテナエージェントがコンテナ用に予約した物理 GPUs の数。タスク内でコンテナ用に予約されているすべての GPU の数は、タスクが起動されたコンテナインスタンスで使用できる GPU の数を超えることはできません。詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。

`Elastic Inference accelerator`

このパラメータは、Fargate でホストされているコンテナではサポートされていません。

タイプ: ResourceRequirement オブジェクト

必須: いいえ

`InferenceAccelerator` タイプでは、`value` はタスク定義で指定される `InferenceAccelerator` の `deviceName` と一致します。詳細については、「the section called “Elastic Inference アクセラレーター名”」を参照してください。

`essential`

型: ブール値

必須: いいえ

コンテナの essential パラメーターが true としてマークされており、そのコンテナが何らかの理由で失敗するか停止するとします。その後、タスクの一部である他のすべてのコンテナが停止されます。コンテナの essential パラメータを false にマークしておくと、そのコンテナ失敗はタスク内にある残りのコンテナに影響を与えません。このパラメータを省略した場合、コンテナは必須と見なされます。

すべてのタスクには少なくとも 1 つの必須コンテナが必要です。複数のコンテナで構成されるアプリケーションがあるとします。次に、共通の目的で使用されるコンテナをコンポーネントにグループ化し、さまざまなコンポーネントを複数のタスク定義に分離します。詳細については、「Amazon ECS 用のアプリケーションの構築」を参照してください。

```
"essential": true|false
```

entryPoint

> **Important**
>
> 初期のバージョンの Amazon ECS コンテナエージェントは、entryPoint パラメータを正しく処理しません。entryPoint の使用時に問題が発生する場合は、コンテナエージェントを更新するか、代わりに command 配列項目としてコマンドと引数を入力します。

タイプ: 文字列配列

必須: いいえ

コンテナに渡されるエントリポイント。

```
"entryPoint": ["string", ...]
```

command

タイプ: 文字列配列

必須: いいえ

コンテナに渡されるコマンド。このパラメータは create-container コマンドの Cmd にマッピングされ、 COMMAND パラメータは docker run にマッピングされます。複数の引数がある場合、各引数は配列内で、区切られた文字列により指定する必要があります。

```
"command": ["string", ...]
```

workingDirectory

タイプ: 文字列

必須: いいえ

コマンドを実行するコンテナ内の作業ディレクトリ。このパラメータは、Docker Remote API の 「Create a container (コンテナを作成する)」セクションの WorkingDir にマップされ、--workdir オプションは docker run にマップされます。

```
"workingDirectory": "string"
```

environmentFiles

これは Fargate の Windows コンテナでは使用できません

タイプ: オブジェクト配列

必須: いいえ

コンテナに渡す環境変数が含まれるファイルのリスト。このパラメータは docker run コマンドの --env-file オプションにマッピングされます。

最大 10 個の環境ファイルを指定できます。ファイルには、ファイル拡張子 .env が必要です。環境ファイルの各行には、VARIABLE=VALUE 形式で環境変数が含まれています。# で始まる行はコメントとして扱われ、無視されます。

コンテナ定義に個別の環境変数が指定されている場合は、環境ファイルに含まれる変数よりも優先されます。同じ変数を含む複数の環境ファイルが指定されている場合、それらのファイルは上から下に処理されます。一意の変数名を使用することをお勧めします。詳細については、「個々の環境変数を Amazon ECS コンテナに渡す」を参照してください。

value

型: 文字列

必須: はい

環境変数ファイルを含む Amazon S3 オブジェクトの Amazon リソースネーム (ARN)。

`type`

型: 文字列

必須: はい

使用するファイルのタイプ。`s3` はサポートされる唯一の値です。

`environment`

タイプ: オブジェクト配列

必須: いいえ

コンテナに渡す環境変数。このパラメータは docker create-container コマンドの `Env` にマッピングされ、`--env` オプションは docker run コマンドにマッピングされます。

> **Important**
> 認証情報データなどの機密情報にプレーンテキストの環境変数を使用することはお勧めしません。

`name`

型: 文字列

必須: はい (`environment` を使用する場合)

環境変数の名前。

`value`

型: 文字列

必須: はい (`environment` を使用する場合)

環境変数の値。

```
"environment" : [
    { "name" : "string", "value" : "string" },
    { "name" : "string", "value" : "string" }
```

```
]
```

`secrets`

タイプ: オブジェクト配列

必須: いいえ

コンテナに公開するシークレットを表すオブジェクトです。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

`name`

型: 文字列

必須: はい

コンテナの環境変数として設定する値。

`valueFrom`

型: 文字列

必須: はい

コンテナに公開するシークレット。サポートされている値は、AWS Secrets Manager シークレットの完全な Amazon リソースネーム (ARN)、または AWS Systems Manager Parameter Store 内のパラメータの完全な ARN のいずれかです。

> **Note**
>
> 起動するタスクと同じ AWS リージョン に Systems Manager パラメータストアのパラメータまたは Secrets Manager のパラメータが存在する場合は、シークレットの完全な ARN または名前のいずれかを使用できます。パラメータが別のリージョンに存在する場合は、完全な ARN を指定する必要があります。

```
"secrets": [
    {
        "name": "environment_variable_name",
        "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter/parameter_name"
    }
```

```
]
```

ネットワーク設定

`disableNetworking`

このパラメータは、Fargate で実行されるタスクではサポートされていません。

型: ブール値

必須: いいえ

このパラメータが true のとき、ネットワークはコンテナ内でオフになります。

デフォルト: `false`。

```
"disableNetworking": true|false
```

`links`

このパラメータは、awsvpc ネットワークモードを使用するタスクではサポートされません。

タイプ: 文字列配列

必須: いいえ

`link` パラメータでは、コンテナがポートマッピングを必要とせずに互いに通信することを許可します。このパラメータは、タスク定義のネットワークモードが `bridge` に設定されている場合にのみサポートされます。`name:internalName` コンストラクトは Docker リンクの `name:alias` に似ています。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコアを使用できます。

> **Important**
>
> 同じコンテナインスタンスに配置されたコンテナ同士は、リンクやホストポートマッピングを必要とせずに、互いに通信する場合があります。コンテナインスタンスでのネットワークの分離は、セキュリティグループと VPC 設定によって制御されます。

```
"links": ["name:internalName", ...]
```

`hostname`

タイプ: 文字列

必須: いいえ

コンテナに使用するホスト名。このパラメータは docker create-container の `Hostname` にマッピングされ、`--hostname` オプションは docker run にマッピングされます。

> **Note**
>
> awsvpc ネットワークモードを使用している場合、hostname パラメータはサポートされません。

```
"hostname": "string"
```

`dnsServers`

このパラメータは、Fargate で実行されるタスクではサポートされません。

タイプ: 文字列配列

必須: いいえ

コンテナに提示する DNS サーバーのリスト。

```
"dnsServers": ["string", ...]
```

`extraHosts`

このパラメータは、awsvpc ネットワークモードを使用するタスクではサポートされていません。

タイプ: オブジェクト配列

必須: いいえ

コンテナ上の `/etc/hosts` ファイルに追加する、ホスト名と IP アドレスのマッピングリスト。

このパラメータは docker create-container コマンドの `ExtraHosts` にマッピングされ、`--add-host` オプションは docker run にマッピングされます。

```
"extraHosts": [
      {
        "hostname": "string",
        "ipAddress": "string"
      }
      ...
    ]
```

`hostname`

タイプ: 文字列

必須: はい (`extraHosts` を使用する場合)

`/etc/hosts` エントリで使用するホスト名。

`ipAddress`

タイプ: 文字列

必須: はい (`extraHosts` を使用する場合)

`/etc/hosts` エントリで使用する IP アドレス。

ストレージとログ記録

`readonlyRootFilesystem`

タイプ: ブール値

必須: いいえ

このパラメータが true のとき、コンテナはそのルートファイルシステムへの読み取り専用アクセスを許可されます。このパラメータは docker create-container コマンドの `ReadonlyRootfs` にマッピングされ、`--read-only` オプションは docker run にマッピングされます。

> **Note**
> このパラメータは Windows コンテナではサポートされません。

デフォルト: `false`。

```
"readonlyRootFilesystem": true|false
```

mountPoints

タイプ: オブジェクト配列

必須: いいえ

コンテナでのデータボリュームのマウントポイント。このパラメータは creat-container Docker API の Volumes にマッピングされ、docker run の --volume オプションにマッピングされます。

Windows コンテナは $env:ProgramData と同じドライブに全部のディレクトリをマウントできます。Windows コンテナは、別のドライブにディレクトリをマウントすることはできません。また、マウントポイントは複数のドライブにまたがることはできません。Amazon EBS ボリュームを Amazon ECS タスクに直接アタッチするには、マウントポイントを指定する必要があります。

sourceVolume

タイプ: 文字列

必須: はい (mountPoints を使用する場合)

マウントするボリュームの名前。

containerPath

型: 文字列

必須: はい (mountPoints を使用する場合)

ボリュームをマウントするコンテナ内のパス。

readOnly

型: ブール値

必須: いいえ

この値が true の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が false の場合、コンテナはボリュームに書き込むことができます。デフォルト値は false です。

Windows オペレーティングシステムを実行している EC2 インスタンスで実行されるタスクの場合、 値をデフォルト の `false` のままにします。

`volumesFrom`

タイプ: オブジェクト配列

必須: いいえ

別コンテナからマウントするデータボリューム。このパラメータは docker create-container コマンドの `VolumesFrom` にマッピングされ、`--volumes-from` オプションは docker run にマッピングされます。

`sourceContainer`

タイプ: 文字列

必須: はい (`volumesFrom` を使用する場合)

ボリュームのマウント元のコンテナの名前。

`readOnly`

タイプ: ブール値

必須: いいえ

この値が `true` の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が `false` の場合、コンテナはボリュームに書き込むことができます。デフォルト値は `false` です。

```
"volumesFrom": [
                {
                  "sourceContainer": "string",
                  "readOnly": true|false
                }
              ]
```

`logConfiguration`

タイプ: LogConfiguration オブジェクト

必須: いいえ

コンテナに対するログ構成の仕様です。

ログ設定を使用したタスク定義の例については、「Amazon ECS のタスク定義の例」を参照してください。

このパラメータは docker create-container コマンドの LogConfig にマッピングされ、--log-driver オプションは docker run にマッピングされます。デフォルトでは、コンテナは Docker デーモンで使用されるのと同じロギングドライバーを使用します。ただし、コンテナ定義の中で、このパラメータによりログドライバーを指定することで、Docker デーモンとは異なるログドライバーをコンテナに使用させることも可能です。コンテナに異なるロギングドライバーを使用するには、コンテナインスタンス (またはリモートログ記録オプションの別のログサーバー) でログシステムを適切に設定する必要があります。

コンテナのログ設定を指定する際には、以下の点に注意してください。

- 現在、Amazon ECS では Docker デーモンに使用可能なログドライバーがいくつかサポートされています。Amazon ECS コンテナエージェントの今後のリリースで他のログドライバーが追加される可能性があります。
- このパラメータを使用するには、コンテナインスタンスで Docker Remote API のバージョン 1.18 以降が必要です。
- 追加のソフトウェアは、タスクの外部にインストールする必要があります。例えば、Fluentd 出力アグリゲータであるか、Gelf ログの送信先として Logstash を実行しているリモートホストです。

```
"logConfiguration": {
      "logDriver": "awslogs","fluentd","gelf","json-
file","journald","logentries","splunk","syslog","awsfirelens",
      "options": {"string": "string"
        ...},
 "secretOptions": [{
  "name": "string",
  "valueFrom": "string"
 }]
}
```

`logDriver`

タイプ: 文字列

有効な値: `"awslogs","fluentd","gelf","json-file","journald","logentries","splunk","syslog","awsfirelens"`

必須: はい (`logConfiguration` を使用する場合)

コンテナに使用するログドライバー。デフォルトでは、上記の有効な値は Amazon ECS コンテナエージェントが通信できるログドライバーです。

サポートされているログドライバーは `awslogs`、`splunk`、`awsfirelens` です。

タスク定義で `awslogs` ログドライバーを使用してコンテナログを CloudWatch Logs に送信する方法については、「Amazon ECS ログを CloudWatch に送信する 」を参照してください。

`awsfirelens` ログドライバーの使用の詳細については、「カスタムログのルーティング」を参照してください。

> **Note**
>
> 上記に示されていないカスタムドライバーがある場合、GitHub で入手できる Amazon ECS コンテナエージェントプロジェクトを fork し、そのドライバーを使用するようにカスタマイズできます。含めたい変更については、プルリクエストを送信することをお勧めします。ただし、現時点では、このソフトウェアの変更されたコピーの実行はサポートされていません。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.18 以上を使用する必要があります。

`options`

型: 文字列から文字列へのマップ

必須: いいえ

ログドライバーに送信する設定オプションの Key-Value マップ。

指定できるオプションは、ログドライバーに応じて異なります。`awslogs` ルーターを使用して Amazon CloudWatch にログをルーティングするときに指定できるオプションには、以下が含まれます。

`awslogs-create-group`

必須: いいえ

ロググループを自動的に作成させるかどうかを指定します。このオプションを指定しない場合、デフォルトは `false` です。

> **Note**
>
> `awslogs-create-group` を使用する前に、IAM ポリシーにはアクセス許可 `logs:CreateLogGroup` が含まれている必要があります。

`awslogs-region`

必須: はい

`awslogs` ログドライバが Docker ログを送信する先の、AWS リージョン を指定します。CloudWatch Logs では、異なるリージョンのクラスターからすべてのログを 1 つのリージョンに送信するように選択できます。これにより、すべてのログを一元的な場所で確認できるようになります。他にも、リージョンごとにそれらを分離して、より細分化することが可能です。このオプションで指定するリージョンに、対象のロググループが存在することを確認してください。

`awslogs-group`

必須: はい

`awslogs` ログドライバーがログストリームを送信する先の、ロググループを指定する必要があります。

`awslogs-stream-prefix`

必須: はい

指定したプレフィックス、コンテナ名、コンテナが属する Amazon ECS タスクの ID にログストリームを関連付けるには、`awslogs-stream-prefix` オプションを使用します。このオプションでプレフィックスを指定した場合、ログストリームの形式は以下のようになります。

```
prefix-name/container-name/ecs-task-id
```

このオプションでプレフィックスを指定しない場合、ログストリームには、コンテナインスタンスの Docker デーモンによって割り当てられたコンテナ ID に基づいた名前が付けられます。Docker コンテナ ID (コンテナインスタンスでのみ使用可能) だけでそのログを送

信したコンテナを追跡するのは難しいため、このオプションでプレフィックスを指定することをお勧めします。

Amazon ECS サービスでは、サービス名をプレフィックスとして使用できます。これにより、コンテナが属するサービスへのログストリームと、それを送信したコンテナの名前、そのコンテナが所属するタスクの ID を追跡できます。

Amazon ECS コンソールを使用する際に [Log] ペインにログを表示するためには、ログのストリームプレフィックスを指定する必要があります。

`awslogs-datetime-format`

必須: いいえ

このオプションは、Python `strftime` 形式で複数行起動パターンを定義します。ログメッセージは、パターンに一致する 1 行と、それに続くパターンに一致しない行で構成されます。一致する 1 行とは、ログメッセージ間の区切りです。

この形式を使用する場合のユースケースの例としては、スタックダンプなどの解析された出力があり、これを使用しなければ、複数のエントリに記録されることになります。適切なパターンにより、単一のエントリにキャプチャさせます。

詳細については、awslogs-datetime-formatを参照してください。

`awslogs-datetime-format` と `awslogs-multiline-pattern` オプションの両方を設定することはできません。

> **Note**
>
> 複数行のログ記録は、すべてのログメッセージの正規表現の解析とマッチングを実行します。これによりログ記録のパフォーマンスに悪影響が及ぶ可能性があります。

`awslogs-multiline-pattern`

必須: いいえ

このオプションでは、正規表現を使用する複数行起動パターンを定義します。ログメッセージは、パターンに一致する 1 行と、それに続くパターンに一致しない行で構成されます。一致する 1 行とは、ログメッセージ間の区切りです。

詳細については、「awslogs-multiline-pattern」を参照してください。

awslogs-datetime-format も設定されている場合は、このオプションは無視されます。

awslogs-datetime-format と awslogs-multiline-pattern オプションの両方を設定することはできません。

> **Note**
>
> 複数行のログ記録は、すべてのログメッセージの正規表現の解析とマッチングを実行します。これによりログ記録のパフォーマンスに悪影響が及ぶ可能性があります。

mode

必須: いいえ

有効な値: non-blocking | blocking

このオプションは、コンテナから awslogs ログドライバーへのログメッセージの配信モードを定義します。選択した配信モードは、コンテナからンテナーからのログの流れが中断されたときのアプリケーションの可用性に影響します。

blocking モードを使用しており、CloudWatch へのログのフローが中断されると、stdout ストリームと stderr ストリームに書き込むためのコンテナコードからの呼び出しがブロックされます。その結果、アプリケーションのロギングスレッドがブロックされます。これにより、アプリケーションが応答しなくなり、コンテナのヘルスチェックが失敗する可能性があります。

non-blocking モードを使用する場合、コンテナのログは代わりに max-buffer-size オプションで設定されたメモリ内の中間バッファに保存されます。これにより、ログを CloudWatch に送信できない場合にアプリケーションが応答しなくなるのを防ぎます。サービスの可用性を確保したいが、多少のログ損失があっても問題ない場合は、このモードを使用することをおすすめします。詳細については、「Preventing log loss with non-blocking mode in the awslogs container log driver」を参照してください。

max-buffer-size

必須: いいえ

デフォルト値: 1m

non-blocking モードが使用されている場合、max-buffer-size ログオプションは、中間メッセージ用のストレージに使用されるバッファのサイズを制御します。アプリケーションに基づいて、必ず適切なバッファサイズを指定してください。バッファがいっぱいになると、それ以上ログを保存できなくなります。保存できないログは失われます。

splunk ログルーターを使用してログをルーティングするには、splunk-token と splunk-url を指定する必要があります。

ログの保存と分析のための AWS のサービス または AWS Partner Network を送信先としたログのルーティングに awsfirelens ログルーターを使用するときは、log-driver-buffer-limit オプションを設定して、イベントがログルーターコンテナに送信される前に、メモリでバッファリングされるイベントの数を制限できます。この制限は、スループットが高い場合に発生する可能性がある、Docker 内のバッファのメモリ不足による、潜在的なログ損失の問題を解決するのに役立ちます。詳細については、「the section called “高スループットのログの設定”」を参照してください。

awsfirelens を使用してログをルーティングするときに指定できるその他のオプションは、送信先に応じて異なります。Amazon Data Firehose にログをエクスポートするときは、region を使用して AWS リージョンを指定し、delivery_stream を使用してログストリームの名前を指定することができます。

Amazon Kinesis Data Streams にログをエクスポートするときは、region を使用して AWS リージョンを指定し、stream を使用してデータストリーム名を指定することができます。

Amazon OpenSearch Service にログをエクスポートするときは、Name、Host (プロトコルを使用しない OpenSearch Service エンドポイント)、Port、Index、Type、Aws_auth、Aws_region、Suppress_Type_Name、および tls といったオプションを指定できます。

Amazon S3 にログをエクスポートするときは、bucket オプションを使用してバケットを指定できます。また、region、total_file_size、upload_timeout、および use_put_object をオプションとして指定することもできます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.19 以上を使用する必要があります。

secretOptions

タイプ: オブジェクト配列

必須: いいえ

ログ設定に渡すシークレットを示すオブジェクト。ログ構成で使用されるシークレットには、認証トークン、証明書、または暗号化キーを含められます。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

name

型: 文字列

必須: はい

コンテナの環境変数として設定する値。

valueFrom

型: 文字列

必須: はい

コンテナのログ設定に公開するシークレット。

```
"logConfiguration": {
 "logDriver": "splunk",
 "options": {
  "splunk-url": "https://cloud.splunk.com:8080",
  "splunk-token": "...",
  "tag": "...",
  ...
 },
 "secretOptions": [{
  "name": "splunk-token",
  "valueFrom": "/ecs/logconfig/splunkcred"
 }]
}
```

firelensConfiguration

タイプ: FirelensConfiguration オブジェクト

必須: いいえ

コンテナの FireLens 構成。これは、コンテナログのログルーターの指定と設定に使用されます。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。

```
{
    "firelensConfiguration": {
        "type": "fluentd",
        "options": {
            "KeyName": ""
        }
    }
}
```

options

型: 文字列間のマッピング

必須: いいえ

ログルーターの設定時に使用するオプションの Key-Value マップ。このフィールドはオプションで、カスタム設定ファイルを指定するか、タスク、タスク定義、クラスター、コンテナインスタンスの詳細などのメタデータを口グイベントに追加するために使用できます。指定した場合、使用する構文は "options":{"enable-ecs-log-metadata":"true|false","config-file-type:"s3|file","config-file-value":"arn:aws:s3:::*amzn-s3-demo-bucket*/fluent.conf|filepath"} です。詳細については、「Amazon ECS タスク定義の例: FireLens に口グをルーティングする」を参照してください。

type

型: 文字列

必須: はい

使用する口グルーター。有効な値は fluentd または fluentbit です。

セキュリティ

コンテナセキュリティの詳細については、「Amazon ECS タスクおよびコンテナ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。

credentialSpecs

タイプ: 文字列配列

必須: いいえ

Active Directory 認証用のコンテナを設定する認証情報仕様 (CredSpec) ファイルへの SSM または Amazon S3 の ARN のリスト。dockerSecurityOptions の代わりに、このパラメータを使用することをお勧めします。ARN の最大数は 1 です。

各 ARN には 2 つの形式があります。

credentialspecdomainless:MyARN

Secrets Manager にシークレットの追加セクションを持つ CredSpec を提供するために credentialspecdomainless:MyARN を使用します。シークレットでドメインへのログイン認証情報を指定します。

任意のコンテナインスタンスで実行される各タスクは、異なるドメインに参加できます。

この形式は、コンテナインスタンスをドメインに結合しなくても使用できます。

credentialspec:MyARN

単一ドメインに対して CredSpec を提供するために credentialspec:MyARN を使用します。

このタスク定義を使用するタスクを開始する前に、コンテナインスタンスをドメインに参加させる必要があります。

どちらの形式でも、SSM または Amazon S3 で MyARN を ARN に置き換えます。

credspec は、ユーザー名、パスワード、接続先のドメインを含むシークレットの ARN を Secrets Manager に提供する必要があります。セキュリティ向上のため、インスタンスはドメインレス認証のドメインに参加しません。インスタンス上の他のアプリケーションは、ドメインレス認証情報を使用できません。このパラメータを使用すると、タスクが別のドメインに参加する必要がある場合でも、同じインスタンスでタスクを実行できます。詳細については、「Windows コンテナでの gMSAs の使用」および「Linux コンテナ向け gMSAs を使用する」を参照してください。

user

タイプ: 文字列

必須: いいえ

コンテナ内で使用するユーザー。このパラメータは docker create-container コマンドの User にマッピングされ、--user オプションは docker run にマッピングされます。

> **Important**
>
> host ネットワークモードを使用してタスクを実行する場合は、ルートユーザー (UID 0) を使用してコンテナを実行しないでください。セキュリティのベストプラクティスとしては、常にルート以外のユーザーを使用します。

以下の形式を使用して、user を指定できます。UID または GID を指定する場合は、正の整数として指定する必要があります。

- user
- user:group
- uid
- uid:gid
- user:gid
- uid:group

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"user": "string"
```

リソースの制限

ulimits

タイプ: オブジェクト配列

必須: いいえ

コンテナに定義する ulimit 値の一覧。この値は、オペレーティングシステムのデフォルトのリソースクォータ設定を上書きします。このパラメータは docker create-container コマンドの Ulimits にマッピングされ、--ulimit オプションは docker run にマッピングされます。

Fargate でホストされる Amazon ECS タスクは、オペレーションシステムで設定されたデフォルトのリソース制限値を使用します。ただし、nofile リソース制限パラメータを除きま

す。nofile リソース制限は、コンテナが使用できるオープンファイルの数の制限を設定します。Fargate では、デフォルトの nofile ソフト制限は　65535 で、ハード制限は 65535 です。両方の制限の値を設定できます (最大 1048576)。詳細については、「タスクリソースの制限」を参照してください。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.18 以上を使用する必要があります。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"ulimits": [
      {
        "name":
 "core"|"cpu"|"data"|"fsize"|"locks"|"memlock"|"msgqueue"|"nice"|"nofile"|"nproc"|"rss"|"rtp
        "softLimit": integer,
        "hardLimit": integer
      }
      ...
    ]
```

name

タイプ: 文字列

有効な値: "core" | "cpu" | "data" | "fsize" | "locks" | "memlock" | "msgqueue" | "nice" | "nofile" | "nproc" | "rss" | "rtprio" | "rttime" | "sigpending" | "stack"

必須: はい (ulimits を使用する場合)

ulimit の type。

hardLimit

タイプ: 整数

必須: はい (ulimits を使用する場合)

ulimit タイプのハード制限。値は、ulimit の type に応じて、バイト、秒、またはカウントとして指定できます。

softLimit

タイプ: 整数

必須: はい (ulimits を使用する場合)

ulimit タイプのソフト制限。値は、ulimit の type に応じて、バイト、秒、またはカウントとして指定できます。

Docker のラベル

dockerLabels

型: 文字列から文字列へのマップ

必須: いいえ

コンテナに追加するラベルのキー/値マップ。このパラメータは docker create-container コマンドの Labels にマッピングされ、--label オプションは docker run にマッピングされます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.18 以上を使用する必要があります。

```
"dockerLabels": {"string": "string"
      ...}
```

その他のコンテナ定義のパラメータ

以下のコンテナ定義パラメータは、[Configure via JSON] (JSON による設定) オプションを使用して、Amazon ECS コンソールでタスク定義を登録する際に使用できます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

トピック

- Linux パラメータ
- コンテナの依存関係
- [コンテナのタイムアウト]

- システムコントロール
- インタラクティブ
- 擬似ターミナル

Linux パラメータ

`linuxParameters`

型: LinuxParameters オブジェクト

必須: いいえ

KernelCapabilities など、コンテナに適用される Linux 固有のオプション。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"linuxParameters": {
      "capabilities": {
        "add": ["string", ...],
        "drop": ["string", ...]
        }
      }
```

`capabilities`

型: KernelCapabilities オブジェクト

必須: いいえ

Docker によって提供されているデフォルト設定から削除されたコンテナ用の Linux 機能。これらの Linux 機能の詳細については、Linux マニュアルページの「機能 (7)」を参照してください。

`add`

タイプ: 文字列配列

有効な値: `"SYS_PTRACE"`

必須: いいえ

Docker によって提供されているデフォルト設定のコンテナに追加する Linux 機能。このパラメータは docker create-container コマンドの `CapAdd` にマッピングされ、`--cap-add` オプションは docker run にマッピングされます。

`drop`

タイプ: 文字列配列

有効な値: `"ALL" | "AUDIT_CONTROL" | "AUDIT_WRITE" | "BLOCK_SUSPEND" | "CHOWN" | "DAC_OVERRIDE" | "DAC_READ_SEARCH" | "FOWNER" | "FSETID" | "IPC_LOCK" | "IPC_OWNER" | "KILL" | "LEASE" | "LINUX_IMMUTABLE" | "MAC_ADMIN" | "MAC_OVERRIDE" | "MKNOD" | "NET_ADMIN" | "NET_BIND_SERVICE" | "NET_BROADCAST" | "NET_RAW" | "SETFCAP" | "SETGID" | "SETPCAP" | "SETUID" | "SYS_ADMIN" | "SYS_BOOT" | "SYS_CHROOT" | "SYS_MODULE" | "SYS_NICE" | "SYS_PACCT" | "SYS_PTRACE" | "SYS_RAWIO" | "SYS_RESOURCE" | "SYS_TIME" | "SYS_TTY_CONFIG" | "SYSLOG" | "WAKE_ALARM"`

必須: いいえ

Docker によって提供されているデフォルト設定のコンテナから削除する Linux 機能。このパラメータは docker create-container コマンドの `CapDrop` にマッピングされ、`--cap-drop` オプションは docker run にマッピングされます。

`devices`

コンテナに公開するすべてのホストデバイス。このパラメータは docker create-container コマンドの `Devices` にマッピングされ、`--device` オプションは docker run にマッピングされます。

> **Note**
>
> Fargate 起動タイプを使用する場合、`devices` パラメータはサポートされません。

型: デバイスオブジェクト配列

必須: いいえ

`hostPath`

ホストコンテナインスタンス上のデバイスのパス。

型: 文字列

必須: はい

`containerPath`

ホストデバイスを公開する先のコンテナ内のパス。

タイプ: 文字列

必須: いいえ

`permissions`

デバイス用のコンテナに提供する明示的な許可。デフォルトでは、コンテナにはデバイスの `read`、`write`、および `mknod` のアクセス許可があります。

タイプ: 文字列の配列

有効な値: `read` | `write` | `mknod`

`initProcessEnabled`

信号を転送しプロセスを利用するコンテナ内で、`init` を実行。このパラメータは docker run の `--init` オプションにマッピングされます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.25 以上を使用する必要があります。

`maxSwap`

このパラメータは、Fargate で実行されるタスクではサポートされません。

コンテナが使用できるスワップメモリの合計 (MiB 単位)。このパラメータは、docker run の `--memory-swap` オプションに変換されます。値はコンテナメモリの合計に `maxSwap` の値を加えた値です。

`0` の `maxSwap` 値を指定した場合、コンテナはスワップを使用しません。許容値は、`0` または任意の正の整数です。`maxSwap` パラメータを省略すると、コンテナは実行中のコンテナイン

スタンスのスワップ設定を使用します。swappiness パラメータを使用するには、maxSwap 値を設定する必要があります。

`sharedMemorySize`

/dev/shm ボリュームのサイズ値 (MiB) です。このパラメータは docker run の --shm-size オプションにマッピングされます。

> **Note**
>
> Fargate 起動タイプを使用するタスクを使用している場合、sharedMemorySize パラメータはサポートされません。

タイプ: 整数

`tmpfs`

tmpfs マウントのコンテナパス、マウントオプション、および最大サイズ (MiB) です。このパラメータは docker run の --tmpfs オプションにマッピングされます。

> **Note**
>
> Fargate 起動タイプを使用するタスクを使用している場合、tmpfs パラメータはサポートされません。

型: Tmpfs オブジェクト配列

必須: いいえ

`containerPath`

tmpfs ボリュームがマウントされる絶対ファイルパスです。

タイプ: 文字列

必須: はい

`mountOptions`

tmpfs ボリュームのマウントオプションのリストです。

タイプ: 文字列の配列

必須: いいえ

有効な値: `"defaults" | "ro" | "rw" | "suid" | "nosuid" | "dev" | "nodev" | "exec" | "noexec" | "sync" | "async" | "dirsync" | "remount" | "mand" | "nomand" | "atime" | "noatime" | "diratime" | "nodiratime" | "bind" | "rbind" | "unbindable" | "runbindable" | "private" | "rprivate" | "shared" | "rshared" | "slave" | "rslave" | "relatime" | "norelatime" | "strictatime" | "nostrictatime" | "mode" | "uid" | "gid" | "nr_inodes" | "nr_blocks" | "mpol"`

`size`

tmpfs ボリュームの最大サイズ (MiB) です。

タイプ: 整数

必須: はい

コンテナの依存関係

`dependsOn`

型: ContainerDependency オブジェクトの配列

必須: いいえ

コンテナの起動と停止に定義されている依存関係。コンテナには複数の依存関係を含めることができます。依存関係がコンテナの起動に対して定義されている場合、コンテナの停止の場合、依存関係は逆になります。例については、「コンテナの依存関係」を参照してください。

> **Note**
>
> あるコンテナが依存関係における制限事項を満たさない場合、または制限を満たす前にタイムアウトした場合、Amazon ECS は、依存関係にある他のコンテナの状態も次に遷移させることはしません。

このパラメータでは、タスクまたはサービスがプラットフォームバージョン `1.3.0` 以降(Linux または `1.0.0`) を使用している必要があります。

```
"dependsOn": [
    {
        "containerName": "string",
        "condition": "string"
    }
]
```

containerName

タイプ: 文字列

必須: はい

コンテナ名が指定された条件を満たしている必要があります。

condition

型: 文字列

必須: はい

コンテナの依存関係の条件です。使用可能な条件とその動作を以下に示します。

- START - この条件は、すぐに現在のリンクとボリュームの動作を工ミュレートします。この条件は、他のコンテナの開始を許可する前に、依存コンテナが開始されていることを検証します。
- COMPLETE - この条件は、他のコンテナの開始を許可する前に、依存コンテナの実行が完了 (終了) することを検証します。これは、スクリプトを実行して終了するだけの、重要性の低いコンテナのために便利です。この条件は、必須コンテナには設定できません。
- SUCCESS - この条件は COMPLETE と同じですが、コンテナが zero ステータスで終了していることも必要です。この条件は、必須コンテナには設定できません。
- HEALTHY — この条件は、他のコンテナの開始を許可する前に、依存コンテナがそのコンテナのヘルスチェックに合格したことを検証します。これには、タスク定義に設定されているヘルスチェックが依存コンテナにある必要があります。タスクの起動時にのみ、この条件が確認されます。

[コンテナのタイムアウト]

startTimeout

タイプ: 整数

必須: いいえ

値の例: 120

コンテナの依存関係解決の再試行を止めるまでの待機時間 (秒)。

例えば、タスク定義内に 2 つのコンテナを指定するとします。containerA は、COMPLETE、SUCCESS、または HEALTHY のいずれかのステータスに到達する containerB に依存関係を持ちます。startTimeout の値に containerB が指定されていて、コンテナが時間内に目標のステータスまで到達しない場合、containerA は開始しません。

> **Note**
>
> あるコンテナが依存関係における制限事項を満たさない場合、または制限を満たす前にタイムアウトした場合、Amazon ECS は、依存関係にある他のコンテナの状態も次に遷移させることはしません。

このパラメータでは、タスクまたはサービスがプラットフォームバージョン 1.3.0 以降 (Linux) を使用している必要があります。最大値は 120 秒です。

stopTimeout

タイプ: 整数

必須: いいえ

値の例: 120

コンテナが正常に終了しなかった場合にコンテナが強制終了されるまでの待機時間 (秒)。

このパラメータでは、タスクまたはサービスがプラットフォームバージョン 1.3.0 以降 (Linux) を使用している必要があります。このパラメータを指定しない場合には、デフォルト値の 30 秒が適用されます。最大値は 120 秒です。

システムコントロール

systemControls

型: SystemControl オブジェクト

必須: いいえ

コンテナ内で設定する名前空間カーネルパラメータのリスト。このパラメータは docker create-container コマンドの Sysctls にマッピングされ、--sysctl オプションは docker run にマッピングされます。例えば、接続をより長く維持するように net.ipv4.tcp_keepalive_time 設定を構成できます。

awsvpc または host ネットワークモードも使用する単一のタスクで、複数のコンテナに対してネットワーク関連の systemControls パラメータを指定することは推奨されません。これを行うと、次のような欠点があります。

- systemControls をいずれかのコンテナ用に設定した場合、タスク内のすべてのコンテナに適用されます。単一のタスクの複数のコンテナに対して異なる systemControls を設定すると、最後に開始されたコンテナによって、有効になる systemControls が決定します。

タスク内でコンテナに使用するため IPC リソース名前空間を設定している場合、システムコントロールには以下の条件が適用されます。詳細については、「IPC モード」を参照してください。

- host IPC モードを使用するタスクの場合、IPC 名前空間の systemControls はサポートされていません。
- task IPC モードを使用するタスクでは、IPC 名前空間の systemControls 値が、タスク内のすべてのコンテナに適用されます。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

> **Note**
>
> このパラメータは、プラットフォームバージョン 1.4.0 以降 (Linux) を使用する場合に、AWS Fargate でホストされたタスクでのみサポートされます。このパラメータは Fargate 上の Windows コンテナではサポートされません。

```
"systemControls": [
    {
        "namespace":"string",
        "value":"string"
```

```
    }
]
```

namespace

タイプ: 文字列

必須: いいえ

value を設定する名前空間カーネルパラメータ。

有効な IPC 名前空間の値: "fs.mqueue.*" で開始する "kernel.msgmax" | "kernel.msgmnb" | "kernel.msgmni" | "kernel.sem" | "kernel.shmall" | "kernel.shmmax" | "kernel.shmmni" | "kernel.shm_rmid_forced"、および Sysctls

有効なネットワーク名前空間値: "net.*" で始まる Sysctls。Fargate では、コンテナ内に存在する名前空間 Sysctls のみが受け入れられます。

これらの値はすべて Fargate でサポートされています。

value

タイプ: 文字列

必須: いいえ

namespace で指定された名前空間カーネルパラメータの値。

インタラクティブ

interactive

型: ブール値

必須: いいえ

このパラメータが true の場合、stdin または tty を割り当てる必要がある、コンテナ化されたアプリケーションをデプロイすることができます。このパラメータは docker create-container コマンドの OpenStdin にマッピングされ、--interactive オプションは docker run にマッピングされます。

デフォルト: `false`。

擬似ターミナル

`pseudoTerminal`

タイプ: ブール値

必須: いいえ

このパラメータが `true` の場合、TTY が割り当てられます。このパラメータは docker create-container コマンドの `Tty` にマッピングされ、`--tty` オプションは docker run にマッピングされます。

デフォルト: `false`。

Elastic Inference アクセラレーター名

タスク定義用の Elastic Inference アクセラレーターのリソース要件。

> **Note**
>
> Amazon Elastic Inference (EI) は利用できなくなりました。

以下のパラメータをタスク定義で使用できます。

`deviceName`

タイプ: 文字列

必須: はい

Elastic Inference アクセラレーターのデバイス名。`deviceName` は、コンテナ定義でも参照されます。`Elastic Inference accelerator` を参照してください。

`deviceType`

タイプ: 文字列

必須: はい

使用する Elastic Inference アクセラレーター。

プロキシ設定

`proxyConfiguration`

タイプ: ProxyConfiguration オブジェクト

必須: いいえ

App Mesh プロキシ設定の詳細。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"proxyConfiguration": {
    "type": "APPMESH",
    "containerName": "string",
    "properties": [
        {
           "name": "string",
           "value": "string"
        }
    ]
}
```

`type`

型: 文字列

重要な値: APPMESH

必須: いいえ

プロキシのタイプ。APPMESH はサポートされる唯一の値です。

`containerName`

型: 文字列

必須: はい

App Mesh プロキシとして機能するコンテナの名前です。

`properties`

タイプ: パラメータオブジェクトの配列

必須: いいえ

Container Network Interface(CNI) プラグインを提供するネットワーク構成パラメータのセットで、キーと値のペアとして指定されます。

- `IgnoredUID` - (必須) コンテナ定義の `user` パラメータで定義されるプロキシコンテナのユーザー ID (UID)。これは、プロキシがそれ自体のトラフィックを無視するようにするために使用されます。`IgnoredGID` を指定した場合は、このフィールドは空にできます。
- `IgnoredGID` - (必須) コンテナ定義の `user` パラメータで定義されるプロキシコンテナのグループ ID (GID)。これは、プロキシがそれ自体のトラフィックを無視するようにするために使用されます。`IgnoredUID` を指定した場合は、このフィールドは空にできます。
- `AppPorts` - (必須) アプリケーションが使用するポートのリスト。これらのポートへのネットワークトラフィックは `ProxyIngressPort` および `ProxyEgressPort` に転送されます。
- `ProxyIngressPort` - (必須) `AppPorts` への着信トラフィックが誘導されるポートを指定します。
- `ProxyEgressPort` - (必須) `AppPorts` からの発信トラフィックが誘導されるポートを指定します。
- `EgressIgnoredPorts` – (必須) 指定されたこれらのポートに向かうアウトバウンドトラフィックは無視され、`ProxyEgressPort` にリダイレクトされません。空のリストを指定できます。
- `EgressIgnoredIPs` – (必須) 指定されたこれらの IP アドレスに向かうアウトバウンドトラフィックは無視され、`ProxyEgressPort` にリダイレクトされません。空のリストを指定できます。

`name`

型: 文字列

必須: いいえ

キーと値のペアの名前。

`value`

型: 文字列

必須: いいえ

キーと値のペアの値。

ボリューム

タスク定義を登録する際、コンテナインスタンスの Docker デーモンに渡されるボリュームのリストを任意で指定することができます。すると、同じコンテナインスタンス上の他のコンテナで使用できるようになります。

使用できるデータボリュームの種類は以下のとおりです。

- Amazon EBS ボリューム – データ集約型のコンテナ化されたワークロード向けに、費用対効果が高く、耐久性があり、高性能なブロックストレージを提供します。スタンドアロンタスクを実行するとき、またはサービスを作成または更新するときに、Amazon ECS タスクごとに 1 つの Amazon EBS ボリュームをアタッチできます。Amazon EBS ボリュームは、Fargate でホストされている Linux タスクでサポートされています。詳細については、「Amazon ECS での Amazon EBS ボリュームの使用」を参照してください。
- Amazon EFS ボリューム - Amazon ECS タスクで使用するためのシンプルかつスケーラブルで、永続的なファイルストレージを提供します。Amazon EFSでは、ストレージ容量は伸縮性があります。この容量は、ファイルの追加や削除に伴い自動的に拡大および縮小されます。アプリケーションは、必要なときに必要なストレージを確保できます。Amazon EFS ボリュームは、Fargate でホストされるタスクでサポートされます。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。
- FSx for Windows File Server ボリューム – 完全マネージド型の Microsoft Windows ファイルサーバーを提供します。これらのファイルサーバは、Windows ファイルシステムによってバックアップされています。Amazon ECS と共に FSx for Windows File Server を使用する場合、永続的、分散型、共有型、および静的なファイルストレージを使用して、Windows タスクをプロビジョニングすることが可能です。詳細については、「Amazon ECS での FSx for Windows File Server ボリュームの使用」を参照してください。

  このオプションは Fargate の Windows コンテナではサポートされません。
- バインドマウント – ホストマシン上のファイルやディレクトリがコンテナにマウントされます。バインドマウントホストボリュームは、タスク実行時にサポートされます。バインドマウントのホ

ストボリュームを使用するには、タスク定義で host およびオプションの sourcePath 値を使用します。

詳細については、「Amazon ECS タスクのストレージオプション」を参照してください。

以下のパラメータをコンテナ定義で使用できます。

name

タイプ: 文字列

必須: いいえ

ボリュームの名前。最大 255 文字の英字 (大文字と小文字の区別あり)、数字、ハイフン (-)、アンダースコア (_) を使用できます。この名前は、コンテナ定義 mountPoints オブジェクトの sourceVolume パラメータで参照されます。

host

必須: いいえ

host パラメーターは、バインドマウントのライフサイクルを、タスクではなくホスト Amazon EC2 インスタンスと、それが格納されている場所に関連付けるために使用されます。host パラメーターが空の場合、Docker デーモンはデータボリュームのホストパスを割り当てますが、関連付けられたコンテナの実行が停止した後にデータが保持されるとは限りません。

Windows コンテナは $env:ProgramData と同じドライブに全部のディレクトリをマウントできます。

> **Note**
>
> sourcePath パラメータは、Amazon EC2 インスタンスでホストされているタスクを使用する場合にのみサポートされます。

sourcePath

タイプ: 文字列

必須: いいえ

host パラメータを使用する場合は、sourcePath を指定して、コンテナに表示されるホスト Amazon EC2 インスタンスのパスを宣言します。このパラメータが空の場合は、Docker デーモンによってホストパスが割り当てられます。host パラメータに sourcePath の場所が含まれている場合、データボリュームは手動で削除するまでホスト Amazon EC2 インスタンスの指定された場所に保持されます。sourcePath の値がホスト Amazon EC2 インスタンスに存在しない場合は、Docker デーモンによって作成されます。その場所が存在する場合は、ソースパスフォルダの内容がエクスポートされます。

configuredAtLaunch

型: ブール値

必須: いいえ

起動時にボリュームを設定可能にするかどうかを指定します。true に設定すると、スタンドアロンタスクを実行するとき、またはサービスを作成または更新するときにボリュームを設定できます。true に設定すると、タスク定義内で別のボリューム設定を提供することはできません。タスクにアタッチする Amazon EBS ボリュームを設定するには、このパラメータを true に設定する必要があります。configuredAtLaunch を true に設定し、ボリューム設定を起動フェーズに先送りすることで、ボリュームタイプや特定のボリューム設定に限定されないタスク定義を作成できます。こうすることで、タスク定義をさまざまな実行環境で再利用できるようになります。詳細については、「Amazon EBS ボリューム」を参照してください。

dockerVolumeConfiguration

タイプ: DockerVolumeConfiguration オブジェクト

必須: いいえ

このパラメータは、Docker ボリュームを使用する場合に指定します。Docker ボリュームは、EC2 インスタンスでタスクを実行する場合にのみサポートされます。Windows コンテナでは、local ドライバーの使用のみがサポートされます。バインドマウントを使用するには、代わりに host を指定します。

scope

型: 文字列

有効な値: task | shared

必須: いいえ

Docker ボリュームのスコープ。これにより、ボリュームのライフサイクルが決定されます。Docker ボリュームの範囲が `task` の場合は、タスクが開始すると自動的にプロビジョンされ、タスクが停止すると破棄されます。Docker ボリュームの範囲が `shared` の場合は、タスクの停止後も保持されます。

`autoprovision`

タイプ: ブール値

デフォルト値: `false`

必須: いいえ

この値が `true` の場合、既に存在していない場合は Docker ボリュームが作成されます。このフィールドは、`scope` が `shared` の場合にのみ使用されます。`scope` が `task` の場合、このパラメータは省略する必要があります。

`driver`

タイプ: 文字列

必須: いいえ

使用する Docker ボリュームドライバー。この名前はタスク配置に使用されるため、ドライバー値は Docker で提供されているドライバー名と一致する必要があります。ドライバーが Docker プラグイン CLI を使用してインストールされた場合は、`docker plugin ls` を使用してコンテナインスタンスからドライバー名を取得します。ドライバーが別の方法でインストール済みである場合は、Docker プラグイン検出を使用してドライバー名を取得します。

`driverOpts`

タイプ: 文字列

必須: いいえ

パススルーする Docker ドライバー固有のオプションのマップ。このパラメータは、Docker の「Create a volume」セクションの `DriverOpts` にマッピングされます。

`labels`

タイプ: 文字列

必須: いいえ

Docker ボリュームに追加するカスタムメタデータ。

`efsVolumeConfiguration`

タイプ: EFSVolumeConfiguration オブジェクト

必須: いいえ

このパラメータは、Amazon EFS ボリュームを使用する場合に指定します。

`fileSystemId`

型: 文字列

必須: はい

使用する Amazon EFS ファイルシステムの ID。

`rootDirectory`

型: 文字列

必須: いいえ

ホスト内にルートディレクトリとしてマウントする Amazon EFS ファイルシステム内のディレクトリ。このパラメータを省略すると、Amazon EFS ボリュームのルートが使用されます。/ を指定すると、このパラメータを省略した場合と同じ結果になります。

> **Important**
>
> `authorizationConfig` で EFS アクセスポイントが指定されている場合は、ルートディレクトリパラメータを省略するか / に設定して、EFS アクセスポイントにパスを設定する必要があります。

`transitEncryption`

タイプ: 文字列

有効な値: `ENABLED` | `DISABLED`

必須: いいえ

Amazon ECS ホストと Amazon EFS サーバー間で、転送中の Amazon EFS データの暗号化を有効にするかどうかを指定します。Amazon EFS IAM 認可を使用する場合は、転送中の暗号化を有効にする必要があります。このパラメータを省略すると、`DISABLED` のデフォル

ト値が使用されます。詳細については、Amazon Elastic ファイルシステムユーザーガイドの「転送中データの暗号化」を参照してください。

`transitEncryptionPort`

タイプ: 整数

必須: いいえ

Amazon ECS ホストと Amazon EFS サーバーとの間で、暗号化されたデータを送信するときに使用するポート。転送暗号化ポートを指定しない場合、タスクでは Amazon EFS マウントヘルパーが使用するポート選択戦略が使用されます。詳細については、Amazon Elastic File System User Guide] (Amazon Elastic File System ユーザーガイド) のEFS Mount Helper] (EFS マウントヘルパー) を参照してください。

`authorizationConfig`

タイプ: EFSAuthorizationConfig オブジェクト

必須: いいえ

Amazon EFS ファイルシステムに対する認可構成の詳細。

`accessPointId`

型: 文字列

必須: いいえ

使用するアクセスポイント ID。アクセスポイントが指定されている場合は、`efsVolumeConfiguration` のルートディレクトリ値を省略するか `/` に設定して、EFS アクセスポイントにパスを設定する必要があります。アクセスポイントを使用する場合は、`EFSVolumeConfiguration` で転送中の暗号化を有効にする必要があります。詳細については、Amazon Elastic ファイルシステムユーザーガイドのAmazon EFS アクセスポイントの使用を参照してください。

`iam`

型: 文字列

有効な値: `ENABLED` | `DISABLED`

必須: いいえ

タスク定義で定義した Amazon ECS タスクの IAM ロールを、Amazon EFS ファイルシステムのマウント時に使用するかどうかを指定します。使用する場合

は、EFSVolumeConfiguration で転送中の暗号化を有効にする必要があります。このパラメータを省略すると、DISABLED のデフォルト値が使用されます。詳細については、「タスク用の IAM ロール」を参照してください。

FSxWindowsFileServerVolumeConfiguration

タイプ: FSxWindowsFileServerVolumeConfiguration オブジェクト

必須: はい

このパラメータは、タスクストレージに Amazon FSx for Windows File Server ファイルシステムを使用する場合に指定します。

fileSystemId

タイプ: 文字列

必須: はい

使用する FSx for Windows File Server ファイルシステムID。

rootDirectory

型: 文字列

必須: はい

ホスト内にルートディレクトリとしてマウントする FSx for Windows File Server ファイルシステム内のディレクトリ。

authorizationConfig

credentialsParameter

型: 文字列

必須: はい

認可の認証情報オプション。

options:

- AWS Secrets Manager シークレットの Amazon リソースネーム (ARN)。
- AWS Systems Manager パラメータの ARN。

domain

タイプ: 文字列

必須: はい

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) ディレクトリまたはセルフホスト型 EC2 Active Directory によってホストされる完全修飾ドメイン名。

[タグ]

タスク定義の登録する際、タスク定義に適用されるメタデータタグをオプションで指定できます。タグは、タスク定義を分類して組織化するのに役立ちます。各タグは、キー、および値 (オプション) で構成されます。両方を定義します。詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。

> **Important**
>
> タグには、個人が特定可能な情報や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグは、多くの AWS のサービス (請求など) からアクセスできます。タグは、プライベートデータや機密データに使用することを意図していません。

タグオブジェクトでは、次のパラメータを使用できます。

`key`

タイプ: 文字列

必須: いいえ

タグを構成するキーと値のペアの一部。キーは、より具体的なタグ値のカテゴリのように動作する、一般的なラベルです。

`value`

タイプ: 文字列

必須: いいえ

タグを構成するキーと値のペアのオプションの一部。値はタグカテゴリ (キー) の記述子として機能します。

その他のタスク定義パラメータ

以下のタスク定義パラメータは、Amazon ECS コンソールから、[Configure via JSON (JSON による設定)] オプションを使用してタスク定義を登録する際に使用します。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

トピック

エフェメラルストレージ

`ephemeralStorage`

タイプ: EphemeralStorage オブジェクト

必須: いいえ

タスクに割り当てるエフェメラルストレージの容量(GB 単位)。このパラメーターは、AWS Fargate でホストされるタスクにおいて、利用可能なエフェメラルストレージの総量をデフォルトの容量を超えて拡張する際に使用します。詳細については、「the section called “バインドマウント”」を参照してください。

> **Note**
>
> このパラメータは、プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) でのみサポートされます。

IPC モード

`ipcMode`

このパラメータは、Fargate で実行されるタスクではサポートされません。

タイプ: 文字列

必須: いいえ

タスクのコンテナで使用する IPC リソースの名前空間。有効な値は host、task または none です。host が指定されている場合、同一のコンテナインスタンス上にある (host IPC モードを指定した) タスク内のすべてのコンテナは、ホスト Amazon EC2 インスタンスと同じ IPC リソースを共有します。task が指定されている場合、指定されたタスク内のすべてのコンテナは同じ IPC リソースを共有します。none が指定されている場合、タスクのコンテナ内の IPC リソースはプライベートです。タスク内またはコンテナインスタンスの他のコンテナと共有されることはありません。値を指定しない場合、IPC リソース名前空間の共有はコンテナインスタンスの Docker デーモンの設定によって異なります。

host IPC モードを使用する場合は、意図せず IPC 名前空間が公開されるリスクが高いことに注意してください。

タスク内のコンテナに、systemControls を使用して名前空間のカーネルパラメータを設定している場合は、以下の点が IPC リソース名前空間に適用されます。

- host IPC モードを使用するタスクの場合、systemControls に関連する IPC 名前空間はサポートされません。
- task IPC モードを使用するタスクでは、IPC 名前空間に関連する systemControls が、タスク内のすべてのコンテナに適用されます。

> **Note**
>
> このパラメータは、Windows コンテナ、または Fargate 起動タイプを使用するタスクではサポートされていません。

PID モード

pidMode

タイプ: 文字列

有効な値: host | task

必須: いいえ

タスクのコンテナで使用するプロセス名前空間。有効な値は host または task です。Linuxコンテナでは、有効な値は task のみです。例えば、サイドカーのモニタリングでは、pidMode が

同じタスクで実行されている他のコンテナに関する情報にアクセスする必要となる場合があります。

`task` が指定されている場合、指定したタスク内のすべてのコンテナは同じプロセス名前空間を共有します。

値が指定されていない場合、デフォルトは各コンテナのプライベート名前空間です。

> **Note**
>
> このパラメータは、プラットフォームバージョン `1.4.0` 以降 (Linux) を使用する場合に、AWS Fargate でホストされたタスクでのみサポートされます。このパラメータは Fargate 上の Windows コンテナではサポートされません。

フォールトインジェクション

`enableFaultInjection`

型: ブール値

有効な値: `true` | `false`

必須: いいえ

このパラメータが `true` に設定されている場合、タスクのペイロードで、Amazon ECS と Fargate はタスクのコンテナからのフォールトインジェクションリクエストを受け入れます。デフォルトでは、このパラメータは `false` に設定されます。

EC2 起動タイプの Amazon ECS タスク定義パラメータ

タスク定義は、タスクファミリー、AWS Identity and Access Management (IAM) タスクロール、ネットワークモード、コンテナ定義、ボリューム、タスク配置の制約、起動タイプの各部分に分かれています。ファミリとコンテナの定義は、タスク定義の必須項目です。これに対して、タスクロール、ネットワークモード、ボリューム、タスク配置の制約、起動タイプは省略することができます。

これらのパラメータを JSON ファイルで使用し、タスク定義を設定できます。

以下に示すのは、EC2 起動タイプの各タスク定義パラメータの詳細な説明です。

ファミリー

`family`

タイプ: 文字列

必須: はい

タスク定義を登録するときに、ファミリー (複数バージョンのタスク定義の名前のようなもの) を指定する必要があります。登録したタスク定義には、リビジョン番号が与えられます。特定のファミリーに登録した最初のタスク定義には、リビジョン 1 が与えられます。その後に登録したタスク定義には、連番でリビジョン番号が与えられます。

起動タイプ

タスク定義の登録時、Amazon ECS がタスク定義の検証基準となる起動タイプを指定できます。タスク定義が指定された互換性を検証しない場合、クライアント例外が返されます。詳しくは、「Amazon ECS 起動タイプ」を参照してください。

タスク定義では、以下のパラメータが使用できます。

`requiresCompatibilities`

タイプ: 文字列配列

必須: いいえ

有効な値: `EC2`

タスク定義が検証された起動タイプ。これにより、タスク定義で使用されているすべてのパラメータが、起動タイプの要件を満たしていることの確認処理が開始されます。

タスクロール

`taskRoleArn`

タイプ: 文字列

必須: いいえ

タスク定義を登録するときに、IAM ロールのタスクロールを割り当てて、タスクのコンテナに、関連するポリシーに指定された AWS API を呼び出すためのアクセス権限を付与できます。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

Amazon ECS に最適化された Windows Server AMI を起動する場合、Windows タスク向けの IAM ロールでは、`-EnableTaskIAMRole` オプションが設定されている必要があります。また、コンテナでは、この機能を利用するために一部の構成コードを実行する必要があります。詳細については、「Amazon EC2 Windows インスタンスの追加設定」を参照してください。

タスク実行ロール

`executionRoleArn`

タイプ: 文字列

必須: 条件による

ユーザーに代わって AWS API コールを実行するアクセス許可を Amazon ECS コンテナエージェントに付与するタスク実行ロールの Amazon リソースネーム (ARN)。

> **Note**
>
> タスク実行 IAM ロールは、タスクの要件に応じて必要です。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

ネットワークモード

`networkMode`

タイプ: 文字列

必須: いいえ

タスクのコンテナで使用する Docker ネットワークモード。Amazon EC2 Linux インスタンスでホストされている Amazon ECS タスクの場合、有効な値は `none`、`bridge`、`awsvpc`、`host` です。ネットワークモードが指定されていない場合、デフォルトのネットワークモードは `bridge` です。Amazon EC2 Windows インスタンスでホストされる Amazon ECS タスクの場合、有効な値は `default` と `awsvpc` です。ネットワークモードが指定されていない場合、`default` ネットワークモードが使用されます。

ネットワークモードに none を設定した場合、タスクのコンテナは外部への接続を持たないため、コンテナ定義でポートマッピングを指定することはできません。

ネットワークモードが bridge の場合、タスクはそのタスクをホストする各 Amazon EC2 インスタンス内で実行される、Linux 上の Docker の組み込み仮想ネットワークを使用します。Linux の組み込み仮想ネットワークでは、bridge Docker ネットワークドライバーが使用されます。

ネットワークモードが host の場合、タスクはそのタスクをホストする Amazon EC2 インスタンスの ENI にコンテナポートを直接マッピングすることで Docker の組み込み仮想ネットワークをバイパスする、ホストのネットワークを使用します。ダイナミックポートマッピングは、このネットワークモードでは使用できません。このモードを使用するタスク定義内のコンテナには、特定の hostPort 番号を指定する必要があります。ホストのポート番号は、複数のタスクで使用できません。その結果として、1 つの Amazon EC2 インスタンスで同じタスク定義のタスクを複数実行することはできません。

> **Important**
>
> host ネットワークモードをによりタスクを実行する場合、より良いセキュリティーのために、ルートユーザー (UID 0) を使用してコンテナを実行しないでください。セキュリティのベストプラクティスとしては、常にルート以外のユーザーを使用します。

ネットワークモードが awsvpc の場合は、タスクに Elastic Network Interface が割り当てられるため、タスク定義を使用したサービスの作成時またはタスクの実行時に NetworkConfiguration を指定する必要があります。詳細については、「EC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。

ネットワークモードが default の場合、タスクはそのタスクをホストする各 Amazon EC2 インスタンス内で実行される、Windows 上の Docker の組み込み仮想ネットワークを使用します。Windows の組み込み仮想ネットワークは nat Docker ネットワークドライバーを使用します。

host および awsvpc のネットワークモードは、Amazon EC2 のネットワークスタックを使用するので、コンテナのネットワークパフォーマンスが最大限発揮されます。host および awsvpc ネットワークモードにおいて公開されるコンテナポートは、対応するホストポート (host ネットワークモードの場合)、またはアタッチされた Elastic Network Interface ポート (awsvpc ネットワークモードの場合) に直接マッピングされます。このため、動的ホストポートマッピングは使用できません。

使用可能なネットワークモードは、基板となる EC2 インスタンスのオペレーティングシステムによって異なります。Linux の場合は、どのネットワークモードも使用できます。Windows の場合、default およびawsvpc モードを使用できます。

ランタイムプラットフォーム

operatingSystemFamily

タイプ: 文字列

必須: 条件による

デフォルト: LINUX

タスク定義を登録する際、オペレーティングシステムファミリを指定します。

有効な値
は、LINUX、WINDOWS_SERVER_2022_CORE、WINDOWS_SERVER_2022_FULL、WINDOWS_SERVER_2
および
WINDOWS_SERVER_2019_CORE、WINDOWS_SERVER_2016_FULL、WINDOWS_SERVER_2004_CORE、W
です。

サービスで使用されるすべてのタスク定義は、このパラメータに対して同じ値を設定する必要があります。

タスク定義がサービスの一部である場合、この値はサービスの platformFamily 値と一致する必要があります。

cpuArchitecture

タイプ: 文字列

必須: 条件による

デフォルト: X86_64

タスク定義を登録する際は、CPU アーキテクチャを指定します。有効な値は X86_64 および ARM64 です。

サービスで使用されるすべてのタスク定義は、このパラメータに対して同じ値を設定する必要があります。

Linux タスクがある場合は、値を ARM64 に設定できます。詳細については、「the section called "64 ビット ARM ワークロードでのタスク定義"」を参照してください。

タスクサイズ

タスク定義の登録時に、そのタスクが使用する CPU とメモリの合計量を指定できます。これは、コンテナ定義レベルの cpu および memory の値とは異なります。Amazon EC2 インスタンスでホストされるタスクの場合、これらのフィールドは省略可能です。

> **Note**
>
> タスクレベル CPU およびメモリのパラメータは Windows コンテナでは無視されます。Windows コンテナではコンテナレベルリソースを指定することをお勧めします。

`cpu`

タイプ: 文字列

必須: 条件による

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

タスクに適用される CPU ユニットのハード制限。JSON ファイルでは、CPU 値を CPU ユニットまたは仮想 CPU (vCPU) の文字列として指定できます。例えば、CPU 値を 1 vCPU (CPU ユニット) または 1024 (vCPU) として指定できます。タスク定義が登録されると、vCPU 値は、CPU ユニットを示す整数に変換されます。

このフィールドはオプションです。クラスターに、要求された CPU ユニットが利用できる登録済みのコンテナインスタンスがない場合、タスクは失敗します。サポートされている値は、0.125 vCPU から 192 vCPU までです。

`memory`

タイプ: 文字列

必須: 条件による

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

タスクに適用されるメモリのハード制限です。タスク定義のメモリの値は、メビバイト (MiB) またはギガバイト (GB) の文字列として指定できます。例えば、メモリの値を 3072 (MiB) または 3 GB (GB) のいずれかで指定できます。タスク定義が登録されると、GB 値は、MiB を示す整数に変換されます。

このフィールドはオプションです。任意の値を使用できます。タスクレベルでメモリ値が指定されている場合、コンテナレベルのメモリ値の設定は省略可能です。クラスターに、要求されたメモリが利用できる登録済みのコンテナインスタンスがない場合、タスクは失敗します。特定のインスタンスタイプについて、タスクにできるだけ多くのメモリを提供することで、リソースの使用率を最大化することができます。詳細については、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

コンテナ定義

タスク定義を登録するときは、コンテナインスタンスの Docker デーモンに渡されるコンテナ定義のリストを指定する必要があります。以下のパラメータをコンテナ定義で使用できます。

トピック

- 標準のコンテナ定義のパラメータ
- 詳細コンテナ定義パラメータ
- その他のコンテナ定義のパラメータ

標準のコンテナ定義のパラメータ

以下のタスク定義のパラメータは必須であるか、ほとんどのコンテナ定義で使用されます。

トピック

- 名前
- イメージ

- 「メモリ」
- ポートマッピング
- プライベートリポジトリの認証情報

名前

`name`

タイプ: 文字列

必須: はい

コンテナの名前。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコアを使用できます。タスク定義で複数のコンテナをリンクしている場合、あるコンテナの `name` を別のコンテナの `links` に入力できます。これにより、コンテナ同士を接続します。

イメージ

`image`

タイプ: 文字列

必須: はい

コンテナの開始に使用するイメージ。この文字列は Docker デーモンに直接渡されます。デフォルトでは、Docker Hub レジストリのイメージを使用できます。*`repository-url`*`/`*`image`*`:`*`tag`* または *`repository-url`*`/`*`image`*`@`*`digest`* で他のリポジトリを指定することもできます。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコア、コロン、ピリオド、スラッシュ、シャープ記号を使用できます。このパラメータは、docker create-container コマンドの `Image` と docker run コマンドの `IMAGE` パラメータにマッピングされます。

- 新しいタスクが開始されると、Amazon ECS コンテナエージェントは、指定されたイメージおよびタグの最新バージョンをプルしてコンテナで使用します。ただし、リポジトリイメージの後続の更新がすでに実行されているタスクに反映されることはありません。
- タスク定義のイメージパスでタグまたはダイジェストを指定しない場合、Amazon ECS コンテナエージェントは指定されたイメージの最新バージョンを取り込みます。
- ただし、リポジトリイメージの後続の更新がすでに実行されているタスクに反映されることはありません。

- プライベートレジストリのイメージがサポートされています。詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。
- Amazon ECR リポジトリのイメージは、`registry/repository:tag` または `registry/repository@digest` の完全な命名規則 (例えば、*aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-web-app*:*latest* や、*aws_account_id*.dkr.ecr.*region*.amazonaws.com/*my-web-app*@*sha256:94afd1f2e64d908bc90dbca0035a5b567EXAMPLE*) を使用して指定します。
- Docker Hub の公式リポジトリのイメージでは、1 つの名前 (例: ubuntu または mongo) を使用します。
- Docker Hub の他のリポジトリのイメージは、組織名で修飾されます (例: amazon/amazon-ecs-agent)。
- 他のオンラインリポジトリのイメージは、さらにドメイン名で修飾されます (例: quay.io/assemblyline/ubuntu)。

`versionConsistency`

タイプ: 文字列

有効な値: `enabled|disabled`

必須: いいえ

コンテナ定義で指定されたコンテナイメージタグを Amazon ECS がイメージダイジェストに解決するかどうかを指定します。デフォルトでは、この動作は `enabled` です。コンテナの値を `disabled` として設定した場合、Amazon ECS はコンテナイメージタグをダイジェストに解決せず、コンテナ定義で指定された元のイメージ URI をデプロイ用に使用します。コンテナイメージの解決の詳細については、「コンテナイメージの解決」を参照してください。

「メモリ」

`memory`

タイプ: 整数

必須: いいえ

コンテナに適用されるメモリの量 (MiB 単位)。コンテナは、ここで指定したメモリを超えようとすると、強制終了されます。タスク内のすべてのコンテナ用に予約されるメモリの合計量は、タスクの `memory` 値より小さくする必要があります (指定されている場合)。このパラメータは

docker create-container コマンドの Memory にマッピングされ、--memory オプションは docker run にマッピングされます。

タスクレベルのメモリ値またはコンテナレベルのメモリ値を指定する必要があります。memory コンテナレベルと memoryReservation 値の両方を指定する場合、memory 値は memoryReservation 値より大きくする必要があります。memoryReservation を指定する場合、コンテナが配置されているコンテナインスタンスで使用可能なメモリリソース量から、上記の値が減算されます。それ以外の場合は、memory の値が使用されます。

Docker デーモン 20.10.0 以降によって、コンテナ用として 6 MiB 以上のメモリが予約されます。従って、このコンテナに対しては 6 MiB 未満のメモリは指定しないようにします。

Docker デーモン 19.03.13-ce 以降では、コンテナ用として 4 MiB 以上のメモリが予約されます。このため、このコンテナ用には 4 MiB 未満のメモリを指定しないようにします。

> **Note**
>
> リソースの使用率を最大化することを目的に、特定のインスタンスタイプにおいて、タスクにできるだけ多くのメモリを提供する場合には、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

`memoryReservation`

タイプ: 整数

必須: いいえ

コンテナ用に予約するメモリのソフト制限 (MiB 単位)。システムメモリに競合がある場合、Docker はコンテナのメモリ量をこのソフト制限値内に維持しようとします。ただし、コンテナは必要に応じてより多くのメモリを使用することができます。コンテナは、memory パラメーターで指定されたハード制限 (該当する場合) またはコンテナインスタンス上の利用可能なすべてのメモリのいずれか早く達する方まで使用できます。このパラメータは docker create-container コマンドの MemoryReservation にマッピングされ、--memory-reservation オプションは docker run にマッピングされます。

タスクレベルでメモリ値を指定しない場合、コンテナ定義で memory または memoryReservation の一方または両方に 0 以外の整数を指定する必要があります。両方を指定する場合、memory は memoryReservation より大きいことが必要で

す。memoryReservation を指定する場合、コンテナが配置されているコンテナインスタンスで使用可能なメモリリソース量から、上記の値が減算されます。それ以外の場合は、memory の値が使用されます。

例えば、コンテナが通常 128 MiB のメモリを使用しているが、短期間にメモリが 256 MiB にバーストする場合があるとします。128 MiB の memoryReservation と 300 MiB の memory ハード制限を設定できます。この設定では、コンテナが、コンテナインスタンスの残りのリソースから 128 MiB のメモリのみを予約できます。同時に、この構成により、コンテナは必要に応じてより多くのメモリ リソースを使用できるようになります。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

Docker デーモン 20.10.0 以降によって、コンテナ用として 6 MiB 以上のメモリが予約されます。従って、このコンテナに対しては 6 MiB 未満のメモリは指定しないようにします。

Docker デーモン 19.03.13-ce 以降では、コンテナ用として 4 MiB 以上のメモリが予約されます。このため、このコンテナ用には 4 MiB 未満のメモリを指定しないようにします。

> **Note**
>
> リソースの使用率を最大化することを目的に、特定のインスタンスタイプにおいて、タスクにできるだけ多くのメモリを提供する場合には、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

ポートマッピング

`portMappings`

タイプ: オブジェクト配列

必須: いいえ

ポートマッピングは、コンテナのネットワークポートを外部に公開します。これは、クライアントがアプリケーションにアクセスすることを可能にします。これは、同じタスク内にあるコンテナ間の通信にも使用されます。

awsvpc ネットワークモードを使用するタスク定義では、containerPort のみを指定します。hostPort は常に無視され、コンテナポートはホスト上の番号が大きいランダムなポートに自動的にマップされます。

Windows のポートマッピングでは、localhost の代わりに NetNAT ゲートウェイを使用します。Windows のポートマッピングにはループバックが存在しないため、ホスト自体からコンテナのマッピングされたポートにアクセスはできません。

このパラメータのほとんどのフィールド (containerPort、hostPort、protocol を含む) は docker create-container コマンドの PortBindings にマッピングされ、--publish オプションは docker run にマッピングされます。タスク定義でネットワークモードを host に設定している場合、ホストポートは未定義とするか、ポートマッピングのコンテナポートと一致させる必要があります。

> **Note**
>
> タスクが RUNNING ステータスに達すると、手動および自動で割り当てられたホストとコンテナポートが次の場所で表示されます:
>
> - コンソール: 指定されたタスクのコンテナ詳細の [Network Bindings] セクション。
> - AWS CLI: networkBindings コマンド出力の describe-tasks セクション。
> - API: DescribeTasks レスポンス。
> - メタデータ: タスクメタデータのエンドポイント。

`appProtocol`

タイプ: 文字列

必須: いいえ

ポートマッピングに使用されるアプリケーションプロトコル。このパラメータは Service Connect にのみ適用されます。アプリケーションが使用するプロトコルと一貫性を持つように、このパラメータを設定することをお勧めします。このパラメータを設定すると、Amazon ECS はサーバー コネクト プロキシにプロトコル固有の接続処理を追加します。このパラメータを設定すると、Amazon ECS は Amazon ECS コンソールと CloudWatch にプロトコル固有のテレメトリを追加します。

このパラメータ値を設定しないと、TCP が使用されます。ただし、Amazon ECS では、TCP 用のプロトコル固有のテレメトリーは追加されません。

詳細については、「the section called “ Service Connect”」を参照してください。

有効なプロトコル値: "HTTP" | "HTTP2" | "GRPC"

containerPort

タイプ: 整数

必須: はい (portMappings を使用する場合)

ユーザーが指定したホストポートまたは自動的に割り当てられたホストポートにバインドされるコンテナポートの番号。

awsvpc ネットワークモードを使用するタスクの場合は、containerPort を使用して公開ポートを指定します。

EC2 起動タイプのタスクでコンテナを使用しており、ホストポートではなくコンテナ ポートを指定するとします。その後、コンテナはエフェメラルポート範囲内のホストポートを自動で受け取ります。詳細については、「hostPort」を参照してください。この方法で自動的に割り当てられるれるポートマッピングは、コンテナインスタンスの予約済みポート数 100 個のクォータに対してはカウントされません。

containerPortRange

タイプ: 文字列

必須: いいえ

動的にマッピングされたホストポート範囲にバインドされるコンテナのポート番号の範囲。

このパラメータは、register-task-definition API を使用してのみ設定できます。このオプションは、portMappings パラメータで使用できます。詳細については、「AWS Command Line Interface リファレンス」の「register-task-definition」を参照してください。

containerPortRange を指定するときは、以下のルールが適用されます。

- bridge ネットワークモードまたは awsvpc ネットワークモードのいずれかを使用する必要があります。
- このパラメータは、Linux と Windows の両オペレーティングシステムで使用できます。
- コンテナインスタンスには、少なくともコンテナエージェントのバージョン 1.67.0 と ecs-init パッケージのバージョン 1.67.0-1 が必要です。
- 各コンテナにつき、最大 100 のポートレンジを指定できます。

- hostPortRange は指定しません。hostPortRange の値は次のように設定されます。
  - awsvpc ネットワークモードのタスク内のコンテナでは、hostPort は containerPort と同じ値に設定されます。これは静的マッピング戦略です。
  - bridge ネットワークモードのタスク内のコンテナの場合、Amazon ECS エージェントはデフォルトの一時範囲から開いているホストポートを見つけ、それを docker に渡してコンテナポートにバインドします。
- containerPortRange の有効な値は 1 ~ 65535 です。
- 1 つのポートは、コンテナごとに 1 つのポートマッピングにのみ含められます。
- 重複するポート範囲は指定できません。
- 範囲内の最初のポートは、最後のポートよりも小さくなければなりません。
- Docker では、ポートの数が多い場合は、Docker デーモン設定ファイルの docker-proxy をオフにすることをお勧めします。

  詳細については、GitHub の Issue #11185 を参照してください。

  Docker デーモン設定ファイルの docker-proxy をオフにする方法については、Amazon ECS 開発者ガイドの「Docker デーモン」を参照してください。

DescribeTasks を呼び出すと、コンテナポートにバインドされているホストポートである hostPortRange を表示できます。

ポート範囲は、EventBridge に送信される Amazon ECS タスクイベントに含まれません。詳細については、「the section called “EventBridge を使用して Amazon ECS エラーへの対応を自動化する”」を参照してください。

hostPortRange

型: 文字列

必須: いいえ

ネットワークバインディングで使用されるホストのポート番号範囲。これは Docker によって割り当てられ、Amazon ECS エージェントによって配信されます。

hostPort

タイプ: 整数

必須: いいえ

コンテナ用に予約するコンテナインスタンスのポート番号。

コンテナポートマッピングに、予約されていないホストポートを指定できます。これは、静的ホストポートマッピングと呼ばれます。または、containerPort を指定するときに hostPort を省略 (または 0 に設定) できます。コンテナは、コンテナインスタンスのオペレーティングシステムと Docker バージョンに応じたエフェメラルポート範囲のポートを自動で受け取ります。これは、動的ホストポートマッピングと呼ばれます。

Docker バージョン 1.6.0 以降のデフォルトの一時ポート範囲は、インスタンスの /proc/sys/net/ipv4/ip_local_port_range にリストされています。このカーネルパラメータが使用できない場合、49153-65535 から始まるデフォルトのエフェメラルポート範囲が使用されます。エフェメラルポート範囲では、ホストポートを指定しないでください。これらの範囲は自動割り当て用に予約済みです。一般的に、32768 より小さい番号のポートは一時ポート範囲に含まれません。

デフォルトの予約済みポートは、SSH 用の 22、Docker ポートの 2375 および 2376、Amazon ECS コンテナエージェントポートの 51678-51680 です。実行中のタスクに対して以前にユーザーが指定したホストポートも、タスクの実行中に予約されます。タスクが停止すると、ホストポートはリリースされます。現在の予約済みポートは、describe-container-instances 出力の remainingResources に表示されます。コンテナインスタンスには、デフォルトの予約済みポートを含めて、一度に最大 100 個の予約済みポートを割り当てられます。自動的に割り当てられるポートは、この 100 個の予約済みポートクォータにはカウントされません。

name

タイプ: 文字列

必須: いいえ。サービスに Service Connect および VPC Lattice を設定する場合は必要です。

ポートマッピングに使用される名前。このパラメータは Service Connect および VPC Lattice にのみ適用されます。このパラメータは、サービスの Service Connect および VPC Lattice 設定で使用する名前です。

詳細については、「Service Connect を使用して Amazon ECS サービスを短縮名で接続する」を参照してください。

次の例では、Service Connect および VPC Lattice の 2 つの必須フィールドが使用されています。

```
"portMappings": [
```

```
    {
        "name": string,
        "containerPort": integer
    }
]
```

`protocol`

タイプ: 文字列

必須: いいえ

ポートマッピングに使用されるプロトコル。有効な値は、`tcp` および `udp` です。デフォルト: `tcp`。

> **Important**
>
> `tcp` は Service Connect でのみサポートされます。このフィールドが設定されていない場合は、`tcp` が暗示されることに注意してください。

> **Important**
>
> UDP サポートは、バージョン 1.2.0 以降の Amazon ECS コンテナエージェント (`amzn-ami-2015.03.c-amazon-ecs-optimized` AMI など)、またはバージョン 1.3.0 以降に更新したコンテナエージェントで起動されたコンテナインスタンスでのみ使用できます。コンテナエージェントを最新バージョンに更新するには、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

ホストポートを指定する際は、以下の構文を使用します。

```
"portMappings": [
    {
        "containerPort": integer,
        "hostPort": integer
    }
    ...
]
```

自動割り当てのホストポートが必要な場合は、以下の構文を使用します。

```
"portMappings": [
    {
        "containerPort": integer
    }
    ...
]
```

プライベートリポジトリの認証情報

`repositoryCredentials`

タイプ: RepositoryCredentials オブジェクト

必須: いいえ

プライベートレジストリ認証用のリポジトリ認証情報。

詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

`credentialsParameter`

タイプ: 文字列

必須: はい (`repositoryCredentials` を使用する場合)

プライベートリポジトリの認証情報が含まれているシークレットの Amazon リソースネーム (ARN)。

詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

> **Note**
>
> Amazon ECS API、AWS CLI、または AWS SDK を使用する場合、起動するタスクと同じリージョンにシークレットが存在する場合は、シークレットの完全な ARN または名前のどちらも使用できます。AWS Management Console を使用する場合は、シークレットの完全な ARN を指定する必要があります。

必要なパラメータが含まれるタスク定義のスニペットを、以下に示します。

```
"containerDefinitions": [
    {
        "image": "private-repo/private-image",
        "repositoryCredentials": {
            "credentialsParameter":
 "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name"
        }
    }
]
```

詳細コンテナ定義パラメータ

以下のコンテナ定義用の詳細パラメータは、Amazon ECS コンテナインスタンスでのコンテナの起動に使用する docker run コマンドの拡張機能を追加します。

トピック

- 再起動ポリシー
- ヘルスチェック
- 環境
- ネットワーク設定
- ストレージとログ記録
- セキュリティ
- リソースの制限
- Docker のラベル

再起動ポリシー

`restartPolicy`

コンテナ再起動ポリシーと関連する設定パラメータ。コンテナの再起動ポリシーを設定すると、Amazon ECS はタスクを置き換えることなくコンテナを再起動できます。詳細については、「コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する」を参照してください。

`enabled`

型: ブール値

必須: はい

コンテナに対して再起動ポリシーを有効にするかどうかを指定します。

`ignoredExitCodes`

タイプ: 整数配列

必須: いいえ

Amazon ECS が無視し、再起動を試みない終了コードのリスト。最大 50 個のコンテナ終了コードを指定できます。デフォルトでは、Amazon ECS はいずれの終了コードも無視しません。

`restartAttemptPeriod`

タイプ: 整数

必須: いいえ

再起動を試みる前にコンテナが実行する必要がある時間 (秒単位) 。コンテナを再起動できるのは、`restartAttemptPeriod` 秒に 1 回のみです。コンテナがこの期間実行できずに早く終了した場合、コンテナは再起動されません。最小の `restartAttemptPeriod` は 60 秒、最大の `restartAttemptPeriod` は 604,800 秒 (7 日間) を指定できます。デフォルトでは、コンテナは再起動の前に 300 秒間実行する必要があります。

ヘルスチェック

`healthCheck`

コンテナに対するヘルスチェックのコマンドと、コンテナのための関連する設定パラメータです。詳細については、「コンテナのヘルスチェックを使用して Amazon ECS タスク状態を判定する」を参照してください。

`command`

正常状態かどうかを決定するために、コンテナが実行するコマンドが格納された文字列配列。この文字列配列の先頭には、コマンド引数を直接実行するための `CMD`、またはコンテナのデフォルトシェルでコマンドを実行するための `CMD-SHELL` を付加できます。これらのいずれも指定しない場合は `CMD` が使用されます。

AWS Management Console にタスク定義を登録する場合は、カンマで区切ったコマンドリストを使用してください。これらのコマンドは、タスク定義が作成された後に文字列に変換されます。ヘルスチェックに対する入力の例を次に示します。

```
CMD-SHELL, curl -f http://localhost/ || exit 1
```

AWS Management Console JSON パネル、AWS CLI、または API を使用してタスク定義を登録するときは、コマンドのリストを角かっこで囲みます。ヘルスチェックに対する入力の例を次に示します。

```
[ "CMD-SHELL", "curl -f http://localhost/ || exit 1" ]
```

stderr が出力されない終了コード 0 は成功を示し、0 以外の終了コードは失敗を示します。

`interval`

各ヘルスチェック間の時間間隔 (秒単位)。5 ～ 300 秒を指定できます。デフォルトの値は 30 秒です。

`timeout`

成功まで待機しているヘルスチェックが、失敗したと見なされるまでの期間 (秒単位) です。2 ～ 60 秒を指定できます。デフォルト値は 5 秒です。

`retries`

コンテナが異常と見なされるまでに、失敗したヘルスチェックを再試行する回数です。1～10 回を指定できます。デフォルト値は 3 回の再試行です。

`startPeriod`

失敗したヘルスチェックの再試行が最大回数に達する前に、コンテナにブートストラップための時間を提供するオプションの猶予期間です。0 ～ 300 秒を指定できます。デフォルトでは、`startPeriod` は無効となっています。

ヘルスチェックが `startPeriod` 内で成功した場合、コンテナは正常であるとみなされ、その後の失敗は最大再試行回数にカウントされます。

環境

`cpu`

タイプ: 整数

必須: いいえ

Amazon ECS コンテナエージェントがコンテナ用に予約した cpu ユニットの数。Linux では、このパラメータは「Create a container」セクションの CpuShares にマッピングされます。

> **Note**
>
> Amazon EC2 インスタンスタイプごとに使用可能な CPU ユニットの数を決定できます。これを行うには、Amazon EC2 インスタンスの詳細ページでそのインスタンスタイプにリストされている vCPU の数を 1,024 倍します。

Linux コンテナは、割り当てられた CPU ユニットと同じ比率を使用して、割り当てられていない CPU ユニットをコンテナインスタンス上の他コンテナと共有します。例えば、そのコンテナ用に 512 個の CPU ユニットが指定された単一コアインスタンスタイプで、唯一のコンテナタスクを実行するとします。さらに、そのタスクはコンテナインスタンスで実行される唯一のタスクです。この場合のコンテナは、1,024 個の CPU ユニット配分を任意のタイミングで使用できます。一方、そのコンテナインスタンスで同じタスクのコピーを別途起動したと仮定します。各タスクには、必要に応じて少なくとも 512 個の CPU ユニットが保証されます。同様に、その他のコンテナが残りの CPU を使用していない場合、各コンテナは CPU 使用率を高められます。ただし、両方のタスクが常に 100% アクティブである場合、使用できるのは 512 CPU ユニットに制限されます。

Linux コンテナインスタンスでは、コンテナインスタンス上の Docker デーモンは、CPU 値を使用して、実行中のコンテナに対する相対 CPU 配分比率を計算します。Linux カーネルが許可する最小の有効な CPU 共有値は 2 で、Linux カーネルが許可する最大の有効な CPU 共有値は 262,144 です。ただし、CPU のパラメータは必須ではなく、コンテナ定義では 2 未満の CPU 値および 262144 より大きな CPU 値を使用できます。CPU 値が 2 未満 (null を含む) および 262144 より大きな値である場合、動作は Amazon ECS コンテナエージェントのバージョンによって異なります。

- Agent versions <= 1.1.0: Null およびゼロの CPU 値は Docker に 0 として渡され、Docker は 1,024 個の CPU 配分に変換します。1 の CPU 値は、Docker に対しては 1 として渡され、Linux カーネルではそれが 2 個の CPU 配分に変換されます。
- エージェントバージョン >= 1.2.0: Null、0、および 1 の CPU 値は、Docker に 2 個の CPU 配分として渡されます。
- エージェントバージョン >= 1.84.0: 256 vCPU を超える CPU 値は Docker に 256 として渡されます。これは 262144 CPU 共有に相当します。

Windows コンテナインスタンスでは、CPU クォータは絶対クォータとして適用されます。Windows コンテナは、タスク定義で定義されている指定された量の CPU にのみアクセスできます。null またはゼロの CPU 値が `0` として Docker に渡されます。次に Windows はこの値を 1 つの CPU の 1% として解釈します。

その他の例については、「Amazon ECS で CPU およびメモリリソースの管理方法」を参照してください。

`gpu`

タイプ: ResourceRequirement オブジェクト

必須: いいえ

Amazon ECS コンテナエージェントがコンテナ用に予約した物理 GPUs の数。タスク内でコンテナ用に予約されているすべての GPU の数は、タスクが起動されたコンテナインスタンスで使用できる GPU の数を超えることはできません。詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

`Elastic Inference accelerator`

タイプ: ResourceRequirement オブジェクト

必須: いいえ

`InferenceAccelerator` タイプでは、`value` はタスク定義で指定される `InferenceAccelerator` の `deviceName` と一致します。詳細については、「the section called “Elastic Inference アクセラレーター名”」を参照してください。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

`essential`

型: ブール値

必須: いいえ

コンテナの essential パラメーターが true としてマークされており、そのコンテナが何らかの理由で失敗するか停止するとします。その後、タスクの一部である他のすべてのコンテナが停止されます。コンテナの essential パラメータを false にマークしておくと、そのコンテナ失敗はタスク内にある残りのコンテナに影響を与えません。このパラメータを省略した場合、コンテナは必須と見なされます。

すべてのタスクには少なくとも 1 つの必須コンテナが必要です。複数のコンテナで構成されるアプリケーションがあるとします。次に、共通の目的で使用されるコンテナをコンポーネントにグループ化し、さまざまなコンポーネントを複数のタスク定義に分離します。詳細については、「Amazon ECS 用のアプリケーションの構築」を参照してください。

```
"essential": true|false
```

entryPoint

> **Important**
>
> 初期のバージョンの Amazon ECS コンテナエージェントは、entryPoint パラメータを正しく処理しません。entryPoint の使用時に問題が発生する場合は、コンテナエージェントを更新するか、代わりに command 配列項目としてコマンドと引数を入力します。

タイプ: 文字列配列

必須: いいえ

コンテナに渡されるエントリポイント。

```
"entryPoint": ["string", ...]
```

command

タイプ: 文字列配列

必須: いいえ

コンテナに渡されるコマンド。このパラメータは create-container コマンドの Cmd にマッピングされ、 COMMAND パラメータは docker run にマッピングされます。複数の引数がある場合、各引数は配列内で、区切られた文字列により指定する必要があります。

```
"command": ["string", ...]
```

workingDirectory

タイプ: 文字列

必須: いいえ

コマンドを実行するコンテナ内の作業ディレクトリ。このパラメータは、Docker Remote API の Create a container (コンテナを作成する) セクションの WorkingDir にマップされ、--workdir オプションは docker run にマップされます。

```
"workingDirectory": "string"
```

environmentFiles

タイプ: オブジェクト配列

必須: いいえ

コンテナに渡す環境変数が含まれるファイルのリスト。このパラメータは docker run コマンドの --env-file オプションにマッピングされます。

FIPS が有効化されている場合、ピリオド (.) が使用されているバケット名 (amzn-s3-demo-bucket1.name.example など) はサポートされません。バケット名にピリオド (.) を使用すると、エージェントが Amazon S3 から環境変数ファイルを取得できなくなるため、タスクが開始されません。

これは Windows コンテナには使用できません。

最大 10 個の環境ファイルを指定できます。ファイルには、ファイル拡張子 .env が必要です。環境ファイルの各行には、VARIABLE=VALUE 形式で環境変数が含まれています。# で始まる行はコメントとして扱われ、無視されます。

コンテナ定義に個別の環境変数が指定されている場合は、環境ファイルに含まれる変数よりも優先されます。同じ変数を含む複数の環境ファイルが指定されている場合、それらのファイルは上から下に処理されます。一意の変数名を使用することをお勧めします。詳細については、「個々の環境変数を Amazon ECS コンテナに渡す」を参照してください。

`value`

型: 文字列

必須: はい

環境変数ファイルを含む Amazon S3 オブジェクトの Amazon リソースネーム (ARN)。

`type`

型: 文字列

必須: はい

使用するファイルのタイプ。`s3` はサポートされる唯一の値です。

`environment`

タイプ: オブジェクト配列

必須: いいえ

コンテナに渡す環境変数。このパラメータは docker create-container コマンドの `Env` にマッピングされ、`--env` オプションは docker run コマンドにマッピングされます。

> **Important**
> 認証情報データなどの機密情報にプレーンテキストの環境変数を使用することはお勧めしません。

`name`

型: 文字列

必須: はい (`environment` を使用する場合)

環境変数の名前。

`value`

型: 文字列

必須: はい (`environment` を使用する場合)

環境変数の値。

```
"environment" : [
    { "name" : "string", "value" : "string" },
    { "name" : "string", "value" : "string" }
]
```

`secrets`

タイプ: オブジェクト配列

必須: いいえ

コンテナに公開するシークレットを表すオブジェクトです。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

`name`

型: 文字列

必須: はい

コンテナの環境変数として設定する値。

`valueFrom`

型: 文字列

必須: はい

コンテナに公開するシークレット。サポートされている値は、AWS Secrets Manager シークレットの完全な Amazon リソースネーム (ARN)、または AWS Systems Manager Parameter Store 内のパラメータの完全な ARN のいずれかです。

> **Note**
>
> 起動するタスクと同じ AWS リージョン に Systems Manager パラメータストアのパラメータまたは Secrets Manager のパラメータが存在する場合は、シークレットの完全な ARN または名前のいずれかを使用できます。パラメータが別のリージョンに存在する場合は、完全な ARN を指定する必要があります。

```
"secrets": [
    {
        "name": "environment_variable_name",
```

```
        "valueFrom": "arn:aws:ssm:region:aws_account_id:parameter/parameter_name"
    }
]
```

ネットワーク設定

disableNetworking

タイプ: ブール値

必須: いいえ

このパラメータが true のとき、ネットワークはコンテナ内でオフになります。

> **Note**
>
> awsvpc ネットワークモードを使用するタスクもしくは Windows コンテナでは、このパラメータはサポートされません。

デフォルト: false。

```
"disableNetworking": true|false
```

links

タイプ: 文字列配列

必須: いいえ

link パラメータでは、コンテナがポートマッピングを必要とせずに互いに通信することを許可します。このパラメータは、タスク定義のネットワークモードが bridge に設定されている場合にのみサポートされます。name:internalName コンストラクトは Docker リンクの name:alias に似ています。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコアを使用できます。

> **Note**
>
> awsvpc ネットワークモードを使用するタスクもしくは Windows コンテナでは、このパラメータはサポートされません。

> **Important**
>
> 同じコンテナインスタンスに配置されたコンテナ同士は、リンクやホストポートマッピングを必要とせずに、互いに通信する場合があります。コンテナインスタンスでのネットワークの分離は、セキュリティグループと VPC 設定によって制御されます。

```
"links": ["name:internalName", ...]
```

`hostname`

タイプ: 文字列

必須: いいえ

コンテナに使用するホスト名。このパラメータは docker create-container の `Hostname` にマッピングされ、`--hostname` オプションは docker run にマッピングされます。

> **Note**
>
> `awsvpc` ネットワークモードを使用している場合、`hostname` パラメータはサポートされません。

```
"hostname": "string"
```

`dnsServers`

タイプ: 文字列配列

必須: いいえ

コンテナに提示する DNS サーバーのリスト。

> **Note**
>
> `awsvpc` ネットワークモードを使用するタスクもしくは Windows コンテナでは、このパラメータはサポートされません。

```
"dnsServers": ["string", ...]
```

`dnsSearchDomains`

タイプ: 文字列配列

必須: いいえ

パターン: ^[a-zA-Z0-9-.]{0,253}[a-zA-Z0-9]$

コンテナに提示する DNS 検索ドメインのリスト。このパラメータは docker create-container コマンドの `DnsSearch` にマッピングされ、`--dns-search` オプションは docker run にマッピングされます。

> **Note**
>
> このパラメータは Windows コンテナまたは、`awsvpc` ネットワークモードを使用するタスクではサポートされていません。

```
"dnsSearchDomains": ["string", ...]
```

`extraHosts`

タイプ: オブジェクト配列

必須: いいえ

コンテナ上の `/etc/hosts` ファイルに追加する、ホスト名と IP アドレスのマッピングリスト。

このパラメータは docker create-container コマンドの `ExtraHosts` にマッピングされ、`--add-host` オプションは docker run にマッピングされます。

> **Note**
>
> このパラメータは Windows コンテナまたは、`awsvpc` ネットワークモードを使用するタスクではサポートされていません。

```
"extraHosts": [
```

```
    {
      "hostname": "string",
      "ipAddress": "string"
    }
    ...
  ]
```

`hostname`

タイプ: 文字列

必須: はい (`extraHosts` を使用する場合)

`/etc/hosts` エントリで使用するホスト名。

`ipAddress`

タイプ: 文字列

必須: はい (`extraHosts` を使用する場合)

`/etc/hosts` エントリで使用する IP アドレス。

ストレージとログ記録

`readonlyRootFilesystem`

タイプ: ブール値

必須: いいえ

このパラメータが true のとき、コンテナはそのルートファイルシステムへの読み取り専用アクセスを許可されます。このパラメータは docker create-container コマンドの `ReadonlyRootfs` にマッピングされ、`--read-only` オプションは docker run にマッピングされます。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

デフォルト: `false`。

```
"readonlyRootFilesystem": true|false
```

`mountPoints`

タイプ: オブジェクト配列

必須: いいえ

コンテナでのデータボリュームのマウントポイント。このパラメータは creat-container Docker API の `Volumes` にマッピングされ、docker run の `--volume` オプションにマッピングされます。

Windows コンテナは `$env:ProgramData` と同じドライブに全部のディレクトリをマウントできます。Windows コンテナは、別のドライブにディレクトリをマウントすることはできません。また、マウントポイントは複数のドライブにまたがることはできません。Amazon EBS ボリュームを Amazon ECS タスクに直接アタッチするには、マウントポイントを指定する必要があります。

`sourceVolume`

タイプ: 文字列

必須: はい (`mountPoints` を使用する場合)

マウントするボリュームの名前。

`containerPath`

型: 文字列

必須: はい (`mountPoints` を使用する場合)

ボリュームをマウントするコンテナ内のパス。

`readOnly`

型: ブール値

必須: いいえ

この値が `true` の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が `false` の場合、コンテナはボリュームに書き込むことができます。デフォルト値は `false` です。

Windows オペレーティングシステムを実行しているタスクの場合、 値をデフォルト の `false` のままにします。

`volumesFrom`

タイプ: オブジェクト配列

必須: いいえ

別コンテナからマウントするデータボリューム。このパラメータは docker create-container コマンドの `VolumesFrom` にマッピングされ、`--volumes-from` オプションは docker run にマッピングされます。

`sourceContainer`

タイプ: 文字列

必須: はい (`volumesFrom` を使用する場合)

ボリュームのマウント元のコンテナの名前。

`readOnly`

タイプ: ブール値

必須: いいえ

この値が `true` の場合、コンテナはボリュームへの読み取り専用アクセスを許可されます。この値が `false` の場合、コンテナはボリュームに書き込むことができます。デフォルト値は `false` です。

```
"volumesFrom": [
                {
                  "sourceContainer": "string",
                  "readOnly": true|false
                }
              ]
```

`logConfiguration`

タイプ: LogConfiguration オブジェクト

必須: いいえ

コンテナに対するログ構成の仕様です。

ログ設定を使用したタスク定義の例については、「Amazon ECS のタスク定義の例」を参照してください。

このパラメータは docker create-container コマンドの LogConfig にマッピングされ、--log-driver オプションは docker run にマッピングされます。デフォルトでは、コンテナは Docker デーモンで使用されるのと同じロギングドライバーを使用します。ただし、コンテナ定義の中で、このパラメータによりログドライバーを指定することで、Docker デーモンとは異なるログドライバーをコンテナに使用させることも可能です。コンテナに異なるロギングドライバーを使用するには、コンテナインスタンス (またはリモートログ記録オプションの別のログサーバー) でログシステムを適切に設定する必要があります。

コンテナのログ設定を指定する際には、以下の点に注意してください。

- 現在、Amazon ECS では Docker デーモンに使用可能なログドライバーがいくつかサポートされています。Amazon ECS コンテナエージェントの今後のリリースで他のログドライバーが追加される可能性があります。
- このパラメータを使用するには、コンテナインスタンスで Docker Remote API のバージョン 1.18 以降が必要です。
- コンテナインスタンスで実行される Amazon ECS コンテナエージェントは、そのインスタンスに配置されたコンテナがこれらのログ設定オプションを使用できるようにする前に、そのインスタンスで使用可能なログドライバーを ECS_AVAILABLE_LOGGING_DRIVERS 環境変数に登録する必要があります。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

```
"logConfiguration": {
      "logDriver": "awslogs","fluentd","gelf","json-
file","journald","logentries","splunk","syslog","awsfirelens",
      "options": {"string": "string"
        ...},
 "secretOptions": [{
  "name": "string",
  "valueFrom": "string"
 }]
}
```

logDriver

タイプ: 文字列

有効な値: "awslogs","fluentd","gelf","json-file","journald","logentries","splunk","syslog","awsfirelens"

必須: はい (logConfiguration を使用する場合)

コンテナに使用するログドライバー。デフォルトでは、上記の有効な値は Amazon ECS コンテナエージェントが通信できるログドライバーです。

サポートされているログドライバーは `awslogs`、`fluentd`、`gelf`、`json-file`、`journald`、`logentries`、`syslog`、`splunk`、`awsfirelens` です。

タスク定義で `awslogs` ログドライバーを使用してコンテナログを CloudWatch Logs に送信する方法については、「Amazon ECS ログを CloudWatch に送信する 」を参照してください。

`awsfirelens` ログドライバーの使用の詳細については、「カスタムログのルーティング」を参照してください。

> **Note**
>
> 上記に示されていないカスタムドライバーがある場合、GitHub で入手できる Amazon ECS コンテナエージェントプロジェクトを fork し、そのドライバーを使用するようにカスタマイズできます。含めたい変更については、プルリクエストを送信することをお勧めします。ただし、現時点では、このソフトウェアの変更されたコピーの実行はサポートされていません。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.18 以上を使用する必要があります。

`options`

型: 文字列から文字列へのマップ

必須: いいえ

ログドライバーに送信する設定オプションの Key-Value マップ。

指定できるオプションは、ログドライバーに応じて異なります。`awslogs` ルーターを使用して Amazon CloudWatch にログをルーティングするときに指定できるオプションには、以下が含まれます。

`awslogs-create-group`

必須: いいえ

ロググループを自動的に作成させるかどうかを指定します。このオプションを指定しない場合、デフォルトは `false` です。

> **Note**
>
> `awslogs-create-group` を使用する前に、IAM ポリシーにはアクセス許可 `logs:CreateLogGroup` が含まれている必要があります。

`awslogs-region`

必須: はい

`awslogs` ログドライバが Docker ログを送信する先の、AWS リージョン を指定します。CloudWatch Logs では、異なるリージョンのクラスターからすべてのログを 1 つのリージョンに送信するように選択できます。これにより、すべてのログを一元的な場所で確認できるようになります。他にも、リージョンごとにそれらを分離して、より細分化することが可能です。このオプションで指定するリージョンに、対象のロググループが存在することを確認してください。

`awslogs-group`

必須: はい

`awslogs` ログドライバーがログストリームを送信する先の、ロググループを指定する必要があります。

`awslogs-stream-prefix`

必須：オプション

指定したプレフィックス、コンテナ名、コンテナが属する Amazon ECS タスクの ID にログストリームを関連付けるには、`awslogs-stream-prefix` オプションを使用します。このオプションでプレフィックスを指定した場合、ログストリームの形式は以下のようになります。

```
prefix-name/container-name/ecs-task-id
```

このオプションでプレフィックスを指定しない場合、ログストリームには、コンテナインスタンスの Docker デーモンによって割り当てられたコンテナ ID に基づいた名前が付けられます。Docker コンテナ ID (コンテナインスタンスでのみ使用可能) だけでそのログを送信したコンテナを追跡するのは難しいため、このオプションでプレフィックスを指定することをお勧めします。

Amazon ECS サービスでは、サービス名をプレフィックスとして使用できます。これにより、コンテナが属するサービスへのログストリームと、それを送信したコンテナの名前、そのコンテナが所属するタスクの ID を追跡できます。

Amazon ECS コンソールを使用する際に [Log] ペインにログを表示するためには、ログのストリームプレフィックスを指定する必要があります。

`awslogs-datetime-format`

必須: いいえ

このオプションは、Python `strftime` 形式で複数行起動パターンを定義します。ログメッセージは、パターンに一致する 1 行と、それに続くパターンに一致しない行で構成されます。一致する 1 行とは、ログメッセージ間の区切りです。

この形式を使用する場合のユースケースの例としては、スタックダンプなどの解析された出力があり、これを使用しなければ、複数のエントリに記録されることになります。適切なパターンにより、単一のエントリにキャプチャさせます。

詳細については、awslogs-datetime-formatを参照してください。

`awslogs-datetime-format` と `awslogs-multiline-pattern` オプションの両方を設定することはできません。

> **Note**
>
> 複数行のログ記録は、すべてのログメッセージの正規表現の解析とマッチングを実行します。これによりログ記録のパフォーマンスに悪影響が及ぶ可能性があります。

`awslogs-multiline-pattern`

必須: いいえ

このオプションでは、正規表現を使用する複数行起動パターンを定義します。ログメッセージは、パターンに一致する 1 行と、それに続くパターンに一致しない行で構成されます。一致する 1 行とは、ログメッセージ間の区切りです。

詳細については、「awslogs-multiline-pattern」を参照してください。

awslogs-datetime-format も設定されている場合は、このオプションは無視されます。

awslogs-datetime-format と awslogs-multiline-pattern オプションの両方を設定することはできません。

> **Note**
>
> 複数行のログ記録は、すべてのログメッセージの正規表現の解析とマッチングを実行します。これによりログ記録のパフォーマンスに悪影響が及ぶ可能性があります。

mode

必須: いいえ

有効な値: non-blocking | blocking

このオプションは、コンテナから awslogs ログドライバーへのログメッセージの配信モードを定義します。選択した配信モードは、コンテナからンテナーからのログの流れが中断されたときのアプリケーションの可用性に影響します。

blocking モードを使用しており、CloudWatch へのログのフローが中断されると、stdout ストリームと stderr ストリームに書き込むためのコンテナコードからの呼び出しがブロックされます。その結果、アプリケーションのロギングスレッドがブロックされます。これにより、アプリケーションが応答しなくなり、コンテナのヘルスチェックが失敗する可能性があります。

non-blocking モードを使用する場合、コンテナのログは代わりに max-buffer-size オプションで設定されたメモリ内の中間バッファに保存されます。これにより、ログを CloudWatch に送信できない場合にアプリケーションが応答しなくなるのを防ぎます。サービスの可用性を確保したいが、多少のログ損失があっても問題ない場合は、このモードを使用することをおすすめします。詳細については、「Preventing log loss with non-blocking mode in the awslogs container log driver」を参照してください。

max-buffer-size

必須: いいえ

デフォルト値: 1m

non-blocking モードが使用されている場合、max-buffer-size ログオプションは、中間メッセージ用のストレージに使用されるバッファのサイズを制御します。アプリケーションに基づいて、必ず適切なバッファサイズを指定してください。バッファがいっぱいになると、それ以上ログを保存できなくなります。保存できないログは失われます。

splunk ログルーターを使用してログをルーティングするには、splunk-token と splunk-url を指定する必要があります。

ログの保存と分析のための AWS のサービス または AWS Partner Network を送信先としたログのルーティングに awsfirelens ログルーターを使用するときは、log-driver-buffer-limit オプションを設定して、イベントがログルーターコンテナに送信される前に、メモリでバッファリングされるイベントの数を制限できます。この制限は、スループットが高い場合に発生する可能性がある、Docker 内のバッファのメモリ不足による、潜在的なログ損失の問題を解決するのに役立ちます。詳細については、「the section called “高スループットのログの設定”」を参照してください。

awsfirelens を使用してログをルーティングするときに指定できるその他のオプションは、送信先に応じて異なります。Amazon Data Firehose にログをエクスポートするときは、region を使用して AWS リージョンを指定し、delivery_stream を使用してログストリームの名前を指定することができます。

Amazon Kinesis Data Streams にログをエクスポートするときは、region を使用して AWS リージョンを指定し、stream を使用してデータストリーム名を指定することができます。

Amazon OpenSearch Service にログをエクスポートするときは、Name、Host (プロトコルを使用しない OpenSearch Service エンドポイント)、Port、Index、Type、Aws_auth、Aws_region、Suppress_Type_Name、および tls といったオプションを指定できます。

Amazon S3 にログをエクスポートするときは、bucket オプションを使用してバケットを指定できます。また、region、total_file_size、upload_timeout、および use_put_object をオプションとして指定することもできます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.19 以上を使用する必要があります。

secretOptions

タイプ: オブジェクト配列

必須: いいえ

ログ設定に渡すシークレットを示すオブジェクト。ログ構成で使用されるシークレットには、認証トークン、証明書、または暗号化キーを含められます。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

`name`

型: 文字列

必須: はい

コンテナの環境変数として設定する値。

`valueFrom`

型: 文字列

必須: はい

コンテナのログ設定に公開するシークレット。

```
"logConfiguration": {
 "logDriver": "splunk",
 "options": {
  "splunk-url": "https://cloud.splunk.com:8080",
  "splunk-token": "...",
  "tag": "...",
  ...
 },
 "secretOptions": [{
  "name": "splunk-token",
  "valueFrom": "/ecs/logconfig/splunkcred"
 }]
}
```

`firelensConfiguration`

タイプ: FirelensConfiguration オブジェクト

必須: いいえ

コンテナの FireLens 構成。これは、コンテナログのログルーターの指定と設定に使用されます。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。

```
{
    "firelensConfiguration": {
        "type": "fluentd",
        "options": {
            "KeyName": ""
        }
    }
}
```

`options`

型: 文字列間のマッピング

必須: いいえ

ログルーターの設定時に使用するオプションの Key-Value マップ。このフィールドはオプションで、カスタム設定ファイルを指定するか、タスク、タスク定義、クラスター、コンテナインスタンスの詳細などのメタデータをログイベントに追加するために使用できます。指定した場合、使用する構文は `"options":{"enable-ecs-log-metadata":"true|false","config-file-type:"s3|file","config-file-value":"arn:aws:s3:::amzn-s3-demo-bucket/fluent.conf|filepath"}` です。詳細については、「Amazon ECS タスク定義の例: FireLens にログをルーティングする」を参照してください。

`type`

型: 文字列

必須: はい

使用するログルーター。有効な値は `fluentd` または `fluentbit` です。

セキュリティ

コンテナセキュリティの詳細については、「Amazon ECS タスクおよびコンテナ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。

`credentialSpecs`

タイプ: 文字列配列

必須: いいえ

Active Directory 認証用のコンテナを設定する認証情報仕様 (CredSpec) ファイルへの SSM または Amazon S3 の ARN のリスト。dockerSecurityOptions の代わりに、このパラメータを使用することをお勧めします。ARN の最大数は 1 です。

各 ARN には 2 つの形式があります。

credentialspecdomainless:MyARN

Secrets Manager にシークレットの追加セクションを持つ CredSpec を提供するために credentialspecdomainless:MyARN を使用します。シークレットでドメインへのログイン認証情報を指定します。

任意のコンテナインスタンスで実行される各タスクは、異なるドメインに参加できます。

この形式は、コンテナインスタンスをドメインに結合しなくても使用できます。

credentialspec:MyARN

単一ドメインに対して CredSpec を提供するために credentialspec:MyARN を使用します。

このタスク定義を使用するタスクを開始する前に、コンテナインスタンスをドメインに参加させる必要があります。

どちらの形式でも、SSM または Amazon S3 で MyARN を ARN に置き換えます。

credspec は、ユーザー名、パスワード、接続先のドメインを含むシークレットの ARN を Secrets Manager に提供する必要があります。セキュリティ向上のため、インスタンスはドメインレス認証のドメインに参加しません。インスタンス上の他のアプリケーションは、ドメインレス認証情報を使用できません。このパラメータを使用すると、タスクが別のドメインに参加する必要がある場合でも、同じインスタンスでタスクを実行できます。詳細については、「Windows コンテナでの gMSAs の使用」および「Linux コンテナ向け gMSAs を使用する」を参照してください。

privileged

型: ブール値

必須: いいえ

このパラメータが true のとき、コンテナには、ホストコンテナインスタンスに対する昇格されたアクセス権限 (root ユーザーと同様) が付与されます。privileged でコンテナを実行することはお勧めしません。ほとんどの場合、privileged を使用する代わりに特定のパラメータを使用することで、必要な権限を正確に指定できます。

このパラメータは docker create-container コマンドの `Privileged` にマッピングされ、`--privileged` オプションは docker run にマッピングされます。

> **Note**
>
> このパラメータは、Windows コンテナ、または Fargate 起動タイプを使用するタスクではサポートされていません。

デフォルト: `false`。

```
"privileged": true|false
```

`user`

タイプ: 文字列

必須: いいえ

コンテナ内で使用するユーザー。このパラメータは docker create-container コマンドの `User` にマッピングされ、`--user` オプションは docker run にマッピングされます。

> **Important**
>
> `host` ネットワークモードを使用してタスクを実行する場合は、ルートユーザー (UID 0) を使用してコンテナを実行しないでください。セキュリティのベストプラクティスとしては、常にルート以外のユーザーを使用します。

以下の形式を使用して、`user` を指定できます。UID または GID を指定する場合は、正の整数として指定する必要があります。

- `user`
- `user:group`
- `uid`
- `uid:gid`
- `user:gid`
- `uid:group`

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"user": "string"
```

`dockerSecurityOptions`

タイプ: 文字列配列

有効な値: "no-new-privileges" | "apparmor:PROFILE" | "label:*value*" | "credentialspec:*CredentialSpecFilePath*"

必須: いいえ

複数のセキュリティシステムのカスタム設定を指定する文字列のリスト。

Linux タスクの場合、このパラメータを使用して、SELinux および AppArmor マルチレベルセキュリティシステムのカスタムラベルを参照できます。

このパラメータを使用して、Active Directory 認証用のコンテナを設定する認証情報仕様ファイルを参照できます。詳細については、Amazon ECS の EC2 Windows コンテナで gMSA を使用する方法について説明します。およびAmazon EC2 の Linux コンテナで gMSA を使用するを参照してください。

このパラメータは docker create-container コマンドの `SecurityOpt` にマッピングされ、`--security-opt` オプションは docker run にマッピングされます。

```
"dockerSecurityOptions": ["string", ...]
```

> **Note**
>
> コンテナインスタンスで実行される Amazon ECS コンテナエージェントは、`ECS_SELINUX_CAPABLE=true` または `ECS_APPARMOR_CAPABLE=true` 環境変数を登録する必要があります。これにより、そのインスタンスに配置されたコンテナが、これらのセキュリティオプションを使用できるようになります。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

リソースの制限

`ulimits`

タイプ: オブジェクト配列

必須: いいえ

コンテナに定義する `ulimit` 値の一覧。この値は、オペレーティングシステムのデフォルトのリソースクォータ設定を上書きします。このパラメータは docker create-container コマンドの `Ulimits` にマッピングされ、`--ulimit` オプションは docker run にマッピングされます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.18 以上を使用する必要があります。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"ulimits": [
      {
        "name":
 "core"|"cpu"|"data"|"fsize"|"locks"|"memlock"|"msgqueue"|"nice"|"nofile"|"nproc"|"rss"|"rtp
        "softLimit": integer,
        "hardLimit": integer
      }
      ...
    ]
```

`name`

タイプ: 文字列

有効な値: `"core" | "cpu" | "data" | "fsize" | "locks" | "memlock" | "msgqueue" | "nice" | "nofile" | "nproc" | "rss" | "rtprio" | "rttime" | "sigpending" | "stack"`

必須: はい (`ulimits` を使用する場合)

`ulimit` の `type`。

`hardLimit`

タイプ: 整数

必須: はい (`ulimits` を使用する場合)

`ulimit` タイプのハード制限。値は、`ulimit` の `type` に応じて、バイト、秒、またはカウントとして指定できます。

`softLimit`

タイプ: 整数

必須: はい (`ulimits` を使用する場合)

`ulimit` タイプのソフト制限。値は、`ulimit` の `type` に応じて、バイト、秒、またはカウントとして指定できます。

Docker のラベル

`dockerLabels`

型: 文字列から文字列へのマップ

必須: いいえ

コンテナに追加するラベルのキー/値マップ。このパラメータは docker create-container コマンドの `Labels` にマッピングされ、`--label` オプションは docker run にマッピングされます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.18 以上を使用する必要があります。

```
"dockerLabels": {"string": "string"
      ...}
```

その他のコンテナ定義のパラメータ

以下のコンテナ定義パラメータは、[Configure via JSON] (JSON による設定) オプションを使用して、Amazon ECS コンソールでタスク定義を登録する際に使用できます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

トピック

Linux パラメータ

`linuxParameters`

型: LinuxParameters オブジェクト

必須: いいえ

KernelCapabilities など、コンテナに適用される Linux 固有のオプション。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"linuxParameters": {
      "capabilities": {
        "add": ["string", ...],
        "drop": ["string", ...]
        }
      }
```

`capabilities`

型: KernelCapabilities オブジェクト

必須: いいえ

Docker によって提供されているデフォルト設定に対して追加または削除する、コンテナ用の Linux 機能。これらの Linux 機能の詳細については、Linux マニュアルページの「機能 (7)」を参照してください。

add

タイプ: 文字列配列

有効な値: "ALL" | "AUDIT_CONTROL" | "AUDIT_READ" | "AUDIT_WRITE" | "BLOCK_SUSPEND" | "CHOWN" | "DAC_OVERRIDE" | "DAC_READ_SEARCH" | "FOWNER" | "FSETID" | "IPC_LOCK" | "IPC_OWNER" | "KILL" | "LEASE" | "LINUX_IMMUTABLE" | "MAC_ADMIN" | "MAC_OVERRIDE" | "MKNOD" | "NET_ADMIN" | "NET_BIND_SERVICE" | "NET_BROADCAST" | "NET_RAW" | "SETFCAP" | "SETGID" | "SETPCAP" | "SETUID" | "SYS_ADMIN" | "SYS_BOOT" | "SYS_CHROOT" | "SYS_MODULE" | "SYS_NICE" | "SYS_PACCT" | "SYS_PTRACE" | "SYS_RAWIO" | "SYS_RESOURCE" | "SYS_TIME" | "SYS_TTY_CONFIG" | "SYSLOG" | "WAKE_ALARM"

必須: いいえ

Docker によって提供されているデフォルト設定に追加する、コンテナ用の Linux 機能。このパラメータは docker create-container コマンドの CapAdd にマッピングされ、--cap-add オプションは docker run にマッピングされます。

add

タイプ: 文字列配列

有効な値: "SYS_PTRACE"

必須: いいえ

Docker によって提供されているデフォルト設定のコンテナに追加する Linux 機能。このパラメータは docker create-container コマンドの CapAdd にマッピングされ、--cap-add オプションは docker run にマッピングされます。

drop

タイプ: 文字列配列

有効な値: "ALL" | "AUDIT_CONTROL" | "AUDIT_WRITE" | "BLOCK_SUSPEND" | "CHOWN" | "DAC_OVERRIDE" | "DAC_READ_SEARCH" | "FOWNER" | "FSETID" | "IPC_LOCK" | "IPC_OWNER" | "KILL" | "LEASE" | "LINUX_IMMUTABLE" | "MAC_ADMIN" | "MAC_OVERRIDE" | "MKNOD" | "NET_ADMIN" | "NET_BIND_SERVICE" | "NET_BROADCAST" | "NET_RAW"

| "SETFCAP" | "SETGID" | "SETPCAP" | "SETUID" | "SYS_ADMIN" | "SYS_BOOT" | "SYS_CHROOT" | "SYS_MODULE" | "SYS_NICE" | "SYS_PACCT" | "SYS_PTRACE" | "SYS_RAWIO" | "SYS_RESOURCE" | "SYS_TIME" | "SYS_TTY_CONFIG" | "SYSLOG" | "WAKE_ALARM"

必須: いいえ

Docker によって提供されているデフォルト設定のコンテナから削除する Linux 機能。このパラメータは docker create-container コマンドの CapDrop にマッピングされ、--cap-drop オプションは docker run にマッピングされます。

devices

コンテナに公開するすべてのホストデバイス。このパラメータは docker create-container コマンドの Devices にマッピングされ、--device オプションは docker run にマッピングされます。

型: デバイスオブジェクト配列

必須: いいえ

hostPath

ホストコンテナインスタンス上のデバイスのパス。

型: 文字列

必須: はい

containerPath

ホストデバイスを公開する先のコンテナ内のパス。

タイプ: 文字列

必須: いいえ

permissions

デバイス用のコンテナに提供する明示的な許可。デフォルトでは、コンテナにはデバイスの read、write、および mknod のアクセス許可があります。

タイプ: 文字列の配列

有効な値: `read` | `write` | `mknod`

`initProcessEnabled`

信号を転送しプロセスを利用するコンテナ内で、`init` を実行。このパラメータは docker run の `--init` オプションにマッピングされます。

このパラメータは、コンテナインスタンスで Docker Remote API バージョン 1.25 以上を使用する必要があります。

`maxSwap`

コンテナが使用できるスワップメモリの合計 (MiB 単位)。このパラメータは、docker run の `--memory-swap` オプションに変換されます。値はコンテナメモリの合計に `maxSwap` の値を加えた値です。

`0` の `maxSwap` 値を指定した場合、コンテナはスワップを使用しません。許容値は、`0` または任意の正の整数です。`maxSwap` パラメータを省略すると、コンテナは実行中のコンテナインスタンスのスワップ設定を使用します。`swappiness` パラメータを使用するには、`maxSwap` 値を設定する必要があります。

`sharedMemorySize`

`/dev/shm` ボリュームのサイズ値 (MiB) です。このパラメータは docker run の `--shm-size` オプションにマッピングされます。

タイプ: 整数

`swappiness`

このパラメータにより、コンテナのメモリスワップ動作を調整できます。`swappiness` の値が `0` であると、必要な場合を除きスワップは発生しません。`swappiness` の値が `100` であると、ページのスワップが頻繁に行われます。使用できる値は、`0` と `100` の間の整数です。値を指定しない場合、デフォルト値の `60` が適用されます。また、`maxSwap` の値が指定されていない場合、このパラメータは無視されます。このパラメータは docker run の `--memory-swappiness` オプションにマッピングされます。

> **Note**
>
> Amazon Linux 2023 でタスクを使用している場合、`swappiness` パラメータはサポートされていません。

`tmpfs`

tmpfs マウントのコンテナパス、マウントオプション、および最大サイズ (MiB) です。このパラメータは docker run の `--tmpfs` オプションにマッピングされます。

型: Tmpfs オブジェクト配列

必須: いいえ

`containerPath`

tmpfs ボリュームがマウントされる絶対ファイルパスです。

タイプ: 文字列

必須: はい

`mountOptions`

tmpfs ボリュームのマウントオプションのリストです。

タイプ: 文字列の配列

必須: いいえ

有効な値: `"defaults" | "ro" | "rw" | "suid" | "nosuid" | "dev" | "nodev" | "exec" | "noexec" | "sync" | "async" | "dirsync" | "remount" | "mand" | "nomand" | "atime" | "noatime" | "diratime" | "nodiratime" | "bind" | "rbind" | "unbindable" | "runbindable" | "private" | "rprivate" | "shared" | "rshared" | "slave" | "rslave" | "relatime" | "norelatime" | "strictatime" | "nostrictatime" | "mode" | "uid" | "gid" | "nr_inodes" | "nr_blocks" | "mpol"`

`size`

tmpfs ボリュームの最大サイズ (MiB) です。

タイプ: 整数

必須: はい

コンテナの依存関係

dependsOn

型: ContainerDependency オブジェクトの配列

必須: いいえ

コンテナの起動と停止に定義されている依存関係。コンテナには複数の依存関係を含めることができます。依存関係がコンテナの起動に対して定義されている場合、コンテナの停止の場合、依存関係は逆になります。例については、「コンテナの依存関係」を参照してください。

> **Note**
>
> あるコンテナが依存関係における制限事項を満たさない場合、または制限を満たす前にタイムアウトした場合、Amazon ECS は、依存関係にある他のコンテナの状態も次に遷移させることはしません。

コンテナの依存関係を有効にするには、インスタンスにバージョン 1.26.0 以上のコンテナエージェントが必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。Amazon ECS に最適化された Amazon Linux AMI を使用している場合、インスタンスでは、ecs-init パッケージの 1.26.0-1 バージョン以降が必要です。バージョン 20190301 以降から起動されるコンテナインスタンスには、必要なバージョンのコンテナエージェントや ecs-init が含まれています。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

```
"dependsOn": [
    {
        "containerName": "string",
        "condition": "string"
    }
]
```

containerName

型: 文字列

必須: はい

コンテナ名が指定された条件を満たしている必要があります。

condition

型: 文字列

必須: はい

コンテナの依存関係の条件です。使用可能な条件とその動作を以下に示します。

- START - この条件は、すぐに現在のリンクとボリュームの動作を工ミュレートします。この条件は、他のコンテナの開始を許可する前に、依存コンテナが開始されていることを検証します。
- COMPLETE - この条件は、他のコンテナの開始を許可する前に、依存コンテナの実行が完了 (終了) することを検証します。これは、スクリプトを実行して終了するだけの、重要性の低いコンテナのために便利です。この条件は、必須コンテナには設定できません。
- SUCCESS - この条件は COMPLETE と同じですが、コンテナが zero ステータスで終了していることも必要です。この条件は、必須コンテナには設定できません。
- HEALTHY — この条件は、他のコンテナの開始を許可する前に、依存コンテナがそのコンテナのヘルスチェックに合格したことを検証します。これには、タスク定義に設定されているヘルスチェックが依存コンテナにある必要があります。タスクの起動時にのみ、この条件が確認されます。

[コンテナのタイムアウト]

startTimeout

タイプ: 整数

必須: いいえ

値の例: 120

コンテナの依存関係解決の再試行を止めるまでの待機時間 (秒)。

例えば、タスク定義内に 2 つのコンテナを指定するとします。containerA は、COMPLETE、SUCCESS、または HEALTHY のいずれかのステータスに到達する containerB に依存関係を持ちます。startTimeout の値に containerB が指定されていて、コンテナが時間内に目標のステータスまで到達しない場合、containerA は開始しません。

> **Note**
>
> あるコンテナが依存関係における制限事項を満たさない場合、または制限を満たす前にタイムアウトした場合、Amazon ECS は、依存関係にある他のコンテナの状態も次に遷移させることはしません。

最大値は 120 秒です。

`stopTimeout`

タイプ: 整数

必須: いいえ

値の例: `120`

コンテナが正常に終了しなかった場合にコンテナが強制終了されるまでの待機時間 (秒)。

`stopTimeout` パラメータが指定されていない場合、Amazon ECS コンテナエージェント構成変数 `ECS_CONTAINER_STOP_TIMEOUT` に設定された値がデフォルトで使用されます。`stopTimeout` パラメータまたは `ECS_CONTAINER_STOP_TIMEOUT` エージェント設定変数のいずれも設定されていない場合、Linux コンテナと Windows コンテナに対して、デフォルト値の 30 秒が適用されます。コンテナインスタンスには、コンテナ停止タイムアウト値を有効にするために、コンテナエージェントのバージョン 1.26.0 以上が必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認方法と最新バージョンへの更新方法については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。Amazon ECS に最適化された Linux Amazon AMI を使用している場合、インスタンスには、少なくとも `ecs-init` パッケージの 1.26.0-1 バージョン以上が必要です。バージョン `20190301` 以降から起動されるコンテナインスタンスには、必要なバージョンのコンテナエージェントや `ecs-init` が含まれています。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

システムコントロール

`systemControls`

型: SystemControl オブジェクト

必須: いいえ

コンテナ内で設定する名前空間カーネルパラメータのリスト。このパラメータは docker create-container コマンドの Sysctls にマッピングされ、--sysctl オプションは docker run にマッピングされます。例えば、接続をより長く維持するように net.ipv4.tcp_keepalive_time 設定を構成できます。

awsvpc または host ネットワークモードも使用する単一のタスクで、複数のコンテナに対してネットワーク関連の systemControls パラメータを指定することは推奨されません。これを行うと、次のような欠点があります。

- awsvpc ネットワークモードを使用するタスクの場合、systemControls をコンテナ用に設定した場合、タスク内のすべてのコンテナに適用されます。単一のタスクの複数のコンテナに対して異なる systemControls を設定すると、最後に開始されたコンテナによって、有効になる systemControls が決定します。
- host ネットワークモードを使用するタスクでは、ネットワーク名前空間の systemControls はサポートされていません。

タスク内でコンテナに使用するため IPC リソース名前空間を設定している場合、システムコントロールには以下の条件が適用されます。詳細については、「IPC モード」を参照してください。

- host IPC モードを使用するタスクの場合、IPC 名前空間の systemControls はサポートされていません。
- task IPC モードを使用するタスクでは、IPC 名前空間の systemControls 値が、タスク内のすべてのコンテナに適用されます。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"systemControls": [
    {
         "namespace":"string",
         "value":"string"
    }
]
```

namespace

タイプ: 文字列

必須: いいえ

value を設定する名前空間カーネルパラメータ。

有効な IPC 名前空間の値: "fs.mqueue.*" で開始する "kernel.msgmax" | "kernel.msgmnb" | "kernel.msgmni" | "kernel.sem" | "kernel.shmall" | "kernel.shmmax" | "kernel.shmmni" | "kernel.shm_rmid_forced"、および Sysctls

有効なネットワーク名前空間値: "net.*" で始まる Sysctls

value

タイプ: 文字列

必須: いいえ

namespace で指定された名前空間カーネルパラメータの値。

インタラクティブ

interactive

型: ブール値

必須: いいえ

このパラメータが true の場合、stdin または tty を割り当てる必要がある、コンテナ化されたアプリケーションをデプロイすることができます。このパラメータは docker create-container コマンドの OpenStdin にマッピングされ、--interactive オプションは docker run にマッピングされます。

デフォルト: false。

擬似ターミナル

pseudoTerminal

タイプ: ブール値

必須: いいえ

このパラメータが true の場合、TTY が割り当てられます。このパラメータは docker create-container コマンドの Tty にマッピングされ、--tty オプションは docker run にマッピングされます。

デフォルト: `false`。

Elastic Inference アクセラレーター名

タスク定義用の Elastic Inference アクセラレーターのリソース要件。

> **Note**
>
> Amazon Elastic Inference (EI) は利用できなくなりました。

以下のパラメータをタスク定義で使用できます。

`deviceName`

タイプ: 文字列

必須: はい

Elastic Inference アクセラレーターのデバイス名。`deviceName` は、コンテナ定義でも参照されます。`Elastic Inference accelerator` を参照してください。

`deviceType`

タイプ: 文字列

必須: はい

使用する Elastic Inference アクセラレーター。

タスク配置の制約事項

タスク定義の登録時、Amazon ECS でのタスク配置方法をカスタマイズするタスク配置の制約を指定できます。

アベイラビリティーゾーン、インスタンスタイプ、またはカスタム属性に基づいたタスク配置の制約を使用できます。詳細については、「Amazon ECS がタスクに使用するコンテナインスタンスを定義する」を参照してください。

以下のパラメータをコンテナ定義で使用できます。

`expression`

型: 文字列

必須: いいえ

制約に適用されるクラスタークエリ言語表現。詳細については、「Amazon ECS タスク用のコンテナインスタンスを定義する式を作成する」を参照してください。

`type`

型: 文字列

必須: はい

制約のタイプ。選択対象を有効な候補グループに制約するには、`memberOf` を使用します。

プロキシ設定

`proxyConfiguration`

タイプ: ProxyConfiguration オブジェクト

必須: いいえ

App Mesh プロキシ設定の詳細。

EC2 起動タイプを使用するタスクでプロキシ設定を有効にする場合、コンテナインスタンスには、コンテナエージェントのバージョン 1.26.0 以上と `ecs-init` パッケージのバージョン 1.26.0-1 以上が必要です。コンテナインスタンスが Amazon ECS に最適化された AMI バージョン `20190301` 以降から起動される場合、コンテナエージェントおよび `ecs-init` の必要なバージョンが含まれます。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

```
"proxyConfiguration": {
    "type": "APPMESH",
    "containerName": "string",
```

```
    "properties": [
        {
           "name": "string",
           "value": "string"
        }
    ]
}
```

type

型: 文字列

重要な値: APPMESH

必須: いいえ

プロキシのタイプ。APPMESH はサポートされる唯一の値です。

containerName

型: 文字列

必須: はい

App Mesh プロキシとして機能するコンテナの名前です。

properties

タイプ: パラメータオブジェクトの配列

必須: いいえ

Container Network Interface(CNI) プラグインを提供するネットワーク構成パラメータのセットで、キーと値のペアとして指定されます。

- IgnoredUID - (必須) コンテナ定義の user パラメータで定義されるプロキシコンテナのユーザー ID (UID)。これは、プロキシがそれ自体のトラフィックを無視するようにするために使用されます。IgnoredGID を指定した場合は、このフィールドは空にできます。
- IgnoredGID - (必須) コンテナ定義の user パラメータで定義されるプロキシコンテナのグループ ID (GID)。これは、プロキシがそれ自体のトラフィックを無視するようにするために使用されます。IgnoredUID を指定した場合は、このフィールドは空にできます。
- AppPorts - (必須) アプリケーションが使用するポートのリスト。これらのポートへのネットワークトラフィックは ProxyIngressPort および ProxyEgressPort に転送されます。

- ProxyIngressPort - (必須) AppPorts への着信トラフィックが誘導されるポートを指定します。
- ProxyEgressPort - (必須) AppPorts からの発信トラフィックが誘導されるポートを指定します。
- EgressIgnoredPorts – (必須) 指定されたこれらのポートに向かうアウトバウンドトラフィックは無視され、ProxyEgressPort にリダイレクトされません。空のリストを指定できます。
- EgressIgnoredIPs – (必須) 指定されたこれらの IP アドレスに向かうアウトバウンドトラフィックは無視され、ProxyEgressPort にリダイレクトされません。空のリストを指定できます。

name

型: 文字列

必須: いいえ

キーと値のペアの名前。

value

型: 文字列

必須: いいえ

キーと値のペアの値。

ボリューム

タスク定義を登録する際、コンテナインスタンスの Docker デーモンに渡されるボリュームのリストを任意で指定することができます。すると、同じコンテナインスタンス上の他のコンテナで使用できるようになります。

使用できるデータボリュームの種類は以下のとおりです。

- Amazon EBS ボリューム – データ集約型のコンテナ化されたワークロード向けに、費用対効果が高く、耐久性があり、高性能なブロックストレージを提供します。スタンドアロンタスクを実行するとき、またはサービスを作成または更新するときに、Amazon ECS タスクごとに 1 つの Amazon EBS ボリュームをアタッチできます。Amazon EBS ボリュームは、Linux タスクでサ

ポートされています。詳細については、「Amazon ECS での Amazon EBS ボリュームの使用」を参照してください。

- Amazon EFS ボリューム - Amazon ECS タスクで使用するためのシンプルかつスケーラブルで、永続的なファイルストレージを提供します。Amazon EFSでは、ストレージ容量は伸縮性があります。この容量は、ファイルの追加や削除に伴い自動的に拡大および縮小されます。アプリケーションは、必要なときに必要なストレージを確保できます。Amazon EFS ボリュームがサポートされています。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。
- FSx for Windows File Server ボリューム – 完全マネージド型の Microsoft Windows ファイルサーバーを提供します。これらのファイルサーバは、Windows ファイルシステムによってバックアップされています。Amazon ECS と共に FSx for Windows File Server を使用する場合、永続的、分散型、共有型、および静的なファイルストレージを使用して、Windows タスクをプロビジョニングすることが可能です。詳細については、「Amazon ECS での FSx for Windows File Server ボリュームの使用」を参照してください。

  このオプションは Fargate の Windows コンテナではサポートされません。
- Docker ボリューム – ホストの Amazon EC2 インスタンスで `/var/lib/docker/volumes` に作成される Docker マネージドボリューム。Docker ボリュームドライバー (プラグインとも呼ばれる) は、ボリュームを外部ストレージシステム (Amazon EBS など) と統合するために使用します。組み込みの `local` ボリュームドライバーまたはサードパーティーのボリュームドライバーを使用できます。Docker ボリュームは、Amazon EC2 インスタンスでタスクを実行する場合にのみサポートされます。Windows コンテナでは、`local` ドライバーの使用のみがサポートされます。Docker ボリュームを使用するには、タスク定義で `dockerVolumeConfiguration` を指定します。
- バインドマウント – ホストマシン上のファイルやディレクトリがコンテナにマウントされます。バインドマウントホストボリュームがサポートされています。バインドマウントのホストボリュームを使用するには、タスク定義で `host` およびオプションの `sourcePath` 値を使用します。

詳細については、「Amazon ECS タスクのストレージオプション」を参照してください。

以下のパラメータをコンテナ定義で使用できます。

`name`

タイプ: 文字列

必須: いいえ

ボリュームの名前。最大 255 文字の英字 (大文字と小文字の区別あり)、数字、ハイフン (-)、アンダースコア (_) を使用できます。この名前は、コンテナ定義 `mountPoints` オブジェクトの `sourceVolume` パラメータで参照されます。

`host`

必須: いいえ

`host` パラメーターは、バインドマウントのライフサイクルを、タスクではなくホスト Amazon EC2 インスタンスと、それが格納されている場所に関連付けるために使用されます。`host` パラメーターが空の場合、Docker デーモンはデータボリュームのホストパスを割り当てますが、関連付けられたコンテナの実行が停止した後にデータが保持されるとは限りません。

Windows コンテナは `$env:ProgramData` と同じドライブに全部のディレクトリをマウントできます。

> **Note**
>
> `sourcePath` パラメータは、Amazon EC2 インスタンスでホストされているタスクを使用する場合にのみサポートされます。

`sourcePath`

タイプ: 文字列

必須: いいえ

`host` パラメータを使用する場合は、`sourcePath` を指定して、コンテナに表示されるホスト Amazon EC2 インスタンスのパスを宣言します。このパラメータが空の場合は、Docker デーモンによってホストパスが割り当てられます。`host` パラメータに `sourcePath` の場所が含まれている場合、データボリュームは手動で削除するまでホスト Amazon EC2 インスタンスの指定された場所に保持されます。`sourcePath` の値がホスト Amazon EC2 インスタンスに存在しない場合は、Docker デーモンによって作成されます。その場所が存在する場合は、ソースパスフォルダの内容がエクスポートされます。

`configuredAtLaunch`

型: ブール値

必須: いいえ

起動時にボリュームを設定可能にするかどうかを指定します。true に設定すると、スタンドアロンタスクを実行するとき、またはサービスを作成または更新するときにボリュームを設定できます。true に設定すると、タスク定義内で別のボリューム設定を提供することはできません。タスクにアタッチする Amazon EBS ボリュームを設定するには、このパラメータを true に設定する必要があります。configuredAtLaunch を true に設定し、ボリューム設定を起動フェーズに先送りすることで、ボリュームタイプや特定のボリューム設定に限定されないタスク定義を作成できます。こうすることで、タスク定義をさまざまな実行環境で再利用できるようになります。詳細については、「Amazon EBS ボリューム」を参照してください。

dockerVolumeConfiguration

タイプ: DockerVolumeConfiguration オブジェクト

必須: いいえ

このパラメータは、Docker ボリュームを使用する場合に指定します。Docker ボリュームは、EC2 インスタンスでタスクを実行する場合にのみサポートされます。Windows コンテナでは、local ドライバーの使用のみがサポートされます。バインドマウントを使用するには、代わりに host を指定します。

scope

型: 文字列

有効な値: task | shared

必須: いいえ

Docker ボリュームのスコープ。これにより、ボリュームのライフサイクルが決定されます。Docker ボリュームの範囲が task の場合は、タスクが開始すると自動的にプロビジョンされ、タスクが停止すると破棄されます。Docker ボリュームの範囲が shared の場合は、タスクの停止後も保持されます。

autoprovision

タイプ: ブール値

デフォルト値: false

必須: いいえ

この値が true の場合、既に存在していない場合は Docker ボリュームが作成されます。このフィールドは、scope が shared の場合にのみ使用されます。scope が task の場合、このパラメータは省略する必要があります。

`driver`

タイプ: 文字列

必須: いいえ

使用する Docker ボリュームドライバー。この名前はタスク配置に使用されるため、ドライバー値は Docker で提供されているドライバー名と一致する必要があります。ドライバーが Docker プラグイン CLI を使用してインストールされた場合は、`docker plugin ls` を使用してコンテナインスタンスからドライバー名を取得します。ドライバーが別の方法でインストール済みである場合は、Docker プラグイン検出を使用してドライバー名を取得します。

`driverOpts`

タイプ: 文字列

必須: いいえ

パススルーする Docker ドライバー固有のオプションのマップ。このパラメータは、Docker の「Create a volume」セクションの `DriverOpts` にマッピングされます。

`labels`

タイプ: 文字列

必須: いいえ

Docker ボリュームに追加するカスタムメタデータ。

`efsVolumeConfiguration`

タイプ: EFSVolumeConfiguration オブジェクト

必須: いいえ

このパラメータは、Amazon EFS ボリュームを使用する場合に指定します。

`fileSystemId`

型: 文字列

必須: はい

使用する Amazon EFS ファイルシステムの ID。

`rootDirectory`

型: 文字列

必須: いいえ

ホスト内にルートディレクトリとしてマウントする Amazon EFS ファイルシステム内のディレクトリ。このパラメータを省略すると、Amazon EFS ボリュームのルートが使用されます。/ を指定すると、このパラメータを省略した場合と同じ結果になります。

> **Important**
>
> `authorizationConfig` で EFS アクセスポイントが指定されている場合は、ルートディレクトリパラメータを省略するか / に設定して、EFS アクセスポイントにパスを設定する必要があります。

`transitEncryption`

タイプ: 文字列

有効な値: `ENABLED` | `DISABLED`

必須: いいえ

Amazon ECS ホストと Amazon EFS サーバー間で、転送中の Amazon EFS データの暗号化を有効にするかどうかを指定します。Amazon EFS IAM 認可を使用する場合は、転送中の暗号化を有効にする必要があります。このパラメータを省略すると、`DISABLED` のデフォルト値が使用されます。詳細については、Amazon Elastic ファイルシステムユーザーガイドの「転送中データの暗号化」を参照してください。

`transitEncryptionPort`

タイプ: 整数

必須: いいえ

Amazon ECS ホストと Amazon EFS サーバーとの間で、暗号化されたデータを送信するときに使用するポート。転送暗号化ポートを指定しない場合、タスクでは Amazon EFS マウントヘルパーが使用するポート選択戦略が使用されます。詳細については、Amazon Elastic File System User Guide] (Amazon Elastic File System ユーザーガイド) のEFS Mount Helper] (EFS マウントヘルパー) を参照してください。

`authorizationConfig`

タイプ: EFSAuthorizationConfig オブジェクト

必須: いいえ

Amazon EFS ファイルシステムに対する認可構成の詳細。

`accessPointId`

型: 文字列

必須: いいえ

使用するアクセスポイント ID。アクセスポイントが指定されている場合は、`efsVolumeConfiguration` のルートディレクトリ値を省略するか `/` に設定して、EFS アクセスポイントにパスを設定する必要があります。アクセスポイントを使用する場合は、`EFSVolumeConfiguration` で転送中の暗号化を有効にする必要があります。詳細については、Amazon Elastic ファイルシステムユーザーガイドのAmazon EFS アクセスポイントの使用を参照してください。

`iam`

型: 文字列

有効な値: `ENABLED` | `DISABLED`

必須: いいえ

タスク定義で定義した Amazon ECS タスクの IAM ロールを、Amazon EFS ファイルシステムのマウント時に使用するかどうかを指定します。使用する場合は、`EFSVolumeConfiguration` で転送中の暗号化を有効にする必要があります。このパラメータを省略すると、`DISABLED` のデフォルト値が使用されます。詳細については、「タスク用の IAM ロール」を参照してください。

`FSxWindowsFileServerVolumeConfiguration`

タイプ: FSxWindowsFileServerVolumeConfiguration オブジェクト

必須: はい

このパラメータは、タスクストレージに Amazon FSx for Windows File Server ファイルシステムを使用する場合に指定します。

`fileSystemId`

タイプ: 文字列

必須: はい

使用する FSx for Windows File Server ファイルシステムID。

`rootDirectory`

型: 文字列

必須: はい

ホスト内にルートディレクトリとしてマウントする FSx for Windows File Server ファイルシステム内のディレクトリ。

`authorizationConfig`

`credentialsParameter`

型: 文字列

必須: はい

認可の認証情報オプション。

options:

- AWS Secrets Manager シークレットの Amazon リソースネーム (ARN)。
- AWS Systems Manager パラメータの ARN。

`domain`

タイプ: 文字列

必須: はい

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) ディレクトリまたはセルフホスト型 EC2 Active Directory によってホストされる完全修飾ドメイン名。

[タグ]

タスク定義の登録する際、タスク定義に適用されるメタデータタグをオプションで指定できます。タグは、タスク定義を分類して組織化するのに役立ちます。各タグは、キー、および値 (オプション)

で構成されます。両方を定義します。詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。

> **Important**
>
> タグには、個人が特定可能な情報や、機密情報あるいは秘匿性の高い情報は追加しないでください。タグは、多くの AWS のサービス (請求など) からアクセスできます。タグは、プライベートデータや機密データに使用することを意図していません。

タグオブジェクトでは、次のパラメータを使用できます。

`key`

タイプ: 文字列

必須: いいえ

タグを構成するキーと値のペアの一部。キーは、より具体的なタグ値のカテゴリのように動作する、一般的なラベルです。

`value`

タイプ: 文字列

必須: いいえ

タグを構成するキーと値のペアのオプションの一部。値はタグカテゴリ (キー) の記述子として機能します。

その他のタスク定義パラメータ

以下のタスク定義パラメータは、Amazon ECS コンソールから、[Configure via JSON (JSON による設定)] オプションを使用してタスク定義を登録する際に使用します。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

トピック

- エフェメラルストレージ
- IPC モード

- PID モード
- フォールトインジェクション

エフェメラルストレージ

`ephemeralStorage`

タイプ: EphemeralStorage オブジェクト

必須: いいえ

IPC モード

`ipcMode`

型: 文字列

必須: いいえ

タスクのコンテナで使用する IPC リソースの名前空間。有効な値は `host`、`task` または `none` です。`host` が指定されている場合、同一のコンテナインスタンス上にある (`host` IPC モードを指定した) タスク内のすべてのコンテナは、ホスト Amazon EC2 インスタンスと同じ IPC リソースを共有します。`task` が指定されている場合、指定されたタスク内のすべてのコンテナは同じ IPC リソースを共有します。`none` が指定されている場合、タスクのコンテナ内の IPC リソースはプライベートです。タスク内またはコンテナインスタンスの他のコンテナと共有されることはありません。値を指定しない場合、IPC リソース名前空間の共有はコンテナインスタンスの Docker デーモンの設定によって異なります。

`host` IPC モードを使用する場合は、意図せず IPC 名前空間が公開されるリスクが高いことに注意してください。

タスク内のコンテナに、`systemControls` を使用して名前空間のカーネルパラメータを設定している場合は、以下の点が IPC リソース名前空間に適用されます。

- `host` IPC モードを使用するタスクの場合、`systemControls` に関連する IPC 名前空間はサポートされません。
- `task` IPC モードを使用するタスクでは、IPC 名前空間に関連する `systemControls` が、タスク内のすべてのコンテナに適用されます。

PID モード

`pidMode`

タイプ: 文字列

有効な値: `host` | `task`

必須: いいえ

タスクのコンテナで使用するプロセス名前空間。有効な値は `host` または `task` です。例えば、サイドカーのモニタリングでは、`pidMode` が同じタスクで実行されている他のコンテナに関する情報にアクセスする必要となる場合があります。

`host` が指定されている場合、同じコンテナインスタンスで `host` PID モードを指定したタスク内のすべてのコンテナは、ホスト Amazon EC2 インスタンスと同じプロセス名前空間を共有します。

`task` が指定されている場合、指定したタスク内のすべてのコンテナは同じプロセス名前空間を共有します。

値が指定されていない場合、デフォルトは各コンテナのプライベート名前空間です。

`host` PID モードを使用する場合は、意図せずプロセス名前空間が公開されるリスクが高いことに注意してください。

> **Note**
>
> このパラメータは Windows コンテナではサポートされません。

フォールトインジェクション

`enableFaultInjection`

型: ブール値

有効な値: `true` | `false`

必須: いいえ

タスクのペイロードでこのパラメータが `true` 設定されている場合、Amazon ECS はタスクのコンテナからのフォールトインジェクションリクエストを受け入れます。デフォルトでは、このパラメータは `false` に設定されます。

Amazon ECS タスク定義テンプレート

以下に示しているのは、空のタスク定義テンプレートです。このテンプレートを使用してタスク定義を作成します。これにより、コンソールの JSON 入力領域に貼り付けるか、ファイルに保存して AWS CLI の `--cli-input-json` オプションで使用できるようになります。詳細については、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」を参照してください。

Amazon EC2 起動タイプテンプレート

```
{
  "family": "",
  "taskRoleArn": "",
  "executionRoleArn": "",
  "networkMode": "none",
  "containerDefinitions": [
    {
      "name": "",
      "image": "",
      "repositoryCredentials": {
        "credentialsParameter": ""
      },
      "cpu": 0,
      "memory": 0,
      "memoryReservation": 0,
      "links": [""],
      "portMappings": [
        {
          "containerPort": 0,
          "hostPort": 0,
          "protocol": "tcp"
        }
      ],
      "restartPolicy": {
        "enabled": true,
        "ignoredExitCodes": [0],
        "restartAttemptPeriod": 180
      },
```

```
      "essential": true,
      "entryPoint": [""],
      "command": [""],
      "environment": [
        {
          "name": "",
          "value": ""
        }
      ],
      "environmentFiles": [
        {
          "value": "",
          "type": "s3"
        }
      ],
      "mountPoints": [
        {
          "sourceVolume": "",
          "containerPath": "",
          "readOnly": true
        }
      ],
      "volumesFrom": [
        {
          "sourceContainer": "",
          "readOnly": true
        }
      ],
      "linuxParameters": {
        "capabilities": {
          "add": [""],
          "drop": [""]
        },
        "devices": [
          {
            "hostPath": "",
            "containerPath": "",
            "permissions": ["read"]
          }
        ],
        "initProcessEnabled": true,
        "sharedMemorySize": 0,
        "tmpfs": [
          {
```

```
            "containerPath": "",
            "size": 0,
            "mountOptions": [""]
          }
        ],
        "maxSwap": 0,
        "swappiness": 0
      },
      "secrets": [
        {
          "name": "",
          "valueFrom": ""
        }
      ],
      "dependsOn": [
        {
          "containerName": "",
          "condition": "COMPLETE"
        }
      ],
      "startTimeout": 0,
      "stopTimeout": 0,
      "hostname": "",
      "user": "",
      "workingDirectory": "",
      "disableNetworking": true,
      "privileged": true,
      "readonlyRootFilesystem": true,
      "dnsServers": [""],
      "dnsSearchDomains": [""],
      "extraHosts": [
        {
          "hostname": "",
          "ipAddress": ""
        }
      ],
      "dockerSecurityOptions": [""],
      "interactive": true,
      "pseudoTerminal": true,
      "dockerLabels": {
        "KeyName": ""
      },
      "ulimits": [
        {
```

```
          "name": "nofile",
          "softLimit": 0,
          "hardLimit": 0
        }
      ],
      "logConfiguration": {
        "logDriver": "splunk",
        "options": {
          "KeyName": ""
        },
        "secretOptions": [
          {
            "name": "",
            "valueFrom": ""
          }
        ]
      },
      "healthCheck": {
        "command": [""],
        "interval": 0,
        "timeout": 0,
        "retries": 0,
        "startPeriod": 0
      },
      "systemControls": [
        {
          "namespace": "",
          "value": ""
        }
      ],
      "resourceRequirements": [
        {
          "value": "",
          "type": "InferenceAccelerator"
        }
      ],
      "firelensConfiguration": {
        "type": "fluentbit",
        "options": {
          "KeyName": ""
        }
      }
    }
  ],
```

```
  "volumes": [
    {
      "name": "",
      "host": {
        "sourcePath": ""
      },
      "configuredAtLaunch": true,
      "dockerVolumeConfiguration": {
        "scope": "shared",
        "autoprovision": true,
        "driver": "",
        "driverOpts": {
          "KeyName": ""
        },
        "labels": {
          "KeyName": ""
        }
      },
      "efsVolumeConfiguration": {
        "fileSystemId": "",
        "rootDirectory": "",
        "transitEncryption": "DISABLED",
        "transitEncryptionPort": 0,
        "authorizationConfig": {
          "accessPointId": "",
          "iam": "ENABLED"
        }
      },
      "fsxWindowsFileServerVolumeConfiguration": {
        "fileSystemId": "",
        "rootDirectory": "",
        "authorizationConfig": {
          "credentialsParameter": "",
          "domain": ""
        }
      }
    }
  ],
  "placementConstraints": [
    {
      "type": "memberOf",
      "expression": ""
    }
  ],
```

```
  "requiresCompatibilities": ["EC2"],
  "cpu": "",
  "memory": "",
  "tags": [
    {
      "key": "",
      "value": ""
    }
  ],
  "pidMode": "task",
  "ipcMode": "task",
  "proxyConfiguration": {
    "type": "APPMESH",
    "containerName": "",
    "properties": [
      {
        "name": "",
        "value": ""
      }
    ]
  },
  "inferenceAccelerators": [
    {
      "deviceName": "",
      "deviceType": ""
    }
  ],
  "ephemeralStorage": {
    "sizeInGiB": 0
  },
  "runtimePlatform": {
    "cpuArchitecture": "X86_64",
    "operatingSystemFamily": "WINDOWS_SERVER_20H2_CORE"
  }
}
```

Fargate 起動タイプテンプレート

> **Important**
>
> Fargate 起動タイプでは、以下のいずれかの値を持つ operatingSystemFamily パラメータを入れる必要があります。

- LINUX

- WINDOWS_SERVER_2019_FULL
- WINDOWS_SERVER_2019_CORE
- WINDOWS_SERVER_2022_FULL
- WINDOWS_SERVER_2022_CORE

```
{
    "family": "",
    "runtimePlatform": {"operatingSystemFamily": ""},
    "taskRoleArn": "",
    "executionRoleArn": "",
    "networkMode": "awsvpc",
    "platformFamily": "",
    "containerDefinitions": [
        {
            "name": "",
            "image": "",
            "repositoryCredentials": {"credentialsParameter": ""},
            "cpu": 0,
            "memory": 0,
            "memoryReservation": 0,
            "links": [""],
            "portMappings": [
                {
                    "containerPort": 0,
                    "hostPort": 0,
                    "protocol": "tcp"
                }
            ],
            "essential": true,
            "entryPoint": [""],
            "command": [""],
            "environment": [
                {
                    "name": "",
                    "value": ""
                }
            ],
```

```
            "environmentFiles": [
                {
                    "value": "",
                    "type": "s3"
                }
            ],
            "mountPoints": [
                {
                    "sourceVolume": "",
                    "containerPath": "",
                    "readOnly": true
                }
            ],
            "volumesFrom": [
                {
                    "sourceContainer": "",
                    "readOnly": true
                }
            ],
            "linuxParameters": {
                "capabilities": {
                    "add": [""],
                    "drop": [""]
                },
                "devices": [
                    {
                        "hostPath": "",
                        "containerPath": "",
                        "permissions": ["read"]
                    }
                ],
                "initProcessEnabled": true,
                "sharedMemorySize": 0,
                "tmpfs": [
                    {
                        "containerPath": "",
                        "size": 0,
                        "mountOptions": [""]
                    }
                ],
                "maxSwap": 0,
                "swappiness": 0
            },
            "secrets": [
```

```
            {
                "name": "",
                "valueFrom": ""
            }
        ],
        "dependsOn": [
            {
                "containerName": "",
                "condition": "HEALTHY"
            }
        ],
        "startTimeout": 0,
        "stopTimeout": 0,
        "hostname": "",
        "user": "",
        "workingDirectory": "",
        "disableNetworking": true,
        "privileged": true,
        "readonlyRootFilesystem": true,
        "dnsServers": [""],
        "dnsSearchDomains": [""],
        "extraHosts": [
            {
                "hostname": "",
                "ipAddress": ""
            }
        ],
        "dockerSecurityOptions": [""],
        "interactive": true,
        "pseudoTerminal": true,
        "dockerLabels": {"KeyName": ""},
        "ulimits": [
            {
                "name": "msgqueue",
                "softLimit": 0,
                "hardLimit": 0
            }
        ],
        "logConfiguration": {
            "logDriver": "awslogs",
            "options": {"KeyName": ""},
            "secretOptions": [
                {
                    "name": "",
```

```
                    "valueFrom": ""
                }
            ]
        },
        "healthCheck": {
            "command": [""],
            "interval": 0,
            "timeout": 0,
            "retries": 0,
            "startPeriod": 0
        },
        "systemControls": [
            {
                "namespace": "",
                "value": ""
            }
        ],
        "resourceRequirements": [
            {
                "value": "",
                "type": "GPU"
            }
        ],
        "firelensConfiguration": {
            "type": "fluentd",
            "options": {"KeyName": ""}
        }
    }
],
"volumes": [
    {
        "name": "",
        "host": {"sourcePath": ""},
        "configuredAtLaunch":true,
        "dockerVolumeConfiguration": {
            "scope": "task",
            "autoprovision": true,
            "driver": "",
            "driverOpts": {"KeyName": ""},
            "labels": {"KeyName": ""}
        },
        "efsVolumeConfiguration": {
            "fileSystemId": "",
            "rootDirectory": "",
```

```
                "transitEncryption": "ENABLED",
                "transitEncryptionPort": 0,
                "authorizationConfig": {
                    "accessPointId": "",
                    "iam": "ENABLED"
                }
            }
        }
    ],
    "requiresCompatibilities": ["FARGATE"],
    "cpu": "",
    "memory": "",
    "tags": [
        {
            "key": "",
            "value": ""
        }
    ],
    "ephemeralStorage": {"sizeInGiB": 0},
    "pidMode": "task",
    "ipcMode": "none",
    "proxyConfiguration": {
        "type": "APPMESH",
        "containerName": "",
        "properties": [
            {
                "name": "",
                "value": ""
            }
        ]
    },
    "inferenceAccelerators": [
        {
            "deviceName": "",
            "deviceType": ""
        }
    ]
}
```

このタスク定義テンプレートは、以下の AWS CLI コマンドにより生成できます。

```
aws ecs register-task-definition --generate-cli-skeleton
```

Amazon ECS のタスク定義の例

これらの例とスニペットをコピーして、ユーザー自身のタスク定義の作成を開始することができます。

例をコピーして、コンソールで [JSON 経由の設定] オプションを使用するときに貼り付けることができます。アカウント ID を使用するなど、例を必ずカスタマイズしてください。スニペットはタスク定義 JSON に含めることができます。詳細については、コンソールを使用した Amazon ECS タスク定義の作成およびFargate 起動タイプでの Amazon ECS タスク定義パラメータを参照してください。

その他のタスク定義の例については、GitHub の「AWS のタスク定義例」を参照してください。

トピック

Web サーバー

以下は、Web サーバーをセットアップするために、Fargate 起動タイプで Linux コンテナを使用するタスク定義の例です。

```
{
   "containerDefinitions": [
      {
         "command": [
            "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample App</
title> <style>body {margin-top: 40px; background-color: #333;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
```

```
 <h2>Congratulations!</h2> <p>Your application is now running on a container in Amazon
 ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html && httpd-
foreground\""
         ],
         "entryPoint": [
            "sh",
            "-c"
         ],
         "essential": true,
         "image": "public.ecr.aws/docker/library/httpd:2.4",
         "logConfiguration": {
            "logDriver": "awslogs",
            "options": {
               "awslogs-group" : "/ecs/fargate-task-definition",
               "awslogs-region": "us-east-1",
               "awslogs-stream-prefix": "ecs"
            }
         },
         "name": "sample-fargate-app",
         "portMappings": [
            {
               "containerPort": 80,
               "hostPort": 80,
               "protocol": "tcp"
            }
         ]
      }
   ],
   "cpu": "256",
   "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
   "family": "fargate-task-definition",
   "memory": "512",
   "networkMode": "awsvpc",
   "runtimePlatform": {
        "operatingSystemFamily": "LINUX"
    },
   "requiresCompatibilities": [
       "FARGATE"
    ]
}
```

以下は、Web サーバーをセットアップするために、Fargate 起動タイプで Windows コンテナを使用するタスク定義の例です。

```
{
    "containerDefinitions": [
        {
            "command": ["New-Item -Path C:\\inetpub\\wwwroot\\index.html -Type file
 -Value '<html> <head> <title>Amazon ECS Sample App</title> <style>body {margin-top:
 40px; background-color: #333;} </style> </head><body> <div style=color:white;text-
align:center> <h1>Amazon ECS Sample App</h1> <h2>Congratulations!</h2> <p>Your
 application is now running on a container in Amazon ECS.</p>'; C:\\ServiceMonitor.exe
 w3svc"],
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "essential": true,
            "cpu": 2048,
            "memory": 4096,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "name": "sample_windows_app",
            "portMappings": [
                {
                    "hostPort": 80,
                    "containerPort": 80,
                    "protocol": "tcp"
                }
            ]
        }
    ],
    "memory": "4096",
    "cpu": "2048",
    "networkMode": "awsvpc",
    "family": "windows-simple-iis-2019-core",
    "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
    "runtimePlatform": {"operatingSystemFamily": "WINDOWS_SERVER_2019_CORE"},
    "requiresCompatibilities": ["FARGATE"]
}
```

splunk ログドライバー

以下のスニペットでは、タスク定義で、リモートサービスにログを送信する splunk ログドライバーを使用する方法を示しています。Splunk トークンパラメータは、機密データとして扱われる可

能性があるため、シークレットのオプションとして指定しています。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

```
"containerDefinitions": [{
  "logConfiguration": {
   "logDriver": "splunk",
   "options": {
    "splunk-url": "https://cloud.splunk.com:8080",
    "tag": "tag_name",
   },
   "secretOptions": [{
    "name": "splunk-token",
    "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:splunk-token-
KnrBkD"
}],
```

fluentd ログドライバー

以下のスニペットでは、タスク定義で、リモートサービスにログを送信する fluentd ログドライバーを使用する方法を示しています。fluentd-address 値は機密データとして扱われる可能性があるため、シークレットのオプションとして指定しています。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

```
"containerDefinitions": [{
 "logConfiguration": {
  "logDriver": "fluentd",
  "options": {
   "tag": "fluentd demo"
  },
  "secretOptions": [{
   "name": "fluentd-address",
   "valueFrom": "arn:aws:secretsmanager:region:aws_account_id:secret:fluentd-address-
KnrBkD"
  }]
 },
 "entryPoint": [],
 "portMappings": [{
             "hostPort": 80,
             "protocol": "tcp",
             "containerPort": 80
             },
             {
```

```
  "hostPort": 24224,
  "protocol": "tcp",
  "containerPort": 24224
 }]
}],
```

gelf ログドライバー

以下のスニペットでは、タスク定義で、Gelf ログを入力として受け取る Logstash を実行しているリモートホストにログを送信する gelf ログドライバーを使用する方法を示しています。詳細については、「logConfiguration」を参照してください。

```
"containerDefinitions": [{
 "logConfiguration": {
  "logDriver": "gelf",
  "options": {
   "gelf-address": "udp://logstash-service-address:5000",
   "tag": "gelf task demo"
  }
 },
 "entryPoint": [],
 "portMappings": [{
   "hostPort": 5000,
   "protocol": "udp",
   "containerPort": 5000
  },
  {
   "hostPort": 5000,
   "protocol": "tcp",
   "containerPort": 5000
  }
 ]
}],
```

外部インスタンス上のワークロード

Amazon ECS タスク定義を登録するときは、requiresCompatibilitiesパラメーターを選択し、EXTERNALで、外部インスタンスで Amazon ECS ワークロードを実行するときに、タスク定義が使用できる互換性があることを検証します。コンソールを使用してタスク定義を登録する場合は、JSON エディターを使用する必要があります。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

> **Important**
>
> タスクにタスク実行 IAM ロールが必要な場合は、タスク定義で指定されていることを確認してください。

ワークロードをデプロイするときは、EXTERNAL起動タイプを、サービスの作成時またはスタンドアロンタスクの実行時に選択します。

以下は、タスク定義の例です。

Linux

```
{
 "requiresCompatibilities": [
  "EXTERNAL"
 ],
 "containerDefinitions": [{
  "name": "nginx",
  "image": "public.ecr.aws/nginx/nginx:latest",
  "memory": 256,
  "cpu": 256,
  "essential": true,
  "portMappings": [{
   "containerPort": 80,
   "hostPort": 8080,
   "protocol": "tcp"
  }]
 }],
 "networkMode": "bridge",
 "family": "nginx"
}
```

Windows

```
{
 "requiresCompatibilities": [
  "EXTERNAL"
 ],
 "containerDefinitions": [{
  "name": "windows-container",
  "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-ltsc2019",
```

```
  "memory": 256,
  "cpu": 512,
  "essential": true,
  "portMappings": [{
   "containerPort": 80,
   "hostPort": 8080,
   "protocol": "tcp"
  }]
 }],
 "networkMode": "bridge",
 "family": "windows-container"
}
```

Amazon ECR イメージとタスク定義 IAM ロール

以下のスニペットでは、aws-nodejs-sample という名前の Amazon ECR イメージで、123456789012.dkr.ecr.us-west-2.amazonaws.com レジストリの v1 タグを使用しています。このタスクのコンテナは、arn:aws:iam::123456789012:role/AmazonECSTaskS3BucketRole ロールから IAM アクセス許可を継承します。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

```
{
    "containerDefinitions": [
        {
            "name": "sample-app",
            "image": "123456789012.dkr.ecr.us-west-2.amazonaws.com/aws-nodejs-
sample:v1",
            "memory": 200,
            "cpu": 10,
            "essential": true
        }
    ],
    "family": "example_task_3",
    "taskRoleArn": "arn:aws:iam::123456789012:role/AmazonECSTaskS3BucketRole"
}
```

コマンドによるエントリポイント

以下のスニペットでは、エントリポイントとコマンド引数を使用する Docker コンテナの構文を示しています。このコンテナは example.com に対して ping を 508 回実行してから終了します。

```
{
    "containerDefinitions": [
        {
            "memory": 32,
            "essential": true,
            "entryPoint": ["ping"],
            "name": "alpine_ping",
            "readonlyRootFilesystem": true,
            "image": "alpine:3.4",
            "command": [
                "-c",
                "4",
                "example.com"
            ],
            "cpu": 16
        }
    ],
    "family": "example_task_2"
}
```

コンテナの依存関係

このスニペットでは、コンテナの依存関係が指定されている複数のコンテナを含むタスク定義の構文を示しています。次のタスク定義では、app コンテナ が開始される前に、envoy コンテナが必要とされるコンテナのヘルスチェックパラメータにより決定される正常なステータスに達する必要があります。詳しくは、「コンテナの依存関係」を参照してください。

```
{
  "family": "appmesh-gateway",
  "runtimePlatform": {
        "operatingSystemFamily": "LINUX"
  },
  "proxyConfiguration":{
      "type": "APPMESH",
      "containerName": "envoy",
      "properties": [
          {
              "name": "IgnoredUID",
              "value": "1337"
          },
          {
              "name": "ProxyIngressPort",
```

```
                "value": "15000"
            },
            {
                "name": "ProxyEgressPort",
                "value": "15001"
            },
            {
                "name": "AppPorts",
                "value": "9080"
            },
            {
                "name": "EgressIgnoredIPs",
                "value": "169.254.170.2,169.254.169.254"
            }
        ]
    },
    "containerDefinitions": [
      {
        "name": "app",
        "image": "application_image",
        "portMappings": [
          {
            "containerPort": 9080,
            "hostPort": 9080,
            "protocol": "tcp"
          }
        ],
        "essential": true,
        "dependsOn": [
          {
            "containerName": "envoy",
            "condition": "HEALTHY"
          }
        ]
      },
      {
        "name": "envoy",
        "image": "840364872350.dkr.ecr.region-code.amazonaws.com/aws-appmesh-
envoy:v1.15.1.0-prod",
        "essential": true,
        "environment": [
          {
            "name": "APPMESH_VIRTUAL_NODE_NAME",
            "value": "mesh/meshName/virtualNode/virtualNodeName"
```

```
        },
        {
          "name": "ENVOY_LOG_LEVEL",
          "value": "info"
        }
      ],
      "healthCheck": {
        "command": [
          "CMD-SHELL",
          "echo hello"
        ],
        "interval": 5,
        "timeout": 2,
        "retries": 3
      }
    }
  ],
  "executionRoleArn": "arn:aws:iam::123456789012:role/ecsTaskExecutionRole",
  "networkMode": "awsvpc"
}
```

Windows のサンプルのタスク定義

Amazon ECS で Windows コンテナを使い始める際に役立つタスク定義サンプルを以下に示します。

Example Windows 用の Amazon ECS コンソールサンプルアプリケーション

次のタスク定義は、Amazon ECS の初回実行ウィザードで生成される Amazon ECS コンソールのサンプルアプリケーションです。`microsoft/iis` Windows コンテナイメージを使用するために移植されています。

```
{
  "family": "windows-simple-iis",
  "containerDefinitions": [
    {
      "name": "windows_sample_app",
      "image": "mcr.microsoft.com/windows/servercore/iis",
      "cpu": 1024,
      "entryPoint":["powershell", "-Command"],
      "command":["New-Item -Path C:\\inetpub\\wwwroot\\index.html -Type file -
Value '<html> <head> <title>Amazon ECS Sample App</title> <style>body {margin-top:
 40px; background-color: #333;} </style> </head><body> <div style=color:white;text-
align:center> <h1>Amazon ECS Sample App</h1> <h2>Congratulations!</h2> <p>Your
```

```
 application is now running on a container in Amazon ECS.</p>'; C:\\ServiceMonitor.exe
 w3svc"],
      "portMappings": [
        {
          "protocol": "tcp",
          "containerPort": 80
        }
      ],
      "memory": 1024,
      "essential": true
    }
  ],
  "networkMode": "awsvpc",
  "memory": "1024",
  "cpu": "1024"
}
```

Amazon ECS クラスター

Amazon ECS クラスターは、タスクまたはサービスの論理グループです。タスクとサービスに加え、クラスターは次のリソースで構成されます。

- 次を組み合わせたものにできるインフラストラクチャキャパシティ:
  - クラウド内 AWS の Amazon EC2 instances
  - AWS クラウドでの (AWS Fargate) サーバーレス
  - オンプレミス仮想マシン (VM) またはサーバー
- タスクとサービスが実行されるネットワーク (VPC およびサブネット)

  キャパシティーとして Amazon EC2 インスタンスを使用する場合、サブネットはアベイラビリティゾーン、ローカルゾーン、Wavelength ゾーン、または AWS Outposts に含められます。
- オプションの名前空間

  名前空間は、Service Connect とのサービス間通信に使用されます。
- モニタリングオプション

  CloudWatch Container Insights は追加料金がかかるフルマネージドサービスです。Amazon ECS のメトリクスとログを自動で収集、集計、要約します。

Amazon ECS クラスターに関する全般的な概念を以下に示します。

- クラスターを作成してリソースを分離します。
- クラスターは AWS リージョン 固有です。
- クラスターは、次のいずれかの状態になります。

  ACTIVE

  クラスターはタスクを受け入れる準備ができており、該当する場合は、クラスターにコンテナインスタンスを登録できます。

  PROVISIONING

  クラスターにはキャパシティプロバイダーが関連付けられており、キャパシティプロバイダーに必要なリソースが作成されています。

プロビジョン解除中

クラスターにはキャパシティプロバイダーが関連付けられており、キャパシティプロバイダーに必要なリソースが削除されています。

FAILED

クラスターにはキャパシティプロバイダーが関連付けられており、キャパシティプロバイダーに必要なリソースの作成に失敗しました。

INACTIVE

クラスターは削除されました。INACTIVE ステータスのクラスターは、一定期間アカウント内で検出可能なままになる場合があります。この動作は今後変更される可能性があるため、INACTIVE クラスターの永続的な使用を前提としないようにしてください。

- クラスターには、AWS Fargate、Amazon EC2 インスタンス、または外部インスタンスでホストされているタスクを混在させることができます。タスクは、起動タイプまたはキャパシティプロバイダー戦略として、Fargate または EC2 のインフラストラクチャで実行できます。EC2 を起動タイプとして使用する場合、Amazon ECS は Amazon EC2 Auto Scaling グループのキャパシティーを追跡およびスケーリングしません。起動タイプの詳細については、「Amazon ECS 起動タイプ」を参照してください。
- クラスターには、Auto Scaling グループキャパシティプロバイダーと Fargate キャパシティプロバイダーの両方を混在させることができます。ただし、キャパシティープロバイダー戦略に含めることができるのは、Auto Scaling グループのキャパシティープロバイダーまたは Fargate のキャパシティープロバイダーのみです。
- EC2 起動タイプまたは Auto Scaling グループキャパシティープロバイダーには、さまざまなインスタンスタイプを使用できます。インスタンスは、一度に 1 つのクラスターにしか登録できません。
- カスタム IAM ポリシーを作成することで、クラスターへのアクセスを制限できます。詳細については、「Amazon Elastic Container Service のアイデンティティベースのポリシーの例」の「Amazon ECS クラスターの例」セクションを参照してください。
- サービス自動スケーリングを使用して Fargate タスクをスケーリングできます。詳細については、「Amazon ECS サービスを自動的にスケールする」を参照してください。
- クラスターのデフォルトの Service Connect 名前空間を設定できます。デフォルトの Service Connect 名前空間を設定したら、Service Connect を有効にすることで、クラスター内で作成された新しいサービスを名前空間のクライアントサービスとして追加できます。追加の設定は必要ありません。詳細については、「Service Connect を使用して Amazon ECS サービスを短縮名で接続する」を参照してください。

Fargate 起動タイプ用の Amazon ECS クラスター

Amazon ECS キャパシティープロバイダーは、クラスター内のタスクに対するインフラストラクチャのスケーリングを管理できます。各クラスターには、1 つ以上のキャパシティプロバイダーがあり、さらにオプションとしてキャパシティプロバイダー戦略があります。キャパシティープロバイダー戦略は、クラスターの複数のキャパシティープロバイダー間にタスクを分散する方法を決定します。スタンドアロンタスクを実行するか、サービスを作成するときは、クラスターのデフォルトのキャパシティプロバイダー戦略か、クラスターのデフォルト戦略をオーバーライドするキャパシティプロバイダー戦略のいずれかを使用します。

AWS Fargate でタスクを実行する場合、キャパシティーを作成または管理する必要はありません。以下のいずれかの事前定義されたキャパシティープロバイダーをクラスターに関連付ける必要があるだけです。

- Fargate
- Fargate Spot

AWS Fargate キャパシティプロバイダーで Amazon ECS を使用すると、Amazon ECS タスクで Fargate と Fargate Spot キャパシティの両方を使用できます。

Fargate Spot を使用すると、割り込み許容のある Amazon ECS タスクを、Fargate 料金と比較して割引料金で実行できます。Fargate Spot は、予備のコンピュートキャパシティーでタスクを実行します。AWS がキャパシティを戻す必要がある場合、タスクは中断され、2 分間の警告が表示されます。

Fargate と Fargate Spot キャパシティープロバイダーを使用するタスクが停止した場合、タスク状態の変更イベントが Amazon EventBridge に対し送信されます。停止した理由は原因を説明しています。詳細については、「Amazon ECS タスク状態変更イベント」を参照してください。

クラスターには、Fargate キャパシティプロバイダーと Auto Scaling グループキャパシティプロバイダーを混在させることができます。ただし、キャパシティプロバイダー戦略に含めることができるのは Fargate または Auto Scaling グループキャパシティプロバイダーのみで、両方を含めることはできません。詳細については、「Auto Scaling グループキャパシティープロバイダー」を参照してください。

キャパシティプロバイダーを使用する場合は、次の点を考慮します。

- キャパシティープロバイダーは、キャパシティープロバイダー戦略に関連付ける前に、クラスターに関連付ける必要があります。

- キャパシティープロバイダー戦略には、最大 20 のキャパシティープロバイダーを指定できます。
- Auto Scaling グループキャパシティプロバイダーを使用するサービスは、Fargate キャパシティプロバイダーを使用するように更新することはできません。逆の場合も同様です。
- キャパシティプロバイダー戦略では、コンソールでキャパシティプロバイダーに `weight` 値が指定されていない場合、1 のデフォルト値が使用されます。API または AWS CLI を使用する場合は、`0` のデフォルト値が使用されます。
- キャパシティプロバイダー戦略内で複数のキャパシティプロバイダーを指定する場合、少なくとも 1 つのキャパシティプロバイダーのウェイト値が 0 より大きい必要があります。ウェイトが 0 のキャパシティープロバイダーはタスクの配置に使用されません。戦略に複数のキャパシティプロバイダーを指定し、すべて同じウェイトを 0 にした場合、キャパシティプロバイダー戦略を使用する `RunTask` または `CreateService` のアクションは失敗します。
- キャパシティプロバイダー戦略では、1 つのキャパシティプロバイダーのみが定義されたベース値を持つことができます。ベース値を指定しない場合は、デフォルト値の 0 が使用されます。
- クラスターには、Auto Scaling グループキャパシティプロバイダーと Fargate キャパシティプロバイダーの両方を混在させることができます。ただし、キャパシティプロバイダー戦略に含めることができるのは Auto Scaling グループまたは Fargate キャパシティプロバイダーのみで、両方を含めることはできません。
- クラスターには、キャパシティプロバイダーと起動タイプの両方を使用するサービスとスタンドアロンタスクを混在させることができます。サービスは、起動タイプではなくキャパシティプロバイダー戦略を使用するように更新できます。ただし、その場合は強制的に新しいデプロイを行う必要があります。

Fargate Spot 終了通知

需要が非常に多い時期は、Fargate Spot のキャパシティーが利用できない場合があります。これにより、Fargate Spot のタスクが遅れる可能性があります。これが発生すると、Amazon ECS サービスは必要なキャパシティーが使用可能になるまでタスクの起動を再試行します。Fargate が Spot キャパシティーをオンデマンドキャパシティに置き換えることはありません。

スポットの中断により Fargate Spot キャパシティーを使用するタスクが停止すると、タスクが停止する前に 2 分間の警告が送信されます。警告は、タスク状態変更イベントとして Amazon EventBridge に送信され、実行中のタスクに SIGTERM シグナルとして送信されます。サービスの一部として Fargate Spot を使用する場合、このシナリオでは、サービススケジューラは中断信号を受信し、利用可能なキャパシティがあれば Fargate Spot で追加のタスクを起動しようとします。タスクが 1 つしかないサービスは、キャパシティが利用可能になるまで中断されます。正常なシャットダウンの詳細については、「ECS による正常なシャットダウン」を参照してください。

タスクが停止する前にコンテナが正常に終了するように、以下を設定できます。

- タスクが使用しているコンテナ定義には、120 秒以下の stopTimeout 値を指定できます。デフォルトの stopTimeout 値は 30 秒です。stopTimeout 値を長く指定すると、タスク状態変更イベントが受信した時点から、コンテナが強制的に停止するまでの時間を長くすることができます。詳細については、「[コンテナのタイムアウト]」を参照してください。
- クリーンアップアクションを実行するには、コンテナ内から SIGTERM シグナルを受信する必要があります。このシグナルの処理に失敗すると、stopTimeout が設定された後に SIGKILL シグナルを受信し、データが損失または破損する可能性があります。

タスク状態変更イベントのスニペットを以下に示します。このスニペットには、Fargate Spot 中断の停止理由と停止コードが表示されます。

```
{
  "version": "0",
  "id": "9bcdac79-b31f-4d3d-9410-fbd727c29fab",
  "detail-type": "ECS Task State Change",
  "source": "aws.ecs",
  "account": "111122223333",
  "resources": [
    "arn:aws:ecs:us-east-1:111122223333:task/b99d40b3-5176-4f71-9a52-9dbd6f1cebef"
  ],
  "detail": {
    "clusterArn": "arn:aws:ecs:us-east-1:111122223333:cluster/default",
    "createdAt": "2016-12-06T16:41:05.702Z",
    "desiredStatus": "STOPPED",
    "lastStatus": "RUNNING",
    "stoppedReason": "Your Spot Task was interrupted.",
    "stopCode": "SpotInterruption",
    "taskArn": "arn:aws:ecs:us-east-1:111122223333:task/
b99d40b3-5176-4f71-9a52-9dbd6fEXAMPLE",
    ...
  }
}
```

以下は、Amazon ECS タスク状態変更イベントの EventBridge ルールを作成するために使用されるイベントパターンです。オプションで、detail フィールドでクラスターを指定できます。そうすると、そのクラスターのタスク状態変更イベントを受信することになります。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「Amazon EventBridge の開始方法」を参照してください。

```
{
    "source": [
        "aws.ecs"
    ],
    "detail-type": [
        "ECS Task State Change"
    ],
    "detail": {
        "clusterArn": [
            "arn:aws:ecs:us-west-2:111122223333:cluster/default"
        ]
    }
}
```

Fargate 起動タイプ用の Amazon ECS クラスターを作成する

クラスターを作成して、タスクとサービスを実行するインフラストラクチャを定義します。

これを開始する前に、「Amazon ECS を使用するようにセットアップする」 の手順を完了し、適切な IAM 許可を割り当てる必要があります。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。Amazon ECS コンソールでは、AWS CloudFormation スタックを作成することで、Amazon ECS クラスターに必要なリソースを作成します。

コンソールは、自動的に Fargate および Fargate Spot キャパシティープロバイダーをクラスターに関連付けます。

クラスターに加えて、コンソールは以下のリソースを自動的に作成します。

- AWS Cloud Map に、クラスターと同じ名前のデフォルトの名前空間を作成します。名前空間を使用すると、クラスターで作成したサービスを、追加の設定なしで名前空間内の他のサービスに接続できます。

  詳細については、「Amazon ECS サービスを相互接続する」を参照してください。

以下のオプションを変更できます。

- クラスターに関連付けられたデフォルトの名前空間を変更します。
- オブザーバビリティが強化された Container Insights、または Container Insights を有効にします。

  CloudWatch Container Insights は、コンテナ化されたアプリケーションおよびマイクロサービスのメトリクスとログを収集、集約、要約します。Container Insights は、問題の迅速な特定と解決

に使用するコンテナの再起動失敗などの診断情報も提供します。詳細については、「the section called “オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する”」を参照してください。

2024 年 12 月 2 日、AWS で Amazon ECS 用にオブザーバビリティが強化された Container Insights がリリースされました。このバージョンでは、Amazon EC2 および Fargate 起動タイプを使用して Amazon ECS 用に強化されたオブザーバビリティがサポートされます。Amazon ECS でオブザーバビリティが強化された Container Insights を設定したら、Container Insights は環境内のクラスターレベルからコンテナレベルまでの詳細なインフラストラクチャテレメトリを自動収集し、さまざまなメトリクスとディメンションを示すダッシュボードにデータを表示します。その後、Container Insights コンソールでこれらのすぐに使えるダッシュボードを使用して、コンテナの健全性とパフォーマンスをよりよく理解し、異常を特定することで問題を迅速に軽減することができます。

コンテナ環境で詳細な可視性を提供し、解決までの平均時間を短縮するため、Container Insights ではなく、オブザーバビリティが強化された Container Insights を使用することをお勧めします。

- クラスターを識別しやすいようにタグを追加します。

手順

新しいクラスターを作成するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [クラスター設定] で以下を設定します。
   - [クラスター名] に一意の名前を入力します。

     名前には、最大 255 文字 (大文字と小文字)、数字、およびハイフンを含めることができます。
   - (オプション) Service Connect に使用する名前空間をクラスター名と別のものにするには、[名前空間] に一意の名前を入力します。
6. (オプション) Container Insights を使用して モニタリング を展開し、次のいずれかのオプションを選択します。

- オブザーバビリティが強化された推奨の Container Insights を使用するには、[オブザーバビリティが強化された Container Insights] を選択します。
- Container Insights を使用するには、[Container Insights] を選択します。

7. (オプション) クラスターを識別しやすくするには、[Tags] (タグ) を展開し、タグを設定します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。

8. [Create] (作成) を選択します。

次のステップ

クラスターを作成したら、アプリケーションのタスク定義を作成し、スタンドアロンタスク、またはサービスの一部として実行できます。詳細については次を参照してください:

- Amazon ECSの タスク定義
- Amazon ECS タスクとしてのアプリケーションの実行
- コンソールを使用した Amazon ECS サービスの作成

EC2 起動タイプ用の Amazon ECS キャパシティープロバイダー

キャパシティーとして Amazon EC2 インスタンスを使用する場合は、Auto Scaling グループを使用し、クラスターに登録されている Amazon EC2 インスタンスを管理します。Auto Scaling により、アプリケーションの負荷を処理するために適切な数の使用可能な Amazon EC2 インスタンスを確保できるようになります。

マネージドスケーリング機能を使用して、Auto Scaling グループのスケールインおよびスケールアウトアクションを Amazon ECS に管理させることも、自分自身でスケーリングアクションを管理することもできます。詳細については、「クラスターの自動スケーリングで Amazon ECS キャパシティーを自動的に管理する」を参照してください。

新しい空の Auto Scaling グループを作成することをお勧めします。既存の Auto Scaling グループを使用する場合、キャパシティプロバイダーの作成に使用される Auto Scaling グループの前に、既に

実行され、Amazon EC2 クラスターに登録されていたグループに関連付けられた Amazon ECS インスタンスが、キャパシティプロバイダーに正しく登録されないことがあります。これにより、キャパシティプロバイダー戦略でキャパシティプロバイダーを使用するときに問題が発生する可能性があります。`DescribeContainerInstances` を使用し、コンテナインスタンスがキャパシティープロバイダーに関連付けられているかどうかを確認できます。

> **Note**
>
> 空の Auto Scaling グループを作成するには、必要なカウントをゼロに設定します。キャパシティプロバイダーを作成してクラスターに関連付けた後、スケールアウトできます。Amazon ECS コンソールを使用する場合、Amazon ECS は、AWS CloudFormation スタックの一部として、ユーザーの代わりに Amazon EC2 起動テンプレートと Auto Scaling グループを作成します。これらには、プレフィックスとして `EC2ContainerService-<ClusterName>` が付きます。Auto Scaling グループは、そのクラスターのキャパシティープロバイダーとして使用できます。

マネージドインスタンスドレイニングを使用して、ワークロードを中断することなく Amazon EC2 インスタンスを正常終了できるようにすることをお勧めします。この機能は、デフォルトでオンになっています。詳細については、「EC2 インスタンスで実行されている Amazon ECS ワークロードを安全に停止する」を参照してください。

コンソール内の Auto Scaling グループキャパシティープロバイダーを使用する場合は、次の点を考慮する必要があります。

- Auto Scaling グループをスケールアウトするには、その `MaxSize` が `0` より大きくなければなりません。
- Auto Scaling グループは、インスタンスの重み付けを設定することはできません。
- Auto Scaling グループが実行されるタスクの数に合わせてスケールアウトできない場合、タスクは `PROVISIONING` の後の状態に移行できません。
- キャパシティプロバイダーによって管理される Auto Scaling グループに関連付けられているスケーリングポリシーリソースは、変更しないでください。
- キャパシティプロバイダーの作成時にマネージドスケーリングがオンになっている場合、Auto Scaling グループの希望するカウントを `0` に設定できます。マネージドスケーリングがオンになっている場合、Amazon ECS は Auto Scaling グループのスケールインアクションとスケールアウトアクションを管理します。

- キャパシティープロバイダーは、キャパシティープロバイダー戦略に関連付ける前に、クラスターに関連付ける必要があります。
- キャパシティープロバイダー戦略には、最大 20 のキャパシティープロバイダーを指定できます。
- Auto Scaling グループキャパシティプロバイダーを使用するサービスは、Fargate キャパシティプロバイダーを使用するように更新することはできません。逆の場合も同様です。
- キャパシティプロバイダー戦略では、コンソールでキャパシティプロバイダーに `weight` 値が指定されていない場合、1 のデフォルト値が使用されます。API または AWS CLI を使用する場合は、`0` のデフォルト値が使用されます。
- キャパシティプロバイダー戦略内で複数のキャパシティプロバイダーを指定する場合、少なくとも 1 つのキャパシティプロバイダーのウェイト値が 0 より大きい必要があります。ウェイトが 0 のキャパシティープロバイダーはタスクの配置に使用されません。戦略に複数のキャパシティプロバイダーを指定し、すべて同じウェイトを 0 にした場合、キャパシティプロバイダー戦略を使用する `RunTask` または `CreateService` のアクションは失敗します。
- キャパシティプロバイダー戦略では、1 つのキャパシティプロバイダーのみが定義されたベース値を持つことができます。ベース値を指定しない場合は、デフォルト値の 0 が使用されます。
- クラスターには、Auto Scaling グループキャパシティプロバイダーと Fargate キャパシティプロバイダーの両方を混在させることができます。ただし、キャパシティプロバイダー戦略に含めることができるのは Auto Scaling グループまたは Fargate キャパシティプロバイダーのみで、両方を含めることはできません。
- クラスターには、キャパシティプロバイダーと起動タイプの両方を使用するサービスとスタンドアロンタスクを混在させることができます。サービスは、起動タイプではなくキャパシティプロバイダー戦略を使用するように更新できます。ただし、その場合は強制的に新しいデプロイを行う必要があります。
- Amazon ECS では、Amazon EC2 Auto Scaling ウォームプールをサポートします。ウォームプールは、事前に初期化済みの Amazon EC2 インスタンスグループでサービス開始が準備されています。アプリケーションがスケールアウトする必要がある場合は、常に Amazon EC2 Auto Scaling はコールドインスタンスを起動するのではなく、ウォームプールから事前に初期化されたインスタンスを使用します。これにより、インスタンスがサービスを開始する前に、最終的な初期化プロセスを実行できるようになります。詳細については、「Amazon ECS Auto Scaling グループ用に事前初期化されたインスタンスを設定する」を参照してください。

Amazon EC2 Auto Scaling 起動テンプレートの作成についての詳細は、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling 起動テンプレート」を参照してください。Amazon EC2 Auto Scaling グループの作成についての詳細は、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループ」を参照してください。

Amazon ECS の Amazon EC2 コンテナインスタンスのセキュリティに関する考慮事項

脅威モデル内での単一のコンテナインスタンスとそのアクセスを考慮する必要があります。たとえば、影響を受けるひとつのタスクが、同じインスタンス上の感染していないタスクの IAM アクセス許可を利用できる場合があります。

これを防ぐには、次のことを行うことをお勧めします。

- タスクを実行するときは、管理者権限を使用しないでください。
- タスクに割り当てるタスクロールは最小特権にします。

  コンテナエージェントは、Amazon ECS リソースへのアクセスに使用される固有の認証情報 ID を持つトークンを自動的に作成します。
- `awsvpc` ネットワークモードを使用するタスクで実行されたコンテナが、Amazon EC2 のインスタンスプロファイルに入力されている認証情報にアクセスするのを防止しつつ、タスクロールで指定されている許可を有効にするには、エージェントの設定ファイルで `ECS_AWSVPC_BLOCK_IMDS` エージェント設定変数を [true] に設定し、そのエージェントを再起動します。
- Amazon GuardDuty ランタイムモニタリングを使用して、AWS 環境内のクラスターとコンテナの脅威を検出します。Runtime Monitoring では、ファイルアクセス、プロセス実行、ネットワーク接続などの個々の Amazon ECS ワークロードを実行時に可視化する、GuardDuty セキュリティエージェントを使用します。詳細については、「GuardDuty ユーザーガイド」の「GuardDuty ランタイムモニタリング」を参照してください。

Amazon EC2 起動タイプ用の Amazon ECS クラスターの作成

クラスターを作成して、タスクとサービスを実行するインフラストラクチャを定義します。

これを開始する前に、「Amazon ECS を使用するようにセットアップする」 の手順を完了し、適切な IAM 許可を割り当てる必要があります。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。Amazon ECS コンソールでは、AWS CloudFormation スタックを作成することで、Amazon ECS クラスターに必要なリソースを簡単に作成できます。

クラスターの作成プロセスをできるだけ簡単にするために、コンソールには、以下で説明する多くの選択肢に対するデフォルトの選択肢があります。コンソール内のほとんどのセクションには、詳細なコンテキストを提供するヘルプパネルもあります。

クラスターの作成時に Amazon EC2 インスタンスを登録することや、作成後のクラスターに対し、追加のインスタンスを登録することもできます。

以下のデフォルトオプションを変更できます。

- インスタンスを起動するサブネットを変更します。
- コンテナインスタンスへのトラフィックを制御するために使用されるセキュリティグループを変更します。
- クラスターに関連付けられたデフォルトの名前空間を変更します。

  名前空間を使用すると、クラスターで作成したサービスを、追加の設定なしで名前空間内の他のサービスに接続できます。デフォルトの名前空間は、クラスター名と同じです。詳細については、「Amazon ECS サービスを相互接続する」を参照してください。
- オブザーバビリティが強化された Container Insights、または Container Insights を有効にします。

  CloudWatch Container Insights は、コンテナ化されたアプリケーションおよびマイクロサービスのメトリクスとログを収集、集約、要約します。Container Insights は、問題の迅速な特定と解決に使用するコンテナの再起動失敗などの診断情報も提供します。詳細については、「the section called “オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する”」を参照してください。

  2024 年 12 月 2 日、AWS で Amazon ECS 用にオブザーバビリティが強化された Container Insights がリリースされました。このバージョンでは、Amazon EC2 および Fargate 起動タイプを使用して Amazon ECS 用に強化されたオブザーバビリティがサポートされます。Amazon ECS でオブザーバビリティが強化された Container Insights を設定したら、Container Insights は環境内のクラスターレベルからコンテナレベルまでの詳細なインフラストラクチャテレメトリを自動収集し、さまざまなメトリクスとディメンションを示すダッシュボードにデータを表示します。その後、Container Insights コンソールでこれらのすぐに使えるダッシュボードを使用して、コンテナの健全性とパフォーマンスをよりよく理解し、異常を特定することで問題を迅速に軽減することができます。

  コンテナ環境で詳細な可視性を提供し、解決までの平均時間を短縮するため、Container Insights ではなく、オブザーバビリティが強化された Container Insights を使用することをお勧めします。
- クラスターを識別しやすいようにタグを追加します。

Auto Scaling グループオプション

Amazon EC2 インスタンスを使用する場合は、タスクとサービスが実行されるインフラストラクチャを管理するために Auto Scaling グループを指定する必要があります。

新しい Auto Scaling グループの作成を選択すると、自動的に次の動作が設定されます。

- Amazon ECS は Auto Scaling グループのスケールインアクションとスケールアウトアクションを管理します。
- Amazon ECS は、タスクを含む Auto Scaling グループ内の Amazon EC2 インスタンスがスケールインアクション中に終了されるのを防ぎます。詳細については、AWS Auto Scaling ユーザーガイドの「インスタンスの保護」を参照してください。

次の Auto Scaling グループプロパティを構成し、グループに対して起動するインスタンスのタイプと数を決定します。

- Amazon ECS に最適化された AMI。
- インスタンスタイプ。
- インスタンスに接続するときに ID を証明する SSH キーペア。SSH キーの作成については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 のキーペアと Linux インスタンス」を参照してください。
- Auto Scaling グループに対して起動するインスタンスの最小数。
- Auto Scaling グループに対して開始されるインスタンスの最大数。

  グループをスケールアウトするには、最大値を 0 より大きくする必要があります。

Amazon ECS は、AWS CloudFormation スタックの一部としてユーザーに代わり Amazon EC2 Auto Scaling 起動テンプレートと Auto Scaling グループを作成します。AMI、インスタンスタイプ、SSH キーペアのために指定した値は、起動テンプレート内に保存されます。テンプレートは `EC2ContainerService-<ClusterName>` プレフィックスが付いているため、識別が容易になります。Auto Scaling グループのプレフィックスは `<ClusterName>-ECS-Infra-ECSAutoScalingGroup` です。

Auto Scaling グループに対して起動されたインスタンスは、起動テンプレートを使用します。

ネットワークのオプション

デフォルトでは、インスタンスはリージョンのデフォルトのサブネットで起動されます。コンテナインスタンスへのトラフィックを制御するセキュリティグループは、現在サブネットに関連付けられているものが使用されます。インスタンスのサブネットとセキュリティグループは変更できます。

既存のサブネットを選択できます。セキュリティグループは、既存のものを使用することも、新しいものを作成することもできます。新しいセキュリティグループを作成するときは、少なくとも 1 つのインバウンドルールを指定する必要があります。

インバウンドルールは、コンテナインスタンスに到達できるトラフィックを決定し、以下のプロパティを含みます。

- 許可するプロトコル
- 許可するポートの範囲
- インバウンドトラフィック (送信元)

特定のアドレスまたは CIDR ブロックからのインバウンドトラフィックを許可するには、許可された CIDR で [送信元] に [カスタム] を使用します。

すべての送信先からのインバウンドトラフィックを許可するには、[送信元] に [すべて] を使用してください。これにより、これにより、0.0.0.0/0 IPv4 CIDR ブロックと::/0 IPv6 CIDR ブロックが自動的に追加されます。

ローカルコンピューターからのインバウンドトラフィックを許可するには、[送信元] に [ソースグループ] を使用します。これにより、ローカルコンピュータの現在の IP アドレスが送信元アドレスとして自動的に追加されます。

新しいクラスターを作成するには (Amazon ECS コンソール)

開始する前に、適切な IAM アクセス許可を割り当ててください。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [クラスター設定] で以下を設定します。

- [クラスター名] に一意の名前を入力します。

  名前には、最大 255 文字 (大文字と小文字)、数字、およびハイフンを含めることができます。

- (オプション) Service Connect に使用する名前空間をクラスター名と別のものにするには、[名前空間] に一意の名前を入力します。

6. Amazon EC2 インスタンスをクラスターに追加します。[インフラストラクチャー] を展開し、次に [Amazon EC2 インスタンス] を選択します。

   次に、キャパシティープロバイダーとして機能する Auto Scaling グループを設定します。

   a. 既存の Auto Scaling グループを使用するには、[Auto Scaling group (ASG)] (Auto Scaling グループ) からグループを選択します。

   b. Auto Scaling グループを作成するには、Auto Scaling group(ASG) (Auto Scaling グループ) から、[Create new group] (新しいグループの作成) を選択し、グループに関する以下の詳細情報を入力します。

      - [プロビジョニングモデル] で、[オンデマンド]インスタンスと[スポット]インスタンスのどちらを使用するかを選択します。
      - スポットインスタンスを使用する場合は、[割り当て戦略] で、インスタンスに使用するスポットキャパシティプール (インスタンスタイプおよびアベイラビリティーゾーン) を選択します。

        ほとんどのワークロードでは、[料金キャパシティ最適化] を選択できます。

        詳細については、「Amazon EC2 ユーザーガイド」の「Allocation strategies for Spot Instances」(スポットインスタンスの割り当て戦略) を参照してください。
      - コンテナインスタンスの Amazon マシンイメージ (AMI) で、Auto Scaling グループインスタンスの [Amazon ECS 最適化 AMI] を選択します。
      - [EC2 instance type] (EC2 インスタンスタイプ) を使用する場合、ワークロードのインスタンスタイプを選択します。

        マネージドスケーリングは、Auto Scaling グループが同じインスタンスタイプまたは類似のインスタンスタイプを使用している場合に最適です。
      - [EC2 インスタンスロール]では、既存のコンテナインスタンスロールを選択するか、新しいコンテナインスタンスロールを作成できます。

詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

- [Capacity] (キャパシティー) には、Auto Scaling グループで起動するインスタンスの最小数と最大数を入力します。
- [SSH key pair] (SSH キーペア) を使用する場合、インスタンスに接続する際に ID を証明するペアを選択してください。
- より大きなイメージとストレージを許容するには、[ルート EBS ボリュームサイズ] に単位 GiB で値を入力します。

7. (オプション) VPC とサブネットを変更するには、[Amazon EC2 インスタンスのネットワーキング] で、次のいずれかの操作を実行します。

   - サブネットを削除するには、[Subnets] (サブネット) で、削除するサブネットごとに [X] を選択します。
   - デフォルト VPC 以外の VPC に変更するには、[VPC] で既存の VPC を選択し、[サブネット] でサブネットを選択します。
   - 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] で、次のいずれかのオプションを選択します。
     - 既存のセキュリティグループを選択するには、[既存のセキュリティグループの選択] を選択してから、セキュリティグループを選択します。
     - 新しいセキュリティグループを作成するには、[新しいセキュリティグループの作成] を選択します。その後、各インバウンドルールについて [ルールの追加] を選択します。

       インバウンドルールの詳細については、「ネットワークのオプション」を参照してください。
   - Amazon EC2 コンテナインスタンスにパブリック IP アドレスを自動的に割り当てるには、[パブリック IP の自動割り当て] で以下のいずれかのオプションを選択します。
     - サブネット設定を使用 — インスタンスが起動するサブネットがパブリックサブネットの場合、パブリック IP アドレスをインスタンスに割り当てます。
     - オンにする — インスタンスにパブリック IP アドレスを割り当てます。

8. (オプション) Container Insights を使用して モニタリング を展開し、次のいずれかのオプションを選択します。

   - オブザーバビリティが強化された推奨の Container Insights を使用するには、[オブザーバビリティが強化された Container Insights] を選択します。

- Container Insights を使用するには、[Container Insights] を選択します。

9. (オプション)

   ランタイムのモニタリングを手動オプションで使用していて、このクラスターを GuardDuty でモニタリングしたい場合は、[タグを追加] を選択して次の操作を行います。

   - [キー] で「**`guardDutyRuntimeMonitoringManaged`**」と入力します。
   - [値] に「**`true`**」と入力します。

10. (オプション) クラスタータグを管理するには、[Tags] (タグ) を展開し、次のいずれかのオペレーションを実行します。

    [タグの追加] [タグの追加] を選択して、以下を実行します。

    - [キー] にはキー名を入力します。
    - [値] にキー値を入力します。

    [タグを削除] タグのキーと値の右側にある [削除] を選択します。

11. [Create] (作成) を選択します。

次のステップ

クラスターを作成したら、アプリケーションのタスク定義を作成し、スタンドアロンタスク、またはサービスの一部として実行できます。詳細については次を参照してください:

- Amazon ECSの タスク定義
- Amazon ECS タスクとしてのアプリケーションの実行
- コンソールを使用した Amazon ECS サービスの作成

クラスターの自動スケーリングで Amazon ECS キャパシティーを自動的に管理する

Amazon ECS では、クラスターに登録された Amazon EC2 インスタンスのスケーリングを管理できます。これは、Amazon ECS クラスターの自動スケーリングと呼ばれます。Amazon ECS Auto Scaling グループのキャパシティープロバイダーを作成するときに、マネージドスケーリングを有効にします。その後、この Auto Scaling グループのインスタンス使用率のターゲットパーセンテージ (`targetCapacity`) を設定します。Amazon ECS は 2 つのカスタム CloudWatch メトリク

ス、および Auto Scaling グループに対するターゲット追跡スケーリングポリシーを作成します。また、Amazon ECS は、タスクが使用するリソース使用率に基づいて、スケールインアクションとスケールアウトアクションを管理します。

クラスターに関連付けられている各 Auto Scaling グループのキャパシティプロバイダーについて、Amazon ECS は次のリソースを作成し、管理します。

- 低いメトリクス値の CloudWatch アラーム
- 高いメトリクス値の CloudWatch アラーム
- ターゲットの追跡スケーリングポリシー

> **Note**
>
> Amazon ECS は、ターゲットの追跡スケーリングポリシーを作成し、Auto Scaling グループにアタッチします。ターゲットの追跡スケーリングポリシーを更新するには、スケーリングポリシーを直接更新するのではなく、キャパシティプロバイダーのマネージドスケーリング設定を更新します。

マネージドスケーリングを無効にするか、クラスターからキャパシティプロバイダーの関連付けを解除すると、Amazon ECS は CloudWatch メトリクスとターゲットの追跡スケーリングポリシーのリソースの両方を削除します。

Amazon ECS では、実行するアクションを決定するのに次のメトリクスを使用します。

`CapacityProviderReservation`

特定のキャパシティプロバイダーで使用されているコンテナインスタンスの割合。Amazon ECS はこのメトリクスを生成します。

Amazon ECS は、`CapacityProviderReservation` の値を 0 ~ 100 の数値に設定します。Amazon ECS は、次の式を使用して Auto Scaling グループに残っているキャパシティの割合を表します。その後、Amazon ECS は CloudWatch にメトリクスをパブリッシュします。メトリクスの算出方法の詳細については、「Amazon ECS クラスター自動スケーリングを詳しく知る」を参照してください。

```
CapacityProviderReservation = (number of instances needed) / (number of running
 instances) x 100
```

`DesiredCapacity`

Auto Scaling グループのキャパシティ量。このメトリクスは CloudWatch に公開されていません。

Amazon ECS は `AWS/ECS/ManagedScaling` 名前空間内の CloudWatch に `CapacityProviderReservation` メトリックを公開します。`CapacityProviderReservation` メトリクスは、次のいずれかのアクションを実行します。

`CapacityProviderReservation` の値は `targetCapacity` に等しいです

Auto Scaling グループはスケールインまたはスケールアウトする必要はありません。目標使用率に達しました。

`CapacityProviderReservation` の値は `targetCapacity` より大きいです

キャパシティのパーセンテージを使用しているタスクの数が、自分の `targetCapacity` のパーセンテージを上回っています。`CapacityProviderReservation` メトリクスの値が増加すると、関連する CloudWatch アラームが動作します。このアラームは Auto Scaling グループの `DesiredCapacity` 値を更新します。Auto Scaling グループはこの値を使用して EC2 インスタンスを起動し、クラスターに登録します。

`targetCapacity` がデフォルト値の 100% の場合、インスタンスにタスクを実行できる空き容量がないため、スケールアウト中は新しいタスクは `PENDING` 状態になります。新しいインスタンスが ECS に登録されると、これらのタスクは新しいインスタンスで開始されます。

`CapacityProviderReservation` の値は `targetCapacity` 未満です

キャパシティのパーセンテージを使用しているタスクが自分の `targetCapacity` のパーセンテージよりも少なく、終了できるインスタンスが少なくとも 1 つあります。`CapacityProviderReservation` メトリクスの値が減少すると、関連する CloudWatch アラームが動作します。このアラームは Auto Scaling グループの `DesiredCapacity` 値を更新します。Auto Scaling グループはこの値を使用して EC2 コンテナインスタンスを終了し、クラスターから登録解除します。

Auto Scaling グループは、終了ポリシーを使用して、スケールインイベント中に最初に終了するインスタンスを決定します。さらに、インスタンスのスケールイン保護の設定は、回避します。クラスター自動スケーリングでは、マネージドターミネーション保護を有効にすると、どのインスタンスにインスタンススケールイン保護が設定されているかを管理できます。終了保護の詳細については、「Amazon ECS が終了するインスタンスの制御」を参照してください。詳細につい

ては、Amazon EC2 Auto Scaling ユーザーガイドの「スケールイン時にどの自動スケーリングインスタンスを終了するかのコントロール」を参照してください。

クラスターの自動スケーリングを使用するときは、次の点を考慮してください。

- キャパシティプロバイダーに関連付けられている Auto Scaling グループが希望するキャパシティは、Amazon ECS が管理しているもの以外のスケーリングポリシーを変更または管理しないでください。
- Amazon ECS が 0 インスタンスからスケールアウトする場合、自動的に 2 つのインスタンスを起動します。
- Amazon ECS は、ユーザーに代わって AWS Auto Scaling を呼び出すために必要なアクセス許可として `AWSServiceRoleForECS` サービスにリンクされた IAM ロールを使用します。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。
- Auto Scaling グループでキャパシティプロバイダーを使用する場合、キャパシティプロバイダーを作成するユーザー、グループ、ロールには `autoscaling:CreateOrUpdateTags` アクセス許可が必要です。これは、Auto Scaling グループが、キャパシティープロバイダーに関連付けるときに、Amazon ECS が Auto Scaling グループにタグを追加するためです。

  > **Important**
  >
  > ツールの使用により `AmazonECSManaged` タグが Auto Scaling グループから削除されないようにしてください。このタグが削除されると、Amazon ECS はスケーリングを管理できません。

- クラスターの自動スケーリングは、グループの [MinimumCapacity] と [MaximumCapacity] を変更しません。グループをスケールアウトするには、[MaximumCapacity] を 0 より大きくする必要があります。
- 自動スケーリング(マネージドスケーリング) がオンになっている場合、キャパシティプロバイダーは、同時に 1 つのクラスターにしか接続できません。キャパシティープロバイダーがマネージドスケーリングをオフにしている場合は、複数のクラスターに関連付けることができます。
- マネージドスケーリングがオフの場合、キャパシティプロバイダーはスケールインまたはスケールアウトを実行しません。キャパシティプロバイダー戦略を使用して、キャパシティプロバイダー間でタスクのバランスを取ることができます。
- `binpack` 戦略は、キャパシティに関して最も効率的な戦略です。

- ターゲットキャパシティが 100% 未満の場合、配置戦略は `binpack` 戦略が `spread` 戦略よりも高い優先順位を持つ必要があります こうすることで、各タスクにハードウェア専有インスタンスが割り当てられるか、上限に達するまで、キャパシティプロバイダーはスケールアウトできなくなります。

クラスターの自動スケーリングをオンにする

コンソールまたは AWS CLI を使用して、クラスターの自動スケーリングをオンにすることができます。

コンソールを使用して EC2 起動タイプのクラスターを作成すると、Amazon ECS がユーザーに代わって Auto Scaling グループを作成し、ターゲット容量を設定します。詳細については、「Amazon EC2 起動タイプ用の Amazon ECS クラスターの作成」を参照してください。

ユーザーが Auto Scaling グループを作成してクラスターに割り当てることもできます。詳細については、「Amazon ECS キャパシティープロバイダーを更新する」を参照してください。

AWS CLI を使用する場合、クラスターを作成した後、次の手順に従います。

1. キャパシティプロバイダーを作成する前に、Auto Scaling グループを作成する必要があります。詳細については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループ」を参照してください。
2. `put-cluster-capacity-providers` を使用して、クラスターキャパシティプロバイダーを変更します。詳細については、「Amazon ECS クラスターの自動スケーリングを有効にする」を参照してください。

Amazon ECS クラスターの自動スケーリングの最適化

Amazon EC2 で Amazon ECS を実行するお客様は、クラスターの自動スケーリングを利用して Amazon EC2 Auto Scaling グループのスケーリングを管理できます。クラスターの自動スケーリングを使用すると、Auto Scaling グループを自動的にスケーリングするように Amazon ECS を設定することができ、ユーザーはタスクの実行に集中できます。Amazon ECS では、追加の操作を必要とせずに、必要に応じて Auto Scaling グループがスケールインおよびスケールアウトします。Amazon ECS キャパシティープロバイダーは、アプリケーションの需要を満たすのに十分なコンテナインスタンスを確保することで、クラスター内のインフラストラクチャを管理するために使用されます。クラスターの自動スケーリングが内部でどのように機能するかについては、「Deep Dive on Amazon ECS Cluster Auto Scaling」を参照してください。

クラスターの自動スケーリングは、Auto Scaling グループとの CloudWatch ベースの 統合を利用して、クラスターキャパシティーを調整します。したがって、次に関連する固有のレイテンシーがあります。

- CloudWatch メトリクスの発行
- メトリクス CapacityProviderReservation が CloudWatch アラームに抵触 (高と低の両方) するまでにかかる時間
- 新しく起動した Amazon EC2 インスタンスがウォームアップするのにかかる時間 以下のアクションを実行して、クラスターの自動スケーリングの応答性を高め、デプロイを高速化できます。

キャパシティープロバイダーのステップスケーリングサイズ

Amazon ECS キャパシティープロバイダーは、アプリケーションの需要に合わせてコンテナインスタンスを拡大/縮小します。Amazon ECS が起動するインスタンスの最小数は、デフォルトでは 1 に設定されています。そのため、保留中のタスクを配置するために複数のインスタンスが必要な場合は、デプロイにさらに時間がかかることがあります。Amazon ECS API を介して minimumScalingStepSize を増やすことで、Amazon ECS が一度にスケールインまたはスケールアウトするインスタンスの最小数を増やすことができます。maximumScalingStepSize が小さすぎると、一度にスケールインまたはスケールアウトされるコンテナインスタンスの数が制限され、デプロイが遅くなる可能性があります。

> **Note**
>
> この設定は現在、CreateCapacityProvider または UpdateCapacityProvider API を介してのみ使用できます。

インスタンスのウォームアップ期間

インスタンスのウォームアップ期間は、新たに起動された Amazon EC2 インスタンスが Auto Scaling グループの CloudWatch メトリックスに反映されるまでの時間です。指定されたウォームアップ期間が終了すると、そのインスタンスは Auto Scaling グループの集計メトリクスにカウントされ、クラスターの自動スケーリングは、必要なインスタンス数を推定するための次の計算ループに進みます。

instanceWarmupPeriod のデフォルト値は 300 秒です。この値を CreateCapacityProvider または UpdateCapacityProvider API を使用して小さい値に設定することで、スケーリングの応

答性の向上させることができます。過剰なプロビジョニングを回避できるように、値を 60 秒以上に設定することをお勧めします。

予備のキャパシティー

キャパシティープロバイダーにタスクを配置するために使用できるコンテナインスタンスがない場合は、Amazon EC2 インスタンスをその場で起動してクラスターキャパシティーを増やし (スケールアウトし)、それらのインスタンスが起動するまで待ってからコンテナを起動する必要があります。これにより、タスクの起動レートが大幅に低下する可能性があります。ここでは 2 つのオプションがあります。

この場合、予備の Amazon EC2 キャパシティーを事前に起動してタスクを実行する準備をしておくことで、実質的なタスク起動レートを上げることができます。`Target Capacity` 設定を使用して、クラスターで予備のキャパシティーを保持するかどうかを指定できます。例えば、`Target Capacity` を 80 % に設定することで、クラスターに常に 20 % の予備のキャパシティーが必要であることを示します。この予備のキャパシティーにより、スタンドアロンタスクをすぐに起動できるようになり、タスクの起動がスロットリングされなくなります。このアプローチのトレードオフは、予備のクラスターキャパシティーを保持するコストが増加する可能性があることです。

検討できる代替アプローチは、キャパシティープロバイダーではなくサービスにヘッドルームを追加することです。つまり、予備のキャパシティーを起動するための `Target Capacity` 設定を小さくする代わりに、ターゲット追跡スケーリングメトリクス、またはサービス自動スケーリングのステップスケーリングのしきい値を変更することで、サービス内のレプリカの数を増やすことができます。このアプローチが有用なのはワークロードの急増に対してのみであり、新しいサービスをデプロイし、初めて 0 から N タスクに移行する場合には効果がないことに注意してください。関連するスケーリングポリシーの詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「ターゲット追跡スケーリングポリシー」または「ステップスケーリングポリシー」を参照してください。

Amazon ECS マネージドスケーリング動作

マネージドスケーリングを使用する Auto Scaling グループキャパシティプロバイダーがある場合、Amazon ECS はクラスターに追加する最適なインスタンス数を見積もり、この値を使用してリクエストまたはリリースするインスタンス数を決定します。

マネージドスケールアウト動作

Amazon ECS は、サービス、スタンドアロンタスク、またはクラスターのデフォルトからのキャパシティープロバイダー戦略に従って、各タスクのキャパシティープロバイダーを選択しま

す。Amazon ECS は、単一のキャパシティプロバイダーのために、これらの残りのステップに従います。

キャパシティプロバイダー戦略のないタスクはキャパシティプロバイダーによって無視されます。キャパシティプロバイダー戦略がない保留中のタスクによって、キャパシティプロバイダーがスケールアウトされることはありません。タスクまたはサービスが起動タイプを設定する場合、タスクまたはサービスはキャパシティプロバイダー戦略を設定できません。

以下では、スケールアウト動作について詳しく説明します。

- このキャパシティプロバイダーのすべてのプロビジョニングタスクをグループ化し、各グループが同じリソース要件を持つようにします。
- グループ内の複数のインスタンスタイプを使用する場合、Auto Scaling グループ内のインスタンスタイプはパラメータによってソートされます。これらのパラメータには vCPU、メモリ、Elastic Network Interface (ENI)、ポート、GPU が含まれます。各パラメータの最小インスタンスタイプと最大インスタンスタイプが選択されます。インスタンスタイプの選択方法の詳細については、「Amazon ECS 用の Amazon EC2 コンテナインスタンス」を参照してください。

  > **Important**
  >
  > タスクのグループに、Auto Scaling グループの最小のインスタンスタイプよりも大きなリソース要件がある場合、そのタスクのグループは、このキャパシティプロバイダーでは実行できません。キャパシティプロバイダーは、Auto Scaling グループをスケールしません。タスクは `PROVISIONING` 状態のままです。
  > タスクが `PROVISIONING` 状態にとどまらないようにするには、最小リソース要件ごとに個別の Auto Scaling グループとキャパシティプロバイダーを作成することをお勧めします。タスクを実行するか、サービスを作成するときは、Auto Scaling グループ内の最小インスタンスタイプでタスクを実行できるキャパシティプロバイダーのみをキャパシティプロバイダー戦略に追加します。他のパラメータでは、配置制約を使用できます

- タスクグループごとに、Amazon ECS は未配置タスクの実行に必要なインスタンス数を計算します。この計算には、`binpack` 戦略が用いられます。この戦略では、タスクの vCPU、メモリ、Elastic Network Interface (ENI)、ポートや GPU の要件を考慮します。また、Amazon EC2 インスタンスのリソースの可用性も考慮されます。最大インスタンスタイプの値は、計算された最大インスタンス数として扱われます。最小のインスタンスタイプの値は、保護として使用されます。最小インスタンスタイプでタスクの少なくとも 1 つのインスタンスを実行できない場合、計算ではタスクが互換性がないと見なされます。その結果、タスクはスケールアウト計算から除外されます。すべてのタスクに最小のインスタンスタイプとの互換性がないときは、クラスター 自動ス

ケーリングは停止し、CapacityProviderReservation 値は targetCapacity のままになります。

- Amazon ECS は、次のいずれかに該当する場合、minimumScalingStepSize に関連した CloudWatch に CapacityProviderReservation メトリクスをパブリッシュします。
  - 計算された最大インスタンス数が最小スケーリングステップサイズを下回っています。
  - maximumScalingStepSize か、計算された最大インスタンス数のどちらか低い方の値。
- CloudWatch アラームは、キャパシティプロバイダーの CapacityProviderReservation メトリクスを使用します。CapacityProviderReservation メトリクスが targetCapacity 値より大きい場合、アラームでは、Auto Scaling グループの DesiredCapacity も増加します。targetCapacity 値は、クラスターの自動スケーリングがアクティブ化されているフェーズ中に CloudWatch アラームに送信されるキャパシティプロバイダー設定です。

  デフォルトの targetCapacity は 100 % です。
- Auto Scaling グループは追加の EC2 インスタンスを起動します。オーバープロビジョニングを防ぐため、Auto Scaling では、最近起動された EC2 インスタンスのキャパシティが新たなインスタンスを起動する前に安定させています。自動スケーリングは、既存のすべてのインスタンスが instanceWarmupPeriod (現在はインスタンスの起動時間を減じたもの) を経過したかどうかを確認します。instanceWarmupPeriod 内にあるインスタンスのスケールアウトはブロックされます。

  新しく起動されたインスタンスがウォームアップに達するまでのデフォルト秒数は 300 です。

詳細については、「Amazon ECS のクラスター自動スケーリングに関する詳細な説明」を参照してください。

スケールアウトの考慮事項

スケールアウトのプロセスでは、次の点を考慮してください。

- 配置制約は複数ありますが、distinctInstance タスク配置の制約事項のみを使用することをお勧めします。サンプリングされたインスタンスと互換性がない配置制約を使用しているため、これにより、スケールアウトプロセスが停止するのを防ぐことができます。
- マネージドスケーリングは、Auto Scaling グループが同じインスタンスタイプまたは類似のインスタンスタイプを使用している場合に最適です。
- スケールアウトプロセスが必要で現在実行中のコンテナインスタンスがない場合は、Amazon ECS は常に 2 つのインスタンスにスケールアウトしてから追加のスケールアウト/インプロセスを実行

します。追加のスケールアウトは、インスタンスのウォームアップ期間を待ちます。スケールインプロセスの場合、Amazon ECS はスケールアウトプロセスの後 15 分待ってから、常にスケールインプロセスを開始します。

- 2 番目のスケールアウトのステップは `instanceWarmupPeriod` が期限切れになるまで待つ必要があるため、全体的なスケール制限に影響する可能性があります。この時間を短縮する必要がある場合は、`instanceWarmupPeriod` が EC2 インスタンスが Amazon ECS エージェントを起動して開始するのに十分な大きさであることを確認してください (オーバープロビジョニングを防げます)。
- クラスターの自動スケーリングは、キャパシティプロバイダーの Auto Scaling グループ内の起動設定、起動テンプレート、複数のインスタンスタイプをサポートします。複数のインスタンスタイプを使用せずに、属性ベースのインスタンスタイプの選択も使用できます。
- オンデマンドインスタンスと複数のインスタンスタイプ、またはスポットインスタンスを持つ Auto Scaling グループを使用する場合は、大きいインスタンスタイプを優先順位リストで上位に配置し、ウェイトを指定しないでください。現時点では、ウェイトの指定はサポートされていません。詳細については、AWS Auto Scalingユーザーガイドの「複数のインスタンスタイプと Auto Scaling グループ」を参照してください。
- Amazon ECS は、計算された最大インスタンス数が最小スケーリングステップサイズより小さい場合は `minimumScalingStepSize` を、あるいは `maximumScalingStepSize` または計算された最大インスタンスカウント値のいずれか小さい方を起動します。
- Amazon ECS サービスまたは `run-task` がタスクを起動し、キャパシティープロバイダーのコンテナインスタンスにタスクを開始するために十分なリソースがない場合、Amazon ECS は、各クラスターでこのステータスのタスク数を制限し、タスクがこの制限を超えることを防ぎます。詳細については、「Service Quotas」を参照してください。

マネージドスケールイン動作

Amazon ECS は、クラスター内の各キャパシティプロバイダーのコンテナインスタンスをモニタリングします。コンテナインスタンスがタスクを実行していない場合、コンテナインスタンスは空であるとみなされ、Amazon ECS はスケールインプロセスを開始します。

CloudWatch スケールインアラームは、Auto Scaling グループのスケールインプロセスが開始する前に 15 データポイント (15 分) を必要とします。スケールインプロセスがスタートされた後から Amazon ECS が登録されたコンテナインスタンス数を減らす必要があるまで、Auto Scaling グループは `DesireCapacity` 値を 1 つのインスタンスより大きく、かつ毎分 50% 未満に設定します。

Amazon ECS がスケールアウトをリクエストしたときに (CapacityProviderReservation が 100 より大きいとき) スケールインプロセスが進行中の場合、スケールインプロセスは停止して、必要に応じて最初から開始されます。

次では、スケールイン動作について詳しく説明します。

1. Amazon ECS は、空のコンテナインスタンスの数を計算します。デーモンタスクが実行されている場合でも、コンテナインスタンスは空であるとみなされます。
2. Amazon ECS では、CapacityProviderReservation 値を 0 ~ 100 の数値に設定します。この数値は、Auto Scaling グループが必要とする規模と実際の規模との比率をパーセンテージで表す次の式を使用します。その後、Amazon ECS は CloudWatch にメトリクスをパブリッシュします。メトリクスの算出方法の詳細については、「Amazon ECS クラスター自動スケーリングの Deep Dive」を参照してください。

   ```
   CapacityProviderReservation = (number of instances needed) / (number of running
    instances) x 100
   ```

3. CapacityProviderReservation メトリクスは CloudWatch アラームを生成します。このアラームは Auto Scaling グループの DesiredCapacity 値を更新します。すると、以下のいずれかのアクションが発生します。
   - キャパシティプロバイダーによるマネージド終了を使用しない場合、Auto Scaling グループは、Auto Scaling グループ終了ポリシーを使用して EC2 インスタンスを選択し、EC2 インスタンス数が DesiredCapacity に達するまでインスタンスを終了します。その後、コンテナインスタンスがクラスターから登録解除されます。
   - すべてのコンテナインスタンスがマネージド型の終了保護を使用している場合、Amazon ECS は空のコンテナインスタンスのスケールイン保護を削除します。Auto Scaling グループは EC2 インスタンスを終了できるようになります。その後、コンテナインスタンスがクラスターから登録解除されます。

Amazon ECS が終了するインスタンスの制御

> **Important**
>
> クラスター自動スケーリングのマネージドターミネーション保護機能を使用するには、Auto Scaling グループで自動スケーリングインスタンスのスケールイン保護を有効にする必要があります。

マネージド終了保護を使用すると、クラスターの自動スケーリングで、どのインスタンスを終了するかを制御できます。マネージド終了保護を使用した場合、Amazon ECS は、実行中の Amazon ECS タスクがない EC2 インスタンスのみを終了します。DAEMON スケジューリング戦略を使用するサービスによって実行されるタスクは無視され、インスタンスがこれらのタスクを実行している場合でも、クラスター自動スケーリングによってインスタンスを終了できます。これは、クラスター内のすべてのインスタンスがこれらのタスクを実行しているためです。

Amazon ECS は最初に Auto Scaling グループの EC2 インスタンスに対するインスタンススケールイン保護オプションを有効にします。次に、Amazon ECS がインスタンスにタスクを配置します。デーモン以外のすべてのタスクがインスタンスで停止すると、Amazon ECS はスケールインプロセスを開始し、EC2 インスタンスのスケールイン保護をオフにします。Auto Scaling グループはインスタンスを終了できます。

自動スケーリングインスタンスのスケールイン保護は、終了できる EC2 インスタンスを制御します。スケールイン機能がオンになっているインスタンスは、スケールインプロセス中に終了できません。自動スケーリングのインスタンススケールイン保護についての詳細は、「Amazon EC2 Auto Scaling ユーザーガイド」の「インスタンススケールイン保護を使用する」を参照してください。

キャパシティに余裕を持たせるように `targetCapacity` の割合を設定できます。こうすると、Auto Scaling グループが起動するインスタンスが増えないため、以降のタスクがより速く起動します。Amazon ECS では、ターゲットキャパシティー値を使用して、サービスによって作成される CloudWatch メトリクスを管理します。Amazon ECS は CloudWatch メトリクスを管理します。Auto Scaling グループが定常状態として扱われるため、スケーリングアクションが必要なくなります。値は 0-100% の範囲で指定できます。例えば、Amazon ECS タスクで使用されるキャパシティーに加えて 10% の空き容量を維持するように Amazon ECS を設定するには、ターゲットキャパシティー値を 90% に設定します。キャパシティプロバイダーで `targetCapacity` 値を設定する際には、次の点を考慮します。

- 100% 未満の `targetCapacity` 値は、クラスター内に必要な空き容量 (Amazon EC2 インスタンス) を表します。空き容量とは、実行中のタスクがないことを意味します。
- アベイラビリティーゾーンなどの配置制約は、追加の `binpack` がなければ、Amazon ECS が最終的にインスタンスごとに 1 つのタスクを実行するように強制しますが、これは望ましい動作ではない可能性があります。

マネージド終了保護を使用するには、Auto Scaling グループで 自動スケーリングインスタンスのスケールイン保護を有効にする必要があります。スケールイン保護を有効にしていない場合、マネージド終了保護を有効にすると、望ましくない動作が発生する可能性があります。例えば、インスタン

スのドレイン状態のままになっている場合を考えてみます。詳細については、「Amazon EC2 Auto Scaling ユーザーガイド」の「インスタンスのスケールイン保護の使用」を参照してください。

キャパシティープロバイダーで終了保護を使用するときは、キャパシティープロバイダーに関連付けられた Auto Scaling グループで、インスタンスのデタッチなどの手動アクションを実行しないでください。手動操作を行うと、キャパシティープロバイダーのスケールイン操作が中断される可能性があります。Auto Scaling グループからインスタンスをデタッチする場合は、Amazon ECS クラスターからもデタッチしたインスタンスを登録解除する必要があります。

Amazon ECS クラスターの自動スケーリングを有効にする

クラスターの自動スケーリングを有効にして、Amazon ECS がクラスターに登録された Amazon EC2 インスタンスのスケーリングを管理するようにします。

コンソールを使用してクラスターの自動スケーリングを有効にする場合は、「Amazon ECS のキャパシティープロバイダーを作成する」を参照してください。

開始する前に、Auto Scaling グループとキャパシティープロバイダーを作成します。詳細については、「the section called “EC2 起動タイプ用のキャパシティープロバイダー”」を参照してください。

クラスターの自動スケーリングを有効にする場合は、キャパシティープロバイダーをクラスターに関連付けてから、クラスターの自動スケーリングを有効にします。

1. `put-cluster-capacity-providers` コマンドを使用して、1 つ以上のキャパシティープロバイダーをクラスターに関連付けます。

   AWS Fargate キャパシティプロバイダーを追加するには、リクエストに FARGATE および FARGATE_SPOT キャパシティプロバイダーを入れます。詳細については、AWS CLI コマンドリファレンスの「`put-cluster-capacity-providers`」を参照してください。

   ```
   aws ecs put-cluster-capacity-providers \
     --cluster ClusterName \
     --capacity-providers CapacityProviderName FARGATE FARGATE_SPOT \
     --default-capacity-provider-strategy capacityProvider=CapacityProvider,weight=1
   ```

   EC2 起動タイプに Auto Scaling グループを追加するには、リクエストに Auto Scaling グループ名を入れます。詳細については、AWS CLI コマンドリファレンスの「`put-cluster-capacity-providers`」を参照してください。

   ```
   aws ecs put-cluster-capacity-providers \
   ```

```
  --cluster ClusterName \
  --capacity-providers CapacityProviderName \
  --default-capacity-provider-strategy capacityProvider=CapacityProvider,weight=1
```

2. describe-clusters コマンドを使用して、関連付けが成功したことを確認します。詳細については、AWS CLI コマンドリファレンスの「describe-clusters」を参照してください。

```
aws ecs describe-clusters \
  --cluster ClusterName \
  --include ATTACHMENTS
```

3. キャパシティープロバイダーのマネージド自動スケーリングを有効にするには、update-capacity-provider コマンドを使用します。詳細については、AWS CLI コマンドリファレンスの「update-capacity-provider」を参照してください。

```
aws ecs update-capacity-provider \
  --capacity-providers CapacityProviderName \
  --auto-scaling-group-provider managedScaling=ENABLED
```

Amazon ECS クラスターの自動スケーリングを無効にする

クラスターに登録されている EC2 インスタンスをよりきめ細かく制御する必要がある場合は、クラスターの自動スケーリングを無効にします。

クラスターの自動スケーリングを無効にするには、キャパシティープロバイダーとクラスターから有効にしたマネージドスケーリングの関連付けを解除するか、キャパシティープロバイダーを更新してマネージドスケーリングを無効にします。

キャパシティープロバイダーの関連付けを解除する

キャパシティープロバイダーとクラスターとの関連付けを解除するには、次の手順を実行します。

1. put-cluster-capacity-providers コマンドを使用して、Auto Scaling グループのキャパシティープロバイダーとクラスターとの関連付けを解除します。クラスターは、AWS Fargate キャパシティープロバイダーとの関連付けを保持できます。詳細については、AWS CLI コマンドリファレンスの「put-cluster-capacity-providers」を参照してください。

```
aws ecs put-cluster-capacity-providers \
  --cluster ClusterName \
  --capacity-providers FARGATE FARGATE_SPOT \
```

```
  --default-capacity-provider-strategy '[]'
```

put-cluster-capacity-providers コマンドを使用して、Auto Scaling グループのキャパシティープロバイダーとクラスターとの関連付けを解除します。詳細については、AWS CLI コマンドリファレンスの「put-cluster-capacity-providers」を参照してください。

```
aws ecs put-cluster-capacity-providers \
  --cluster ClusterName \
  --capacity-providers [] \
  --default-capacity-provider-strategy '[]'
```

2. describe-clusters コマンドを使用して、関連付けの解除が成功したことを確認します。詳細については、AWS CLI コマンドリファレンスの「describe-clusters」を参照してください。

```
aws ecs describe-clusters \
  --cluster ClusterName \
  --include ATTACHMENTS
```

キャパシティープロバイダーのマネージドスケーリングを無効にする

キャパシティープロバイダーのマネージドスケーリングを無効にするには、次のステップに従います。

- キャパシティープロバイダーのマネージド自動スケーリングを無効にするには、update-capacity-provider コマンドを使用します。詳細については、AWS CLI コマンドリファレンスの「update-capacity-provider」を参照してください。

```
aws ecs update-capacity-provider \
  --capacity-providers CapacityProviderName \
  --auto-scaling-group-provider managedScaling=DISABLED
```

Amazon ECS のキャパシティープロバイダーを作成する

クラスターの作成が完了したら、EC2 起動タイプの新しいキャパシティプロバイダー (Auto Scaling グループ) を作成できます。キャパシティプロバイダーは、アプリケーションのインフラストラクチャの管理およびスケールに役立ちます。

キャパシティプロバイダーを作成する前に、Auto Scaling グループを作成する必要があります。詳細については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループ」を参照してください。

クラスターのキャパシティプロバイダーを作成するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [Cluster : ***name***] (クラスター : 名) ページで、[Infrastructure] (インフラストラクチャ) を選択し、[Create] (作成) を選択します。
5. [Create capacity providers] (キャパシティプロバイダーの作成) ページで、次のオプションを設定します。

   a. [Basic details] (基本的な詳細) の下の [Capacity provider name] (キャパシティプロバイダー名) に、一意のキャパシティプロバイダー名を入力します。

   b. [Auto Scaling group] (Auto Scaling グループ) の [Use an existing Auto Scaling group] (既存の Auto Scaling グループを使用する) で、Auto Scaling グループを選択します。

   c. (オプション) スケーリングポリシーを設定するには、[Scaling policies] (スケーリングポリシー) で次のオプションを設定します。

      - スケールインおよびスケールアウトアクションを Amazon ECS に管理させるには、[Turn on managed scaling] (マネージドスケーリングをオンにする) を選択します。
      - Amazon ECS タスクが実行されている EC2 インスタンスが終了しないようにするには、[Turn on scaling protection] (スケーリング保護を有効にする) を選択します。
      - [Set target capacity] (ターゲットキャパシティの設定) に、Amazon ECS マネージド対象ターゲット追跡スケーリングポリシーで使用される CloudWatch メトリクスのターゲット値を入力します。

6. [Create] (作成) を選択します。

Amazon ECS キャパシティープロバイダーを更新する

Auto Scaling グループをキャパシティプロバイダーとして使用する場合、グループのスケーリングポリシーを変更できます。

クラスターのキャパシティプロバイダーを更新するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [Cluster : ***name***] (クラスター : 名) ページで、[Infrastructure] (インフラストラクチャ) を選択し、[Update] (更新) を選択します。
5. [Create capacity providers] (キャパシティプロバイダーの作成) ページで、次のオプションを設定します。
   - [Auto Scaling グループ] の [スケーリングポリシー] で、以下のオプションを設定します。
     - スケールインおよびスケールアウトアクションを Amazon ECS に管理させるには、[Turn on managed scaling] (マネージドスケーリングをオンにする) を選択します。
     - Amazon ECS タスクが実行されている EC2 インスタンスが終了しないようにするには、[スケーリング保護をオンにする] を選択します。
     - [Set target capacity] (ターゲットキャパシティの設定) に、Amazon ECS マネージド対象ターゲット追跡スケーリングポリシーで使用される CloudWatch メトリクスのターゲット値を入力します。
6. [Update] (更新) を選択します。

Amazon ECS キャパシティープロバイダーを削除する

Auto Scaling グループキャパシティープロバイダーは、使い終わったら削除できます。グループが削除されると、Auto Scaling グループのキャパシティープロバイダーは `INACTIVE` 状態に移行します。`INACTIVE` ステータスのキャパシティープロバイダーは、一定期間アカウント内で検出可能になる場合があります。ただし、この動作は今後変更される予定であり、`INACTIVE` のキャパシティープロバイダーを永続的に使用するのは避けてください。Auto Scaling グループキャパシティプロバイダーを削除する前に、すべてのサービスのキャパシティプロバイダー戦略からキャパシティプロバイダーを削除する必要があります。サービスのキャパシティプロバイダー戦略からキャパシティプロバイダーを削除するには、`UpdateService` API または Amazon ECS コンソールのサービス更新ワークフローを使用できます。[新しいデプロイの強制] オプションを使用すると、キャパシティプロバイダーが提供する Amazon EC2 インスタンスキャパシティを使用している任意のタスクを、残りのキャパシティプロバイダーのキャパシティを使用するように移行できます。

クラスターのキャパシティプロバイダーを削除するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [Cluster : ***name***] (クラスター : 名) ページで、[Infrastructure] (インフラストラクチャ) を選択し、Auto Scaling グループを選択して、[Delete] (削除) を選択します。
5. 確認ボックスに、「delete ***Auto Scaling #######***」と入力します。
6. [削除] を選択します。

EC2 インスタンスで実行されている Amazon ECS ワークロードを安全に停止する

マネージドインスタンスドレイニングを使用すると、Amazon EC2 インスタンスの正常な終了が容易になります。この結果、ワークロードを安全に停止し、終了しないインスタンスに再スケジュールできます。インフラストラクチャのメンテナンスと更新は、ワークロードの中断を心配することなく実行できます。マネージドインスタンスドレイニングを使用することで、Amazon EC2 インスタンスの置換を必要とするインフラストラクチャ管理ワークフローを簡素化しつつ、アプリケーションの耐障害性と可用性を確保できます。

Amazon ECS マネージドインスタンスドレイニングは、Auto Scaling グループのインスタンス置換と連動します。インスタンスの更新とインスタンスの最大有効期間に基づいて、お客様は最新の OS およびキャパシティに関するセキュリティ要件に常に準拠できます。

マネージドインスタンスドレイニングは、Amazon ECS キャパシティープロバイダーでのみ使用できます。Amazon ECS コンソール、AWS CLI、または SDK を使用して Auto Scaling グループのキャパシティープロバイダーを作成または更新するときに、マネージドインスタンスドレイニングを有効にできます。

以下のイベントは Amazon ECS マネージドインスタンスドレイニングの対象となります。

- Auto Scaling グループのインスタンス更新 - インスタンス更新を使用すると、バッチによる手動ではなく、Auto Scaling グループ内の Amazon EC2 インスタンスのローリング置換を実行できます。これは、多数のインスタンスを置換する必要がある場合に便利です。インスタンス更新は、Amazon EC2 コンソールまたは `StartInstanceRefresh` API により開始されます。マネージドターミネーション保護を使用している場合は、`StartInstanceRefresh` を呼び出す際に必ず `Replace` を選択してスケールイン保護をしてください。

- インスタンスの最大有効期間 - Auto Scaling グループインスタンスの置換に至るまでの最大有効期間を定義できます。これは、内部のセキュリティポリシーやコンプライアンスに基づいて置換インスタンスをスケジュールするのに役立ちます。
- Auto Scaling グループのスケールイン - スケーリングポリシーとスケジュールされたスケーリングアクションに基づいて、Auto Scaling グループはインスタンスの自動スケーリングをサポートします。Amazon ECS キャパシティープロバイダーとして Auto Scaling グループを使用することで、タスクが実行されていないときに Auto Scaling グループのインスタンスをスケールインすることができます。
- Auto Scaling グループのヘルスチェック - Auto Scaling グループは、異常のあるインスタンスの終了を管理するための多くのヘルスチェックをサポートしています。
- AWS CloudFormation スタックの更新 - AWS CloudFormation スタックに `UpdatePolicy` 属性を追加することで、グループが変更されたときにローリング更新を実行できます。
- スポットキャパシティーの再調整 - Auto Scaling グループは、Amazon EC2 のキャパシティー再調整通知に基づいて、中断のリスクが高いスポットインスタンスを事前対応的に置換しようとします。Auto Scaling グループは、置換インスタンスが起動して正常になると、古いインスタンスを終了します。Amazon ECS マネージドインスタンスドレイニングでは、非スポットインスタンスをドレインするのと同じ方法でスポットインスタンスをドレインします。
- スポット中断 - スポットインスタンスは 2 分間の通知の後に終了します。Amazon ECS マネージドインスタンスドレイニングでは、それに応じてインスタンスがドレイニング状態になります。

マネージドインスタンスドレイニングがある Amazon EC2 Auto Scaling のライフサイクルフック

Auto Scaling グループのライフサイクルフックを使用すると、お客様はインスタンスライフサイクルの特定のイベントによってトリガーされるソリューションを作成し、その特定のイベントが発生したときにカスタムアクションを実行できます。Auto Scaling グループでは、最大 50 個のフックを使用できます。複数の終了フックが存在する場合があり、それらは同時に実行されるため、Auto Scaling グループはすべてのフックが終了するのを待ってからインスタンスを終了します。

Amazon ECS マネージド型のフック終了に加えて、独自のライフサイクル終了フックを設定することもできます。ライフサイクルフックには `default action` があります。Amazon ECS マネージドフックなどの他のフックがカスタムフックによるエラーの影響を受けないようにするために、`continue` をデフォルトとして設定することをお勧めします。

Auto Scaling グループの終了ライフサイクルフックを既に設定していて、Amazon ECS マネージドインスタンスドレイニングも有効にしている場合、両方のライフサイクルフックが実行されます。ただし、相対的なタイミングは保証されません。ライフサイクルフックには、タイムアウトが終了したときに実行するアクションを指定する `default action` 設定があります。障害が発生した場合

は、continue をカスタムフックのデフォルト結果として使用することをお勧めします。このようにすることで、他のフック、特に Amazon ECS マネージドフックは、カスタムライフサイクルフックのエラーの影響を受けなくなります。abandon による別の結果では、ほかのすべてのフックがスキップされるので、避けるべきです。Auto Scaling グループのライフサイクルフックの詳細については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Amazon EC2 Auto Scaling のライフサイクルフック」を参照してください。

タスクとマネージドインスタンスドレイニング

Amazon ECS マネージドインスタンスドレイニングでは、コンテナインスタンスにある既存のドレイニング機能を使用します。コンテナインスタンスドレイニング機能は、Amazon ECS サービスに属するレプリカタスクの置換と停止を実行します。スタンドアロンタスク (RunTask によって呼び出されたタスクなど) は、PENDING または RUNNING の状態にある場合には影響を受けません。そのようなタスクは、完了するまで待つか、手動で停止する必要があります。コンテナインスタンスは、すべてのタスクが停止されるか、48 時間が経過するまで DRAINING 状態のままになります。デーモンタスクは、すべてのレプリカタスクが停止した後に、最後に停止します。

マネージドインスタンスドレイニングとマネージドターミネーション保護

マネージドインスタンスドレイニングは、マネージド終了が無効になっている場合でも機能します。マネージド終了保護の詳細については、「Amazon ECS が終了するインスタンスの制御」を参照してください。

次の表は、マネージドターミネーションとマネージドドレイニングのさまざまな組み合わせの動作をまとめたものです。

マネージドターミネーション	マネージドドレイニング	結果
有効	有効	Amazon ECS は、タスクを実行している Amazon EC2 インスタンスがスケールインイベントによって終

マネージドターミネーション	マネージドドレイニング	結果
		了するのを防ぎます。終了保護が設定されていないインスタンス、スポット中断を受けたインスタンス、インスタンス更新によって強制されたインスタンスなど、終了中のインスタンスがすべて正常にドレインされます。

マネージドターミネーション	マネージドドレイニング	結果
無効	有効	Amazon ECS は、タスクを実行している Amazon EC2 インスタンスがスケールインされないように保護することはしません。ただし、終了されるインスタンスはすべて正常にドレインされます。

マネージドターミネーション	マネージドドレイニング	結果
有効	無効	Amazon ECS は、タスクを実行している Amazon EC2 インスタンスがスケールインイベントによって終了するのを防ぎます。ただし、スポット中断や強制的なインスタンス更新によって、またはタスクがまったく実行されていない場合に、インスタンスは終了する可能性があります。Amazon ECS はこれらのインスタンスに対して正常なドレインを実行せ

マネージドターミネーション	マネージドドレイニング	結果
		ず、停止後に置換サービスタスクを起動します。
無効	無効	Amazon EC2 インスタンスは、Amazon ECS タスクを実行している場合でも、いつでもスケールインまたは終了できます。Amazon ECS は、インスタンスが停止した後に置換サービスタスクを起動します。

マネージドインスタンスドレイニングとスポットインスタンスドレイニング

スポットインスタンスドレイニングでは、Amazon ECS エージェントに環境変数 `ECS_ENABLE_SPOT_INSTANCE_DRAINING` を設定できます。これにより、Amazon ECS は 2 分間のスポット中断に応答して、インスタンスをドレイン中ステータスに移行できます。Amazon ECS マネージドインスタンスドレイニングを使用すると、スポット中断だけでなく、さまざまな理由で

終了中の Amazon EC2 インスタンスを正常にシャットダウンできます。例えば、Amazon EC2 Auto Scaling のキャパシティー再調整を使用して、中断のリスクが高まっているスポットインスタンスを事前対応的に置換できます。そして、マネージドインスタンスドレイニングにより、置換対象のスポットインスタンスの正常シャットダウンが実行されます。マネージドインスタンスドレイニングを使用する場合、スポットインスタンスドレイニングを個別に有効にする必要がないため、Auto Scaling グループのユーザーデータの `ECS_ENABLE_SPOT_INSTANCE_DRAINING` が冗長になります。スポットインスタンスドレイニングの詳細については、「スポットインスタンス」を参照してください。

マネージドインスタンスドレイニングと EventBridge の連携

Amazon ECS マネージドインスタンスドレイニングイベントは Amazon EventBridge に発行され、Amazon ECS はマネージドインスタンスドレイニングをサポートするために、アカウントのデフォルトバスに EventBridge マネージドルールを作成します。これらのイベントを Lambda、Amazon SNS、および Amazon SQS などのほかの AWS サービスにフィルタリングして、モニタリングおよびトラブルシューティングできます。

- Amazon EC2 Auto Scaling は、ライフサイクルフックを呼び出すときに EventBridge にイベントを送信します。
- スポット中断通知は EventBridge に発行されます。
- Amazon ECS は、エラーメッセージを生成します。このエラーメッセージは、Amazon ECS コンソールおよび API を介して取得することができます。
- EventBridge には、一時的な障害を軽減するための再試行メカニズムが組み込まれています。

インスタンスを安全にシャットダウンするように Amazon ECS キャパシティープロバイダーを設定する

Amazon ECS コンソールと AWS CLI を使用して Auto Scaling グループのキャパシティープロバイダーを作成または更新するときに、マネージドインスタンスドレイニングを有効にできます。

> **Note**
>
> キャパシティープロバイダーを作成すると、マネージドインスタンスドレイニングはデフォルトで有効になります。

以下に、AWS CLI を使用してマネージドインスタンスドレイニングを有効にしたキャパシティプロバイダーを作成し、クラスターの既存のキャパシティプロバイダーのマネージドインスタンスドレイニングを有効にする例を示します。

マネージドインスタンスドレイニングを有効にしたキャパシティプロバイダーを作成する

マネージドインスタンスドレイニングを有効にしたキャパシティプロバイダーを作成するには、`create-capacity-provider` コマンドを使用します。`managedDraining` パラメータを ENABLED に設定します。

```
aws ecs create-capacity-provider \
--name capacity-provider \
--auto-scaling-group-provider '{
  "autoScalingGroupArn": "asg-arn",
  "managedScaling": {
    "status": "ENABLED",
    "targetCapacity": 100,
    "minimumScalingStepSize": 1,
    "maximumScalingStepSize": 1
  },
  "managedDraining": "ENABLED",
  "managedTerminationProtection": "ENABLED",
}'
```

レスポンス:

```
{
    "capacityProvider": {
        "capacityProviderArn": "capacity-provider-arn",
        "name": "capacity-provider",
        "status": "ACTIVE",
        "autoScalingGroupProvider": {
            "autoScalingGroupArn": "asg-arn",
            "managedScaling": {
                "status": "ENABLED",
                "targetCapacity": 100,
                "minimumScalingStepSize": 1,
                "maximumScalingStepSize": 1
            },
            "managedTerminationProtection": "ENABLED"
            "managedDraining": "ENABLED"
        }
```

```
    }
}
```

クラスターの既存のキャパシティプロバイダーに対してマネージドインスタンスドレイニングを有効にします。

update-capacity-provider コマンドを使用して、クラスターの既存のキャパシティプロバイダーに対してマネージドインスタンスドレイニングを有効にします。現在 managedDraining が DISABLED で、updateStatus が UPDATE_IN_PROGRESS になっているのがわかります。

```
aws ecs update-capacity-provider \
--name cp-draining \
--auto-scaling-group-provider '{
  "managedDraining": "ENABLED"
}
```

レスポンス:

```
{
    "capacityProvider": {
        "capacityProviderArn": "cp-draining-arn",
        "name": "cp-draining",
        "status": "ACTIVE",
        "autoScalingGroupProvider": {
            "autoScalingGroupArn": "asg-draining-arn",
            "managedScaling": {
                "status": "ENABLED",
                "targetCapacity": 100,
                "minimumScalingStepSize": 1,
                "maximumScalingStepSize": 1,
                "instanceWarmupPeriod": 300
            },
            "managedTerminationProtection": "DISABLED",
            "managedDraining": "DISABLED" // before update
        },
        "updateStatus": "UPDATE_IN_PROGRESS", // in progress and need describe again to
 find out the result
        "tags": [
        ]
    }
}
```

describe-clusters コマンドを使用して ATTACHMENTS を含めます。マネージドインスタンスドレイニングアタッチメントの status は PRECREATED で、全体の attachmentsStatus は UPDATING です。

```
aws ecs describe-clusters --clusters cluster-name --include ATTACHMENTS
```

レスポンス:

```
{
    "clusters": [
        {
            ...

            "capacityProviders": [
                "cp-draining"
            ],
            "defaultCapacityProviderStrategy": [],
            "attachments": [
                # new precreated managed draining attachment
                {
                    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                    "type": "managed_draining",
                    "status": "PRECREATED",
                    "details": [
                        {
                            "name": "capacityProviderName",
                            "value": "cp-draining"
                        },
                        {
                            "name": "autoScalingLifecycleHookName",
                            "value": "ecs-managed-draining-termination-hook"
                        }
                    ]
                },

                ...

            ],
            "attachmentsStatus": "UPDATING"
        }
    ],
    "failures": []
```

```
}
```

更新が終了したら、describe-capacity-providers を使用します。すると、managedDraining が ENABLED になったのがわかります。

```
aws ecs describe-capacity-providers --capacity-providers cp-draining
```

レスポンス:

```
{
    "capacityProviders": [
        {
            "capacityProviderArn": "cp-draining-arn",
            "name": "cp-draining",
            "status": "ACTIVE",
            "autoScalingGroupProvider": {
                "autoScalingGroupArn": "asg-draning-arn",
                "managedScaling": {
                    "status": "ENABLED",
                    "targetCapacity": 100,
                    "minimumScalingStepSize": 1,
                    "maximumScalingStepSize": 1,
                    "instanceWarmupPeriod": 300
                },
                "managedTerminationProtection": "DISABLED",
                "managedDraining": "ENABLED" // successfully update
            },
            "updateStatus": "UPDATE_COMPLETE",
            "tags": []
        }
    ]
}
```

Amazon ECS マネージドインスタンスドレイニングのトラブルシューティング

マネージドインスタンスドレイニングに関する問題のトラブルシューティングが必要になる場合があります。以下は、使用中に発生する可能性のある問題と解決方法の例です。

自動スケーリングの使用時に、最大インスタンス有効期間を超えてもインスタンスが終了しません。

Auto Scaling グループの使用中に最大インスタンス有効期間に到達および超過した後もインスタンスが終了しない場合、スケールインから保護されていることが原因である可能性があります。マネージ

ド終了を無効にし、マネージドドレイニングがインスタンスのリサイクルを処理できるようにすることができます。

AWS Management Console を使用した Amazon ECS クラスターの自動スケーリング用のリソースの作成

AWS Management Console を使用してクラスターの自動スケーリング用のリソースを作成する方法について説明します。リソースに名前が必要な場合は、プレフィックス `ConsoleTutorial` を使用して、すべてのリソースに一意の名前があることを確認し、見つけやすくします。

トピック

前提条件

このチュートリアルでは、以下の前提条件が完了済みであることを前提としています。

- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- Amazon ECS コンテナインスタンス IAM ロールが作成されます。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。
- Amazon ECS サービスにリンクされた IAM ロールが作成されます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。
- 自動スケーリングのサービスにリンクされたIAMロールを作成する 詳細については、Amazon EC2 Auto Scaling ユーザーガイドの「Amazon EC2 Auto Scaling のサービスにリンクされたロール」を参照してください。
- VPC およびセキュリティグループが使用できるように作成されていること。詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。

ステップ 1: Amazon ECS クラスターを作成する

次の手順に従って Amazon ECS クラスターを作成します。

Amazon ECS は、AWS CloudFormation スタックの一部としてユーザーに代わり Amazon EC2 Auto Scaling 起動テンプレートと Auto Scaling グループを作成します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、[クラスター] を選択し、[クラスターの作成] を選択します。
3. [クラスター設定] の [クラスター名] に、「`ConsoleTutorial-cluster`」と入力します。
4. [インフラストラクチャ] で、[AWS Fargate (サーバーレス)] を選択解除し、[Amazon EC2 インスタンス] を選択します。次に、キャパシティプロバイダーとして動作する、Auto Scaling グループを設定します。
   - [自動スケーリンググループ (ASG)] の下です。[新しい ASG を作成] を選択し、次に、そのグループに関する詳細を以下のように入力します。
     - [オペレーティングシステム/アーキテクチャ] で、[Amazon Linux 2] を選択します。
     - [EC2 インスタンスタイプ] で [t3.nano] を選択します。
     - [Capacity] (キャパシティー) には、Auto Scaling グループで起動するインスタンスの最小数と最大数を入力します。
5. (オプション) クラスタータグを管理するには、[Tags] (タグ) を展開し、次のいずれかのオペレーションを実行します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。
6. [Create] (作成) を選択します。

ステップ 2: タスク定義を登録する

クラスターでタスクを実行する前に、タスク定義を登録する必要があります。タスク定義とは、1 つにグループ化されたコンテナのリストです。次の例は、Docker Hub から取得した `amazonlinux` イ

メージを使用し、スリープ状態になるシンプルなタスク定義です。使用できるタスク定義パラメータの詳細については、「Amazon ECSの タスク定義」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
4. [JSON エディタ] ボックスには、以下の内容を貼り付けます。

```
{
    "family": "ConsoleTutorial-taskdef",
    "containerDefinitions": [
        {
            "name": "sleep",
            "image": "public.ecr.aws/amazonlinux/amazonlinux:latest",
            "memory": 20,
            "essential": true,
            "command": [
                "sh",
                "-c",
                "sleep infinity"
            ]
        }
    ],
    "requiresCompatibilities": [
        "EC2"
    ]
}
```

5. [Create] (作成) を選択します。

ステップ 3: タスクを実行する

アカウントのタスク定義を登録したら、クラスターでタスクを実行できます。このチュートリアルでは、ConsoleTutorial-cluster クラスターで ConsoleTutorial-taskdef タスク定義のインスタンスを 5 つ実行します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [クラスター] ページで、[コンソールチュートリアル – クラスター] を選択します。
3. [タスク] で、[新しいタスクの実行] を選択します

4. [環境] セクションの [コンピューティングオプション] で、[キャパシティープロバイダー戦略] を選択します。
5. [デプロイメント構成] の [アプリケーション タイプ] で、[タスク] を選択します。
6. [ファミリー] ドロップダウン リストから [ConsoleTutorial-taskdef] を選択します。
7. [希望するタスク] で、「5」と入力します。
8. [Create] (作成) を選択します。

ステップ 4: 確認する

チュートリアルのこの時点で、5 つのタスクが実行されているクラスターと、キャパシティープロバイダーを備えた Auto Scaling グループができているはずです。キャパシティープロバイダーが Amazon ECS マネージドスケーリングを有効にしています。

CloudWatch メトリクス、Auto Scaling グループ設定、最後に Amazon ECS クラスタータスク数を表示することで、すべてが正常に機能していることを確認できます。

クラスターの CloudWatch メトリクスを表示するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. 画面上部のナビゲーションバーで、 リージョンを選択します。
3. ナビゲーションペインで、[メトリクス] から [すべてのメトリクス] を選択します。
4. [すべてのメトリクス] ページの [参照] タブで、`AWS/ECS/ManagedScaling` を選択します。
5. [CapacityProviderName, ClusterName] を選択します。
6. `ConsoleTutorial-cluster` [クラスター名] に対応するチェックボックスを選択します。
7. [グラフ化メトリクス] タブで、[期間] を [30 秒]、[統計] を [最大] に変更します。

   グラフに表示される値は、キャパシティープロバイダーのターゲットキャパシティー値を示します。これは、設定したターゲットキャパシティーパーセントである `100` から開始する必要があります。`200` までスケールアップすると、ターゲット追跡スケーリングポリシーのアラームがトリガーされます。その後、アラームが発生し Auto Scaling グループがスケールアウトします。

次のステップに従って、Auto Scaling グループの詳細を表示し、スケールアウトアクションが発生したことを確認します。

Auto Scaling グループがスケールアウトされたことを確認するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. 画面上部のナビゲーションバーで、 リージョンを選択します。
3. ナビゲーションペインの 自動スケーリング で、[Auto Scaling Groups] (Auto Scaling グループ) を選択します。
4. このチュートリアルで作成した `ConsoleTutorial-cluster` Auto Scaling グループを選択します。[必要なキャパシティー] の値を表示し、[インスタンス管理] タブでインスタンスを表示して、グループが 2 つのインスタンスにスケールアウトされていることを確認します。

次のステップを使用して Amazon ECS クラスターを表示し、Amazon EC2 インスタンスがクラスターに登録され、タスクが `RUNNING` ステータスに移行したことを確認します。

Auto Scaling グループに含まれるインスタンスを確認する方法

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [クラスター] ページで、`ConsoleTutorial-cluster` クラスターを選択します。
4. [タスク] タブで、5 つのタスクが `RUNNING` ステータスになっていることを確認します。

ステップ 5 : クリーンアップ

このチュートリアルが終了したら、使用していないリソースに対する料金が発生しないように、チュートリアルに関連付けられたリソースをクリーンアップします。キャパシティープロバイダーとタスク定義の削除はサポートされていませんが、これらのリソースに関連するコストは発生しません。

チュートリアルリソースをクリーンアップするには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [クラスター] ページで、[コンソールチュートリアル – クラスター] を選択します。
4. [ConsoleTutorial-cluster] ページで、[タスク] タブを選択し、[停止]、[すべて停止] の順に選択します。
5. ナビゲーションペインで [Clusters] (クラスター) を選択します。
6. [クラスター] ページで、[コンソールチュートリアル – クラスター] を選択します。

7. ページの右上で、[クラスターを削除] を選択します。
8. 確認ボックスに [ConsoleTutorial-cluster を削除] と入力し、[削除] を選択します。
9. 以下のステップに従って Auto Scaling グループを削除します。

    a. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
    b. 画面上部のナビゲーションバーで、 リージョンを選択します。
    c. ナビゲーションペインの 自動スケーリング で、[Auto Scaling Groups] (Auto Scaling グループ) を選択します。
    d. `ConsoleTutorial-cluster` Auto Scaling グループ > [アクション] の順に選択します。
    e. [アクション] メニューから、[削除] を選択します。確認ボックスに [削除] と入力し、[削除] を選択します。

Amazon ECS 用の Amazon EC2 コンテナインスタンス

Amazon ECS コンテナインスタンスは、Amazon ECS コンテナエージェントを実行し、クラスターに登録されている Amazon EC2 インスタンスです。EC2 起動タイプ、外部起動タイプ、または Auto Scaling グループキャパシティープロバイダーを使用して Amazon ECS でタスクを実行すると、タスクはアクティブなコンテナインスタンスに配置されます。コンテナインスタンスの管理とメンテナンスはお客様の責任となります。

Amazon ECS で一元化されたワークロードを実行するために必要な基本的な仕様を満たす独自の Amazon EC2 インスタンス AMI を作成することはできますが、Amazon ECS に最適化された AMI は事前設定され、AWS エンジニアにより Amazon ECS でテストされています。これは最も簡単に開始できる方法であり、AWS でコンピューティングリソースをすばやく実行できます。

コンソールを使用してクラスターを作成すると、Amazon ECS は選択したオペレーティングシステムに関連付けられた最新の AMI を使用してインスタンスの起動テンプレートを作成します。

AWS CloudFormation を使用してクラスターを作成する場合、SSM パラメータは Auto Scaling グループインスタンスの Amazon EC2 起動テンプレートの一部となります。動的な Systems Manager パラメータを使用して、デプロイする Amazon ECS Optimized AMI を決定するようにテンプレートを設定できます。このパラメータにより、スタックをデプロイするたびに、EC2 インスタンスに適用する必要がある利用可能な更新があるかどうかがチェックされます。Systems Manager パラメータの使用方法の例については、「AWS CloudFormation ユーザーガイド」の「Create an Amazon ECS cluster with the Amazon ECS-optimized Amazon Linux 2023 AMI」を参照してください。

- Amazon ECS に最適化された Linux AMI メタデータを取得する

- Amazon ECS に最適化された Bottlerocket AMI メタデータを取得する
- Amazon ECS に最適化された Windows AMI メタデータを取得する

アプリケーションと互換性のあるインスタンスタイプから選択できます。大きいインスタンスでは、同時に多くのタスクを起動できます。インスタンスが小さい場合は、よりきめ細かくスケールアウトしてコストを節約できます。クラスター内のすべてのアプリケーションに対応する Amazon EC2 インスタンスタイプを 1 つ選択する必要はありません。代わりに、複数の Auto Scaling グループを作成し、各グループが異なるインスタンスタイプを持つこともできます。次に、これらのグループごとに Amazon EC2 キャパシティープロバイダーを作成できます。

使用するインスタンスファミリータイプとインスタンスタイプを決定するには、以下のガイドラインを使用します。

- アプリケーションの特定の要件を満たしていないインスタンスタイプまたはインスタンスファミリーを除外します。例えば、アプリケーションに GPU が必要な場合は、GPU がないインスタンスタイプをすべて除外できます。
- ネットワークスループットやストレージなどの要件を検討します。
- CPU とメモリを検討します。原則として、CPU とメモリは、実行するタスクのレプリカを少なくとも 1 つ保存できる大きさである必要があります。

スポットインスタンス

Spot キャパシティーは、オンデマンドインスタンスに比べて大幅なコスト削減が可能です。Spot キャパシティーとは、オンデマンドまたはリザーブドキャパシティーよりも大幅に低価格の余剰容量です。Spot キャパシティーは、バッチ処理や機械学習のワークロード、開発環境やステージング環境に適しています。より一般的には、一時的なダウンタイムを許容するあらゆるワークロードに適しています。

Spot キャパシティーが常に利用できるわけではないため、次のような結果が生じることを理解してください。

- 需要が非常に多い時期には、Spot キャパシティーが利用できない場合があります。これにより、Amazon EC2 スポットインスタンスの起動が遅れる場合があります。このようなイベントで、Amazon ECS サービスはタスクの起動を再試行し、Amazon EC2 Auto Scaling グループも、必要なキャパシティーが利用可能になるまでインスタンスの起動を再試行します。Amazon EC2 は Spot キャパシティーをオンデマンドキャパシティーに置き換えません。

- キャパシティーに対する全体的な需要が高まると、スポットインスタンスとタスクは 2 分間の警告だけで終了する場合があります。警告が送信されたら、インスタンスが完全に終了する前に、必要に応じてタスクを順番にシャットダウンする必要があります。これにより、エラーの可能性を最小限に抑えられます。正常なシャットダウンの詳細については、「ECS による正常なシャットダウン」を参照してください。

スポットのキャパシティー不足を最小限に抑えるために、次の推奨事項を検討してください。

- 複数のリージョンとアベイラビリティーゾーンを使用する - Spot キャパシティーはリージョンとアベイラビリティーゾーンによって異なります。複数のリージョンとアベイラビリティーゾーンでワークロードを実行することで、スポットの可用性を向上できます。可能な場合は、タスクとインスタンスを実行するリージョンのすべてのアベイラビリティーゾーンのサブネットを指定してください。
- 複数の Amazon EC2 インスタンスタイプを使用する- Amazon EC2 Auto Scaling で混合インスタンスポリシーを使用すると、複数のインスタンスタイプが Auto Scaling グループに起動されます。これにより、Spot キャパシティーのリクエストを必要なときに確実に処理できます。信頼性を最大化し、複雑さを最小限に抑えるには、混合インスタンスポリシーでほぼ同じ量の CPU とメモリを備えたインスタンスタイプを使用してください。これらのインスタンスは、異なる世代のものでも、同じ基本インスタンスタイプのバリアントのものでもかまいません。不要な追加機能が付属している場合があることに注意してください。このようなリストの例としては、m4.large、m5.large、m5a.large、m5d.large、m5n.large、m5dn.large、m5ad.large などがあります。詳細については「Amazon EC2 Auto Scaling ユーザーガイド」の「複数のインスタンスタイプと購入オプションを使用する Auto Scaling グループ」を参照してください。
- キャパシティーが最適化されたスポット割り当て戦略を使用する - Amazon EC2 スポットでは、容量を最適化する割り当て戦略とコストを最適化する割り当て戦略のどちらかを選択できます。新しいインスタンスを起動するときにキャパシティー最適化戦略を選択した場合、Amazon EC2 スポットは選択したアベイラビリティーゾーンで最も可用性の高いインスタンスタイプを選択します。これにより、インスタンスが起動後すぐに終了する可能性が低くなります。

コンテナインスタンスでスポット終了通知を設定する方法については、以下を参照してください。

- スポットインスタンス通知を受信するように Amazon ECS Linux コンテナインスタンスを設定する
- スポットインスタンス通知を受信するように Amazon ECS Windows コンテナインスタンスを設定する

Amazon ECS に最適化された Linux AMI

Amazon ECS は、コンテナワークロードを実行する要件と推奨事項で事前設定された Amazon ECS に最適化された AMI を備えています。アプリケーションが Amazon EC2 GPU ベースのインスタンスや、特定のオペレーティングシステム、またはその AMI でまだ使用できない Docker バージョンを必要とする場合を除き、Amazon EC2 インスタンスには Amazon ECS に最適化された Amazon Linux 2023 AMI の使用をお勧めします。Amazon Linux 2 および Amazon Linux 2023 インスタンスの詳細については、「Amazon Linux 2023 ユーザーガイド」の「Amazon Linux 2 と Amazon Linux 2023 の比較」を参照してください。最新の Amazon ECS に最適化された AMI からコンテナインスタンスを起動することで、最新のセキュリティアップデートや、現行バージョンのコンテナエージェントを確実に取得できます。インスタンスを起動する方法についての詳細は、Amazon ECS Linux コンテナインスタンスの起動 を参照してください。

コンソールを使用してクラスターを作成すると、Amazon ECS は選択したオペレーティングシステムに関連付けられた最新の AMI を使用してインスタンスの起動テンプレートを作成します。

AWS CloudFormation を使用してクラスターを作成する場合、SSM パラメータは Auto Scaling グループインスタンスの Amazon EC2 起動テンプレートの一部となります。動的な Systems Manager パラメータを使用して、デプロイする Amazon ECS Optimized AMI を決定するようにテンプレートを設定できます。このパラメータにより、スタックをデプロイするたびに、EC2 インスタンスに適用する必要がある利用可能な更新があるかどうかがチェックされます。Systems Manager パラメータの使用方法の例については、「AWS CloudFormation ユーザーガイド」の「Create an Amazon ECS cluster with the Amazon ECS-optimized Amazon Linux 2023 AMI」を参照してください。

Amazon ECS に最適化された AMI をカスタマイズする必要がある場合は、GitHub の「Amazon ECS Optimized AMI Build Recipes」を参照してください。

Amazon ECS に最適化された AMI の Linux バリアントは、Amazon Linux 2 AMI をベースとして使用しています。Amazon Linux 2 AMI リリースノートも公開されています。詳細については、「Amazon Linux 2 リリースノート」を参照してください。

Linux カーネル 4.14 は 2024 年 1 月 10 日にサポート終了となったため、Linux カーネル 5.10 を搭載した AMI を使用することをお勧めします。

Amazon Linux 2023 オペレーティングシステムを実行する Amazon EC2 インスタンスでは、Amazon ECS に最適化された AMI の次のバリアントを使用できます。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2023	Amazon ECS 最適化 Amazon Linux 2023 AMI	Amazon Linux 2023 は、AWS の次世代 Amazon Linux です。ほとんどの場合、Amazon ECS ワークロードのために Amazon EC2 インスタンスを起動するためにお勧めします。詳細については、「Amazon Linux 2023 ユーザーガイド」の「Amazon Linux 2023 とは」を参照してください。	デフォルトでは、Amazon ECS 最適化 Amazon Linux 2023 AMI は 単一の 30 GiB ルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS 最適化 Amazon Linux 2023 AMI のデフォルトファイルシステムは`xfs`を使用しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを

オペレーティングシステム	AMI	説明	ストレージ設定
			使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2023 (arm64)	Amazon ECS 最適化 Amazon Linux 2023 (arm64) AMI	この AMI は Amazon Linux 2023 に基づいており、ARM ベースの AWS Graviton/Graviton 2/Graviton 3/Graviton 4 プロセッサを搭載した Amazon EC2 インスタンスを、Amazon ECS ワークロードのために起動する場合に使用することが推奨されています。詳細については、「Amazon EC2 インスタンスタイプガイド」の「Amazon EC2 汎用インスタンスの仕様」を参照してください。	デフォルトでは、Amazon ECS 最適化 Amazon Linux 2023 AMI は 単一の 30 GiB ルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS 最適化 Amazon Linux 2023 AMI のデフォルトファイルシステムは`xfs`を使用しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを

オペレーティングシステム	AMI	説明	ストレージ設定
			使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2023 (Neuron)	Amazon ECS 最適化 Amazon Linux 2023 AMI	これは Amazon Linux 2023 をベースにした、Amazon EC2 Inf1、Trn1、または Inf2 インスタンス用の AMI です。AWS Inferentia および AWS Trainium ドライバーと Docker 用の AWS Neuron ランタイムが事前設定されており、Amazon ECS での機械学習推論ワークロードの実行が容易になります。詳細については、「AWS Neuron 機械学習ワークロードでの Amazon ECS タスク定義」を参照してください。 Amazon ECS に最適化された Amazon Linux 2023 (Neuron) AMI には、AWS CLI はプリインストールされていません。	デフォルトでは、Amazon ECS 最適化 Amazon Linux 2023 AMI は 単一の 30 GiB ルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS 最適化 Amazon Linux 2023 AMI のデフォルトファイルシステムは`xfs`を使用しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを

オペレーティングシステム	AMI	説明	ストレージ設定
			使用する」を参照してください。

Amazon Linux 2 オペレーティングシステムを実行する Amazon EC2 インスタンスでは、Amazon ECS に最適化された AMI の次のバリアントを使用できます。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2	Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 AMI	この AMI は Amazon Linux 2 をベースにしており、Amazon ECS ワークロードに Linux カーネル 4.14 ではなく Linux カーネル 5.10 を使用して、Amazon EC2 インスタンスを起動したい場合に使用します。Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 AMI では、AWS CLI は事前インストールされていません。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペ

オペレーティングシステム	AMI	説明	ストレージ設定
			レーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2	Amazon ECS に最適化された Amazon Linux 2 AMI	これは Amazon ECS のワークロード用です。Amazon ECS に最適化された Amazon Linux 2 AMI には、AWS CLI はプリインストールされていません。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2 (arm64)	Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 (arm64) AMI	この AMI は Amazon Linux 2 をベースにし、ARM ベースの AWS Graviton/Graviton 2/Graviton 3/Graviton 4 プロセッサを搭載したAmazon EC2 インスタンス用であり、Amazon EC2 S ワークロードに Linux カーネル 4.14 ではなく Linux カーネル 5.10を使用する場合に使用します。詳細については、「Amazon EC2 インスタンスタイプガイド」の 「Amazon EC2 汎用インスタンスの仕様」を参照してください。 Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI には、AWS CLI はプリインストールされていません。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2 (arm64)	Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI	この AMI は Amazon Linux 2 をベースにしており、Amazon ECS ワークロードに ARM ベースの AWS Graviton/Graviton 2/Graviton 3/Graviton 4 プロセッサを搭載した Amazon EC2 インスタンスを起動する場合に使用します。 Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI には、AWS CLI はプリインストールされていません。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2 (GPU)	Amazon ECS GPU に最適化されたカーネル 5.10 AMI	この AMI は Amazon Linux 2 に基づいており、Amazon ECS ワークロード用に Linux カーネル 5.10 で Amazon EC2 GPU ベースのインスタンスを起動する場合に使用することをお勧めします。NVIDIA カーネルドライバーと Docker GPU ランタイムが事前に構成されており、Amazon ECS で GPU を利用する実行中のワークロードになります。詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2 (GPU)	Amazon ECS GPU に最適化された AMI	この AMI は Amazon Linux 2 に基づいており、Amazon ECS ワークロード用に Linux カーネル 4.14 で Amazon EC2 GPU ベースのインスタンスを起動する場合に使用することをお勧めします。NVIDIA カーネルドライバーと Docker GPU ランタイムが事前に構成されており、Amazon ECS で GPU を利用する実行中のワークロードになります。詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2 (Neuron)	Amazon ECS に最適化された Amazon Linux 2 (Neuron) カーネル 5.10 AMI	これは Amazon Linux 2 をベースにした、Amazon EC2 Inf1、Trn1、または Inf2 インスタンス用の AMI です。Linux カーネル 5.10 搭載 AWS Inferentia および AWS Trainium ドライバーと Docker 用の AWS Neuron ランタイムが事前設定されており、Amazon ECS での機械学習推論ワークロードの実行が容易になります。詳細については、「AWS Neuron 機械学習ワークロードでの Amazon ECS タスク定義」を参照してください。Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI には、AWS CLI はプリインストールされていません。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は `overlay2` ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

オペレーティングシステム	AMI	説明	ストレージ設定
Amazon Linux 2 (Neuron)	Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI	これは Amazon Linux 2 をベースにした、Amazon EC2 Inf1、Trn1、または Inf2 インスタンス用の AMI です。AWS Inferentia および AWS Trainium ドライバーと Docker 用の AWS Neuron ランタイムが事前設定されており、Amazon ECS での機械学習推論ワークロードの実行が容易になります。詳細については、「AWS Neuron 機械学習ワークロードでの Amazon ECS タスク定義」を参照してください。Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI には、AWS CLI はプリインストールされていません。	デフォルトでは、Amazon Linux 2 ベースの Amazon ECS に最適化された AMI (Amazon ECS に最適化された Amazon Linux 2 AMI、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI、および Amazon ECS GPU に最適化された AMI) には、1 つの 30 GiB のルートボリュームが付属しています。30 GiB ルートボリュームのサイズを起動時に変更して、コンテナインスタンスで使用可能なストレージを増やすことができます。このストレージは、オペレーティングシステム用と Docker イメージおよびメタデータ用に使用されます。 Amazon ECS に最適化された Amazon Linux 2 AMI のデフォルトファイルシステムは`xfs`を使用

オペレーティングシステム	AMI	説明	ストレージ設定
			しており、Docker は overlay2 ストレージドライバーを使用しています。詳細については、Docker ドキュメントの「OverlayFS ストレージドライバーを使用する」を参照してください。

Amazon ECS は、GitHub で Amazon ECS を使用して最適化した AMI の Linux バリアントの変更ログを提供します。詳細については、「Changelog」を参照してください。

Amazon ECS 最適化 AMI の Linux バリエーションは、Amazon Linux 2 AMI または Amazon Linux 2023 AMI をベースとして使用します。各バリアントの Amazon Linux 2 ソース AMI 名 もしくは Amazon Linux 2023 を取得するには、Systems Manager Parameter Store API をクエリします。詳細については、「Amazon ECS に最適化された Linux AMI メタデータを取得する」を参照してください。Amazon Linux 2 AMI リリースノートも公開されています。詳細については、「Amazon Linux 2 リリースノート」を参照してください。Amazon Linux 2023 リリースノートも公開されています。詳細については、「Amazon Linux 2023 リリースノート」を参照してください。

次のページでは、変更に関する追加情報を説明します。

- GitHub のソース AMI リリースノート
- Docker ドキュメントの「Docker Engine リリースノート」
- NVIDIA ドキュメントの「NVIDIA ドライバードキュメント」
- GitHub での Amazon ECS エージェントの変更ログ

  ecs-init アプリケーションのソースコード、エージェントをパッケージ化するためのスクリプトと構成は、エージェントリポジトリの一部になりました。ecs-init の古いバージョンおよびパッケージについては、GitHub で「Amazon ecs-init の変更ログ」を参照してください。

Amazon ECS に最適化された AMI へのセキュリティ更新の適用

Amazon Linux に基づく Amazon ECS に最適化された AMI には、cloud-init のカスタマイズされたバージョンが含まれています。Cloud-init は、Linux イメージをクラウドコンピューティング環境でブートストラップし、インスタンスの起動時に必要なアクションを実行するために使用されるパッケージです。デフォルトで、2024 年 6 月 12 日より前にリリースされた Amazon Linux に基づくすべての Amazon ECS に最適化された AMI では、インスタンスの起動時にすべての「重大」および「重要」なセキュリティ更新が適用されます。

2024 年 6 月 12 日のリリース以降、Amazon Linux 2 に基づく Amazon ECS に最適化された AMI の デフォルトの動作には、起動時のパッケージの更新が含まれなくなります。代わりに、リリースが利用可能になりしだい、Amazon ECS に最適化された新しい AMI に更新することをお勧めします。Amazon ECS に最適化された AMI は、利用可能なセキュリティ更新またはベース AMI の変更があったときにリリースされます。この結果、最新のパッケージバージョンとセキュリティ更新が確実に適用され、パッケージバージョンはインスタンスの起動を通じて不変です。Amazon ECS に最適化された最新の AMI の取得方法の詳細については、「Amazon ECS に最適化された Linux AMI メタデータを取得する」を参照してください。

新しい AMI が利用可能になりしだい更新するように環境を自動化することをお勧めします。利用可能なオプションの詳細については、「Amazon ECS のマネージドインスタンスドレインにより Amazon EC2 キャパシティの管理が容易に」を参照してください。

特定の AMI バージョンに「重大」および「重要」のセキュリティ更新を引き続き手動で適用する場合は、Amazon EC2 インスタンスで次のコマンドを実行します。

```
yum update --security
```

起動時にセキュリティ更新を再度有効にする場合は、Amazon EC2 インスタンスの起動時に cloud-init ユーザーデータの `#cloud-config` セクションに次の行を追加できます。詳細については、「Amazon Linux ユーザーガイド」の「Amazon Linux 2 で cloud-init を使用する」を参照してください。

```
#cloud-config
repo_upgrade: security
```

Amazon ECS に最適化された Linux AMI メタデータを取得する

Amazon ECS に最適化された AMI のメタデータをプログラムで取得できます。メタデータには、AMI 名、Amazon ECS コンテナエージェントバージョン、Docker バージョンを含む ECS ランタイムバージョンなどが入っています。

コンソールを使用してクラスターを作成すると、Amazon ECS は選択したオペレーティングシステムに関連付けられた最新の AMI を使用してインスタンスの起動テンプレートを作成します。

AWS CloudFormation を使用してクラスターを作成する場合、SSM パラメータは Auto Scaling グループインスタンスの Amazon EC2 起動テンプレートの一部となります。動的な Systems Manager パラメータを使用して、デプロイする Amazon ECS Optimized AMI を決定するようにテンプレートを設定できます。このパラメータにより、スタックをデプロイするたびに、EC2 インスタンスに適用する必要がある利用可能な更新があるかどうかがチェックされます。Systems Manager パラメータの使用方法の例については、「AWS CloudFormation ユーザーガイド」の「Create an Amazon ECS cluster with the Amazon ECS-optimized Amazon Linux 2023 AMI」を参照してください。

Amazon ECS に最適化された AMI の各バリアントの AMI ID、イメージ名、オペレーティングシステム、コンテナエージェントバージョン、ソースイメージ名、ランタイムバージョンは、Systems Manager Parameter Store API にクエリすることでプログラムで取得できます。Systems Manager パラメータストア API の詳細については、「GetParameters」および「GetParametersByPath」を参照してください。

> **Note**
>
> Amazon ECS に最適化された AMI メタデータを取得するには、管理ユーザーに次の IAM アクセス権限が必要です。`AmazonECS_FullAccess` IAM ポリシーには、次の許可が追加されています。
>
> - ssm:GetParameters
> - ssm:GetParameter
> - ssm:GetParametersByPath

Systems Manager パラメータストアのパラメータフォーマット

以下は、各 Amazon ECS に最適化された AMI バリアントのパラメータ名のフォーマットです。

Linux Amazon ECS に最適化された AMI

- Amazon Linux 2023 AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2023/<version>
```

- Amazon Linux 2023 (arm64) AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2023/arm64/<version>
```

- Amazon Linux 2023 (Neuron) AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2023/neuron/<version>
```

- Amazon Linux 2 AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/<version>
```

- Amazon Linux 2 カーネル 5.10 AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/kernel-5.10/<version>
```

- Amazon Linux 2 (arm64) AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/arm64/<version>
```

- Amazon Linux 2 カーネル 5.10 (arm64) AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/kernel-5.10/arm64/<version>
```

- Amazon ECS GPU に最適化されたカーネル 5.10 AMI のメタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/kernel-5.10/gpu/<version>
```

- Amazon Linux 2 (GPU) AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/gpu/<version>
```

- Amazon ECS に最適化された Amazon Linux 2 (Neuron) カーネル 5.10 AMI のメタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/kernel-5.10/inf/<version>
```

- Amazon Linux 2 (Neuron) AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/inf/<version>
```

以下のパラメータ名の形式は、サブパラメータ image_id を使用して、推奨される最新の Amazon ECS に最適化された Amazon Linux 2 AMI のイメージ ID を取得します。

```
/aws/service/ecs/optimized-ami/amazon-linux-2/recommended/image_id
```

以下のパラメータ名の形式は、AMI 名を指定して、特定の Amazon ECS に最適化された AMI バージョンのメタデータを取得します。

- Amazon ECS に最適化された Amazon Linux 2 AMI メタデータ:

```
/aws/service/ecs/optimized-ami/amazon-linux-2/amzn2-ami-ecs-hvm-2.0.20181112-x86_64-ebs
```

> **Note**
>
> Amazon ECS に最適化された Amazon Linux 2 AMI のすべてのバージョンを取得できます。Amazon ECS に最適化された AMI バージョン amzn-ami-2017.09.l-amazon-ecs-optimized (Linux) 以降のみ取得できます。

例

以下の例は、それぞれの Amazon ECS に最適化された AMI バリアントのメタデータを取得する方法を示しています。

推奨される最新の Amazon ECS に最適化された AMI メタデータを取得する

推奨される最新の Amazon ECS に最適化された AMI を取得するには、AWS CLI で次の AWS CLI コマンドを使用します。

Linux Amazon ECS に最適化された AMI

- Amazon ECS 最適化 Amazon Linux 2023 AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2023/recommended --region us-east-1
```

- Amazon ECS 最適化 Amazon Linux 2023 (arm64) AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2023/
arm64/recommended --region us-east-1
```

- Amazon ECS に最適化された Amazon Linux 2023 (Neuron) AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2023/
neuron/recommended --region us-east-1
```

- Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
kernel-5.10/recommended --region us-east-1
```

- Amazon ECS に最適化された Amazon Linux 2 AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
recommended --region us-east-1
```

- Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 (arm64) AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
kernel-5.10/arm64/recommended --region us-east-1
```

- Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/arm64/
recommended --region us-east-1
```

- Amazon ECS GPU に最適化されたカーネル 5.10 AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
kernel-5.10/gpu/recommended --region us-east-1
```

- Amazon ECS GPU に最適化された AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/gpu/
recommended --region us-east-1
```

- Amazon ECS に最適化された Amazon Linux 2 (Neuron) カーネル 5.10 AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
kernel-5.10/inf/recommended --region us-east-1
```

- Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI の場合:

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/inf/
recommended --region us-east-1
```

推奨される最新の Amazon ECS に最適化された Amazon Linux 2023 AMI のイメージ ID を取得する

推奨される最新の Amazon ECS に最適化された Amazon Linux 2023 AMI ID のイメージ ID を取得するには、サブパラメータ `image_id` を使用します。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-
linux-2023/recommended/image_id --region us-east-1
```

`image_id` 値のみを取得するには、特定のパラメータ値のみのクエリを行うことができます。次に例を示します。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2023/
recommended/image_id --region us-east-1 --query "Parameters[0].Value"
```

Amazon ECS に最適化された特定の Amazon Linux 2 AMI バージョンのメタデータを取得する

Amazon ECS に最適化された特定の Amazon Linux AMI バージョンのメタデータを取得するには、AWS CLI で次の AWS CLI コマンドを使用します。AMI 名を、Amazon ECS に最適化された Amazon Linux AMI の名前と置き換えます。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/amzn2-ami-
ecs-hvm-2.0.20200928-x86_64-ebs --region us-east-1
```

Systems Manager の GetParametersByPath API を使用した Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 AMI メタデータの取得

Systems Manager の GetParametersByPath API を使用して、Amazon ECS に最適化された Amazon Linux 2 AMI メタデータを取得します。AWS CLI で次のコマンドを使用します。

```
aws ssm get-parameters-by-path --path /aws/service/ecs/optimized-ami/amazon-linux-2/
kernel-5.10/ --region us-east-1
```

推奨される最新の Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 AMI のイメージ ID を取得する

サブパラメータ image_id を使用することで、推奨される最新の Amazon ECS に最適化された Amazon Linux 2 カーネル 5.10 AMI ID のイメージ ID を取得できます。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
kernel-5.10/recommended/image_id --region us-east-1
```

image_id 値のみを取得するには、特定のパラメータ値のみのクエリを行うことができます。次に例を示します。

```
aws ssm get-parameters --names /aws/service/ecs/optimized-ami/amazon-linux-2/
recommended/image_id --region us-east-1 --query "Parameters[0].Value"
```

AWS CloudFormation テンプレートの推奨される最新の Amazon ECS に最適化された AMI を使用する

Systems Manager パラメータストア名を参照することにより、AWS CloudFormation テンプレートで推奨される最新の Amazon ECS に最適化された AMI を参照できます。

Linux の例

```
Parameters:kernel-5.10
  LatestECSOptimizedAMI:
    Description: AMI ID
    Type: AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>
    Default: /aws/service/ecs/optimized-ami/amazon-linux-2/kernel-5.10/recommended/
image_id
```

Amazon ECS 最適化 Linux AMI のビルドスクリプト

Amazon ECS は、Amazon ECS に最適化された AMI の Linux バリアントの構築に使用するビルドスクリプトをオープンソース化しました。これらのビルドスクリプトは、現在 GitHub で入手できます。詳細については、GitHub の「amazon-ecs-ami」を参照してください。

Amazon ECS に最適化された AMI をカスタマイズする必要がある場合は、GitHub の「Amazon ECS Optimized AMI Build Recipies」を参照してください。

ビルドスクリプトレポジトリには、HashiCorp Packer テンプレートと、Amazon ECS に最適化された AMI の各 Linux バリアントを生成するためのビルドスクリプトが含まれています。ここに置かれているものは、Amazon ECS 最適化 AMI のビルド用として最も信頼できるソーススクリプトであるため、GitHub リポジトリの状態をフォローすることで、AMI に対し実施された変更をモニタリングできます。例えば、独自の AMI で、Amazon ECS チームが正式な AMI に使用するのと同じバージョンの Docker を使用できます。

詳細については、GitHub の Amazon ECS AMI リポジトリにある「aws/amazon-ecs-ami」を参照してください。

Amazon ECS に最適化された Linux AMI を構築するには

1. `aws/amazon-ecs-ami` GitHub リポジトリのクローンを作成する

   ```
   git clone https://github.com/aws/amazon-ecs-ami.git
   ```

2. AMI の作成時に使用する AWS リージョンの環境変数を追加します。`us-west-2` 値を使用するリージョンに置き換えます。

   ```
   export REGION=us-west-2
   ```

3. AMI を構築するための Makefile が提供されます。クローンされたリポジトリのルートディレクトリから、構築する Amazon ECS 最適化 AMI の Linux バリアントに対応する次のコマンドのいずれかを使用します。

   - Amazon ECS に最適化された Amazon Linux 2 AMI

     ```
     make al2
     ```

   - Amazon ECS に最適化された Amazon Linux 2(arm64) AMI

     ```
     make al2arm
     ```

   - Amazon ECS GPU に最適化された AMI

     ```
     make al2gpu
     ```

   - Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI

```
make al2inf
```

- Amazon ECS 最適化 Amazon Linux 2023 AMI

```
make al2023
```

- Amazon ECS 最適化 Amazon Linux 2023 (arm64) AMI

```
make al2023arm
```

- Amazon ECS 最適化 Amazon Linux 2023 (Neuron) AMI

```
make al2023neu
```

Amazon ECS 最適化 Bottlerocket AMI

Bottlerocket は Linux ベースのオープンソースのオペレーティングシステムで、仮想マシンやベアメタルホスト上でコンテナを実行するために AWS によって専用に構築されています。Amazon ECS 最適化 Bottlerocket AMI は安全で、コンテナの実行に必要な最小数のパッケージのみが含まれています。これは、リソースの使用量を改善し、セキュリティのアタックサーフェスを縮小し、管理オーバーヘッドを削減するのに役立ちます。Bottlerocket AMI は Amazon ECS とも統合するため、クラスター内のコンテナインスタンスの更新に伴う運用上のオーバーヘッドを削減するのに役立ちます。

Bottlerocket は、次の点で Amazon Linux とは異なります。

- Bottlerocket にはパッケージマネージャーが含まれておらず、そのソフトウェアはコンテナとしてのみ実行できます。Bottlerocket に対する更新は、1 つのステップで適用され、1 つのステップでロールバックできるため、更新エラーの可能性が低くなります。
- Bottlerocket ホストを管理する主なメカニズムでは、コンテナスケジューラを使用します。Amazon Linux とは異なり、個別の Bottlerocket インスタンスへのログインは、高度なデバッグとトラブルシューティングのみを目的として、低頻度で実行される操作であることを想定しています。

Bottlerocket の詳細については、「GitHub」の「ドキュメント」と「リリース」を参照してください。

Amazon ECS に最適化された Bottlerocket AMI には、カーネル 6.1 用とカーネル 5.10 用のバリアントがあります。

以下のバリアントはカーネル 6.1 を使用します。

- `aws-ecs-2`
- `aws-ecs-2-nvidia`

以下のバリアントはカーネル 5.10 を使用します。

- `aws-ecs-1`
- `aws-ecs-1-nvidia`

  `aws-ecs-1-nvidia` バリアントの詳細については、「Amazon ECS での Bottlerocket 向け NVIDIA GPU サポートの発表」を参照してください。

考慮事項

Amazon ECS で Bottlerocket AMI を使用する場合は、次の点を考慮してください。

- Bottlerocket は、`x86_64` と `arm64` プロセッサを搭載した Amazon EC2 インスタンスをサポートします。Bottlerocket AMI を Inferentia チップを搭載した Amazon EC2 インスタンスで使用することはお勧めしません。
- Bottlerocket イメージには、SSH サーバーまたはシェルは含まれません。ただし、帯域外管理ツールを使用して、SSH 管理者アクセスを取得し、ブートストラップを実行できます。詳細については、「GitHub」の「bottlerocket README.md」のセクションを参照してください。
  - 探査
  - 管理者コンテナ
- デフォルトで、Bottlerocket には有効になっているコントロールコンテナがあります。このコンテナは、Amazon EC2 Bottlerocket インスタンス上でのコマンドの実行やシェルセッションの開始に使用できる AWS Systems Manager エージェントを実行します。詳細については、AWS Systems Manager ユーザーガイドの Session Manager のセットアップを参照してください。
- Bottlerocketはコンテナのワークロード向けに最適化されており、セキュリティに重点を置いています。Bottlerocket にはパッケージマネージャーが含まれておらず、イミュータブルです。セキュ

リティ機能とガイダンスについては、GitHub の「セキュリティ機能」および「セキュリティガイダンス」を参照してください。

- `awsvpc` ネットワークモードは、`1.1.0` 以降の Bottlerocket AMI バージョンでサポートされています。
- タスク定義の App Mesh は Bottlerocket AMI バージョン `1.15.0` 以降でサポートされています。
- タスク定義パラメータ `initProcessEnabled` は Bottlerocket AMI バージョン `1.19.0` 以降でサポートされています。
- Bottlerocket AMI は、次のサービスと機能もサポートしていません。
  - ECS Anywhere
  - Service Connect
  - 暗号化モードの Amazon EFS
  - `awsvpc` ネットワークモードの Amazon EFS
  - Elastic Inference アクセラレーター

Amazon ECS に最適化された Bottlerocket AMI メタデータを取得する

AWS Systems Manager パラメータストア API をクエリすることで、Amazon ECS に最適化された AMI の Amazon マシンイメージ (AMI) ID を取得できます。このパラメータを使用することで、Amazon ECS 最適化 AMI ID を手動で検索する必要がなくなります。Systems Manager Parameter Store API の詳細については、GetParameter を参照してください。使用するユーザーには、Amazon ECS 最適化 AMI メタデータを取得するための `ssm:GetParameter` IAM 許可が必要です。

`aws-ecs-2` Bottlerocket AMI バリアント

AWS CLI または AWS Management Console を使用して、AWS リージョン およびアーキテクチャ別に、最新の安定した `aws-ecs-2` Bottlerocket AMI バリアントを取得できます。

- AWS CLI – サブパラメータ `image_id` を指定しながら次の AWS CLI コマンドを使用することで、推奨される最新の Amazon ECS 最適化 Bottlerocket AMI のイメージ ID を取得できます。*`region`* を、AMI ID が必要な地域コードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。最新バージョン以外を取得するには、`latest` をバージョン番号に置き換えてください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-2 --name "/aws/service/bottlerocket/aws-ecs-2/x86_64/latest/image_id" --query Parameter.Value --output text
```

- 64 ビット Arm (arm64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-2 --name "/aws/service/bottlerocket/aws-ecs-2/arm64/latest/image_id" --query Parameter.Value --output text
```

- AWS Management Console – AWS Management Console で URL を使用して、推奨される Amazon ECS 最適化 AMI ID をクエリできます。この URL により、Amazon EC2 Systems Manager コンソールが開き、パラメータに対応した ID 値が表示されます 次の URL で、*region* を、AMI ID が必要なリージョンコードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
https://console.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-ecs-2/x86_64/latest/image_id/description?region=region#
```

  - 64 ビット Arm (arm64) アーキテクチャの場合:

```
https://console.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-ecs-2/arm64/latest/image_id/description?region=region#
```

aws-ecs-2-nvidia Bottlerocket AMI バリアント

AWS CLI または AWS Management Console を使用して、リージョンおよびアーキテクチャ別に、最新の安定した aws-ecs-2-nvdia Bottlerocket AMI バリアントを取得できます。

- AWS CLI – サブパラメータ image_id を指定しながら次の AWS CLI コマンドを使用することで、推奨される最新の Amazon ECS 最適化 Bottlerocket AMI のイメージ ID を取得できます。*region* を、AMI ID が必要な地域コードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。最新バージョン以外を取得するには、latest をバージョン番号に置き換えてください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-1 --name "/aws/service/bottlerocket/aws-ecs-2-nvidia/x86_64/latest/image_id" --query Parameter.Value --output text
```

- 64 ビット Arm (arm64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-1 --name "/aws/service/bottlerocket/aws-ecs-2-nvidia/arm64/latest/image_id" --query Parameter.Value --output text
```

- AWS Management Console – AWS Management Console で URL を使用して、推奨される Amazon ECS 最適化 AMI ID をクエリできます。この URL により、Amazon EC2 Systems Manager コンソールが開き、パラメータに対応した ID 値が表示されます 次の URL で、*region* を、AMI ID が必要なリージョンコードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
https://regionconsole.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-ecs-2-nvidia/x86_64/latest/image_id/description?region=region#
```

  - 64 ビット Arm (arm64) アーキテクチャの場合:

```
https://regionconsole.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-ecs-2-nvidia/arm64/latest/image_id/description?region=region#
```

aws-ecs-1 Bottlerocket AMI バリアント

AWS CLI または AWS Management Console を使用して、AWS リージョン およびアーキテクチャ別に、最新の安定した aws-ecs-1 Bottlerocket AMI バリアントを取得できます。

- AWS CLI – サブパラメータ image_id を指定しながら次の AWS CLI コマンドを使用することで、推奨される最新の Amazon ECS 最適化 Bottlerocket AMI のイメージ ID を取得できます。*region* を、AMI ID が必要な地域コードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。最新バージョン以外を取得するには、latest をバージョン番号に置き換えてください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-1 --name "/aws/service/bottlerocket/aws-ecs-1/x86_64/latest/image_id" --query Parameter.Value --output text
```

  - 64 ビット Arm (arm64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-1 --name "/aws/service/bottlerocket/aws-
ecs-1/arm64/latest/image_id" --query Parameter.Value --output text
```

- AWS Management Console – AWS Management Console で URL を使用して、推奨される Amazon ECS 最適化 AMI ID をクエリできます。この URL により、Amazon EC2 Systems Manager コンソールが開き、パラメータに対応した ID 値が表示されます 次の URL で、*region* を、AMI ID が必要なリージョンコードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
https://region.console.aws.amazon.com/systems-manager/parameters/aws/service/
bottlerocket/aws-ecs-1/x86_64/latest/image_id/description
```

  - 64 ビット Arm (arm64) アーキテクチャの場合:

```
https://region.console.aws.amazon.com/systems-manager/parameters/aws/service/
bottlerocket/aws-ecs-1/arm64/latest/image_id/description
```

aws-ecs-1-nvidia Bottlerocket AMI バリアント

AWS CLI または AWS Management Console を使用して、リージョンおよびアーキテクチャ別に、最新の安定した aws-ecs-1-nvdia Bottlerocket AMI バリアントを取得できます。

- AWS CLI – サブパラメータ image_id を指定しながら次の AWS CLI コマンドを使用することで、推奨される最新の Amazon ECS 最適化 Bottlerocket AMI のイメージ ID を取得できます。*region* を、AMI ID が必要な地域コードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。最新バージョン以外を取得するには、latest をバージョン番号に置き換えてください。
  - 64 ビット (x86_64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-1 --name "/aws/service/bottlerocket/aws-
ecs-1-nvidia/x86_64/latest/image_id" --query Parameter.Value --output text
```

  - 64 ビット Arm (arm64) アーキテクチャの場合:

```
aws ssm get-parameter --region us-east-1 --name "/aws/service/bottlerocket/aws-
ecs-1-nvidia/arm64/latest/image_id" --query Parameter.Value --output text
```

- AWS Management Console – AWS Management Console で URL を使用して、推奨される Amazon ECS 最適化 AMI ID をクエリできます。この URL により、Amazon EC2 Systems Manager コンソールが開き、パラメータに対応した ID 値が表示されます 次の URL で、*region* を、AMI ID が必要なリージョンコードに置き換えます。サポートされている AWS リージョン については、GitHub での「AMI の検索」を参照してください。
  - 64 ビット (x86_64) アーキテクチャの場合:

    ```
    https://console.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-ecs-1-nvidia/x86_64/latest/image_id/description?region=region#
    ```

  - 64 ビット Arm (arm64) アーキテクチャの場合:

    ```
    https://console.aws.amazon.com/systems-manager/parameters/aws/service/bottlerocket/aws-ecs-1-nvidia/arm64/latest/image_id/description?region=region#
    ```

次のステップ

Amazon ECS で Bottlerocket オペレーティングシステムの使用を開始する方法の詳細なチュートリアルについては、GitHub の「Using a Bottlerocket AMI with Amazon ECS」および AWS ブログサイトの「Getting started with Bottlerocket and Amazon ECS」を参照してください。

Bottlerocket インスタンスを起動する方法については、「Amazon ECS の Bottlerocket インスタンスの起動」を参照してください。

Amazon ECS の Bottlerocket インスタンスの起動

Bottlerocket インスタンスを起動することで、コンテナワークロードを実行することができます。

AWS CLI を使用して Bottlerocket インスタンスを起動できます。

1. `userdata.toml` というファイルを作成します。このファイルは、インスタンスのユーザーデータに使用されます。*cluster-name* をクラスターの名前に置き換えます。

   ```
   [settings.ecs]
   cluster = "cluster-name"
   ```

2. the section called “Amazon ECS に最適化された Bottlerocket AMI メタデータを取得する” に含まれているコマンドのいずれかを使用して、Bottlerocket AMI ID を取得します。これは次のステップで使用します。

3. 次のコマンドを実行して、Bottlerocket インスタンスを起動します。次のパラメータを必ず置き換えてください。

   - *subnet* を、インスタンスを起動するプライベートまたはパブリックサブネットの ID に置き換えます。
   - *bottlerocket_ami* を、前のステップの AMI ID に置き換えます。
   - *t3.large* を、使用するインスタンスタイプに置き換えます。
   - *region* を、リージョンコードに置き換えます。

```
aws ec2 run-instances --key-name ecs-bottlerocket-example \
   --subnet-id subnet \
   --image-id bottlerocket_ami \
   --instance-type t3.large \
   --region region \
   --tag-specifications
 'ResourceType=instance,Tags=[{Key=bottlerocket,Value=example}]' \
   --user-data file://userdata.toml \
   --iam-instance-profile Name=ecsInstanceRole
```

4. 次のコマンドを実行して、コンテナインスタンスがクラスターに登録されていることを検証します。このコマンドを実行するときは、次のパラメータを必ず置き換えてください。

   - *cluster* を、自分のクラスター名に置き換えます。
   - *region* を、リージョンコードに置き換えます。

```
aws ecs list-container-instances --cluster cluster-name --region region
```

Amazon ECS で Bottlerocket オペレーティングシステムの使用を開始する方法の詳細なチュートリアルについては、GitHub の「Amazon ECS での Bottlerocket AMI の使用」および AWS ブログサイトの「Bottlerocket および Amazon ECS の開始方法」を参照してください。

Amazon ECS Linux コンテナインスタンスの管理

Amazon ECS ワークロードに EC2 インスタンスを使用する場合、インスタンスを維持するのはユーザーの責任です。

管理手順

- Amazon ECS Linux コンテナインスタンスの起動
- Amazon ECS Linux コンテナインスタンスをブートストラップしてデータを渡す
- スポットインスタンス通知を受信するように Amazon ECS Linux コンテナインスタンスを設定する
- Amazon ECS Linux コンテナインスタンスの起動時にスクリプトを実行する
- Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす
- Amazon ECS Linux コンテナインスタンスのメモリを予約する
- AWS Systems Manager を使用して Amazon ECS コンテナインスタンスをリモートで管理する
- Amazon ECS Linux コンテナインスタンスに HTTP プロキシを使用する
- Amazon ECS Auto Scaling グループ用に事前初期化されたインスタンスを設定する
- Amazon ECS コンテナエージェントをアップデートする

Amazon ECSコンテナエージェントの各バージョンは、異なる機能セットをサポートし、以前のバージョンのバグ修正を提供します。可能であれば、最新バージョンの Amazon ECSコンテナエージェントを使用することを常にお勧めします。コンテナエージェントを最新バージョンに更新するには、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

どの機能と拡張が各エージェントリリースに含まれているか確認するには、https://github.com/aws/amazon-ecs-agent/releases を参照してください。

> **Important**
>
> 信頼できるメトリクスの最小 Docker バージョンは、Amazon ECS 最適化 AMI `20220607` 以降に含まれる Docker バージョン `v20.10.13` 以降です。
> バージョン `1.20.0` 以降のAmazon ECSエージェントでは、`1.9.0` より前のバージョンの Docker のサポートが廃止されました。

Amazon ECS Linux コンテナインスタンスの起動

Amazon EC2 コンソールを使用して Amazon ECS コンテナインスタンスを作成できます。

インスタンスは、Amazon EC2 コンソール、AWS CLI、SDK など、さまざまな方法で起動できます。インスタンスを起動する他の方法については、「Amazon EC2 ユーザーガイド」の「Launch your instance」を参照してください。

起動ウィザードの詳細については、「Amazon EC2 ユーザーガイド」の「新しいインスタンス起動ウィザードを使用してインスタンスを起動する」を参照してください。

開始する前に、「Amazon ECS を使用するようにセットアップする」のステップを完了します。

新しい Amazon EC2 ウィザードを使用してインスタンスを起動できます。インスタンス起動ウィザードでは、インスタンスの起動に必要な起動パラメータを指定します。

インスタンス設定のパラメータ

- 手順
- 名前とタグ
- アプリケーションと OS イメージ (Amazon マシンイメージ)
- インスタンスタイプ
- キーペア (ログイン)
- ネットワーク設定
- ストレージの設定
- 高度な詳細

手順

開始する前に、「Amazon ECS を使用するようにセットアップする」のステップを完了します。

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. 画面の上のナビゲーションバーで、現在の AWS リージョンが表示されます (例: 米国東部 (オハイオ))。インスタンスを起動するリージョンを選択します。
3. Amazon EC2 コンソールダッシュボードで、[インスタンスを起動] を選択してください。

名前とタグ

インスタンス名はタグで、キーは [Name] (名前)、値は指定した名前です。インスタンス、ボリューム、および伸縮自在なグラフィックスにタグ付けできます。スポットインスタンスの場合、スポットインスタンスリクエストにのみタグを付けることができます。

インスタンス名と追加のタグを指定することはオプションです。

- [Name] (名前) に、インスタンスのわかりやすい名前を入力します。名前を指定しない場合は、インスタンスをその ID で識別できます。ID は、インスタンスの起動時に自動的に生成されます。

- タグを追加するには、[Add additional tag] (追加のタグを追加) を選択します。[Add tag] (タグを追加) を選択し、キーと値を入力し、タグ付けするリソースタイプを選択します。追加するタグごとに [Add tag] (タグの追加) を選択します。

アプリケーションと OS イメージ (Amazon マシンイメージ)

Amazon マシンイメージ (AMI) には、インスタンスの起動に必要な情報が含まれています。例えば、ある AMI には、ウェブサーバーとして動作するために必要なソフトウェア (Apache やウェブサイトなど) が含まれています。

[Search] (検索) バーを使用して、AWS によって発行された適切な Amazon ECS 最適化 AMI を検索します。

1. [Search] (検索) バーに次のいずれかの用語を入力します。
   - **`ami-ecs`**
   - Amazon ECS 最適化 AMI の [Value] (値)。

     最新の Amazon ECS 最適化 AMI とその値については、「Linux Amazon ECS に最適化された AMI」を参照してください。
2. [Enter] キーを押します。
3. [Choose an Amazon Machine Image (AMI)] (Amazon マシンイメージ (AMI) を選択) ページで、[AWS Marketplace AMIs] タブを選択します。
4. 左側の [結果を絞り込む] ペインから、[Amazon Web Services] を [パブリッシャー] として選択します。
5. 使用する AMI の行で [Select] (選択) を選択します。

   または、[Cancel] (キャンセル) (右上) を選択することで、AMI を選択せずにインスタンス起動ウィザードに戻ります。デフォルトの AMI が選択されます。AMI が、「Amazon ECS に最適化された Linux AMI」で概説されている要件を満たしていることを確認します。

インスタンスタイプ

インスタンスタイプは、インスタンスのハードウェア設定とサイズを定義します。インスタンスタイプが大きくなると、CPU およびメモリも増えます。詳細については、インスタンスタイプを参照してください。

- [Instance type] (インスタンスタイプ) で、インスタンスのインスタンスタイプを選択します。

選択したインスタンスタイプによって、タスクの実行に使用できるリソースが決まります。

キーペア (ログイン)

[Key pair name] (キーペア名) には、既存のキーペアを選択するか、[Create new key pair] (新しいキーペアを作成) を選択して新しいキーペアを作成します。

> **Important**
>
> [Proceed without key pair] (キーペアなしで進む) オプションを選択した場合 (非推奨)、ユーザーが別の方法でログインすることを許可するように設定された AMI を選択した場合でなければ、インスタンスに接続できなくなります。

ネットワーク設定

必要に応じて、ネットワーク設定を設定します。

- [Networking platform] (ネットワーキングプラットフォーム): [Virtual Private Cloud (VPC)] を選択して、[Network interfaces] (ネットワークインターフェイス) セクションでサブネットを指定します。
- [VPC]: セキュリティグループを作成する既存の VPC を選択します。
- [サブネット]: インスタンスは、アベイラビリティーゾーン、ローカルゾーン、Wavelength Zone、Outpost のいずれかに関連付けられたサブネットで起動できます。

  アベイラビリティーゾーンでインスタンスを起動するには、インスタンスを起動するサブネットを選択します。新しいサブネットを作成するには、[Create new subnet] を選択して Amazon VPC コンソールに移動します。終了したらインスタンス起動ウィザードに戻り、[Refresh] (更新) アイコンを選択して一覧にサブネットを読み込みます。

  ローカルゾーンでインスタンスを起動するには、ローカルゾーン内に作成したサブネットを選択します。

  アウトポストでインスタンスを起動するには、アウトポストに関連付けられた VPC 内のサブネットを選択します。
- [Auto-assign Public IP] (パブリック IP の自動割り当て): インスタンスをインターネットからアクセス可能にする場合は、[Auto-assign Public IP] (パブリック IP の自動割り当て) フィールドが

[Enable] (有効) に設定されていることを確認します。可能にしない場合には、このフィールドを [無効] に設定します。

> **Note**
>
> コンテナインスタンスには、Amazon ECS サービスエンドポイントと通信するためのアクセスが必要です。これは、インターフェイス VPC エンドポイントを介して、またはパブリック IP アドレスを持つコンテナインスタンスを通じて可能になります。
> インターフェイス VPC エンドポイントについての詳細は、「Amazon ECS とインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。
> インターフェイス VPC エンドポイントが設定されておらず、コンテナインスタンスがパブリック IP アドレスを持たない場合、ネットワークアドレス変換 (NAT) を使用してこのアクセスを提供する必要があります。詳細については、「Amazon VPC ユーザーガイド」の「NAT ゲートウェイ」、およびこのガイドの「Amazon ECS Linux コンテナインスタンスに HTTP プロキシを使用する」を参照してください。

- [Firewall (security groups)] (ファイアウォール (セキュリティグループ)): セキュリティグループを使用して、コンテナインスタンスのファイアウォールルールを定義します。このルールでは、どの着信ネットワークトラフィックをコンテナインスタンスに配信するかを指定します。他のトラフィックはすべて無視されます。
  - 既存のセキュリティグループを選択するには、[Select existing security group] (既存のセキュリティグループを選択) を選択し、Amazon ECS を使用するようにセットアップする で作成したセキュリティグループを選択します。

ストレージの設定

選択した AMI には、ルートボリュームを含む、1 つまたは複数のストレージボリュームが含まれます。インスタンスにアタッチする追加のボリュームを指定できます。

[Simple] (シンプル) ビューを使用できます。

- [Storage type] (ストレージタイプ): コンテナインスタンスのストレージを設定します。

  Amazon ECS に最適化された Amazon Linux 2 AMI を使用している場合、1 つの 30 GiB ボリュームがインスタンスに設定されます。これは、オペレーティングシステムと Docker の間で共有されます。

Amazon ECS に最適化された AMI を使用している場合、インスタンスには 2 つのボリュームが設定されます。[Root] ボリュームはオペレーティングシステム用で、2 番目の Amazon EBS ボリューム (/dev/xvdcz にアタッチ) は Docker 用です。

オプションで、アプリケーションのニーズに合わせてインスタンスのボリュームサイズを増減できます。

高度な詳細

[Advanced details] で、セクションを開いてフィールドを表示し、インスタンスの追加パラメータを指定します。

- [Purchasing option] (購入のオプション): [Request Spot Instances] (スポットインスタンスのリクエスト) を選択して、スポットインスタンスをリクエストします。また、スポットインスタンスに関連する他のフィールドも設定する必要があります。詳細については、「スポットインスタンスのリクエスト」を参照してください。

  > **Note**
  >
  > スポットインスタンスを使用していて、"Not available" メッセージが表示される場合は、別のインスタンスタイプを選択する必要があります。

  .

- [IAM instance profile] (IAM インスタンスプロフィール): コンテナインスタンス IAM ロールを選択します。通常、これは ecsInstanceRole という名前です。

  > **Important**
  >
  > 適切な IAM アクセス許可を使用してコンテナインスタンスを起動しないと、Amazon ECS エージェントはクラスターに接続できません。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

- [ユーザーデータ]: Amazon ECS コンテナエージェントの設定からのエージェント環境変数のようなユーザーデータを使用して、Amazon ECS コンテナインスタンスを設定します。Amazon EC2 ユーザーデータスクリプトはインスタンスの初回起動時に 1 回のみ実行されます。以下に、ユーザーデータを使用する目的の一般的な例を紹介します。

- デフォルトでは、コンテナインスタンスはデフォルトのクラスターで起動されます。デフォルト以外のクラスターで起動するには、[Advanced Details] (高度な詳細) リストを選択します。次に、[User data] フィールドに以下のスクリプトを貼り付け、*your_cluster_name* を使用するクラスターの名前に置き換えます。

```
#!/bin/bash
echo ECS_CLUSTER=your_cluster_name >> /etc/ecs/ecs.config
```

- Amazon S3 に ecs.config ファイルがあり、コンテナインスタンスロールへの Amazon S3 読み取り専用アクセスを有効にしている場合は、[高度な詳細] リストを選択します。次に、[User data (ユーザーデータ)] フィールドに以下のスクリプトを貼り付け、*your_bucket_name* を、AWS CLI をインストールして起動時に設定ファイルを書き込むバケットに置き換えます。

> **Note**
>
> この設定の詳細については、「Amazon S3 に Amazon ECS コンテナインスタンスの設定を保存する」を参照してください。

```
#!/bin/bash
yum install -y aws-cli
aws s3 cp s3://your_bucket_name/ecs.config /etc/ecs/ecs.config
```

- ECS_CONTAINER_INSTANCE_TAGS 設定パラメータを使用して、コンテナインスタンスのタグを指定します。これにより Amazon ECS にのみ関連付けられているタグが作成され、そのタグは Amazon EC2 API ではリスト取得できません。

> **Important**
>
> Amazon EC2 Auto Scaling グループを使用してコンテナインスタンスを起動する場合は、ECS_CONTAINER_INSTANCE_TAGS エージェント設定パラメータを使用してタグを追加する必要があります。これは、Auto Scaling グループを使用して起動される Amazon EC2 インスタンスにタグを追加する方法によるものです。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=your_cluster_name
```

```
ECS_CONTAINER_INSTANCE_TAGS={"tag_key": "tag_value"}
EOF
```

- コンテナインスタンスのタグを指定してから、ECS_CONTAINER_INSTANCE_PROPAGATE_TAGS_FROM 設定パラメータを使用してそれらを Amazon EC2 から Amazon ECS に伝播します。

  次に、コンテナインスタンスに関連付けられたタグを伝達し、さらに your_cluster_name という名前のクラスターでコンテナインスタンスを登録するユーザーデータスクリプトの例を示します。

  ```
  #!/bin/bash
  cat <<'EOF' >> /etc/ecs/ecs.config
  ECS_CLUSTER=your_cluster_name
  ECS_CONTAINER_INSTANCE_PROPAGATE_TAGS_FROM=ec2_instance
  EOF
  ```

詳細については、「Amazon ECS Linux コンテナインスタンスをブートストラップしてデータを渡す」を参照してください。

Amazon ECS Linux コンテナインスタンスをブートストラップしてデータを渡す

Amazon EC2 インスタンスを起動するときに、ユーザーデータを EC2 インスタンスに渡すことができます。インスタンスの起動時に、データを使って、一般的な自動設定タスクを実行したり、スクリプトを実行したりできます。Amazon ECS では、ユーザーデータの最も一般的なユースケースは、設定情報を Docker デーモンと Amazon ECS コンテナエージェントに渡すことです。

クラウドブートフック、シェルスクリプト、cloud-init ディレクティブなど、複数タイプのユーザーデータを Amazon EC2 に渡すことができます。これらおよびその他の形式の種類の詳細については、「Cloud-Init のドキュメント」を参照してください。

Amazon EC2 起動ウィザードの使用時にユーザーデータを渡すには、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

コンテナインスタンスがデータを渡すようにするための設定を、コンテナエージェント設定または Docker デーモン設定で行うことができます。

Amazon ECS コンテナエージェント

Amazon ECS に最適化された AMI の Linux バリアントは、コンテナエージェントの開始時に /etc/ecs/ecs.config ファイルでエージェント設定データを検索します。Amazon EC2 ユーザーデータ

を使用して、起動時に、この設定データを指定することができます。利用可能な Amazon ECS コンテナエージェントの設定変数の詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

クラスター名など、単一エージェントの設定変数のみを設定するには、echo を使用して、変数を設定ファイルにコピーします。

```
#!/bin/bash
echo "ECS_CLUSTER=MyCluster" >> /etc/ecs/ecs.config
```

/etc/ecs/ecs.config に書き込む変数が複数ある場合は、以下の heredoc 形式を使用します。この形式は cat で始まる行と EOF の間のすべてを設定ファイルに書き込みます。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
ECS_ENGINE_AUTH_TYPE=docker
ECS_ENGINE_AUTH_DATA={"https://index.docker.io/v1/":
{"username":"my_name","password":"my_password","email":"email@example.com"}}
ECS_LOGLEVEL=debug
ECS_WARM_POOLS_CHECK=true
EOF
```

カスタムインスタンス属性を設定するには、ECS_INSTANCE_ATTRIBUTES 環境変数を設定します。

```
#!/bin/bash
cat <<'EOF' >> ecs.config
ECS_INSTANCE_ATTRIBUTES={"envtype":"prod"}
EOF
```

Docker デーモン

Docker デーモンの構成情報は Amazon EC2 ユーザーデータで指定できます。設定オプションの詳細については、「Docker デーモンのドキュメント」を参照してください。

以下の例では、カスタムオプションが Docker デーモン構成ファイル /etc/docker/daemon.json に追加され、インスタンスの起動時にユーザーデータで指定されます。

```
#!/bin/bash
```

```
cat <<EOF >/etc/docker/daemon.json
{"debug": true}
EOF
systemctl restart docker --no-block
```

以下の例では、カスタムオプションが Docker デーモン構成ファイル `/etc/docker/daemon.json` に追加され、インスタンスの起動時にユーザーデータで指定されます。この例は、Docker デーモン設定ファイルの docker-proxy を無効にする方法を示します。

```
#!/bin/bash
cat <<EOF >/etc/docker/daemon.json
{"userland-proxy": false}
EOF
systemctl restart docker --no-block
```

スポットインスタンス通知を受信するように Amazon ECS Linux コンテナインスタンスを設定する

利用可能なキャパシティーがなくなった場合、または、スポット料金がお客様のリクエストの上限料金を超えた場合には、Amazon EC2 はスポットインスタンスを終了、停止、または休止状態にします。Amazon EC2 は、終了アクションおよび停止アクションに対して、スポットインスタンスに 2 分間の中断通知を提供します。休止状態のアクションについては、2 分間の通知は提供されません。インスタンスで Amazon ECS スポットインスタンスドレイニングが有効になっている場合、Amazon ECS はスポットインスタンスの中断通知を受け取り、インスタンスを `DRAINING` ステータスにします。

> **Important**
>
> 自動スケーリングキャパシティの再分散よってインスタンスが削除された場合、Amazon ECS は Amazon EC2 から通知を受信しません。詳細については、「Amazon EC2 Auto Scaling キャパシティの再分散」を参照してください。

コンテナインスタンスを `DRAINING` に設定すると、Amazon ECS によって新規タスクがそのコンテナインスタンスに配置されなくなります。ドレインしているコンテナインスタンス上にある `PENDING` 状態のサービスタスクは即時停止されます。クラスター内に使用可能なコンテナインスタンスがある場合、そのインスタンスで代わりのサービスタスクが開始されます。

デフォルトでは、スポットインスタンスドレイニングは無効になっています。

インスタンスの起動時にスポットインスタンスドレイニングを有効にできます。次のスクリプトを [ユーザーデータ] フィールドに追加します。*MyCluster* は、コンテナインスタンスを登録するクラスターの名前に置き換えてください。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
ECS_ENABLE_SPOT_INSTANCE_DRAINING=true
EOF
```

詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

既存のコンテナインスタンスに対してスポットインスタンスのドレインを有効にするには

1. SSH 経由でスポットインスタンスに接続します。
2. `/etc/ecs/ecs.config` ファイルを編集して、以下を追加します。

   ```
   ECS_ENABLE_SPOT_INSTANCE_DRAINING=true
   ```

3. `ecs` サービスを再起動します。

   - Amazon ECS に最適化された Amazon Linux 2 AMI の場合:

     ```
     sudo systemctl restart ecs
     ```

4. (オプション) エージェント詳細分析 API オペレーションをクエリして、エージェントが実行されていることを確認し、新しいコンテナインスタンスに関する情報の一部を表示できます。詳細については、「the section called “コンテナの詳細分析”」を参照してください。

   ```
   curl http://localhost:51678/v1/metadata
   ```

Amazon ECS Linux コンテナインスタンスの起動時にスクリプトを実行する

すべてのコンテナインスタンスで特定のコンテナを実行して、モニタリング、セキュリティ、メトリクス、サービス検出、ログ記録などのオペレーションやセキュリティの問題に対処する必要がある場合があります。

これを行うには、起動時にユーザーデータスクリプトで、または Upstart や systemd などの一部の init システムで、docker run コマンドを呼び出すように、コンテナインスタンスを設定できます。こ

れは機能しますが、いくつかの欠点があります。Amazon ECS は、コンテナに関する情報を渡されず、CPU、メモリ、ポートなどのリソースをモニタリングできないためです。Amazon ECS がすべてのタスクリソースについて適切に情報を得られるように、コンテナインスタンスで実行するコンテナのタスク定義を作成します。その後、Amazon ECS を使用して、起動時に Amazon EC2 ユーザーデータを渡してタスクを配置します。

以下の手順の Amazon EC2 ユーザーデータスクリプトは、Amazon ECS イントロスペクション API を使用してコンテナインスタンスを識別します。次に、AWS CLI と start-task コマンドを使用して、指定されたタスクをスタートアップ時に実行します。

コンテナインスタンスの起動時にタスクを開始するには

1. `ecsInstanceRole` IAM ロールを変更して、`StartTask` API オペレーションに対するアクセス権限を追加します。詳細については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。
2. Amazon ECS に最適化された Amazon Linux 2 AMI を使用して、1 つ以上のコンテナインスタンスを起動します。新しいコンテナインスタンスを起動し、EC2 ユーザーデータで次のサンプルスクリプトを使用します。*`your_cluster_name`* は、コンテナインスタンスに登録するクラスターに置き換え、*`my_task_def`* は、起動時にインスタンスで実行するタスク定義に置き換えてください。

   詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

   > **Note**
   >
   > 以下の MIME マルチパートの内容では、シェルスクリプトを使用して値を設定し、パッケージをインストールしています。また、systemd ジョブを使用して、ecs サービスが実行されイントロスペクション API が使用可能になった後にタスクが開始されるようにしています。

```
Content-Type: multipart/mixed; boundary="==BOUNDARY=="
MIME-Version: 1.0

--==BOUNDARY==
Content-Type: text/x-shellscript; charset="us-ascii"

#!/bin/bash
# Specify the cluster that the container instance should register into
```

```
cluster=your_cluster_name

# Write the cluster configuration variable to the ecs.config file
# (add any other configuration variables here also)
echo ECS_CLUSTER=$cluster >> /etc/ecs/ecs.config

START_TASK_SCRIPT_FILE="/etc/ecs/ecs-start-task.sh"
cat <<- 'EOF' > ${START_TASK_SCRIPT_FILE}
 exec 2>>/var/log/ecs/ecs-start-task.log
 set -x

 # Install prerequisite tools
 yum install -y jq aws-cli

 # Wait for the ECS service to be responsive
 until curl -s http://localhost:51678/v1/metadata
 do
  sleep 1
 done

 # Grab the container instance ARN and AWS Region from instance metadata
 instance_arn=$(curl -s http://localhost:51678/v1/metadata | jq -r '.
 | .ContainerInstanceArn' | awk -F/ '{print $NF}' )
 cluster=$(curl -s http://localhost:51678/v1/metadata | jq -r '. | .Cluster' | awk
 -F/ '{print $NF}' )
 region=$(curl -s http://localhost:51678/v1/metadata | jq -r '.
 | .ContainerInstanceArn' | awk -F: '{print $4}')

 # Specify the task definition to run at launch
 task_definition=my_task_def

 # Run the AWS CLI start-task command to start your task on this container instance
 aws ecs start-task --cluster $cluster --task-definition $task_definition --
container-instances $instance_arn --started-by $instance_arn --region $region
EOF

# Write systemd unit file
UNIT="ecs-start-task.service"
cat <<- EOF > /etc/systemd/system/${UNIT}
      [Unit]
      Description=ECS Start Task
      Requires=ecs.service
      After=ecs.service
```

```
      [Service]
      Restart=on-failure
      RestartSec=30
      ExecStart=/usr/bin/bash ${START_TASK_SCRIPT_FILE}

      [Install]
      WantedBy=default.target
EOF

# Enable our ecs.service dependent service with `--no-block` to prevent systemd
 deadlock
# See https://github.com/aws/amazon-ecs-agent/issues/1707
systemctl enable --now --no-block "${UNIT}"
--==BOUNDARY==--
```

3. コンテナインスタンスが正しいクラスターで起動し、タスクが開始されていることを確認します。

   a. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
   b. ナビゲーションバーから、クラスターがあるリージョンを選択します。
   c. ナビゲーションペインで [Clusters] を選択し、コンテナインスタンスをホストするクラスターを選択します。
   d. [クラスター] ページで [タスク] を選択した後、使用するタスクを選択します。

      起動した各コンテナインスタンスでは、このタスクが実行状態になります。

      タスクが表示されない場合は、SSH を使用してコンテナインスタンスにログインし、`/var/log/ecs/ecs-start-task.log` ファイルでデバッグの情報を確認できます。

Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす

> **Note**
>
> この機能は Fargate では使用できません。

`awsvpc` ネットワークモードを使用するタスクには、それぞれ独自の Elastic Network Interface (ENI) が提供されます。この ENI は、ENI をホストするコンテナインスタンスにアタッチされています。Amazon EC2 インスタンスにアタッチできるネットワークインターフェイスの数にはデフォルトの制限があり、プライマリネットワークインターフェイスも 1 つとしてカウントされます。例え

ば、デフォルトでは c5.large インスタンスには最大 3 つの ENI がアタッチされています。このインスタンスのプライマリネットワークインターフェイスも 1 つとしてカウントされるため、このインスタンスに追加でアタッチできる ENI は 2 つです。awsvpc ネットワークモードを使用する各タスクには ENI が必要なため、通常このインスタンスタイプでは、このようなタスクを 2 つだけ実行できます。

Amazon ECS は、サポートされている Amazon EC2 インスタンスタイプを使用して、ENI 密度が高いコンテナインスタンスの起動をサポートしています。これらのインスタンスタイプを使用し、awsvpcTrunking アカウント設定を有効にすると、新しく起動されたコンテナインスタンスで追加の ENI を利用できます。この設定により、各コンテナインスタンスにより多くのタスクを配置できます。コンソールを使用して機能を有効にするには、「Amazon ECS アカウント設定の変更」を参照してください。AWS CLI を使用して機能を有効にするには、「AWS CLI を使用した Amazon ECS アカウント設定の管理」を参照してください。

例えば、awsvpcTrunking を持つ c5.large インスタンスでは、ENI の制限が 12 に引き上げられています。コンテナインスタンスはプライマリネットワークインターフェイスを持ち、Amazon ECS はコンテナインスタンスの「トランク」ネットワークインターフェイスを作成およびアタッチします。したがって、この設定では、現在の 2 個ではなく 10 個のタスクをコンテナインスタンスで起動できます。

トランクネットワークインターフェイスは Amazon ECS によって完全に管理され、コンテナインスタンスを削除またはクラスターから登録解除するときに削除されます。詳細については、「EC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。

考慮事項

ENI トランキング機能を使用する場合は、以下の点を考慮してください。

- ENI の制限引き上げに対応しているのは、Amazon ECS に最適化された AMI の Linux バリアント、バージョン 1.28.1 以降のコンテナエージェントを備えたその他の Amazon Linux バリアント、バージョン 1.28.1-2 以降の ecs-init パッケージのみです。Amazon ECS に最適化された AMI の最新の Linux バリアントを使用する場合、これらの要件が満たされます。現時点では、Windows コンテナはサポートされていません。
- awsvpcTrunking を有効にした後に起動した新しい Amazon EC2 インスタンスのみに、引き上げられた ENI 制限とトランクネットワークインターフェイスが適用されます。以前に起動されたインスタンスは、実行されたアクションに関係なく、これらの機能を受け取りません。
- Amazon EC2 インスタンスでは、リソースベースの IPv4 DNS リクエストがオフになっている必要があります。このオプションを無効にする場合、Amazon EC2 コンソールをで新しいインスタ

ンスを作成する際に、[Enable resource-based IPV4 (A record) DNS requests](リソースベースの IPV4 (A レコード) DNS リクエストを有効化) オプションの選択を外します。AWS CLI を使ってこのオプションを無効にするには、次のコマンドを使用します。

```
aws ec2 modify-private-dns-name-options --instance-id i-xxxxxxx --no-enable-resource-name-dns-a-record --no-dry-run
```

- 共有サブネットの Amazon EC2 インスタンスはサポートされません。これらを使用すると、クラスターへの登録に失敗します。
- タスクは、awsvpc ネットワークモードと EC2 起動タイプを使用する必要があります。Fargate 起動タイプを使用するタスクは、起動数に関係なく、常に専用の ENI が割り当てられるため、この機能は必要ありません。
- タスクは、コンテナインスタンスと同じ Amazon VPC で起動する必要があります。タスクが同じ VPC 内にない場合は属性エラーが発生し、タスクを開始することができません。
- 新しいコンテナインスタンスを起動するときに、インスタンスは REGISTERING 状態に移行し、トランク Elastic Network Interface がインスタンスに対してプロビジョニングされます。登録に失敗した場合、インスタンスは REGISTRATION_FAILED 状態に移行します。失敗した登録のトラブルシューティングを行うには、コンテナインスタンスを記述して、失敗の原因を説明する statusReason フィールドを表示するようにします。その後、コンテナインスタンスは手動で登録解除または終了できます。コンテナインスタンスが正常に登録解除または終了すると、Amazon ECS はトランク ENI を削除します。

> **Note**
>
> Amazon ECS は、REGISTRATION_FAILED 状態に移行するインスタンスを監視できるコンテナインスタンスの状態変更イベントを発行します。詳細については、「Amazon ECS コンテナインスタンス状態変更イベント」を参照してください。

- コンテナインスタンスが削除されると、インスタンスは DEREGISTERING 状態に移行し、トランク Elastic Network Interface が解放されます。次に、インスタンスは INACTIVE 状態に移行します。
- ENI 制限が引き上げられたパブリックサブネットのコンテナインスタンスが停止した後再起動されると、インスタンスはパブリック IP アドレスを失い、コンテナエージェントは接続を失います。
- awsvpcTrunking を有効にすると、コンテナインスタンスは VPC のデフォルトセキュリティグループを使用する追加の ENI が割り当てられ、Amazon ECS によって管理されます。

前提条件

ENI 制限が引き上げられたコンテナインスタンスを起動する前に、次の前提条件を満たす必要があります。

- Amazon ECS のサービスにリンクされたロールを作成する必要があります。Amazon ECS のサービスにリンクされたロールは、Amazon ECS に、お客様に代わって他のAWSサービスを呼び出すアクセス権限を付与します。このロールは、クラスターを作成する際、または AWS Management Console でサービスを作成または更新すると、自動的に作成されます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。サービスにリンクされたロールは、次の AWS CLI コマンドを使用して作成することもできます。

```
aws iam create-service-linked-role --aws-service-name ecs.amazonaws.com
```

- お客様のアカウントまたはコンテナインスタンスの IAM ロールは、`awsvpcTrunking` アカウント設定に有効化する必要があります。2 つのコンテナインスタンスロール (`ecsInstanceRole`) を作成することをお勧めします。そして、1 つのロールの `awsvpcTrunking` アカウント設定を有効にして、そのロールを ENI トランキングを必要とするタスクに使用することができます。コンテナインスタンスロールについては、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

前提条件が満たされると、サポートされているいずれかの Amazon EC2 インスタンスタイプを使用して新しいコンテナインスタンスを起動でき、インスタンスの ENI 制限が引き上げられています。サポートされているインスタンスタイプについてはAmazon ECS コンテナネットワークインターフェイスの増加でサポートされるインスタンスを参照してください。コンテナインスタンスで、バージョン `1.28.1` 以降のコンテナエージェントと、バージョン `1.28.1-2` 以降の ecs-init パッケージが必要です。Amazon ECS に最適化された AMI の最新の Linux バリアントを使用する場合、これらの要件が満たされます。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

> **Important**
>
> Amazon EC2 インスタンスでは、リソースベースの IPv4 DNS リクエストがオフになっている必要があります。このオプションを無効にする場合は、Amazon EC2 コンソールを使用した新しいインスタンスの作成時に [Enable resource-based IPV4 (A record) DNS requests] (リソースベースの IPV4 (A レコード) DNS リクエストを有効化) オプションを選択していないことを確認してください。AWS CLI を使ってこのオプションを無効にするには、次のコマンドを使用します。

```
aws ec2 modify-private-dns-name-options --instance-id i-xxxxxxx --no-enable-
resource-name-dns-a-record --no-dry-run
```

AWS CLI を使用して、ENI 制限が引き上げられたコンテナインスタンスを表示するには

各コンテナインスタンスにはデフォルトのネットワークインターフェイスがあり、これはトランクネットワークインターフェイストランクと呼ばれます。トランクネットワークインターフェイスがあることを示す ecs.awsvpc-trunk-id 属性のクエリを実行して、ENI 制限が引き上げられたコンテナインスタンスを一覧表示するには、次のコマンドを使用します。

- list-attributes (AWS CLI)

```
aws ecs list-attributes \
      --target-type container-instance \
      --attribute-name ecs.awsvpc-trunk-id \
      --cluster cluster_name \
      --region us-east-1
```

- Get-ECSAttributeList (AWS Tools for Windows PowerShell)

```
Get-ECSAttributeList -TargetType container-instance -AttributeName ecs.awsvpc-trunk-
id -Region us-east-1
```

Amazon ECS コンテナネットワークインターフェイスの増加でサポートされるインスタンス

以下に示しているのは、サポートされる Amazon EC2 インスタンスタイプと、awsvpcTrunking アカウント設定を有効化する前後で各インスタンスタイプにおいて awsvpc ネットワークモードを使用して起動できるタスクの数です。

Important

同じインスタンスファミリーでは、他のインスタンスタイプがサポートされていますが、a1.metal、c5.metal、c5a.8xlarge、c5ad.8xlarge、c5d.metal、m5.metal、p3dn.24 の各インスタンスタイプはサポートされていません。
c5n、d3、d3en、g3、g3s、g4dn、i3、i3en、inf1、m5dn、m5n、m5zn、mac1、r5b、r5n、r5 および z1d インスタンスファミリーはサポートされていません。

トピック

汎用

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
a1.medium	1	10
a1.large	2	10
a1.xlarge	3	20
a1.2xlarge	3	40
a1.4xlarge	7	60
m5.large	2	10
m5.xlarge	3	20
m5.2xlarge	3	40
m5.4xlarge	7	60
m5.8xlarge	7	60
m5.12xlarge	7	60
m5.16xlarge	14	120
m5.24xlarge	14	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m5a.large	2	10
m5a.xlarge	3	20
m5a.2xlarge	3	40
m5a.4xlarge	7	60
m5a.8xlarge	7	60
m5a.12xlarge	7	60
m5a.16xlarge	14	120
m5a.24xlarge	14	120
m5ad.large	2	10
m5ad.xlarge	3	20
m5ad.2xlarge	3	40
m5ad.4xlarge	7	60
m5ad.8xlarge	7	60
m5ad.12xlarge	7	60
m5ad.16xlarge	14	120
m5ad.24xlarge	14	120
m5d.large	2	10
m5d.xlarge	3	20
m5d.2xlarge	3	40
m5d.4xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m5d.8xlarge	7	60
m5d.12xlarge	7	60
m5d.16xlarge	14	120
m5d.24xlarge	14	120
m5d.metal	14	120
m6a.large	2	10
m6a.xlarge	3	20
m6a.2xlarge	3	40
m6a.4xlarge	7	60
m6a.8xlarge	7	90
m6a.12xlarge	7	120
m6a.16xlarge	14	120
m6a.24xlarge	14	120
m6a.32xlarge	14	120
m6a.48xlarge	14	120
m6a.metal	14	120
m6g.medium	1	4
m6g.large	2	10
m6g.xlarge	3	20
m6g.2xlarge	3	40

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m6g.4xlarge	7	60
m6g.8xlarge	7	60
m6g.12xlarge	7	60
m6g.16xlarge	14	120
m6g.metal	14	120
m6gd.medium	1	4
m6gd.large	2	10
m6gd.xlarge	3	20
m6gd.2xlarge	3	40
m6gd.4xlarge	7	60
m6gd.8xlarge	7	60
m6gd.12xlarge	7	60
m6gd.16xlarge	14	120
m6gd.metal	14	120
m6i.large	2	10
m6i.xlarge	3	20
m6i.2xlarge	3	40
m6i.4xlarge	7	60
m6i.8xlarge	7	90
m6i.12xlarge	7	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m6i.16xlarge	14	120
m6i.24xlarge	14	120
m6i.32xlarge	14	120
m6i.metal	14	120
m6id.large	2	10
m6id.xlarge	3	20
m6id.2xlarge	3	40
m6id.4xlarge	7	60
m6id.8xlarge	7	90
m6id.12xlarge	7	120
m6id.16xlarge	14	120
m6id.24xlarge	14	120
m6id.32xlarge	14	120
m6id.metal	14	120
m6idn.large	2	10
m6idn.xlarge	3	20
m6idn.2xlarge	3	40
m6idn.4xlarge	7	60
m6idn.8xlarge	7	90
m6idn.12xlarge	7	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m6idn.16xlarge	14	120
m6idn.24xlarge	14	120
m6idn.32xlarge	15	120
m6idn.metal	15	120
m6in.large	2	10
m6in.xlarge	3	20
m6in.2xlarge	3	40
m6in.4xlarge	7	60
m6in.8xlarge	7	90
m6in.12xlarge	7	120
m6in.16xlarge	14	120
m6in.24xlarge	14	120
m6in.32xlarge	15	120
m6in.metal	15	120
m7a.medium	1	4
m7a.large	2	10
m7a.xlarge	3	20
m7a.2xlarge	3	40
m7a.4xlarge	7	60
m7a.8xlarge	7	90

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m7a.12xlarge	7	120
m7a.16xlarge	14	120
m7a.24xlarge	14	120
m7a.32xlarge	14	120
m7a.48xlarge	14	120
m7a.metal-48xl	14	120
m7g.medium	1	4
m7g.large	2	10
m7g.xlarge	3	20
m7g.2xlarge	3	40
m7g.4xlarge	7	60
m7g.8xlarge	7	60
m7g.12xlarge	7	60
m7g.16xlarge	14	120
m7g.metal	14	120
m7gd.medium	1	4
m7gd.large	2	10
m7gd.xlarge	3	20
m7gd.2xlarge	3	40
m7gd.4xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m7gd.8xlarge	7	60
m7gd.12xlarge	7	60
m7gd.16xlarge	14	120
m7gd.metal	14	120
m7i.large	2	10
m7i.xlarge	3	20
m7i.2xlarge	3	40
m7i.4xlarge	7	60
m7i.8xlarge	7	90
m7i.12xlarge	7	120
m7i.16xlarge	14	120
m7i.24xlarge	14	120
m7i.48xlarge	14	120
m7i.metal-24xl	14	120
m7i.metal-48xl	14	120
m7i-flex.large	2	4
M7i-flex.xlarge	3	10
m7i-flex.2xlarge	3	20
m7i-flex.4xlarge	7	40
m7i-flex.8xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
m7i-flex.12xlarge	7	120
m7i-flex.16xlarge	14	120
m8g.medium	1	4
m8g.large	2	10
m8g.xlarge	3	20
m8g.2xlarge	3	40
m8g.4xlarge	7	60
m8g.8xlarge	7	60
m8g.12xlarge	7	60
m8g.16xlarge	14	120
m8g.24xlarge	14	120
m8g.48xlarge	14	120
m8g.metal-24xl	14	120
m8g.metal-48xl	14	120
mac2.metal	7	12
mac2-m1ultra.metal	7	12
mac2-m2.metal	7	12
mac2-m2pro.metal	7	12

コンピューティングの最適化

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c5.large	2	10
c5.xlarge	3	20
c5.2xlarge	3	40
c5.4xlarge	7	60
c5.9xlarge	7	60
c5.12xlarge	7	60
c5.18xlarge	14	120
c5.24xlarge	14	120
c5a.large	2	10
c5a.xlarge	3	20
c5a.2xlarge	3	40
c5a.4xlarge	7	60
c5a.12xlarge	7	60
c5a.16xlarge	14	120
c5a.24xlarge	14	120
c5ad.large	2	10
c5ad.xlarge	3	20
c5ad.2xlarge	3	40
c5ad.4xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c5ad.12xlarge	7	60
c5ad.16xlarge	14	120
c5ad.24xlarge	14	120
c5d.large	2	10
c5d.xlarge	3	20
c5d.2xlarge	3	40
c5d.4xlarge	7	60
c5d.9xlarge	7	60
c5d.12xlarge	7	60
c5d.18xlarge	14	120
c5d.24xlarge	14	120
c6a.large	2	10
c6a.xlarge	3	20
c6a.2xlarge	3	40
c6a.4xlarge	7	60
c6a.8xlarge	7	90
c6a.12xlarge	7	120
c6a.16xlarge	14	120
c6a.24xlarge	14	120
c6a.32xlarge	14	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c6a.48xlarge	14	120
c6a.metal	14	120
c6g.medium	1	4
c6g.large	2	10
c6g.xlarge	3	20
c6g.2xlarge	3	40
c6g.4xlarge	7	60
c6g.8xlarge	7	60
c6g.12xlarge	7	60
c6g.16xlarge	14	120
c6g.metal	14	120
c6gd.medium	1	4
c6gd.large	2	10
c6gd.xlarge	3	20
c6gd.2xlarge	3	40
c6gd.4xlarge	7	60
c6gd.8xlarge	7	60
c6gd.12xlarge	7	60
c6gd.16xlarge	14	120
c6gd.metal	14	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c6gn.medium	1	4
c6gn.large	2	10
c6gn.xlarge	3	20
c6gn.2xlarge	3	40
c6gn.4xlarge	7	60
c6gn.8xlarge	7	60
c6gn.12xlarge	7	60
c6gn.16xlarge	14	120
c6i.large	2	10
c6i.xlarge	3	20
c6i.2xlarge	3	40
c6i.4xlarge	7	60
c6i.8xlarge	7	90
c6i.12xlarge	7	120
c6i.16xlarge	14	120
c6i.24xlarge	14	120
c6i.32xlarge	14	120
c6i.metal	14	120
c6id.large	2	10
c6id.xlarge	3	20

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c6id.2xlarge	3	40
c6id.4xlarge	7	60
c6id.8xlarge	7	90
c6id.12xlarge	7	120
c6id.16xlarge	14	120
c6id.24xlarge	14	120
c6id.32xlarge	14	120
c6id.metal	14	120
c6in.large	2	10
c6in.xlarge	3	20
c6in.2xlarge	3	40
c6in.4xlarge	7	60
c6in.8xlarge	7	90
c6in.12xlarge	7	120
c6in.16xlarge	14	120
c6in.24xlarge	14	120
c6in.32xlarge	15	120
c6in.metal	15	120
c7a.medium	1	4
c7a.large	2	10

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c7a.xlarge	3	20
c7a.2xlarge	3	40
c7a.4xlarge	7	60
c7a.8xlarge	7	90
c7a.12xlarge	7	120
c7a.16xlarge	14	120
c7a.24xlarge	14	120
c7a.32xlarge	14	120
c7a.48xlarge	14	120
c7a.metal-48xl	14	120
c7g.medium	1	4
c7g.large	2	10
c7g.xlarge	3	20
c7g.2xlarge	3	40
c7g.4xlarge	7	60
c7g.8xlarge	7	60
c7g.12xlarge	7	60
c7g.16xlarge	14	120
c7g.metal	14	120
c7gd.medium	1	4

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c7gd.large	2	10
c7gd.xlarge	3	20
c7gd.2xlarge	3	40
c7gd.4xlarge	7	60
c7gd.8xlarge	7	60
c7gd.12xlarge	7	60
c7gd.16xlarge	14	120
c7gd.metal	14	120
c7gn.medium	1	4
c7gn.large	2	10
c7gn.xlarge	3	20
c7gn.2xlarge	3	40
c7gn.4xlarge	7	60
c7gn.8xlarge	7	60
c7gn.12xlarge	7	60
c7gn.16xlarge	14	120
c7gn.metal	14	120
c7i.large	2	10
c7i.xlarge	3	20
c7i.2xlarge	3	40

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c7i.4xlarge	7	60
c7i.8xlarge	7	90
c7i.12xlarge	7	120
c7i.16xlarge	14	120
c7i.24xlarge	14	120
c7i.48xlarge	14	120
c7i.metal-24xl	14	120
c7i.metal-48xl	14	120
c7i-flex.large	2	4
c7i-flex.xlarge	3	10
c7i-flex.2xlarge	3	20
c7i-flex.4xlarge	7	40
c7i-flex.8xlarge	7	60
c7i-flex.12xlarge	7	120
c7i-flex.16xlarge	14	120
c8g.medium	1	4
c8g.large	2	10
c8g.xlarge	3	20
c8g.2xlarge	3	40
c8g.4xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
c8g.8xlarge	7	60
c8g.12xlarge	7	60
c8g.16xlarge	14	120
c8g.24xlarge	14	120
c8g.48xlarge	14	120
c8g.metal-24xl	14	120
c8g.metal-48xl	14	120

メモリ最適化

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r5.large	2	10
r5.xlarge	3	20
r5.2xlarge	3	40
r5.4xlarge	7	60
r5.12xlarge	7	60
r5.16xlarge	14	120
r5.24xlarge	14	120
r5a.large	2	10
r5a.xlarge	3	20

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r5a.2xlarge	3	40
r5a.4xlarge	7	60
r5a.8xlarge	7	60
r5a.12xlarge	7	60
r5a.16xlarge	14	120
r5a.24xlarge	14	120
r5ad.large	2	10
r5ad.xlarge	3	20
r5ad.2xlarge	3	40
r5ad.4xlarge	7	60
r5ad.8xlarge	7	60
r5ad.12xlarge	7	60
r5ad.16xlarge	14	120
r5ad.24xlarge	14	120
r5b.16xlarge	14	120
r5d.large	2	10
r5d.xlarge	3	20
r5d.2xlarge	3	40
r5d.4xlarge	7	60
r5d.8xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r5d.12xlarge	7	60
r5d.16xlarge	14	120
r5d.24xlarge	14	120
r5dn.16xlarge	14	120
r6a.large	2	10
r6a.xlarge	3	20
r6a.2xlarge	3	40
r6a.4xlarge	7	60
r6a.8xlarge	7	90
r6a.12xlarge	7	120
r6a.16xlarge	14	120
r6a.24xlarge	14	120
r6a.32xlarge	14	120
r6a.48xlarge	14	120
r6a.metal	14	120
r6g.medium	1	4
r6g.large	2	10
r6g.xlarge	3	20
r6g.2xlarge	3	40
r6g.4xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r6g.8xlarge	7	60
r6g.12xlarge	7	60
r6g.16xlarge	14	120
r6g.metal	14	120
r6gd.medium	1	4
r6gd.large	2	10
r6gd.xlarge	3	20
r6gd.2xlarge	3	40
r6gd.4xlarge	7	60
r6gd.8xlarge	7	60
r6gd.12xlarge	7	60
r6gd.16xlarge	14	120
r6gd.metal	14	120
r6i.large	2	10
r6i.xlarge	3	20
r6i.2xlarge	3	40
r6i.4xlarge	7	60
r6i.8xlarge	7	90
r6i.12xlarge	7	120
r6i.16xlarge	14	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r6i.24xlarge	14	120
r6i.32xlarge	14	120
r6i.metal	14	120
r6idn.large	2	10
r6idn.xlarge	3	20
r6idn.2xlarge	3	40
r6idn.4xlarge	7	60
r6idn.8xlarge	7	90
r6idn.12xlarge	7	120
r6idn.16xlarge	14	120
r6idn.24xlarge	14	120
r6idn.32xlarge	15	120
r6idn.metal	15	120
r6in.large	2	10
r6in.xlarge	3	20
r6in.2xlarge	3	40
r6in.4xlarge	7	60
r6in.8xlarge	7	90
r6in.12xlarge	7	120
r6in.16xlarge	14	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r6in.24xlarge	14	120
r6in.32xlarge	15	120
r6in.metal	15	120
r6id.large	2	10
r6id.xlarge	3	20
r6id.2xlarge	3	40
r6id.4xlarge	7	60
r6id.8xlarge	7	90
r6id.12xlarge	7	120
r6id.16xlarge	14	120
r6id.24xlarge	14	120
r6id.32xlarge	14	120
r6id.metal	14	120
r7a.medium	1	4
r7a.large	2	10
r7a.xlarge	3	20
r7a.2xlarge	3	40
r7a.4xlarge	7	60
r7a.8xlarge	7	90
r7a.12xlarge	7	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r7a.16xlarge	14	120
r7a.24xlarge	14	120
r7a.32xlarge	14	120
r7a.48xlarge	14	120
r7a.metal-48xl	14	120
r7g.medium	1	4
r7g.large	2	10
r7g.xlarge	3	20
r7g.2xlarge	3	40
r7g.4xlarge	7	60
r7g.8xlarge	7	60
r7g.12xlarge	7	60
r7g.16xlarge	14	120
r7g.metal	14	120
r7gd.medium	1	4
r7gd.large	2	10
r7gd.xlarge *	3	20
r7gd.2xlarge	3	40
r7gd.4xlarge	7	60
r7gd.8xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r7gd.12xlarge	7	60
r7gd.16xlarge	14	120
r7gd.metal	14	120
r7i.large	2	10
r7i.xlarge	3	20
r7i.2xlarge	3	40
r7i.4xlarge	7	60
r7i.8xlarge	7	90
r7i.12xlarge	7	120
r7i.16xlarge	14	120
r7i.24xlarge	14	120
r7i.48xlarge	14	120
r7i.metal-24xl	14	120
r7i.metal-48xl	14	120
r7iz.large	2	10
r7iz.xlarge	3	20
r7iz.2xlarge	3	40
r7iz.4xlarge	7	60
r7iz.8xlarge	7	90
r7iz.12xlarge	7	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
r7iz.16xlarge	14	120
r7iz.32xlarge	14	120
r7iz.metal-16xl	14	120
r7iz.metal-32xl	14	120
r8g.medium	1	4
r8g.large	2	10
r8g.xlarge	3	20
r8g.2xlarge	3	40
r8g.4xlarge	7	60
r8g.8xlarge	7	60
r8g.12xlarge	7	60
r8g.16xlarge	14	120
r8g.24xlarge	14	120
r8g.48xlarge	14	120
r8g.metal-24xl	14	120
r8g.metal-48xl	14	120
u-3tb1.56xlarge	7	12
u-6tb1.56xlarge	14	12
u-18tb1.112xlarge	14	12
u-18tb1.metal	14	12

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
u-24tb1.112xlarge	14	12
u-24tb1.metal	14	12
u7i-6tb.112xlarge	14	120
u7i-8tb.112xlarge	14	120
u7i-12tb.224xlarge	14	120
u7in-16tb.224xlarge	15	120
u7in-24tb.224xlarge	15	120
u7in-32tb.224xlarge	15	120
u7inh-32tb.480xlarge	15	120
x2gd.medium	1	10
x2gd.large	2	10
x2gd.xlarge	3	20
x2gd.2xlarge	3	40
x2gd.4xlarge	7	60
x2gd.8xlarge	7	60
x2gd.12xlarge	7	60
x2gd.16xlarge	14	120
x2gd.metal	14	120
x2idn.16xlarge	14	120
x2idn.24xlarge	14	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
x2idn.32xlarge	14	120
x2idn.metal	14	120
x2iedn.xlarge	3	13
x2iedn.2xlarge	3	29
x2iedn.4xlarge	7	60
x2iedn.8xlarge	7	120
x2iedn.16xlarge	14	120
x2iedn.24xlarge	14	120
x2iedn.32xlarge	14	120
x2iedn.metal	14	120
x2iezn.2xlarge	3	64
x2iezn.4xlarge	7	120
x2iezn.6xlarge	7	120
x2iezn.8xlarge	7	120
x2iezn.12xlarge	14	120
x2iezn.metal	14	120
x8g.medium	1	4
x8g.large	2	10
x8g.xlarge	3	20
x8g.2xlarge	3	40

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
x8g.4xlarge	7	60
x8g.8xlarge	7	60
x8g.12xlarge	7	60
x8g.16xlarge	14	120
x8g.24xlarge	14	120
x8g.48xlarge	14	120
x8g.metal-24xl	14	120
x8g.metal-48xl	14	120

ストレージの最適化

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
i4g.large	2	10
i4g.xlarge	3	20
i4g.2xlarge	3	40
i4g.4xlarge	7	60
i4g.8xlarge	7	60
i4g.16xlarge	14	120
i4i.xlarge	3	8
i4i.2xlarge	3	28

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
i4i.4xlarge	7	58
i4i.8xlarge	7	118
i4i.12xlarge	7	118
i4i.16xlarge	14	248
i4i.24xlarge	14	118
i4i.32xlarge	14	498
i4i.metal	14	498
i7ie.large	2	20
i7ie.xlarge	3	29
i7ie.2xlarge	3	29
i7ie.3xlarge	3	29
i7ie.6xlarge	7	60
i7ie.12xlarge	7	60
i7ie.18xlarge	14	120
i7ie.24xlarge	14	120
i7ie.48xlarge	14	120
i8g.large	2	10
i8g.xlarge	3	20
i8g.2xlarge	3	40
i8g.4xlarge	7	60

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
i8g.8xlarge	7	60
i8g.12xlarge	7	60
i8g.16xlarge	14	120
i8g.24xlarge	14	120
i8g.metal-24xl	14	120
im4gn.large	2	10
im4gn.xlarge	3	20
im4gn.2xlarge	3	40
im4gn.4xlarge	7	60
im4gn.8xlarge	7	60
im4gn.16xlarge	14	120
is4gen.medium	1	4
is4gen.large	2	10
is4gen.xlarge	3	20
is4gen.2xlarge	3	40
is4gen.4xlarge	7	60
is4gen.8xlarge	7	60

高速コンピューティング

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
dl1.24xlarge	59	120
dl2q.24xlarge	14	120
f2.6xlarge	7	90
f2.12xlarge	7	120
f2.48xlarge	14	120
g4ad.xlarge	1	12
g4ad.2xlarge	1	12
g4ad.4xlarge	2	12
g4ad.8xlarge	3	12
g4ad.16xlarge	7	12
g5.xlarge	3	6
g5.2xlarge	3	19
g5.4xlarge	7	40
g5.8xlarge	7	90
g5.12xlarge	14	120
g5.16xlarge	7	120
g5.24xlarge	14	120
g5.48xlarge	6	120
g5g.xlarge	3	20

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
g5g.2xlarge	3	40
g5g.4xlarge	7	60
g5g.8xlarge	7	60
g5g.16xlarge	14	120
g5g.metal	14	120
g6.xlarge	3	20
g6.2xlarge	3	40
g6.4xlarge	7	60
g6.8xlarge	7	90
g6.12xlarge	7	120
g6.16xlarge	14	120
g6.24xlarge	14	120
g6.48xlarge	14	120
g6e.xlarge	3	20
g6e.2xlarge	3	40
g6e.4xlarge	7	60
g6e.8xlarge	7	90
g6e.12xlarge	9	120
g6e.16xlarge	14	120
g6e.24xlarge	19	120

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
g6e.48xlarge	39	120
gr6.4xlarge	7	60
gr6.8xlarge	7	90
inf2.xlarge	3	20
inf2.8xlarge	7	90
inf2.24xlarge	14	120
inf2.48xlarge	14	120
p4d.24xlarge	59	120
p4de.24xlarge	59	120
p5.48xlarge	63	242
p5e.48xlarge	63	242
p5en.48xlarge	63	242
trn1.2xlarge	3	19
trn1.32xlarge	39	120
trn1n.32xlarge	79	242
trn2.48xlarge	31	242
trn2u.48xlarge	31	242
vt1.3xlarge	3	40
vt1.6xlarge	7	60
vt1.24xlarge	14	120

ハイパフォーマンスコンピューティング

インスタンスタイプ	ENI トランキングなしのタスク制限	ENI トランキングありのタスク制限
hpc6a.48xlarge	1	120
hpc6id.32xlarge	1	120
hpc7g.4xlarge	3	120
hpc7g.8xlarge	3	120
hpc7g.16xlarge	3	120

Amazon ECS Linux コンテナインスタンスのメモリを予約する

Amazon ECS コンテナエージェントがクラスターにコンテナインスタンスを登録する場合、エージェントは、コンテナインスタンスがタスク用に予約できるメモリ容量を決定する必要があります。プラットフォームのメモリオーバーヘッドとシステムカーネルが占めるメモリのため、この数値は、Amazon EC2 インスタンスとして公開されているインストール済みメモリ量とは異なります。例えば、`m4.large` インスタンスには 8 GiB のメモリがインストールされています。しかし、これはコンテナインスタンスが登録されたときに、タスクに使用できるメモリが正確に 8192 MiB に変換されるとは限りません。

Amazon ECS コンテナエージェントには、タスクに割り当てられたプールから指定したメモリ容量 (MiB) を削除するのに使用できる、`ECS_RESERVED_MEMORY` という設定変数があります。これにより、重要なシステムプロセスのメモリを効果的に確保することができます。

タスクでコンテナインスタンスのすべてのメモリを占有している場合、メモリが不可欠なシステムプロセスとタスクが競合し、システム障害が発生する可能性があります。

例えば、コンテナエージェント設定ファイルで `ECS_RESERVED_MEMORY=256` を指定すると、そのインスタンスの総メモリマイナス 256 MiB が登録され、256 MiBのメモリは ECS タスクに割り当てされなくなります。エージェント構成変数とその設定方法の詳細については、Amazon ECS コンテナエージェントの設定 および Amazon ECS Linux コンテナインスタンスをブートストラップしてデータを渡す を参照してください 。

タスクに 8192 MiB を指定して、使用可能なメモリが 8192 MiB 以上のコンテナインスタンスがなくこの要件を満たせない場合、そのタスクはクラスターに配置できません。マネージド型コンピューティング環境を使用している場合、リクエストに対応するために AWS Batch はより大きなインスタンスタイプを起動する必要があります。

また、コンテナインスタンスの Amazon ECS コンテナエージェントやその他の重要なシステムプロセス用のメモリを確保しなくてはならず、そうでないとタスクのコンテナが同じメモリに対して競合し、システム障害を引き起こす可能性があります。

Amazon ECS コンテナエージェントは、Docker `ReadMemInfo()`関数を使用してオペレーティングシステムで使用可能な合計メモリのクエリを実行します。Linux と Windows の両方に、合計メモリを判断できるコマンドラインユーティリティが備わっています。

Example -Linux 合計メモリを決定

free コマンドは、オペレーティングシステムによって認識される合計メモリを返します。

```
$ free -b
```

Amazon ECS に最適化された Amazon Linux AMI を実行する `m4.large` インスタンスの出力例。

```
             total       used       free     shared    buffers     cached
Mem:    8373026816  348180480 8024846336      90112   25534464  205418496
-/+ buffers/cache:  117227520 8255799296
```

このインスタンスには 8373026816 バイトの合計メモリーがあり、タスクに使用できる 7985 MiB に変換されます。

Example -Windows 合計メモリを決定

wmic コマンドは、オペレーティングシステムによって認識される合計メモリを返します。

```
C:\> wmic ComputerSystem get TotalPhysicalMemory
```

Amazon ECS に最適化された Windows Server AMI を実行する `m4.large` インスタンスの出力例。

```
TotalPhysicalMemory
8589524992
```

このインスタンスには合計メモリーが 8589524992 バイトあり、タスクに使用可能な 8191 MiB に変換されます。

コンテナインスタンスのメモリを表示する

Amazon ECS コンソール (または DescribeContainerInstances API 操作) で、コンテナインスタンスに登録されているメモリ容量を表示できます。特定のインスタンスタイプに対して、可能な限り多くのメモリをタスクに割り当て、リソース使用率を最大化しようとしている場合は、そのコンテナインスタンスに使用可能なメモリを確認してから、そのタスクに十分なメモリを割り当てることができます。

コンテナインスタンスメモリを表示するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [クラスター] を選択し、コンテナインスタンスをホストするクラスターを選択します。
3. [インフラストラクチャ] を選択し、[コンテナインスタンス] でコンテナインスタンスを選択します。
4. [リソース] セクションに、コンテナインスタンス用に登録された使用可能なメモリが表示されます。

   [登録済み] メモリの値は、Amazon ECS の初回起動時に登録されたときのコンテナインスタンスのメモリの値で、[利用可能] メモリの値は、まだ タスクに割り当てられていないメモリの値です。

AWS Systems Manager を使用して Amazon ECS コンテナインスタンスをリモートで管理する

AWS Systems Manager (Systems Manager) で Run Command 機能を使用すると、Amazon ECS コンテナインスタンスの設定を安全にリモートで管理できます。Run Command を使用すると、インスタンスにローカルにログオンしなくても一般的な管理タスクを簡単に実行することができます。複数のコンテナインスタンスでコマンドを同時に実行することで、クラスター全体の設定の変更を管理できます。Run Command は各コマンドのステータスと結果をレポートします。

ここでは、Run Command を使用して実行できるタスクのタイプについていくつか例を示します。

- パッケージをインストールまたはアンインストールする。
- セキュリティ更新プログラムを実行する。
- Docker イメージをクリーンアップする。

- サービスを停止または起動する。
- システムリソースを表示する。
- ログファイルを表示する。
- ファイルオペレーションを実行する。

Run Command の詳細については、の「AWS Systems Managerユーザーガイド」の「AWS Systems ManagerRun Command」を参照してください。

Amazon ECS で Systems Manager を使用するには、以下の前提条件があります。

1. コンテナインスタンスロール (ecsInstanceRole) に、Systems Manager API にアクセス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、AmazonSSMManagedInstanceCore を `ecsInstanceRole` ロールに割り当てます。ポリシーをロールにアタッチする方法については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。
2. SSM Agent がコンテナインスタンスにインストールされていることを確認します。詳細については、「Linux 用 EC2 インスタンスに SSM Agent を手動でインストールおよびアンインストールする」を参照してください。

Systems Manager 管理ポリシーを `ecsInstanceRole` にアタッチして、AWS Systems Manager エージェント (SSM Agent) がコンテナインスタンスにインストールされていることを確認したら、Run Command を使用してコマンドをコンテナインスタンスに送信することができます。インスタンスでのコマンドおよびシェルスクリプトの実行と、その結果の出力の表示については、AWS Systems Managerユーザーガイド の「Systems Manager Run Command を使用したコマンドの実行」および「Run Command のチュートリアル」を参照してください。

一般的なユースケースは、Run Command でコンテナインスタンスソフトウェアを更新することです。「AWS Systems Manager ユーザーガイド」の手順を実行し、以下のパラメータを指定します。

パラメータ	値
コマンドのドキュメント	`AWS-RunShellScript`
コマンド	`$ yum update -y`
ターゲットインスタンス	コンテナインスタンス

Amazon ECS Linux コンテナインスタンスに HTTP プロキシを使用する

Amazon ECS コンテナエージェントと Docker デーモンの両方に HTTP プロキシを使用するように Amazon ECS コンテナインスタンスを設定できます。これは、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合に便利です。

HTTP プロキシを使用するように Amazon ECS Linux コンテナインスタンスを設定するには、起動時に該当するファイルで以下の変数に Amazon EC2 ユーザーデータを設定します。手動で設定ファイルを編集してから、エージェントを再起動することもできます。

`/etc/ecs/ecs.config` (Amazon Linux 2 および Amazon Linux AMI)

`HTTP_PROXY=10.0.0.131:3128`

この値を、Amazon ECS エージェントがインターネットへの接続に使用する HTTP プロキシのホスト名 (または IP アドレス) とポート番号に設定します。例えば、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合です。

`NO_PROXY=169.254.169.254,169.254.170.2,/var/run/docker.sock`

この値を `169.254.169.254,169.254.170.2,/var/run/docker.sock` に設定して、EC2 インスタンスのメタデータ、タスク用の IAM; ロール、および Docker デーモンのトラフィックをプロキシからフィルタリングします。

`/etc/systemd/system/ecs.service.d/http-proxy.conf` (Amazon Linux 2 のみ)

`Environment="HTTP_PROXY=10.0.0.131:3128/"`

この値を、`ecs-init` がインターネットへの接続に使用する HTTP プロキシのホスト名 (または IP アドレス) とポート番号に設定します。例えば、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合です。

```
Environment="NO_PROXY=169.254.169.254,169.254.170.2,/var/run/
docker.sock"
```

この値を `169.254.169.254,169.254.170.2,/var/run/docker.sock` に設定して、EC2 インスタンスのメタデータ、タスク用の IAM; ロール、および Docker デーモンのトラフィックをプロキシからフィルタリングします。

`/etc/init/ecs.override` (Amazon Linux AMI のみ)

```
env HTTP_PROXY=10.0.0.131:3128
```

この値を、ecs-init がインターネットへの接続に使用する HTTP プロキシのホスト名 (または IP アドレス) とポート番号に設定します。例えば、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合です。

```
env NO_PROXY=169.254.169.254,169.254.170.2,/var/run/docker.sock
```

この値を 169.254.169.254,169.254.170.2,/var/run/docker.sock に設定して、EC2 インスタンスのメタデータ、タスク用の IAM; ロール、および Docker デーモンのトラフィックをプロキシからフィルタリングします。

`/etc/systemd/system/docker.service.d/http-proxy.conf` (Amazon Linux 2 のみ)

```
Environment="HTTP_PROXY=http://10.0.0.131:3128"
```

この値を、Docker デーモンがインターネットへの接続に使用する HTTP プロキシのホスト名 (または IP アドレス) とポート番号に設定します。例えば、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合です。

```
Environment="NO_PROXY=169.254.169.254,169.254.170.2"
```

この値を 169.254.169.254,169.254.170.2 に設定して、EC2 インスタンスのメタデータをプロキシからフィルタリングします。

`/etc/sysconfig/docker` (Amazon Linux AMI および Amazon Linux 2 のみ)

```
export HTTP_PROXY=http://10.0.0.131:3128
```

この値を、Docker デーモンがインターネットへの接続に使用する HTTP プロキシのホスト名 (または IP アドレス) とポート番号に設定します。例えば、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合です。

```
export NO_PROXY=169.254.169.254,169.254.170.2
```

この値を 169.254.169.254,169.254.170.2 に設定して、EC2 インスタンスのメタデータをプロキシからフィルタリングします。

これらの環境変数を上記のファイルで設定すると、Amazon ECS コンテナエージェント、ecs-init、および Docker デーモンのみに影響があります。プロキシを使用する他のサービス (yum など) を設定することはありません。

プロキシを保護する方法については、「How do I set up an HTTP proxy for Docker and the Amazon ECS container agent in Amazon Linux 2 or AL2023」を参照してください。

Amazon ECS Auto Scaling グループ用に事前初期化されたインスタンスを設定する

Amazon ECS では、Amazon EC2 Auto Scaling ウォームプールをサポートします。ウォームプールは、事前に初期化済みの Amazon EC2 インスタンスグループでサービス開始が準備されています。アプリケーションがスケールアウトする必要がある場合は、常に Amazon EC2 Auto Scaling はコールドインスタンスを起動するのではなく、ウォームプールから事前に初期化されたインスタンスを使用し、最終的な初期化プロセスの実行を許可し、インスタンスを使用開始します。

ウォームプールの詳細、および Auto Scaling グループにウォームプールを追加する方法については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Amazon EC2 Auto Scaling のウォームプール」を参照してください。

Amazon ECS の Auto Scaling グループのウォームプールを作成または更新する場合、スケールイン (ReuseOnScaleIn) 時にインスタンスをウォームプールに戻すオプションを設定することはできません。詳細については、「AWS Command Line Interface リファレンス」の「put-warm-pool」を参照してください。

Amazon ECS クラスターでウォームプールを使用するには、Amazon EC2 Auto Scaling グループ起動テンプレートの [User data] (ユーザーデータ) フィールドで ECS_WARM_POOLS_CHECK エージェント設定変数を true に設定します。

以下は、Amazon EC2 起動テンプレートの [User data] (ユーザーデータ) フィールドでエージェント設定変数の指定方法の例を示しています。*MyCluster* は、自分のクラスターの名前に置き換えてください。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
ECS_WARM_POOLS_CHECK=true
EOF
```

この ECS_WARM_POOLS_CHECK 変数は、エージェントバージョン 1.59.0 以降でのみサポートされています。変数の詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

Amazon ECS コンテナエージェントをアップデートする

場合によっては、バグの修正や新機能を取得するために Amazon ECS コンテナエージェントを更新する必要があります。Amazon ECS コンテナエージェントの更新によって、コンテナインスタンスで実行中のタスクやサービスが中断されることはありません。エージェントを更新するプロセスは、コンテナインスタンスが Amazon ECS 対応 AMI で起動されたか、別のオペレーティングシステムで起動されたかによって異なります。

> **Note**
>
> エージェント更新は Windows コンテナインスタンスに適用されません。Windows クラスター内のエージェントバージョンを更新するには、新しいコンテナインスタンスを起動することをお勧めします。

Amazon ECSコンテナエージェントバージョンの確認

コンテナインスタンスで実行中のコンテナエージェントのバージョンをチェックして、更新が必要かどうかを確認できます。Amazon ECSコンソールのコンテナインスタンスビューにエージェントバージョンが表示されます。以下の手順を使用してエージェントバージョンを確認します。

Amazon ECS console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、外部インスタンスが存在するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択し、外部インスタンスをホストするクラスターを選択します。
4. [Cluster : ***name***] (クラスター: 名前) のページで、[Infrastructure] (インフラストラクチャ) タブを選択します。
5. [Container instances] (コンテナインスタンス) で、コンテナインスタンスの [Agent version] (エージェントバージョン) 列に注意してください。コンテナインスタンスに最新バージョンのコンテナエージェントが含まれていない場合、コンソールにアラートメッセージが表示され、古いエージェントバージョンにフラグが設定されます。

   エージェントバージョンが古い場合、次の手順でコンテナエージェントを更新できます。

   - コンテナインスタンスで Amazon ECS 対応AMIを実行している場合は、「Amazon ECS 対応 AMI での Amazon ECS コンテナエージェントのアップデート」を参照してください。

- コンテナインスタンスで Amazon ECS 対応AMI を実行してない場合は、「Amazon ECS コンテナエージェントの手動更新 (Amazon ECS 最適化以外の AMI の場合)」を参照してください。

> **Important**
>
> Amazon ECS 対応AMIで Amazon ECSエージェントバージョンを v1.0.0 より古いバージョンから更新するには、現行のコンテナインスタンスを終了し、最新バージョンの AMI で新しいインスタンスを起動することをお勧めします。プレビューバージョンを使用しているコンテナインスタンスは削除し、最新バージョンの AMI に置き換える必要があります。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

Amazon ECS container agent introspection API

また、コンテナインスタンス自体からAmazon ECS コンテナエージェントの詳細分析 API のバージョンを確認するために使用できます。詳細については、「Amazon ECS コンテナの詳細分析」を参照してください。

詳細分析 API を使用して、Amazon ECS コンテナエージェントで最新バージョンが実行されているかどうかを確認するには

1. SSH 経由でコンテナインスタンスにログインします。
2. 詳細分析 API をクエリします。

```
[ec2-user ~]$ curl -s 127.0.0.1:51678/v1/metadata | python3 -mjson.tool
```

> **Note**
>
> 詳細分析 API はVersion 情報を Amazon ECS コンテナエージェントのバージョン v1.0.0 に追加しました。詳細分析 API をクエリして Version が存在しない場合、または詳細分析 API 自体がエージェントに存在しない場合、実行しているバージョンが v0.0.3 以前であり、更新する必要があります。

Amazon ECS 対応 AMI での Amazon ECS コンテナエージェントのアップデート

Amazon ECS対応AMI を使用している場合は、いくつかの方法で最新バージョンの Amazon ECS コンテナエージェントを取得できます (推奨される順に示します)。

- 現在のコンテナインスタンスを終了して Amazon ECS 対応 Amazon Linux 2 AMI最新バージョンを起動します (手動で起動するか、最新の AMI で自動スケーリング起動設定を更新して起動します)。これにより、最新のテスト済みおよび検証済みバージョンの Amazon Linux、Docker、`ecs-init`、および Amazon ECS コンテナエージェントを備えたの新しいコンテナインスタンスが提供されます。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。
- インスタンスに SSH で接続し、`ecs-init` パッケージ (および依存関係) を最新バージョンに更新します。このオペレーションにより、Amazon Linux リポジトリで最新のテスト済みおよび検証済みバージョンの Docker と `ecs-init`、およびAmazon ECS コンテナエージェントの最新バージョンが提供されます。詳細については、「Amazon ECS対応 &AMI; の `ecs-init` パッケージを更新するには」を参照してください。
- コンソールまたは AWS CLI や AWS SDK 経由で `UpdateContainerAgent` API オペレーションを使用し、コンテナエージェントを更新します。詳細については、「`UpdateContainerAgent` API オペレーションで Amazon ECS コンテナエージェントを更新する」を参照してください。

> **Note**
>
> エージェント更新は Windows コンテナインスタンスに適用されません。Windows クラスター内のエージェントバージョンを更新するには、新しいコンテナインスタンスを起動することをお勧めします。

Amazon ECS対応 &AMI; の **`ecs-init`** パッケージを更新するには

1. SSH 経由でコンテナインスタンスにログインします。
2. 次のコマンドを使用して、`ecs-init` パッケージを更新します。

```
sudo yum update -y ecs-init
```

> **Note**
>
> `ecs-init` パッケージと Amazon ECS コンテナエージェントが即座に更新されます。ただし、新しいバージョンの Docker は、Docker デーモンを再起動するまでロードされ

ません。インスタンスを再起動するか、インスタンスで次のコマンドを実行して、再起動します。

- Amazon ECS 対応 Amazon Linux AMI

```
sudo systemctl restart docker
```

- Amazon ECS に最適化された Amazon Linux AMI

```
sudo service docker restart && sudo start ecs
```

UpdateContainerAgent API オペレーションで Amazon ECS コンテナエージェントを更新する

> **Important**
>
> -UpdateContainerAgentAPI は、Amazon ECS に最適化された AMI の Linux バリアントでのみサポートされます。ただし、Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI は例外です。Amazon ECS に最適化された Amazon Linux 2 (arm64) AMI を使用するコンテナインスタンスの場合、ecs-initパッケージを使用してエージェントを更新します。他のオペレーティングシステムを実行しているコンテナインスタンスについては、「Amazon ECS コンテナエージェントの手動更新 (Amazon ECS 最適化以外の AMI の場合)」を参照してください。Windows コンテナインスタンスを使用している場合は、新しいコンテナインスタンスを起動して、Windows クラスター内のエージェントバージョンを更新することをお勧めします。

UpdateContainerAgentAPI 処理は、コンソールまたは AWS CLI または AWS SDKを使ってエージェントのアップデートを要求したときに始まります。Amazon ECS は、現在のエージェントバージョンと使用可能な最新バージョンを比較し、更新が可能かどうかを確認します。更新が利用できない場合 (例えばすでに最新バージョンがエージェントで実行されている場合) は、NoUpdateAvailableException が返されます。

上に示した更新プロセスのステージは、次のとおりです。

PENDING

エージェントを更新できます。更新プロセスが開始されました。

`STAGING`

エージェントで、エージェントの更新のダウンロードが開始されています。エージェントで更新をダウンロードできない場合や、更新の内容が正しくないか破損している場合、エージェントは失敗通知を送信し、更新は `FAILED` 状態に遷移します。

`STAGED`

エージェントのダウンロードが完了し、エージェントの内容が確認されました。

`UPDATING`

`ecs-init` サービスが再起動され、新しいエージェントバージョンが取得されます。エージェントが何らかの理由で再起動できない場合、更新は `FAILED` 状態に遷移します。それ以外の場合は、エージェントから Amazon ECS に更新完了のシグナルが送信されます。

> **Note**
>
> エージェント更新は Windows コンテナインスタンスに適用されません。Windows クラスター内のエージェントバージョンを更新するには、新しいコンテナインスタンスを起動することをお勧めします。

Amazon ECSに最適化されたAMIのAmazon ECS コンテナエージェントをコンソールでアップデートするには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、外部インスタンスが存在するリージョンを選択します。
3. ナビゲーションペインで、[Clusters] を選択し、クラスターを選択します。
4. [Cluster : ***name***] (クラスター: 名前) のページで、[Infrastructure] (インフラストラクチャ) タブを選択します。
5. [コンテナインスタンス] で、更新するインスタンスを選択し、[アクション]、[エージェントの更新] を選択します。

Amazon ECS コンテナエージェントの手動更新 (Amazon ECS 最適化以外の AMI の場合)

場合によっては、バグの修正や新機能を取得するために Amazon ECS コンテナエージェントを更新する必要があります。Amazon ECS コンテナエージェントの更新によって、コンテナインスタンスで実行中のタスクやサービスが中断されることはありません。

> **Note**
>
> エージェント更新は Windows コンテナインスタンスに適用されません。Windows クラスター内のエージェントバージョンを更新するには、新しいコンテナインスタンスを起動することをお勧めします。

1. SSH 経由でコンテナインスタンスにログインします。
2. エージェントが ECS_DATADIR 環境変数を使用して状態を保存しているかどうかを確認します。

   ```
   ubuntu:~$ docker inspect ecs-agent | grep ECS_DATADIR
   ```

   出力:

   ```
   "ECS_DATADIR=/data",
   ```

   > **Important**
   >
   > 前のコマンドで ECS_DATADIR 環境変数が返されない場合は、エージェントを更新する前に、このコンテナインスタンスで実行されているタスクをすべて停止する必要があります。より新しいエージェントは ECS_DATADIR 環境変数を使用して状態を保存するため、タスクが実行中でも問題なく更新できます。

3. Amazon ECS コンテナエージェントを停止します。

   ```
   ubuntu:~$ docker stop ecs-agent
   ```

4. エージェントコンテナを削除します。

   ```
   ubuntu:~$ docker rm ecs-agent
   ```

5. /etc/ecs ディレクトリと Amazon ECS コンテナエージェント設定ファイルが /etc/ecs/ecs.config に存在することを確認します。

   ```
   ubuntu:~$ sudo mkdir -p /etc/ecs && sudo touch /etc/ecs/ecs.config
   ```

6. /etc/ecs/ecs.config ファイルを編集して、少なくとも以下の変数宣言が必ず含まれるようにします。コンテナインスタンスをデフォルトのクラスターに登録しない場合は、クラスター名を ECS_CLUSTER の値として指定します。

```
ECS_DATADIR=/data
ECS_ENABLE_TASK_IAM_ROLE=true
ECS_ENABLE_TASK_IAM_ROLE_NETWORK_HOST=true
ECS_LOGFILE=/log/ecs-agent.log
ECS_AVAILABLE_LOGGING_DRIVERS=["json-file","awslogs"]
ECS_LOGLEVEL=info
ECS_CLUSTER=default
```

これらや他のエージェントランタイムオプションの詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

> **Note**
>
> オプションで、エージェント環境変数を Amazon S3 に保存できます (これらの環境変数は、Amazon EC2 ユーザーデータを使用して、起動時にコンテナインスタンスにダウンロードできます)。これは、プライベートリポジトリの認証情報のような機密情報の場合に推奨されます。詳細については、Amazon S3 に Amazon ECS コンテナインスタンスの設定を保存するおよびAmazon ECS での AWS 以外のコンテナイメージの使用を参照してください。

7. Amazon Elastic Container Registry Public から最新の Amazon ECS コンテナエージェントイメージを取得します。

```
ubuntu:~$ docker pull public.ecr.aws/ecs/amazon-ecs-agent:latest
```

出力:

```
Pulling repository amazon/amazon-ecs-agent
a5a56a5e13dc: Download complete
511136ea3c5a: Download complete
9950b5d678a1: Download complete
c48ddcf21b63: Download complete
Status: Image is up to date for amazon/amazon-ecs-agent:latest
```

8. コンテナインスタンスで最新の Amazon ECS コンテナエージェントを実行します。

> **Note**
>
> Docker 再起動ポリシーまたはプロセスマネージャー (upstart または systemd など) を使用してコンテナエージェントをサービスまたはデーモンとして扱い、終了後に確実に再起動されるようにします。Amazon ECS に最適化された AMI はこのために `ecs-init` RPM を使用します。この[RPM のソースコード]は、GitHub で参照できます。

次のエージェント実行コマンドの例は、各オプションを示すために複数の行に分けられています。これらや他のエージェントランタイムオプションの詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

> **Important**
>
> SELinux 対応オペレーティングシステムでは、docker run コマンドに `--privileged` オプションが必要です。さらに、SELinux 対応コンテナインスタンスの場合は、`/log` および `/data` ボリュームマウントに `:Z` オプションを追加することをお勧めします。ただし、コマンドを実行する前に、これらのボリュームのホストマウントが存在する必要があります。存在しないと、`no such file or directory` エラーが発生します。SELinux 対応コンテナインスタンスで Amazon ECS エージェントの実行に問題が発生する場合は、次のアクションを実行します。
>
> - コンテナインスタンスにホストボリュームマウントポイントを作成します。
>
>   ```
>   ubuntu:~$ sudo mkdir -p /var/log/ecs /var/lib/ecs/data
>   ```
>
> - `--privileged` オプションを次の docker run コマンドに追加します。
> - 以下の docker run コマンドで、`/log` および `/data` コンテナボリュームマウントに `:Z` オプションを追加します (`--volume=/var/log/ecs/:/log:Z` など)。

```
ubuntu:~$ sudo docker run --name ecs-agent \
--detach=true \
--restart=on-failure:10 \
--volume=/var/run:/var/run \
--volume=/var/log/ecs/:/log \
--volume=/var/lib/ecs/data:/data \
```

```
--volume=/etc/ecs:/etc/ecs \
--volume=/etc/ecs:/etc/ecs/pki \
--net=host \
--env-file=/etc/ecs/ecs.config \
amazon/amazon-ecs-agent:latest
```

> **Note**
>
> `Error response from daemon: Cannot start container` メッセージが表示された場合は、sudo docker rm ecs-agent コマンドを使用して障害のあるコンテナを削除し、再度エージェントの実行を試みることができます。

Amazon ECS に最適化された Windows AMI

Amazon ECS に最適化された AMI には、Amazon ECS ワークロードの実行に必要なコンポーネントがあらかじめ設定されています。Amazon ECSで一元化されたワークロードを実行するために必要な基本的な仕様を満たす独自のコンテナインスタンス AMI を作成することはできますが、Amazon ECS に最適化された AMI は事前設定され、AWS エンジニアにより Amazon ECS でテストされています。これは最も簡単に開始できる方法であり、AWS でコンピューティングリソースをすばやく実行できます。

Amazon ECS に最適化された AMI メタデータ (各バリアントの AMI 名、Amazon ECS コンテナエージェントバージョン、Docker バージョンを含む Amazon ECS ランタイムバージョンなど) は、プログラムで取得できます。詳細については、「the section called “Amazon ECS に最適化された Windows AMI メタデータを取得する”」を参照してください。

> **Important**
>
> 2022 年 8 月以降に作成された ECS に最適化された AMI バリアントはすべて Docker EE (Mirantis) から Docker CE (Moby プロジェクト) に移行されます。
> お客様がデフォルトで最新のセキュリティ更新を受けられるように、Amazon ECS は Windows ECS に最適化された AMI を 3 つ以上維持しています。Amazon ECS は、新しい Windows Amazon ECS に最適化された AMI をリリースした後、古いプライベートである Windows Amazon ECS に最適化された AMI を作成します。アクセスが必要なプライベート AMI がある場合は、クラウドSupport のチケットを提出してください。

Amazon ECS に最適化された AMI バリアント

Amazon EC2 インスタンスでは、Amazon ECS に最適化された AMI の次の Windows Server バリアントを使用できます。

> **Important**
>
> 8 月以降に製造された ECS に最適化された AMI バリアントはすべて Docker EE (Mirantis) から Docker CE (Moby プロジェクト) に移行される予定です。

- Amazon ECS に最適化された Windows Server 2022 Full AMI
- Amazon ECS に最適化された Windows Server 2022 Core AMI
- Amazon ECS に最適化された Windows Server 2019 Full AMI
- Amazon ECS に最適化された Windows Server 2019 Core AMI
- Amazon ECS に最適化された Windows Server 2016 Full AMI

> **Important**
>
> Windows Server 2016 は、25.x.x などの最新の Docker バージョンをサポートしていません。そのため、Windows Server 2016 Full AMI には Docker ランタイムに対するセキュリティパッチやバグパッチは適用されません。次の Windows プラットフォームのいずれかに移行することをお勧めします。
>
> - Windows Server 2022 Full
> - Windows Server 2022 Core
> - Windows Server 2019 Full
> - Windows Server 2019 Core

2022 年 8 月 9 日、Amazon ECS に最適化された Windows Server 20H2 Core AMI はサポートを終了しました。この AMI の新しいバージョンはリリースされません。詳細については、「Windows Server のリリース情報」を参照してください。

Windows Server 2022、Windows Server 2019 および Windows Server 2016 は、長期サービスチャネル (LTSC) リリースです。Windows Server 20H2 は、半期チャネル (SAC) リリースです。詳細については、「Windows Server のリリース情報」を参照してください。

考慮事項

以下は、Amazon EC2 Windows コンテナと Amazon ECS についての留意点です。

- Windows コンテナは Linux コンテナインスタンスでは実行できません。逆の場合も同様です。Windows タスクと Linux タスクをより適切に配置するには、Windows コンテナインスタンスと Linux コンテナインスタンスを別々のクラスターに保持し、Windows タスクは Windows クラスターにのみ配置します。次の配置制約 `memberOf(ecs.os-type=='windows')` を設定して、Windows のタスク定義が Windows インスタンスのみに配置されるようにする必要があります。
- Windowsコンテナは、EC2 および Fargate 起動タイプを使用するタスクでサポートされています。
- Windows コンテナとコンテナインスタンスでは、Linux コンテナとコンテナインスタンス用のタスク定義パラメータは全面的にはサポートされていません。まったくサポートされないパラメータもあり、Windows での動作と Linux での動作が異なるパラメータもあります。詳細については、「Windows を実行している EC2 インスタンスでの Amazon ECS タスク定義の違い」を参照してください。
- タスクの IAM ロール 機能については、起動時に機能を許可するように Windows コンテナインスタンスを設定する必要があります。コンテナは、この機能を使用するときに、指定された PowerShell コードの一部を実行する必要があります。詳細については、「 Amazon EC2 Windows インスタンスの追加設定」を参照してください。
- タスク用の IAM ロール の機能では認証情報プロキシを使用してコンテナに認証情報を提供します。この認証情報プロキシは、コンテナインスタンスのポート 80 を占有するため、タスク用の IAM ロール を使用する場合、タスクにポート 80 を使用することができません。ウェブサービスコンテナの場合は、 Application Load Balancer と動的なポートマッピングを使用して標準の HTTP ポート 80 接続をコンテナに提供できます。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。
- Windows サーバーのドッカーイメージは大きめです (9 GiB)。そのため、Windows コンテナインスタンスには Linux コンテナインスタンスよりも多くのストレージスペースが必要です。
- Windows Server で Windows コンテナを実行するには、コンテナのベースイメージの OS バージョンがホストのバージョンと一致する必要があります。詳細については、マイクロソフトのドキュメント Web サイトの「Windows コンテナバージョンの互換性」を参照してください。クラスターが複数の Windows バージョンを実行している場合、次の配置制約を使用して、同じバージョンで実行されている EC2 インスタンスにタスクが配置されるようにすることができます: `memberOf(attribute:ecs.os-family == WINDOWS_SERVER_<OS_Release>_<FULL or`

CORE>)。詳細については、「the section called “Amazon ECS に最適化された Windows AMI メタデータを取得する”」を参照してください。

Amazon ECS に最適化された Windows AMI メタデータを取得する

Amazon ECS に最適化された AMI の各バリアントの AMI ID、イメージ名、オペレーティングシステム、コンテナエージェントバージョン、ランタイムバージョンは、Systems Manager パラメータストア API のクエリを実行してプログラムで取得できます。Systems Manager パラメータストア API の詳細については、「GetParameters」および「GetParametersByPath」を参照してください。

> **Note**
>
> Amazon ECS に最適化された AMI メタデータを取得するには、管理ユーザーに次の IAM アクセス権限が必要です。AmazonECS_FullAccess IAM ポリシーには、次の許可が追加されています。
>
> - ssm:GetParameters
> - ssm:GetParameter
> - ssm:GetParametersByPath

Systems Manager パラメータストアのパラメータフォーマット

> **Note**
>
> 以下の Systems Manager Parameter Store API パラメータは廃止されているため、最新の Windows AMI の取得には使用しないでください。
>
> - `/aws/service/ecs/optimized-ami/windows_server/2016/english/full/recommended/image_id`
> - `/aws/service/ecs/optimized-ami/windows_server/2019/english/full/recommended/image_id`

以下は、各 Amazon ECS に最適化された AMI バリアントのパラメータ名のフォーマットです。

- Windows Server 2022 Full AMI メタデータ:

```
/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-ECS_Optimized
```

- Windows Server 2022 Core AMI メタデータ:

```
/aws/service/ami-windows-latest/Windows_Server-2022-English-Core-ECS_Optimized
```

- Windows Server 2019 フル AMI メタデータ:

```
/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-ECS_Optimized
```

- Windows Server 2019 コア AMI メタデータ:

```
/aws/service/ami-windows-latest/Windows_Server-2019-English-Core-ECS_Optimized
```

- Windows Server 2016 フル AMI メタデータ:

```
/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-ECS_Optimized
```

次のパラメーター名の形式は、最新の安定した Windows Server 2019 Full AMI のメタデータを取得します

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2019-
English-Full-ECS_Optimized
```

以下は、パラメータ値で返る JSON オブジェクトの例です。

```
{
    "Parameters": [
        {
            "Name": "/aws/service/ami-windows-latest/Windows_Server-2019-English-Full-
ECS_Optimized",
            "Type": "String",
            "Value": "{\"image_name\":\"Windows_Server-2019-English-Full-
ECS_Optimized-2023.06.13\",\"image_id\":\"ami-0debc1fb48e4aee16\",\"ecs_runtime_version
\":\"Docker (CE) version 20.10.21\",\"ecs_agent_version\":\"1.72.0\"}",
            "Version": 58,
            "LastModifiedDate": "2023-06-22T19:37:37.841000-04:00",
            "ARN": "arn:aws:ssm:us-east-1::parameter/aws/service/ami-windows-latest/
Windows_Server-2019-English-Full-ECS_Optimized",
```

```
            "DataType": "text"
        }
    ],
    "InvalidParameters": []
}
```

上記の出力の各フィールドは、サブパラメータとしてクエリに利用できます。サブパラメータのパラメータパスを構築するには、選択した AMI のパスにサブパラメータ名を追加します。以下のサブパラメータが利用可能です。

- `schema_version`
- `image_id`
- `image_name`
- `os`
- `ecs_agent_version`
- `ecs_runtime_version`

例

以下の例は、それぞれの Amazon ECS に最適化された AMI バリアントのメタデータを取得する方法を示しています。

安定している最新の Amazon ECS に最適化された AMI メタデータを取得する

安定している最新の Amazon ECS に最適化された AMI を取得するには、AWS CLI で次の AWS CLI コマンドを使用します。

- Amazon ECS に最適化された Windows Server 2022 Full AMI

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2022-English-Full-ECS_Optimized --region us-east-1
```

- Amazon ECS に最適化された Windows Server 2022 Core AMI

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2022-English-Core-ECS_Optimized --region us-east-1
```

- Amazon ECS に最適化された Windows Server 2019 Full AMI

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2019-English-Full-ECS_Optimized --region us-east-1
```

- Amazon ECS に最適化された Windows Server 2019 Core AMI

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2019-English-Core-ECS_Optimized --region us-east-1
```

- Amazon ECS に最適化された Windows Server 2016 Full AMI

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2016-English-Full-ECS_Optimized --region us-east-1
```

AWS CloudFormation テンプレートの推奨される最新の Amazon ECS に最適化された AMI を使用する

Systems Manager パラメータストア名を参照することにより、AWS CloudFormation テンプレートで推奨される最新の Amazon ECS に最適化された AMI を参照できます。

```
Parameters:
  LatestECSOptimizedAMI:
    Description: AMI ID
    Type: AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>
    Default: /aws/service/ami-windows-latest/Windows_Server-2019-English-Full-ECS_Optimized/image_id
```

Amazon ECS に最適化された Windows AMI バージョン

Amazon ECS に最適化された AMI の現在のバージョンと以前のバージョン、それらに対応する Amazon ECS コンテナエージェント、Docker、`ecs-init` パッケージのバージョンを表示します。

AMI ID を含む、Amazon ECS に最適化された AMI のメタデータでは、各バリアントをプログラム的に取得することができます。詳細については、「the section called “Amazon ECS に最適化された Windows AMI メタデータを取得する”」を参照してください。

次のタブには、Windows Amazon ECS に最適化された AMI のバージョンの一覧が表示されます。AWS CloudFormation テンプレートで Systems Manager パラメータストアのパラメータを参照する方法については、AWS CloudFormation テンプレートの推奨される最新の Amazon ECS に最適化された AMI を使用する を参照してください。

Important

お客様がデフォルトで最新のセキュリティ更新を受けられるように、Amazon ECS は Windows ECS に最適化された AMI を 3 つ以上維持しています。Amazon ECS は、新しい Windows Amazon ECS に最適化された AMI をリリースした後、古いプライベートである Windows Amazon ECS に最適化された AMI を作成します。アクセスが必要なプライベート AMI がある場合は、クラウドSupport のチケットを提出してください。
Windows Server 2016 は、25.x.x などの最新の Docker バージョンをサポートしていません。そのため、Windows Server 2016 Full AMI には Docker ランタイムに対するセキュリティパッチやバグパッチは適用されません。次の Windows プラットフォームのいずれかに移行することをお勧めします。

- Windows Server 2022 Full
- Windows Server 2022 Core
- Windows Server 2019 Full
- Windows Server 2019 Core

Windows Server 2022 Full AMI versions

下の表は、Amazon ECS に最適化された Windows Server 2022 Full AMI の現在のバージョンと以前のバージョン、およびそれらに対応するバージョンの Amazon ECS コンテナエージェントと Docker のリスト表示です。

Amazon ECS に最適化された Windows Server 2022 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2022-English-Full-ECS_Optimized-2025.2.14	`1.90.0`	`25.0.6 (Docker CE)`	Public
Windows_Server-2022-English-Full-ECS_Optimized-2025.1.21	`1.89.2`	`25.0.6 (Docker CE)`	Public

Amazon ECS に最適化された Windows Server 2022 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2022-English-Full-ECS_Optimized-2024.12.11	1.89.1	25.0.6 (Docker CE)	Public
[Windows_Server-2022-English-Full-ECS_Optimized-2024.11.13]	1.88.0	25.0.6 (Docker CE)	Public
Windows_Server-2022-English-Full-ECS_Optimized-2024.10.17	1.87.0	25.0.6 (Docker CE)	プライベート
Windows_Server-2022-English-Full-ECS_Optimized-2024.09.10	1.86.3	25.0.6 (Docker CE)	プライベート
Windows_Server-2022-English-Full-ECS_Optimized-2024.08.19	1.86.2	25.0.6 (Docker CE)	プライベート
[Windows_Server-2022-English-Full-ECS_Optimized-2024.07.09]	1.84.0	25.0.3 (Docker CE)	プライベート
[Windows_Server-2022-English-Full-ECS_Optimized-2024.06.14]	1.83.0	25.0.3 (Docker CE)	プライベート

Amazon ECS に最適化された Windows Server 2022 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2022-English-Full-ECS_Optimized-2024.05.14	1.82.3	25.0.3 (Docker CE)	プライベート
[Windows_Server-2022-English-Full-ECS_Optimized-2024.04.09]	1.82.2	25.0.3 (Docker CE)	プライベート
[Windows_Server-2022-English-Full-ECS_Optimized-2024.03.12]	1.82.0	20.10.23 (Docker CE)	プライベート

現在の Amazon ECS に最適化された Windows Server 2022 Full AMI は、AWS CLI の次のコマンドで取得できます。

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2022-English-Full-ECS_Optimized
```

Windows Server 2022 Core AMI versions

下の表は、Amazon ECS に最適化された Windows Server 2022 Core AMI の現在のバージョンと以前のバージョン、およびそれらに対応するバージョンの Amazon ECS コンテナエージェントと Docker のリスト表示です。

Amazon ECS に最適化された Windows Server 2022 Core AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2022-English-Core-ECS_Optimized-2025.2.14	1.90.0	25.0.6 (Docker CE)	Public
Windows_Server-2022-English-Core-ECS_Optimized-2025.1.21	1.89.2	25.0.6 (Docker CE)	Public
Windows_Server-2022-English-Core-ECS_Optimized-2024.12.11	1.89.1	25.0.6 (Docker CE)	Public
[Windows_Server-2022-English-Core-ECS_Optimized-2024.11.13]	1.88.0	25.0.6 (Docker CE)	Public
Windows_Server-2022-English-Core-ECS_Optimized-2024.10.17	1.87.0	25.0.6 (Docker CE)	プライベート
Windows_Server-2022-English-Core-ECS_Optimized-2024.09.10	1.86.3	25.0.6 (Docker CE)	プライベート
Windows_Server-2022-English-Core-ECS	1.86.2	25.0.6 (Docker CE)	プライベート

Amazon ECS に最適化された Windows Server 2022 Core AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
_Optimized-2024.08.19			
[Windows_Server-2022-English-Core-ECS_Optimized-2024.07.09]	1.84.0	25.0.3 (Docker CE)	プライベート
[Windows_Server-2022-English-Core-ECS_Optimized-2024.06.14]	1.83.0	25.0.3 (Docker CE)	プライベート
Windows_Server-2022-English-Core-ECS_Optimized-2024.05.14	1.82.3	25.0.3 (Docker CE)	プライベート
[Windows_Server-2022-English-Core-ECS_Optimized-2024.04.09]	1.82.2	25.0.3 (Docker CE)	プライベート
[Windows_Server-2022-English-Core-ECS_Optimized-2024.03.12]	1.82.0	20.10.23 (Docker CE)	プライベート

現在の Amazon ECS に最適化された Windows Server 2022 Full AMI は、AWS CLI の次のコマンドで取得できます。

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2022-English-Core-ECS_Optimized
```

Windows Server 2019 Full AMI versions

下の表は、Amazon ECS に最適化された Windows Server 2019 Full AMI の現在のバージョンと以前のバージョン、およびそれらに対応するバージョンの Amazon ECS コンテナエージェントと Docker のリスト表示です。

Amazon ECS に最適化された Windows Server 2019 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2019-English-Full-ECS_Optimized-2025.2.14	1.90.0	25.0.6 (Docker CE)	Public
Windows_Server-2019-English-Full-ECS_Optimized-2025.1.21	1.89.2	25.0.6 (Docker CE)	Public
Windows_Server-2019-English-Full-ECS_Optimized-2024.12.11	1.89.1	25.0.6 (Docker CE)	Public
[Windows_Server-2019-English-Full-ECS_Optimized-2024.11.13]	1.88.0	25.0.6 (Docker CE)	Public
Windows_Server-2019-English-Full-ECS_Optimized-2024.10.17	1.87.0	25.0.6 (Docker CE)	プライベート
Windows_Server-2019-English-Full-ECS	1.86.3	25.0.6 (Docker CE)	プライベート

Amazon ECS に最適化された Windows Server 2019 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
_Optimized-2024.09.10			
Windows_Server-2019-English-Full-ECS_Optimized-2024.08.16	1.86.2	25.0.6 (Docker CE)	プライベート
[Windows_Server-2019-English-Full-ECS_Optimized-2024.07.09]	1.84.0	25.0.3 (Docker CE)	プライベート
[Windows_Server-2019-English-Full-ECS_Optimized-2024.06.14]	1.83.0	25.0.3 (Docker CE)	プライベート
Windows_Server-2019-English-Full-ECS_Optimized-2024.05.14	1.82.3	25.0.3 (Docker CE)	プライベート
[Windows_Server-2019-English-Full-ECS_Optimized-2024.04.09]	1.82.2	25.0.3 (Docker CE)	プライベート
[Windows_Server-2019-English-Full-ECS_Optimized-2024.03.12]	1.82.0	20.10.23 (Docker CE)	プライベート

現在の Amazon ECS に最適化された Windows Server 2019 Full AMI は、AWS CLI の次のコマンドで取得できます。

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2019-English-Full-ECS_Optimized
```

Windows Server 2019 Core AMI versions

下の表は、Amazon ECS に最適化された Windows Server 2019 Core AMI の現在のバージョンと以前のバージョン、およびそれらに対応するバージョンの Amazon ECS コンテナエージェントと Docker のリスト表示です。

Amazon ECS に最適化された Windows Server 2019 Core AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2019-English-Core-ECS_Optimized-2025.2.14	1.90.0	25.0.6 (Docker CE)	Public
Windows_Server-2019-English-Core-ECS_Optimized-2025.1.21	1.89.2	25.0.6 (Docker CE)	Public
Windows_Server-2019-English-Core-ECS_Optimized-2024.12.11	1.89.1	25.0.6 (Docker CE)	Public
[Windows_Server-2019-English-Core-ECS_Optimized-2024.11.13]	1.88.0	25.0.6 (Docker CE)	Public
Windows_Server-2019-English-Core-ECS	1.87.0	25.0.6 (Docker CE)	Public

Amazon ECS に最適化された Windows Server 2019 Core AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
_Optimized-2024.10.17			
Windows_Server-2019-English-Core-ECS_Optimized-2024.09.10	1.86.3	25.0.6 (Docker CE)	プライベート
Windows_Server-2019-English-Core-ECS_Optimized-2024.08.19	1.86.2	25.0.6 (Docker CE)	プライベート
[Windows_Server-2019-English-Core-ECS_Optimized-2024.07.09]	1.84.0	25.0.3 (Docker CE)	プライベート
[Windows_Server-2019-English-Core-ECS_Optimized-2024.06.14]	1.83.0	25.0.3 (Docker CE)	プライベート
Windows_Server-2019-English-Core-ECS_Optimized-2024.05.14	1.82.3	25.0.3 (Docker CE)	プライベート
[Windows_Server-2019-English-Core-ECS_Optimized-2024.04.09]	1.82.2	25.0.3 (Docker CE)	プライベート

Amazon ECS に最適化された Windows Server 2019 Core AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
[Windows_Server-2019-English-Core-ECS_Optimized-2024.03.12]	1.82.0	20.10.23 (Docker CE)	プライベート

現在の Amazon ECS に最適化された Windows Server 2019 Full AMI は、AWS CLI の次のコマンドで取得できます。

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2019-English-Core-ECS_Optimized
```

Windows Server 2016 Full AMI versions

> **Important**
>
> Windows Server 2016 は、25.x.x などの最新の Docker バージョンをサポートしていません。そのため、Windows Server 2016 Full AMI には Docker ランタイムに対するセキュリティパッチやバグパッチは適用されません。次の Windows プラットフォームのいずれかに移行することをお勧めします。
>
> - Windows Server 2022 Full
> - Windows Server 2022 Core
> - Windows Server 2019 Full
> - Windows Server 2019 Core

下の表は、Amazon ECS に最適化された Windows Server 2016 Full AMI の現在のバージョンと以前のバージョン、およびそれらに対応するバージョンの Amazon ECS コンテナエージェントと Docker のリスト表示です。

Amazon ECS に最適化された Windows Server 2016 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
Windows_Server-2016-English-Full-ECS_Optimized-2025.2.14	1.90.0	20.10.23 (Docker CE)	Public
Windows_Server-2016-English-Full-ECS_Optimized-2025.1.21	1.89.2	20.10.23 (Docker CE)	Public
Windows_Server-2016-English-Full-ECS_Optimized-2024.12.11	1.89.1	20.10.23 (Docker CE)	Public
[Windows_Server-2016-English-Full-ECS_Optimized-2024.11.13]	1.88.0	20.10.23 (Docker CE)	Public
Windows_Server-2016-English-Full-ECS_Optimized-2024.10.17	1.87.0	20.10.23 (Docker CE)	プライベート
Windows_Server-2016-English-Full-ECS_Optimized-2024.09.10	1.86.3	20.10.23 (Docker CE)	プライベート
Windows_Server-2016-English-Full-ECS_Optimized-2024.08.19	1.86.2	20.10.23 (Docker CE)	プライベート

Amazon ECS に最適化された Windows Server 2016 Full AMI	Amazon ECS コンテナエージェントバージョン	Docker バージョン	[可視性]
[Windows_Server-2016-English-Full-ECS_Optimized-2024.07.09]	1.84.0	20.10.23 (Docker CE)	プライベート
[Windows_Server-2016-English-Full-ECS_Optimized-2024.06.14]	1.82.3	20.10.23 (Docker CE)	プライベート
[Windows_Server-2016-English-Full-ECS_Optimized-2024.05.14]	1.82.2	20.10.23 (Docker CE)	プライベート
[Windows_Server-2016-English-Full-ECS_Optimized-2024.04.09]	1.82.2	20.10.23 (Docker CE)	プライベート
[Windows_Server-2016-English-Full-ECS_Optimized-2024.03.12]	1.82.0	20.10.23 (Docker CE)	プライベート

次の AWS CLI Amazon ECS に最適化された Windows Server 2016 Full AMI を使用します。

```
aws ssm get-parameters --names /aws/service/ami-windows-latest/Windows_Server-2016-English-Full-ECS_Optimized
```

Amazon ECS に最適化された独自の Windows AMI の作成

EC2 Image Builder を使用して、Amazon ECS に最適化された独自のカスタム Windows AMI を構築します。これにより、Amazon ECS の独自のライセンスを持つ Windows AMI を簡単に使用できます。Amazon ECS は、コンテナをホストするために Windows インスタンスを実行するために必要なシステム設定を行うマネージド Image Builder コンポーネントを提供します。各 Amazon ECS マネージドコンポーネントには、特定のコンテナエージェントと Docker バージョンが含まれます。最新の Amazon ECS マネージドコンポーネントを使用するようにイメージをカスタマイズできます。また、古いコンテナエージェントまたは Docker バージョンが必要な場合は、別のコンポーネントを指定できます。

EC2 Image Builder 全体の使用に関するチュートリアルについては、「EC2 Image Builder ユーザーガイド」の「EC2 Image Builder入門」を参照してください。

EC2 Image Builder を使ってAmazon ECS に最適化された Windows AMI を構築する場合は、イメージ recipe を作成します。イメージ recipe は、次の要件を満たしている必要があります。

- [ソースイメージ] は、Windows Server 2019 Core、Windows Server 2019 Full、Windows Server 2022 Core、または Windows Server 2022 Full に基づいている必要があります。その他の Windows オペレーティングシステムはサポートされておらず、コンポーネントと互換性がない可能性があります。
- ビルドコンポーネントを指定する場合、`ecs-optimized-ami-windows` コンポーネントは必須です。`update-windows` コンポーネントをお勧めします。これにより、イメージに最新のセキュリティ更新プログラムが含まれるようになります。

  別のコンポーネントバージョンを指定するには、[Versioning options] メニューを展開し、使用するコンポーネントバージョンを指定します。詳細については、「`ecs-optimized-ami-windows` コンポーネントバージョンの一覧表示」を参照してください。

`ecs-optimized-ami-windows` コンポーネントバージョンの一覧表示

EC2 Image Builder recipe を作成して `ecs-optimized-ami-windows` コンポーネントを指定するときは、デフォルトのオプションを使用するか、特定のコンポーネントバージョンを指定できます。コンポーネント内に含まれる Amazon ECS コンテナエージェントおよび Docker バージョンとともに、使用可能なコンポーネントバージョンを確認するには、AWS Management Console を使用します。

使用可能な **ecs-optimized-ami-windows** コンポーネントバージョンを一覧表示するには

1. で EC2 Image Builder コンソールを開きます。https://console.aws.amazon.com/imagebuilder/。
2. ナビゲーションバーで、イメージを構築しているリージョンを選択します。
3. ナビゲーションペインの [Saved configurations] メニューで、[Components] を選択します。
4. [Components] ページの検索バーに `ecs-optimized-ami-windows` を入力して認証情報メニューをプルダウンし、[Quick start (Amazon-managed)] を選択します。
5. [説明] 列を用いて、Amazon ECS コンテナエージェントを使用したコンポーネントのバージョンと、イメージに必要なバージョンの Docker バージョンを特定します。

Amazon ECS Windows コンテナインスタンスの管理

Amazon ECS ワークロードに EC2 インスタンスを使用する場合は、インスタンスを維持するのはユーザーの責任です。

エージェント更新は Windows コンテナインスタンスに適用されません。Windows クラスター内のエージェントバージョンを更新するには、新しいコンテナインスタンスを起動することをお勧めします。

管理手順

- Amazon ECS Windows コンテナインスタンスの起動
- Amazon ECS Windows コンテナインスタンスをブートストラップしてデータを渡す
- Amazon ECS Windows コンテナインスタンスに HTTP プロキシを使用する
- スポットインスタンス通知を受信するように Amazon ECS Windows コンテナインスタンスを設定する

Amazon ECS Windows コンテナインスタンスの起動

Amazon ECS コンテナインスタンスは、Amazon EC2 コンソールを使用して作成されます。開始する前に、Amazon ECS を使用するようにセットアップする のステップを完了するようにしてください。

起動ウィザードの詳細については、「Amazon EC2 ユーザーガイド」の「新しいインスタンス起動ウィザードを使用してインスタンスを起動する」を参照してください。

新しい Amazon EC2 ウィザードを使用してインスタンスを起動できます。パラメータには次のリストを使用できます。リストされていないパラメータは、デフォルトのままにしてください。次の手順では、各パラメータグループについて説明します。

手順

開始する前に、「Amazon ECS を使用するようにセットアップする」のステップを完了します。

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. 画面の上のナビゲーションバーで、現在の AWS リージョンが表示されます (例: 米国東部 (オハイオ))。インスタンスを起動するリージョンを選択します。一部の Amazon EC2 リソースはリージョン間で共有できるため、この選択は重要です。
3. Amazon EC2 コンソールダッシュボードで、[インスタンスを起動] を選択してください。

名前とタグ

インスタンス名はタグで、キーは [Name] (名前)、値は指定した名前です。インスタンス、ボリューム、および伸縮自在なグラフィックスにタグ付けできます。スポットインスタンスの場合、スポットインスタンスリクエストにのみタグを付けることができます。

インスタンス名と追加のタグを指定することはオプションです。

- [Name] (名前) に、インスタンスのわかりやすい名前を入力します。名前を指定しない場合は、インスタンスをその ID で識別できます。ID は、インスタンスの起動時に自動的に生成されます。
- タグを追加するには、[Add additional tag] (追加のタグを追加) を選択します。[Add tag] (タグを追加) を選択し、キーと値を入力し、タグ付けするリソースタイプを選択します。追加するタグごとに [Add tag] (タグの追加) を選択します。

アプリケーションと OS イメージ (Amazon マシンイメージ)

Amazon マシンイメージ (AMI) には、インスタンスの起動に必要な情報が含まれています。例えば、ある AMI には、ウェブサーバーとして動作するために必要なソフトウェア (Apache やウェブサイトなど) が含まれています。

最新の Amazon ECS 最適化 AMI とその値については、「Windows Amazon ECS-optimized AMI」(Windows Amazon ECS に最適化された AMI) を参照してください。

[Search] (検索) バーを使用して、AWS によって発行された適切な Amazon ECS 最適化 AMI を検索します。

1. 要件に基づいて、[Search] (検索) バーに次の AMI のいずれかを入力し、[Enter] を押します。
   - Windows_Server-2022-English-Full-ECS_Optimized
   - Windows_Server-2022-English-Core-ECS_Optimized
   - Windows_Server-2019-English-Full-ECS_Optimized
   - Windows_Server-2019-English-Core-ECS_Optimized
   - Windows_Server-2016-English-Full-ECS_Optimized
2. [Choose an Amazon Machine Image (AMI]) (Amazon マシンイメージ (AMI) を選択) ページで、[Community AMIs] (コミュニティ AMI) タブを選択します。
3. 表示されるリストから、発行日が最新の Microsoft 検証済み AMI を選択し、[Select] (選択) をクリックします。

インスタンスタイプ

インスタンスタイプは、インスタンスのハードウェア設定とサイズを定義します。インスタンスタイプが大きくなると、CPU およびメモリも増えます。詳細については、インスタンスタイプを参照してください。

- [Instance type] (インスタンスタイプ) で、インスタンスのインスタンスタイプを選択します。

  選択したインスタンスタイプによって、タスクの実行に使用できるリソースが決まります。

キーペア (ログイン)

[Key pair name] (キーペア名) には、既存のキーペアを選択するか、[Create new key pair] (新しいキーペアを作成) を選択して新しいキーペアを作成します。

> **Important**
>
> [Proceed without key pair] (キーペアなしで進む) オプションを選択した場合 (非推奨)、ユーザーが別の方法でログインすることを許可するように設定された AMI を選択した場合でなければ、インスタンスに接続できなくなります。

ネットワーク設定

必要に応じて、ネットワーク設定を設定します。

- [Networking platform] (ネットワーキングプラットフォーム): [Virtual Private Cloud (VPC)] を選択して、[Network interfaces] (ネットワークインターフェイス) セクションでサブネットを指定します。
- [VPC]: セキュリティグループを作成する既存の VPC を選択します。
- [サブネット]: インスタンスは、アベイラビリティーゾーン、ローカルゾーン、Wavelength Zone、Outpost のいずれかに関連付けられたサブネットで起動できます。

  アベイラビリティーゾーンでインスタンスを起動するには、インスタンスを起動するサブネットを選択します。新しいサブネットを作成するには、[Create new subnet] を選択して Amazon VPC コンソールに移動します。終了したらインスタンス起動ウィザードに戻り、[Refresh] (更新) アイコンを選択して一覧にサブネットを読み込みます。

  ローカルゾーンでインスタンスを起動するには、ローカルゾーン内に作成したサブネットを選択します。

  アウトポストでインスタンスを起動するには、アウトポストに関連付けられた VPC 内のサブネットを選択します。
- [Auto-assign Public IP] (パブリック IP の自動割り当て): インスタンスをインターネットからアクセス可能にする場合は、[Auto-assign Public IP] (パブリック IP の自動割り当て) フィールドが [Enable] (有効) に設定されていることを確認します。可能にしない場合には、このフィールドを [無効] に設定します。

  > **Note**
  >
  > コンテナインスタンスには、Amazon ECS サービスエンドポイントと通信するためのアクセスが必要です。これは、インターフェイス VPC エンドポイントを介して、またはパブリック IP アドレスを持つコンテナインスタンスを通じて可能になります。
  > インターフェイス VPC エンドポイントについての詳細は、「Amazon ECS とインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。
  > インターフェイス VPC エンドポイントが設定されておらず、コンテナインスタンスがパブリック IP アドレスを持たない場合、ネットワークアドレス変換 (NAT) を使用してこのアクセスを提供する必要があります。詳細については、「Amazon VPC ユーザーガイド」の「NAT ゲートウェイ」、およびこのガイドの「Amazon ECS Linux コンテナインスタンスに HTTP プロキシを使用する」を参照してください。
- [Firewall (security groups)] (ファイアウォール (セキュリティグループ)): セキュリティグループを使用して、コンテナインスタンスのファイアウォールルールを定義します。このルールでは、ど

の着信ネットワークトラフィックをコンテナインスタンスに配信するかを指定します。他のトラフィックはすべて無視されます。

- 既存のセキュリティグループを選択するには、[Select existing security group] (既存のセキュリティグループを選択) を選択し、Amazon ECS を使用するようにセットアップする で作成したセキュリティグループを選択します。

ストレージの設定

選択した AMI には、ルートボリュームを含む、1 つまたは複数のストレージボリュームが含まれます。インスタンスにアタッチする追加のボリュームを指定できます。

[Simple] (シンプル) ビューを使用できます。

- [Storage type] (ストレージタイプ): コンテナインスタンスのストレージを設定します。

  Amazon ECS に最適化された Amazon Linux AMI を使用している場合、インスタンスには 2 つのボリュームが設定されます。[Root] ボリュームはオペレーティングシステム用で、2 番目の Amazon EBS ボリューム (`/dev/xvdcz` にアタッチ) は Docker 用です。

  オプションで、アプリケーションのニーズに合わせてインスタンスのボリュームサイズを増減できます。

高度な詳細

[Advanced details] で、セクションを開いてフィールドを表示し、インスタンスの追加パラメータを指定します。

- [Purchasing option] (購入のオプション): [Request Spot Instances] (スポットインスタンスのリクエスト) を選択して、スポットインスタンスをリクエストします。また、スポットインスタンスに関連する他のフィールドも設定する必要があります。詳細については、「スポットインスタンスのリクエスト」を参照してください。

  > **Note**
  >
  > スポットインスタンスを使用していて、"`Not available`" メッセージが表示される場合は、別のインスタンスタイプを選択する必要があります。

.

- [IAM instance profile] (IAM インスタンスプロフィール): コンテナインスタンス IAM ロールを選択します。通常、これは `ecsInstanceRole` という名前です。

  > **Important**
  >
  > 適切な IAM アクセス許可を使用してコンテナインスタンスを起動しないと、Amazon ECS エージェントはクラスターに接続できません。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

- (オプション) [User data] (ユーザーデータ): Amazon ECS コンテナエージェントの設定 からのエージェント環境変数のようなユーザーデータを使用して、Amazon ECS コンテナインスタンスを設定します。Amazon EC2 ユーザーデータスクリプトはインスタンスの初回起動時に 1 回のみ実行されます。以下に、ユーザーデータを使用する目的の一般的な例を紹介します。

  - デフォルトでは、コンテナインスタンスはデフォルトのクラスターで起動されます。デフォルト以外のクラスターで起動するには、[Advanced Details] (高度な詳細) リストを選択します。次に、[User data] フィールドに以下のスクリプトを貼り付け、*`your_cluster_name`* を使用するクラスターの名前に置き換えます。

    `EnableTaskIAMRole`は、タスクの Task IAM ロール機能をオンにします。

    さらに、以下のオプションは、`awsvpc` ネットワークモードを使用する場合に使用できます。

    - `EnableTaskENI`: このフラグは、`awsvpc`ネットワークモードを使用する場合に、タスクネットワークをオンにします。
    - `AwsvpcBlockIMDS`: `awsvpc`ネットワークモードで実行中のタスクコンテナが IMDS にアクセスするのをブロックします。
    - `AwsvpcAdditionalLocalRoutes`: このオプションフラグを使用すると、タスクの名前空間に追加のルートを持つことができます。

      置換 `ip-address`を追加ルートの IP アドレス (例えば 172.31.42.23/32) に置き換えます。

    ```
    <powershell>
    Import-Module ECSTools
    Initialize-ECSAgent -Cluster your_cluster_name -EnableTaskIAMRole -EnableTaskENI -
    AwsvpcBlockIMDS -AwsvpcAdditionalLocalRoutes
    '["ip-address"]'
    </powershell>
    ```

Amazon ECS Windows コンテナインスタンスをブートストラップしてデータを渡す

Amazon EC2 インスタンスを起動するときに、ユーザーデータを EC2 インスタンスに渡すことができます。インスタンスの起動時に、データを使って、一般的な自動設定タスクを実行したり、スクリプトを実行したりできます。Amazon ECS では、ユーザーデータの最も一般的なユースケースは、設定情報を Docker デーモンと Amazon ECS コンテナエージェントに渡すことです。

クラウドブートフック、シェルスクリプト、`cloud-init` ディレクティブなど、複数タイプのユーザーデータを Amazon EC2 に渡すことができます。これらおよびその他の形式の種類の詳細については、「Cloud-Init のドキュメント」を参照してください。

Amazon EC2 起動ウィザードを使用するときに、このユーザーデータを渡すことができます。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

デフォルト Windows ユーザーデータ

このユーザーデータスクリプト例で、コンソールを使用する場合、Windows コンテナインスタンスが受け取るデフォルトのユーザーデータが確認できます。以下のスクリプトでは下記を実行します。

- クラスター名に入力した名前を設定します。
- タスクの IAM ロールを設定します。
- `json-file` および `awslogs` を使用可能なロギングドライバーとして設定します。

さらに、以下のオプションは、`awsvpc` ネットワークモードを使用する場合に使用できます。

- `EnableTaskENI`: このフラグは、`awsvpc`ネットワークモードを使用する場合に、タスクネットワークをオンにします。
- `AwsvpcBlockIMDS`: このオプションのフラグは、`awsvpc`ネットワークモードで実行されているタスクコンテナに対する IMDS アクセスをブロックします。
- `AwsvpcAdditionalLocalRoutes`: このオプションフラグを使用すると、追加のルートを持つことができます。

  置換 `ip-address`を追加ルートの IP アドレス (例えば 172.31.42.23/32) に置き換えます。

このスクリプトは、独自のコンテナインスタンスに使用できます (Amazon ECS 最適化　Windows Server AMI から起動される場合)。

`-Cluster` *`cluster-name`* 行を置き換えて、独自のクラスター名を指定します。

```
<powershell>
Initialize-ECSAgent -Cluster cluster-name -EnableTaskIAMRole -LoggingDrivers '["json-
file","awslogs"]' -EnableTaskENI -AwsvpcBlockIMDS -AwsvpcAdditionalLocalRoutes
'["ip-address"]'
</powershell>
```

awslogs ログドライバーを使用するように設定された Windows タスクの場合は、コンテナインスタンスで ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE 環境変数も設定する必要があります。以下の構文を使用します。

-Cluster *cluster-name* 行を置き換えて、独自のクラスター名を指定します。

```
<powershell>
[Environment]::SetEnvironmentVariable("ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE",
 $TRUE, "Machine")
Initialize-ECSAgent -Cluster cluster-name -EnableTaskIAMRole -LoggingDrivers '["json-
file","awslogs"]'
</powershell>
```

Windows エージェントのインストールユーザーデータ

この例のユーザーデータスクリプトは、Windows_Server-2016-English-Full-Containers AMI で起動されたインスタンスにAmazon ECS コンテナエージェントをインストールします。これは、Amazon ECS コンテナエージェントの GitHub リポジトリ README ページのエージェントのインストール手順から変更されています。

> **Note**
>
> このスクリプトは、サンプル目的で共有されます。Amazon ECS に最適化された Windows AMI を使用すると、Windows コンテナの使用を開始するほうが、はるかに簡単です。詳細については、「Fargate 起動タイプ用の Amazon ECS クラスターを作成する」を参照してください。

Windows Server 2022 Full に Amazon ECS エージェントをインストールする方法については、GitHub の「Issue 3753」を参照してください。

このスクリプトは、独自のコンテナインスタンスに使用できます (それらのインスタンスが Windows_Server-2016-English-Full-Containers AMI のバージョンで起動される場合)。*windows* 行を置き換えて、独自のクラスターの名前を指定します (windows クラスターを使用しない場合)。

```
<powershell>
# Set up directories the agent uses
New-Item -Type directory -Path ${env:ProgramFiles}\Amazon\ECS -Force
New-Item -Type directory -Path ${env:ProgramData}\Amazon\ECS -Force
New-Item -Type directory -Path ${env:ProgramData}\Amazon\ECS\data -Force
# Set up configuration
$ecsExeDir = "${env:ProgramFiles}\Amazon\ECS"
[Environment]::SetEnvironmentVariable("ECS_CLUSTER", "windows", "Machine")
[Environment]::SetEnvironmentVariable("ECS_LOGFILE", "${env:ProgramData}\Amazon\ECS\log
\ecs-agent.log", "Machine")
[Environment]::SetEnvironmentVariable("ECS_DATADIR", "${env:ProgramData}\Amazon\ECS
\data", "Machine")
# Download the agent
$agentVersion = "latest"
$agentZipUri = "https://s3.amazonaws.com/amazon-ecs-agent/ecs-agent-windows-
$agentVersion.zip"
$zipFile = "${env:TEMP}\ecs-agent.zip"
Invoke-RestMethod -OutFile $zipFile -Uri $agentZipUri
# Put the executables in the executable directory.
Expand-Archive -Path $zipFile -DestinationPath $ecsExeDir -Force
Set-Location ${ecsExeDir}
# Set $EnableTaskIAMRoles to $true to enable task IAM roles
# Note that enabling IAM roles will make port 80 unavailable for tasks.
[bool]$EnableTaskIAMRoles = $false
if (${EnableTaskIAMRoles}) {
  $HostSetupScript = Invoke-WebRequest https://raw.githubusercontent.com/aws/amazon-
ecs-agent/master/misc/windows-deploy/hostsetup.ps1
  Invoke-Expression $($HostSetupScript.Content)
}
# Install the agent service
New-Service -Name "AmazonECS" `
        -BinaryPathName "$ecsExeDir\amazon-ecs-agent.exe -windows-service" `
        -DisplayName "Amazon ECS" `
        -Description "Amazon ECS service runs the Amazon ECS agent" `
        -DependsOn Docker `
        -StartupType Manual
sc.exe failure AmazonECS reset=300 actions=restart/5000/restart/30000/restart/60000
sc.exe failureflag AmazonECS 1
Start-Service AmazonECS
</powershell>
```

Amazon ECS Windows コンテナインスタンスに HTTP プロキシを使用する

Amazon ECS コンテナエージェントと Docker デーモンの両方に HTTP プロキシを使用するように Amazon ECS コンテナインスタンスを設定できます。これは、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合に便利です。

Amazon ECS Windows コンテナインスタンスが HTTP プロキシを使用するように設定するには、起動時に (Amazon EC2ユーザーデータを使用して) 以下の変数を設定します。

```
[Environment]::SetEnvironmentVariable("HTTP_PROXY",
"http://proxy.mydomain:port", "Machine")
```

HTTP_PROXY を、Amazon ECS エージェントがインターネットへの接続に使用する HTTP プロキシのホスト名 (または IP アドレス) とポート番号に設定します。例えば、コンテナインスタンスに、Amazon VPC インターネットゲートウェイ、NAT ゲートウェイ、またはインスタンスを介した外部ネットワークアクセスがない場合です。

```
[Environment]::SetEnvironmentVariable("NO_PROXY",
"169.254.169.254,169.254.170.2,\\.\pipe\docker_engine", "Machine")
```

NO_PROXY を 169.254.169.254,169.254.170.2,\\.\pipe\docker_engine に設定して、EC2 インスタンスのメタデータ、タスク用の IAM ロール、および Docker デーモンのトラフィックをプロキシからフィルタリングします。

Example Windows HTTP プロキシのユーザーデータスクリプト

以下のユーザーデータ PowerShell スクリプトの例では、 Amazon ECS コンテナエージェント、および Docker デーモンが指定された HTTP プロキシを使用するように設定します。コンテナインスタンス自体が登録されているクラスターを指定することもできます。

コンテナインスタンスの起動時にこのスクリプトを使用するには、「the section called “コンテナインスタンスの起動”」のステップに従います。以下の PowerShell スクリプトをコピーして [ユーザーデータ] フィールドに貼り付けます (必ず、赤いサンプル値を実際のプロキシおよびクラスターの情報に置き換えてください)。

> **Note**
>
> この -EnableTaskIAMRole オプションは、タスクの IAM ロールを有効にするために必要です。詳細については、「Amazon EC2 Windows インスタンスの追加設定」を参照してください。

```
<powershell>
Import-Module ECSTools

$proxy = "http://proxy.mydomain:port"
[Environment]::SetEnvironmentVariable("HTTP_PROXY", $proxy, "Machine")
[Environment]::SetEnvironmentVariable("NO_PROXY", "169.254.169.254,169.254.170.2,\\.
\pipe\docker_engine", "Machine")

Restart-Service Docker
Initialize-ECSAgent -Cluster MyCluster -EnableTaskIAMRole
</powershell>
```

スポットインスタンス通知を受信するように Amazon ECS Windows コンテナインスタンスを設定する

利用可能なキャパシティーがなくなった場合、または、スポット料金がお客様のリクエストの上限料金を超えた場合には、Amazon EC2 はスポットインスタンスを終了、停止、または休止状態にします。Amazon EC2 はスポットインスタンスが中断される 2 分前に、そのインスタンスに対し中断を警告するための通知を送信します。インスタンスで Amazon ECS スポットインスタンスのドレインが有効になっている場合、ECS はスポットインスタンスの中断通知を受け取り、インスタンスを DRAINING ステータスにします。

> **Important**
>
> Amazon ECS は、terminate および stop インスタンスアクションがあるスポットインスタンスの中断通知をモニタリングします。スポットインスタンスまたはスポットフリートのリクエスト時に hibernate インスタンスの中断動作を指定した場合、Amazon ECS スポットインスタンスのドレインはこれらのインスタンスではサポートされません。

コンテナインスタンスを DRAINING に設定すると、Amazon ECS によって新規タスクがそのコンテナインスタンスに配置されなくなります。ドレインしているコンテナインスタンス上にある

PENDING 状態のサービスタスクは即時停止されます。クラスター内に使用可能なコンテナインスタンスがある場合、そのインスタンスで代わりのサービスタスクが開始されます。

インスタンスの起動時にスポットインスタンスドレイニングを有効にできます。コンテナエージェントを開始する前に ECS_ENABLE_SPOT_INSTANCE_DRAINING パラメータを設定する必要があります。*#######* の部分は自分のクラスター名に置き換えます。

```
[Environment]::SetEnvironmentVariable("ECS_ENABLE_SPOT_INSTANCE_DRAINING", "true",
 "Machine")

# Initialize the agent
Initialize-ECSAgent -Cluster my-cluster
```

詳細については、「the section called “コンテナインスタンスの起動”」を参照してください。

外部起動タイプ用の Amazon ECS クラスター

Amazon ECS Anywhere は、オンプレミスサーバーや仮想マシン (VM) などの外部インスタンスを Amazon ECS クラスターに登録するためのサポートを提供します。外部インスタンスは、アウトバウンドトラフィックを生成したり、データを処理したりするアプリケーションを実行するために最適化されています。アプリケーションがインバウンドトラフィックを必要とする場合、Elastic Load Balancing のサポートがないため、これらのワークロードの実行効率が低下します。Amazon ECS は、新しいEXTERNAL起動タイプで、サービスを作成したり、外部インスタンスでタスクを実行したりできます。

サポートされるオペレーティングシステムとシステムアーキテクチャ

以下は、サポートされるオペレーティングシステムとシステムアーキテクチャのリストです。

- Amazon Linux 2
- Amazon Linux 2023
- CentOS 7
- CentOS Stream 9
- RHEL 7、RHEL 8 - DockerとRHELのオープンパッケージリポジトリはどっちも、RHELへのDockerのネイティブなインストールに対応していません。このドキュメントで説明されているインストールスクリプトを実行する前に、Docker がインストールされていることを確認する必要があります。
- Fedora 32、Fedora 33、Fedora 40

- openSUSE タンブルウィード
- Ubuntu 18、Ubuntu 20、Ubuntu 22、Ubuntu 24
- Debian 10

> **Important**
>
> Debian 9 の長期 Support (LTS) は 2022 年 6 月 30 日にサポート期間が終了となり、Amazon ECS Anywhere によるサポート対象外となります。

- Debian 11
- Debian 12
- SUSE Enterprise Server 15
- x86_64およびARM64CPU アーキテクチャがサポートされています。
- 次の Windows オペレーティングシステムのバージョンがサポートされています。
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 20H2

考慮事項

外部インスタンスの使用を開始する前に、以下の考慮事項に注意してください。

- 外部インスタンスは、一度に 1 つずつクラスターに登録できます。外部インスタンスを別のクラスターに登録する方法については、「Amazon ECS 外部インスタンスの登録を解除する」を参照してください。
- 外部インスタンスには、AWS API との通信を許可する IAM ロールが必要です。詳細については、「Amazon ECS Anywhere IAM ロール」を参照してください。
- 外部インスタンスには、事前設定されたインスタンス認証情報チェーンをローカルに定義しないでください。これは、登録スクリプトに干渉するためです。
- コンテナログを CloudWatch Logs に送信するには、タスク定義でタスク実行 IAM ロールを作成し、指定してください。
- 外部インスタンスがクラスターに登録されると、`ecs.capability.external`属性がインスタンスに関連付けられています。この属性は、インスタンスを外部インスタンスとして識別します。カ

スタム属性を外部インスタンスに追加して、タスクの配置制約として使用できます。詳細については、「カスタム属性」を参照してください。

- 外部インスタンスにリソースタグを追加できます。詳細については、「外部コンテナインスタンス」を参照してください。
- ECS Exec は、外部インスタンスでサポートされています。詳細については、「ECS Exec を使用して Amazon ECS コンテナをモニタリングする」を参照してください。
- 外部インスタンスとのネットワーキングに固有の追加の考慮事項を次に示します。詳細については、「ネットワーク」を参照してください。
  - サービスの負荷分散はサポートされていません。
  - サービス検出はサポートされていません。
  - 外部インスタンスで実行されるタスクは、`bridge`,`host`, または`none` ネットワークモードを使用する必要があります。`awsvpc` ネットワークモードはサポートされていません。
  - 各 AWS リージョンに Amazon ECS サービスドメインがあります。これらのサービスドメインは、外部インスタンスへのトラフィックの送信を許可する必要があります。
  - 外部インスタンスにインストールされた SSM Agent は、ハードウェアフィンガープリントを使用して 30 分ごとにローテーションされる IAM 認証情報を保持します。外部インスタンスがAWSに設定されている場合、SSM Agent は接続の再確立後にクレデンシャルを自動的に更新します。詳細については、AWS Systems Managerユーザーガイドの「ハードウェアフィンガープリントを使用したオンプレミスサーバーと仮想マシンの検証」を参照してください。
- `UpdateContainerAgent` API はサポートされません。外部インスタンスで SSM Agent または Amazon ECS エージェントを更新する方法については、「外部インスタンス上の AWS Systems Manager エージェントと Amazon ECS コンテナエージェントを更新する」を参照してください。
- Amazon ECS キャパシティープロバイダーはサポートされていません。外部インスタンスでサービスを作成したり、スタンドアロンタスクを実行するには、`EXTERNAL`起動タイプを使用するタスクにのみ使用されます。
- SELinux はサポートされません。
- Amazon EFS ボリュームの使用、または `EFSVolumeConfiguration` はサポートされていません。
- App Mesh との統合はサポートされていません。
- コンソールを使用して外部インスタンスタスク定義を作成する場合は、コンソール JSON エディタでタスク定義を作成する必要があります。
- Windows で ECS Anywhere を実行する場合は、オンプレミスのインフラストラクチャで独自の Windows ライセンスを使用する必要があります。

- Amazon ECS に最適化されていない AMI を使用する場合は、外部コンテナインスタンスで次のコマンドを実行して、タスクに IAM ロールを使用するルールを設定します。詳細については、「外部インスタンスの追加設定」を参照してください。

```
$ sysctl -w net.ipv4.conf.all.route_localnet=1
$ iptables -t nat -A PREROUTING -p tcp -d 169.254.170.2 --dport 80 -j DNAT --to-
destination 127.0.0.1:51679
$ iptables -t nat -A OUTPUT -d 169.254.170.2 -p tcp -m tcp --dport 80 -j REDIRECT --
to-ports 51679
```

ネットワーク

Amazon ECS 外部インスタンスは、アウトバウンドトラフィックを生成したり、データを処理したりするアプリケーションを実行するために最適化されています。アプリケーションがウェブサービスなどのインバウンドトラフィックを必要とする場合、Elastic Load Balancing のサポートがないため、これらのワークロードをロードバランサーの背後に配置するためのサポートがないため、これらのワークロードの実行効率が低下します。

外部インスタンスとのネットワークに固有の追加の考慮事項を次に示します。

- サービスの負荷分散はサポートされていません。
- サービス検出はサポートされていません。
- 外部インスタンスで実行される Linux タスクは、`bridge`、`host`、または`none` ネットワークモードを使用する必要があります。`awsvpc` ネットワークモードはサポートされていません。

  各ネットワークモードの詳細については、「EC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。
- 外部インスタンスで実行される Windows タスクは、`default` ネットワークモードを使用する必要があります。
- 各リージョンには Amazon ECS サービスドメインがあり、外部インスタンスへのトラフィックの送信を許可する必要があります。
- 外部インスタンスにインストールされた SSM Agent は、ハードウェアフィンガープリントを使用して 30 分ごとにローテーションされる IAM 認証情報を保持します。外部インスタンスがAWSに設定されている場合、SSM Agent は接続の再確立後にクレデンシャルを自動的に更新します。詳細については、AWS Systems Managerユーザーガイドの「ハードウェアフィンガープリントを使用したオンプレミスサーバーと仮想マシンの検証」を参照してください。

次のドメインは、Amazon ECS サービスと外部インスタンスにインストールされている Amazon ECS エージェント間の通信に使用されます。トラフィックが許可されていることと、DNS 解決が機能していることを確認します。各エンドポイントでは、*#####*は、米国東部 (オハイオ) リージョンの us-east-2 のように、Amazon ECS でサポートされている AWS リージョンのリージョン識別子を表します。使用するすべてのリージョンのエンドポイントを許可する必要があります。ecs-aおよびecs-tエンドポイントを使用する場合は、アスタリスク (例えば、ecs-a-*) を含める必要があります。

- ecs-a-*.*region*.amazonaws.com— このエンドポイントは、タスクを管理するときに使用されます。
- ecs-t-*.*region*.amazonaws.com— このエンドポイントは、タスクとコンテナのメトリクスを管理するために使用されます。
- ecs.*region*.amazonaws.com — これは、Amazon ECS のサービスエンドポイントです。
- ssm.*region*.amazonaws.com — これは、AWS Systems Manager のサービスエンドポイントです。
- ec2messages.*region*.amazonaws.com — これは、AWS Systems Manager がクラウド内の Systems Manager エージェントと Systems Manager サービスの間の通信に使用するサービスエンドポイントです。
- ssmmessages.*region*.amazonaws.com — これは、クラウド内の Session Manager サービスでセッションチャネルを作成および削除するために必要なサービスエンドポイントです。
- タスクが他のタスクとの通信を必要とする場合AWSサービスを使用する場合は、これらのサービスエンドポイントが許可されていることを確認します。アプリケーション例としては、Amazon ECR を使用してコンテナイメージを取得したり、CloudWatch Logs に CloudWatch を使用したりすることが挙げられます。詳細については、AWS 全般のリファレンスガイドの「サービスエンドポイント」を参照してください。

ECS Anywhere を使用した Amazon FSx for Windows File Server

Amazon ECS 外部インスタンスで Amazon FSx for Windows File Server を使用するには、オンプレミスのデータセンターと AWS クラウド の間に接続を確立する必要があります。ネットワークを VPC に接続するオプションについては、「Amazon Virtual Private Cloud 接続オプション」を参照してください。

ECS Anywhere を使用した gMSA

ECS Anywhere は、次のユースケースをサポートしています。

- アクティブディレクトリは、AWS クラウド にあります。この構成では、AWS クラウド 接続を使用してオンプレミスネットワークと AWS Direct Connect の間の接続を確立します。接続を作成する方法については、「Amazon 仮想プライベートクラウド接続オプション」を参照してください。AWS クラウド にアクティブディレクトリを作成します。AWS Directory Service の使用開始方法の詳細については、「AWS Directory Service 管理ガイド」の「AWS Directory Service の設定」を参照してください。その後、AWS Direct Connect 接続を使用して、外部インスタンスをドメインに参加させることができます。Amazon ECS での gMSA の操作方法については、「the section called “EC2 Windows コンテナで gMSAs を使用する方法について説明します。”」を参照してください。
- アクティブディレクトリは、オンプレミスデータセンターで管理されています。-この設定では、外部インスタンスをオンプレミスのアクティブディレクトリに参加させます。その後、Amazon ECS タスクを実行する際に、ローカルで使用可能な認証情報を使用します。

外部起動タイプ用の Amazon ECS クラスターを作成する

クラスターを作成して、タスクとサービスを実行するインフラストラクチャを定義します。

これを開始する前に、「Amazon ECS を使用するようにセットアップする」 の手順を完了し、適切な IAM 許可を割り当てる必要があります。詳細については、「the section called “Amazon ECS クラスターの例”」を参照してください。Amazon ECS コンソールでは、AWS CloudFormation スタックを作成することで、Amazon ECS クラスターに必要なリソースを簡単に作成できます。

クラスターの作成プロセスをできるだけ簡単にするために、コンソールには、以下で説明する多くの選択肢に対するデフォルトの選択肢があります。コンソール内のほとんどのセクションには、詳細なコンテキストを提供するヘルプパネルもあります。

- AWS Cloud Map に、クラスターと同じ名前のデフォルトの名前空間を作成します。名前空間を使用すると、クラスターで作成したサービスを、追加の設定なしで名前空間内の他のサービスに接続できます。

  詳細については、「Amazon ECS サービスを相互接続する」を参照してください。

以下のオプションを変更できます。

- クラスターに関連付けられたデフォルトの名前空間を変更します。

名前空間を使用すると、クラスターで作成したサービスを、追加の設定なしで名前空間内の他のサービスに接続できます。デフォルトの名前空間は、クラスター名と同じです。詳細については、「Amazon ECS サービスを相互接続する」を参照してください。

- クラスターを外部インスタンス用に設定します。
- オブザーバビリティが強化された Container Insights、または Container Insights を有効にします。

  CloudWatch Container Insights は、コンテナ化されたアプリケーションおよびマイクロサービスのメトリクスとログを収集、集約、要約します。Container Insights は、問題の迅速な特定と解決に使用するコンテナの再起動失敗などの診断情報も提供します。詳細については、「the section called “オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する”」を参照してください。

  2024 年 12 月 2 日、AWS で Amazon ECS 用にオブザーバビリティが強化された Container Insights がリリースされました。このバージョンでは、Amazon EC2 および Fargate 起動タイプを使用して Amazon ECS 用に強化されたオブザーバビリティがサポートされます。Amazon ECS でオブザーバビリティが強化された Container Insights を設定したら、Container Insights は環境内のクラスターレベルからコンテナレベルまでの詳細なインフラストラクチャテレメトリを自動収集し、さまざまなメトリクスとディメンションを示すダッシュボードにデータを表示します。その後、Container Insights コンソールでこれらのすぐに使えるダッシュボードを使用して、コンテナの健全性とパフォーマンスをよりよく理解し、異常を特定することで問題を迅速に軽減することができます。

  コンテナ環境で詳細な可視性を提供し、解決までの平均時間を短縮するため、Container Insights ではなく、オブザーバビリティが強化された Container Insights を使用することをお勧めします。
- クラスターを識別しやすいようにタグを追加します。

新しいクラスターを作成するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、[Create Cluster] (クラスターの作成) を選択します。
5. [クラスター設定] で以下を設定します。
   - [クラスター名] に一意の名前を入力します。

名前には、最大 255 文字 (大文字と小文字)、数字、およびハイフンを含めることができます。

- (オプション) Service Connect に使用する名前空間をクラスター名と別のものにするには、[名前空間] に一意の名前を入力します。

6. (オプション) Container Insights を使用して モニタリング を展開し、次のいずれかのオプションを選択します。

   - オブザーバビリティが強化された推奨の Container Insights を使用するには、[オブザーバビリティが強化された Container Insights] を選択します。
   - Container Insights を使用するには、[Container Insights] を選択します。

7. (オプション) クラスターを識別しやすくするには、[Tags] (タグ) を展開し、タグを設定します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

8. [Create] (作成) を選択します。

次のステップ

インスタンスをクラスターに登録する必要があります。詳細については、「Amazon ECS クラスターに外部インスタンスを登録する」を参照してください。

外部起動タイプのタスク定義を作成します。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

スタンドアロンタスクとして、またはサービスの一部としてアプリケーションを実行します。詳細については次を参照してください:

- Amazon ECS タスクとしてのアプリケーションの実行
- コンソールを使用した Amazon ECS サービスの作成

Amazon ECS クラスターに外部インスタンスを登録する

Amazon ECS クラスターに登録する外部インスタンスごとに、SSM Agent、Amazon ECS コンテナエージェント、および Docker がインストールされている必要があります。外部インスタンスを

Amazon ECS クラスターに登録するには、最初に AWS Systems Manager マネージドインスタンスを登録する必要があります。インストールスクリプトは、Amazon ECS コンソールで数回クリックするだけで作成できます。インストールスクリプトには、Systems Manager のアクティベーションキーと、必要なエージェントと Docker をインストールするためのコマンドが含まれています。インストールと登録の手順を完了するには、オンプレミスのサーバーまたは VM でインストールスクリプトを実行する必要があります。

> **Note**
>
> Linux の外部インスタンスをクラスターに登録する前に、`/etc/ecs/ecs.config` ファイルを作成し、必要なコンテナエージェント設定パラメータを追加します。外部インスタンスをクラスターに登録した後は、これを行うことはできません。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

AWS Management Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. リポジトリの [クラスター] ページで、外部インスタンスを登録するクラスターを選択します。
5. [Cluster : ***name***] (クラスター: 名前) のページで、[Infrastructure] (インフラストラクチャ) タブを選択します。
6. [Register external instances] (外部インスタンスの登録) ページで、次のステップを完了します。

    a. [Activation key duration (in days)] (アクティベーションキーの期間 (日数)) を使用する場合、アクティベーションキーがアクティブなままになる日数を入力します。入力した日数が経過すると、外部インスタンスの登録時にキーが機能しなくなります。

    b. インスタンス数を使用する場合　アクティベーションキーを使用してクラスターに登録する外部インスタンスの数を入力します。

    c. インスタンスロールを使用する場合、外部インスタンスに関連付ける IAM ロールを選択します。ロールがまだ作成されていない場合は、新規ロールの作成を選択すると、Amazon ECS がユーザーに代わってロールを作成します。外部インスタンスに必要

な IAM 許可の詳細については、「Amazon ECS Anywhere IAM ロール」を参照してください。

d. 登録コマンドをコピーします。このコマンドは、クラスターに登録する各外部インスタンスで実行する必要があります。

> **Important**
>
> スクリプトの bash 部分は root として実行する必要があります。コマンドが root として実行されない場合、エラーが返されます。

e. [閉じる] を選択します。

AWS CLI for Linux operating systems

1. Systems Manager のアクティベーションペアを作成します。これは、Systems Manager が管理するインスタンスのアクティベーションに使用されます。出力には、`ActivationId`および`ActivationCode`が含まれます。これらは、後のステップで使用します。作成した ECS Anywhere IAM ロールを指定していることを確認します。詳細については、「Amazon ECS Anywhere IAM ロール」を参照してください。

```
aws ssm create-activation --iam-role ecsAnywhereRole | tee ssm-activation.json
```

2. オンプレミスのサーバーまたは仮想マシン (VM) で、インストールスクリプトをダウンロードします。

```
curl --proto "https" -o "/tmp/ecs-anywhere-install.sh" "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh"
```

3. (オプション) オンプレミスサーバーまたは仮想マシン (VM) で、次の手順を使用して、スクリプト署名ファイルを使用してインストールスクリプトを確認します。

a. GnuPG をダウンロードし、インストールします。GNUpg の詳細については、「GnuPG ウェブサイト」を参照してください。Linux システムの場合は、お使いの Linux ディストリビューションでパッケージマネージャーを使用して gpg をインストールします。

b. Amazon ECS PGP パブリックキーを取得します。

```
gpg --keyserver hkp://keys.gnupg.net:80 --recv BCE9D9A42D51784F
```

c. インストールスクリプトの署名をダウンロードします。署名は、ASCII でデタッチ済みの PGP 署名で、拡張子が .asc のファイルに保存されています。

```
curl --proto "https" -o "/tmp/ecs-anywhere-install.sh.asc" "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh.asc"
```

d. キーを使用してインストールスクリプトファイルを確認します。

```
gpg --verify /tmp/ecs-anywhere-install.sh.asc /tmp/ecs-anywhere-install.sh
```

予想される出力は次のようになります。

```
gpg: Signature made Tue 25 May 2021 07:16:29 PM UTC
gpg:                using RSA key 50DECCC4710E61AF
gpg: Good signature from "Amazon ECS <ecs-security@amazon.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the
 owner.
Primary key fingerprint: F34C 3DDA E729 26B0 79BE  AEC6 BCE9 D9A4 2D51 784F
     Subkey fingerprint: D64B B6F9 0CF3 77E9 B5FB  346F 50DE CCC4 710E 61AF
```

4. オンプレミスのサーバーまたは仮想マシン (VM) で、インストールスクリプトを実行します。クラスター名、リージョン、Systems Manager のアクティベーション ID とアクティベーションコードを、最初のステップで指定します。

```
sudo bash /tmp/ecs-anywhere-install.sh \
    --region $REGION \
    --cluster $CLUSTER_NAME \
    --activation-id $ACTIVATION_ID \
    --activation-code $ACTIVATION_CODE
```

オンプレミスサーバーまたは仮想マシン (VM) で、GPU ワークロード用の NVIDIA ドライバーがインストールされている場合は、インストールスクリプトに --enable-gpu フラグを設定する必要があります。このフラグを指定すると、インストールスクリプトは NVIDIA ドライバが実行中であることを確認してから、Amazon ECS タスクを実行するために必要な構成変数を追加します。GPU ワークロードの実行と、タスク定義での GPU 要件の指定の詳細については、「Amazon ECS タスク定義での GPU の指定」を参照してください。

```
sudo bash /tmp/ecs-anywhere-install.sh \
    --region $REGION \
```

```
    --cluster $CLUSTER_NAME \
    --activation-id $ACTIVATION_ID \
    --activation-code $ACTIVATION_CODE \
    --enable-gpu
```

既存の外部インスタンスを別のクラスターに登録するには、次のステップを実行します。

既存の外部インスタンスを別のクラスターに登録するには

1. Amazon ECS コンテナエージェントを停止します。

```
sudo systemctl stop ecs.service
```

2. /etc/ecs/ecs.configファイルとECS_CLUSTER行を編集して、クラスター名が外部インスタンスを登録するクラスターの名前と一致していることを確認します。
3. 既存の Amazon ECS エージェントデータを削除します。

```
sudo rm /var/lib/ecs/data/agent.db
```

4. Amazon ECS コンテナエージェントを開始する

```
sudo systemctl start ecs.service
```

AWS CLI for Windows operating systems

1. Systems Manager のアクティベーションペアを作成します。これは、Systems Manager が管理するインスタンスのアクティベーションに使用されます。出力には、ActivationIdおよびActivationCodeが含まれます。これらは、後のステップで使用します。作成した ECS Anywhere IAM ロールを指定していることを確認します。詳細については、「Amazon ECS Anywhere IAM ロール」を参照してください。

```
aws ssm create-activation --iam-role ecsAnywhereRole | tee ssm-activation.json
```

2. オンプレミスのサーバーまたは仮想マシン (VM) で、インストールスクリプトをダウンロードします。

```
Invoke-RestMethod -URI "https://amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-
install.ps1" -OutFile “ecs-anywhere-install.ps1”
```

3. (オプション) Powershell スクリプトは Amazon によって署名されているため、Windows は同じ場所で証明書の検証を自動的に実行します。手動で検証を実行する必要はありません。

   証明書を手動で検証するには、ファイルを右クリックしてプロパティに移動し、[Digital Signatures] (デジタル署名) タブを使用して詳細を取得します。

   このオプションは、ホストが証明書ストアに証明書がある場合にのみ使用できます。

   検証の結果、次のような情報が返されます。

   ```
   # Verification (PowerShell)
   Get-AuthenticodeSignature -FilePath .\ecs-anywhere-install.ps1

   SignerCertificate                         Status      Path
   -----------------                         ------      ----
   EXAMPLECERTIFICATE                        Valid       ecs-anywhere-install.ps1

   ...

   Subject              : CN="Amazon Web Services, Inc.",...

   ----
   ```

4. オンプレミスのサーバーまたは仮想マシン (VM) で、インストールスクリプトを実行します。クラスター名、リージョン、Systems Manager のアクティベーション ID とアクティベーションコードを、最初のステップで指定します。

   ```
   .\ecs-anywhere-install.ps1 -Region $Region -Cluster $Cluster -
   ActivationID $ActivationID -ActivationCode $ActivationCode
   ```

5. Amazon ECS コンテナエージェントが実行されていることを確認します。

   ```
   Get-Service AmazonECS

   Status   Name               DisplayName
   ------   ----               -----------
   Running  AmazonECS          Amazon ECS
   ```

既存の外部インスタンスを別のクラスターに登録するには、次のステップを実行します。

既存の外部インスタンスを別のクラスターに登録するには

1. Amazon ECS コンテナエージェントを停止します。

```
Stop-Service AmazonECS
```

2. クラスター名が外部インスタンスを登録するクラスターの名前と一致するように ECS_CLUSTER パラメータを変更します。

```
[Environment]::SetEnvironmentVariable("ECS_CLUSTER", $ECSCluster,
 [System.EnvironmentVariableTarget]::Machine)
```

3. 既存の Amazon ECS エージェントデータを削除します。

```
Remove-Item -Recurse -Force $env:ProgramData\Amazon\ECS\data\*
```

4. Amazon ECS コンテナエージェントを開始する

```
Start-Service AmazonECS
```

AWS CLIを使用して、外部インスタンスの登録プロセスを完了するためにインストールスクリプトを実行する前に、Systems Manager のアクティベーションを作成できます

Amazon ECS 外部インスタンスの登録を解除する

インスタンスの使用が終了したら、Amazon ECS とAWS Systems Manager をインスタンスから登録解除することをお勧めします。登録解除後、コンテナインスタンスは新しいタスクを受けることができなくなります。

登録解除するときにコンテナインスタンスでタスクが実行されている場合、インスタンスを削除するかタスクが他の手段で停止するまで、これらのタスクは実行されたままになります。ただし、これらのタスクは Amazon ECS によるモニタリングや情報収集の対象外になります。外部インスタンス上のこれらのタスクが Amazon ECS サービスに含まれる場合、サービススケジューラは、可能であれば、別のコンテナインスタンスでそのタスクの別のコピーを開始します。

インスタンスの登録を解除した後、インスタンス上の残りの AWS リソースをクリーンアップします。その後、新しいクラスターに登録できます。

手順

AWS Management Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、外部インスタンスが存在するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択し、外部インスタンスをホストするクラスターを選択します。
4. [Cluster : ***name***] (クラスター: 名前) のページで、[Infrastructure] (インフラストラクチャ) タブを選択します。
5. [Container instances] (コンテナインスタンス)で、登録解除する外部のインスタンス ID を選択します。コンテナインスタンスの詳細ページにリダイレクトされます。
6. [Container Instance : ***id***] (コンテナインスタンス: id) ページで、[Deregister] (登録解除) を選択します。
7. 登録解除メッセージを確認します。[Deregistered fromAWS Systems Manager]を選択して、外部インスタンスを Systems Manager 管理対象インスタンスとして登録解除することもできます。[Deregister] (登録解除) を選択します。

   > **Note**
   >
   > Systems Manager コンソールで、外部インスタンスを Systems Manager 管理対象インスタンスとして登録解除できます。手順については、「AWS Systems Manager ユーザーガイド」の「ハイブリッドおよびマルチクラウド環境でのマネージドノードの登録解除」を参照してください。

8. インスタンスの登録を解除した後は、オンプレミスサーバーまたは VM にある AWS リソースをクリーンアップします。

オペレーティングシステム	ステップ	
リナックス	a. インスタンスの Amazon ECS コンテナエージェントと SSM Agent サービスを停止します。	

オペレーティングシステム	ステップ

	`sudo systemctl stop ecs amazon-ssm-agent`
	b. Amazon ECS パッケージおよびSystems Manager パッケージを削除します。
	CentOS 7、CentOS 8、および RHEL 7 の場合
	`sudo yum remove -y amazon-ecs-init amazon-ssm-agent`
	SUSE Linux Enterprise Server 15 の場合
	`sudo zypper remove -y amazon-ecs-init amazon-ssm-agent`
	Ubuntu と Debian の場合
	`sudo apt remove -y amazon-ecs-init amazon-ssm-agent`
	c. 残ったディレクトリを削除します。
	`sudo rm -rf /var/lib/ecs /etc/ecs /var/lib/amazon/ss`

オペレーティングシステム	ステップ
	`m /var/log/ecs / var/log/amazon/ssm`

Windows	a. インスタンスの Amazon ECS コンテナエージェントと SSM Agent サービスを停止します。
	`Stop-Service AmazonECS`
	`Stop-Service AmazonSSMAgent`
	b. Amazon ECS パッケージを削除します。
	`.\ecs-anywhere-install.ps1 -Uninstall`

AWS CLI

1. コンテナインスタンスを登録解除するには、インスタンス ID とコンテナインスタンス ARN が必要です。これらの値がない場合は、次のコマンドを実行してください

   次のコマンドを実行して、インスタンス ID を取得します。

   インスタンス ID (`instanceID`) を使用し、コンテナインスタンス ARN (`containerInstanceARN`) を取得します。

   ```
   instanceId=$(aws ssm describe-instance-information --region "{{ region }}" |
    jq ".InstanceInformationList[] |select(.IPAddress==\"{{ IPv4 Address }}\")
    | .InstanceId" | tr -d'"'
   ```

   以下のコマンドを実行します。

インスタンス (deregister-container-instance) を登録解除するには、コマンドのパラメータとして containerInstanceArn を使用します。

```
instances=$(aws ecs list-container-instances --cluster "{{ cluster }}" --region
 "{{ region }}" | jq -c '.containerInstanceArns')
containerInstanceArn=$(aws ecs describe-container-instances --cluster
 "{{ cluster }}" --region "{{ region }}" --container-instances $instances
 | jq ".containerInstances[] | select(.ec2InstanceId==\"{{ instanceId }}\")
 | .containerInstanceArn" | tr -d '"')
```

2. 次のコマンドを実行して、インスタンスをドレインします。

```
aws ecs update-container-instances-state --cluster "{{ cluster }}" --region
 "{{ region }}" --container-instances "{{ containerInstanceArn }}" --status
 DRAINING
```

3. コンテナインスタンスのドレインが終了したら、次のコマンドを実行してインスタンスを登録解除します。

```
aws ecs deregister-container-instance --cluster "{{ cluster }}" --region
 "{{ region }}" --container-instance "{{ containerInstanceArn }}"
```

4. 次のコマンドを実行し、SSM からコンテナインスタンスを削除します。

```
aws ssm deregister-managed-instance --region "{{ region }}" --instance-id
 "{{ instanceId }}"
```

5. インスタンスの登録を解除した後は、オンプレミスサーバーまたは VM にある AWS リソースをクリーンアップします。

オペレーティングシステム	ステップ
リナックス	a. インスタンスの Amazon ECS コンテナエージェントと SSM Agent サービスを停止します。

オペレーティングシステム	ステップ	

	`sudo systemctl stop ecs amazon-ssm-agent`
	b. Amazon ECS パッケージおよびSystems Manager パッケージを削除します。
	`sudo (yum/apt/zypper) remove amazon-ecs-init amazon-ssm-agent`
	c. 残ったディレクトリを削除します。
	`sudo rm -rf /var/lib/ecs /etc/ecs /var/lib/amazon/ssm /var/log/ecs /var/log/amazon/ssm`	

オペレーティングシステム	ステップ	

Windows	a. インスタンスの Amazon ECS コンテナエージェントと SSM Agent サービスを停止します。
	`Stop-Service AmazonECS`
	`Stop-Service AmazonSSMAgent`
	b. Amazon ECS パッケージを削除します。
	`.\ecs-anywhere-install.ps1 -Uninstall`	

外部インスタンス上の AWS Systems Manager エージェントと Amazon ECS コンテナエージェントを更新する

オンプレミスのサーバーまたは VM で、AWS Systems Managerエージェント（SSM Agent）と Amazon ECS コンテナエージェント（Amazon ECS ワークロードの実行時）AWSは、機能が追加または更新されたときに、これらのエージェントの新しいバージョンをリリースします。外部インスタンスがいずれかのエージェントの以前のバージョンを使用している場合は、次の手順を使用して更新できます。

外部インスタンスでの SSM Agent の更新

AWS Systems Managerインスタンスで SSM Agent を更新するプロセスを自動化することをお勧めします。これらは、更新を自動化するためのいくつかの方法を提供します。詳細については、AWS Systems Managerユーザーガイドの「SSM Agent の更新を自動化する」を参照してください。

外部インスタンス上の Amazon ECS エージェントを更新しています

外部インスタンスでは、Amazon ECS コンテナエージェントはecs-initパッケージをアップグレードすることで更新されます。Amazon ECS エージェントを更新しても、実行中のタスクやサービスが中断されることはありません。Amazon ECS がecs-initパッケージと署名ファイルを、各リージョンの Amazon S3 バケットに作成します。ecs-initから始まるバージョン1.52.1-1では、Amazon ECS は、外部インスタンスが使用するオペレーティングシステムとシステムアーキテクチャに応じて個別の ecs-init パッケージを提供します。

以下の表を使用して、ecs-initパッケージは、外部インスタンスが使用するオペレーティングシステムとシステムアーキテクチャに基づいてダウンロードする必要があります。

> **Note**
>
> 次のコマンドを使用して、外部インスタンスが使用するオペレーティングシステムおよびシステムアーキテクチャを決定できます。
>
> ```
> cat /etc/os-release
> uname -m
> ```

オペレーティングシステム (アーキテクチャ)	ecs-init パッケージ
CentOS 7 (x86-64) CentOS 8 (x86_64) CentOS Stream 9 (x86_64) SUSE Enterprise Server 15 (x86_64) RHEL 7 (x86_64) RHEL 8 (x86_64)	amazon-ecs-init-latest.x86_64.rpm
CentOS 7 (aarch64) CentOS 8 (aarch64) CentOS Stream 9 (aarch64)	amazon-ecs-init-latest.aarch64.rpm

オペレーティングシステム (アーキテクチャ)	ecs-init パッケージ
RHEL 7 (aarch64)	
Debian 9 (x86_64) Debian 10 (x86_64) Debian 11 (x86_64) Debian 12 (x86_64) Ubuntu 18 (x86_64) Ubuntu 20 (x86_64) Ubuntu 22 (x86_64) Ubuntu 24 (x86_64)	`amazon-ecs-init-latest.amd64.deb`
Debian 9 (aarch64) Debian 10 (aarch64) Debian 11 (aarch64) Debian 12 (aarch64) Ubuntu 18 (aarch64) Ubuntu 20 (aarch64) Ubuntu 22 (aarch64) Ubuntu 24 (aarch64)	`amazon-ecs-init-latest.arm64.deb`

Amazon ECS エージェントを更新するには、以下の手順に従います。

Amazon ECS エージェントを更新するには

1. 実行している Amazon ECS エージェントのバージョンを確認します。

```
curl -s 127.0.0.1:51678/v1/metadata | python3 -mjson.tool
```

2. オペレーティングシステムとシステムアーキテクチャー用のecs-initパッケージをダウンロードします。Amazon ECS がecs-initパッケージファイルを、各リージョンの Amazon S3 バケットに作成します。置き換えることを確認します。*<region>*コマンド内の識別子を、地理的に最も近いリージョン名 (例:us-west-2) に置き換えることを確認します。

   amazon-ecs-init-latest.x86_64.rpm

   ```
   curl -o amazon-ecs-init.rpm https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.x86_64.rpm
   ```

   amazon-ecs-init-latest.aarch64.rpm

   ```
   curl -o amazon-ecs-init.rpm https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.aarch64.rpm
   ```

   amazon-ecs-init-latest.amd64.deb

   ```
   curl -o amazon-ecs-init.deb https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.amd64.deb
   ```

   amazon-ecs-init-latest.arm64.deb

   ```
   curl -o amazon-ecs-init.deb https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.arm64.deb
   ```

3. (オプション) PGP 署名を使用して、ecs-initパッケージファイルの妥当性を検証します。

   a. GnuPG をダウンロードし、インストールします。GNUpg の詳細については、「GnuPG ウェブサイト」を参照してください。Linux システムの場合は、お使いの Linux ディストリビューションでパッケージマネージャーを使用して gpg をインストールします。

   b. Amazon ECS PGP パブリックキーを取得します。

      ```
      gpg --keyserver hkp://keys.gnupg.net:80 --recv BCE9D9A42D51784F
      ```

   c. ecs-init パッケージ署名ファイルをダウンロードします。署名は、ASCII でデタッチ済みの PGP 署名で、拡張子が .asc のファイルに保存されています。Amazon ECS は、各リー

ジョンの Amazon S3 バケットに署名ファイルを提供します。置き換えることを確認します。*<region>*コマンド内の識別子を、地理的に最も近いリージョン名 (例:us-west-2) に置き換えることを確認します。

amazon-ecs-init-latest.x86_64.rpm

```
curl -o amazon-ecs-init.rpm.asc https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.x86_64.rpm.asc
```

amazon-ecs-init-latest.aarch64.rpm

```
curl -o amazon-ecs-init.rpm.asc https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.aarch64.rpm.asc
```

amazon-ecs-init-latest.amd64.deb

```
curl -o amazon-ecs-init.deb.asc https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.amd64.deb.asc
```

amazon-ecs-init-latest.arm64.deb

```
curl -o amazon-ecs-init.deb.asc https://s3.<region>.amazonaws.com/amazon-ecs-agent-<region>/amazon-ecs-init-latest.arm64.deb.asc
```

d. キーを使用してecs-initパッケージファイルを検証します。

rpmパッケージ向け

```
gpg --verify amazon-ecs-init.rpm.asc ./amazon-ecs-init.rpm
```

debパッケージ向け

```
gpg --verify amazon-ecs-init.deb.asc ./amazon-ecs-init.deb
```

予想される出力は次のようになります。

```
gpg: Signature made Fri 14 May 2021 09:31:36 PM UTC
gpg:                using RSA key 50DECCC4710E61AF
gpg: Good signature from "Amazon ECS <ecs-security@amazon.com>" [unknown]
```

```
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: F34C 3DDA E729 26B0 79BE  AEC6 BCE9 D9A4 2D51 784F
     Subkey fingerprint: D64B B6F9 0CF3 77E9 B5FB  346F 50DE CCC4 710E 61AF
```

4. ecs-init パッケージをインストールします。

   rpmパッケージ向けは、CentOS 7、CentOS 8、および RHEL 7 に搭載されています。

   ```
   sudo yum install -y ./amazon-ecs-init.rpm
   ```

   SUSE Enterprise Server 15 の**rpm**パッケージ向け

   ```
   sudo zypper install -y --allow-unsigned-rpm ./amazon-ecs-init.rpm
   ```

   debパッケージ向け

   ```
   sudo dpkg -i ./amazon-ecs-init.deb
   ```

5. ecs サービスを再起動します。

   ```
   sudo systemctl restart ecs
   ```

6. Amazon ECS エージェントのバージョンが更新されたことを確認します。

   ```
   curl -s 127.0.0.1:51678/v1/metadata | python3 -mjson.tool
   ```

Amazon ECS クラスターを更新する

次のクラスタープロパティを変更できます。

- デフォルトのキャパシティプロバイダーを設定する

  各クラスターには、1 つ以上のキャパシティプロバイダーがあり、さらにオプションとしてキャパシティプロバイダー戦略があります。キャパシティープロバイダー戦略は、クラスターの複数のキャパシティープロバイダー間にタスクを分散する方法を決定します。スタンドアロンタスクを実行するか、サービスを作成するときは、クラスターのデフォルトのキャパシティプロバイダー戦略か、クラスターのデフォルト戦略をオーバーライドするキャパシティプロバイダー戦略のいずれかを使用します。

- Container Insights をオンにします。

  CloudWatch Container Insights は、コンテナ化されたアプリケーションおよびマイクロサービスのメトリクスとログを収集、集約、要約します。Container Insights は、問題の迅速な特定と解決に使用するコンテナの再起動失敗などの診断情報も提供します。詳細については、「the section called “オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する”」を参照してください。
- クラスターを識別しやすいようにタグを追加します。

手順

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [クラスター: ***name***] ページで、[クラスターを更新] を選択します。
5. デフォルトのキャパシティプロバイダーを設定するには、[デフォルトのキャパシティプロバイダー戦略] で [さらに追加] を選択します。

   a. [キャパシティプロバイダー] で、キャパシティプロバイダーを選択します。
   b. (オプション) [ベース] で、キャパシティプロバイダーで実行されるタスクの最小数を入力します。

      1 つのキャパシティプロバイダーには、1 つの [ベース] 値のみを設定できます。
   c. (オプション) [重み] で、指定されたキャパシティプロバイダーを使用する、起動されたタスクの合計数の相対的な割合を入力します。
   d. (オプション) 追加のキャパシティプロバイダーについて、ステップを繰り返します。
6. Container Insights をオンまたはオフにするには、[モニタリング] を展開し、[Container Insights を使用] をオンにします。
7. クラスターを識別しやすくするには、[タグ] を展開し、タグを設定します。

   [タグの追加] [タグの追加] を選択して、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。

   [タグを削除] タグのキーと値の右側にある [削除] を選択します。

8. [Update] (更新) を選択します。

Amazon ECS クラスターを削除する

クラスターの使用を終了する場合は、クラスターを削除できます。クラスターを削除すると、INACTIVE 状態に移行します。INACTIVE ステータスのクラスターは、一定期間アカウント内で検出可能なままになる場合があります。ただし、この動作は今後変更される可能性があるため、INACTIVE クラスターの永続化に頼るべきではありません。

クラスターを削除する前に、次のオペレーションを実行する必要があります。

- クラスター内のすべてのサービスを削除します。詳細については、「the section called “サービスの削除”」を参照してください。
- 現在実行中のタスクをすべて停止します。詳細については、「the section called “タスクの停止”」を参照してください。
- クラスターに登録されているすべてのコンテナインスタンスの登録を解除します。詳細については、「the section called “コンテナインスタンスの登録解除”」を参照してください。
- 名前空間を削除します。詳細については、AWS Cloud Map デベロッパーガイドの名前空間の削除を参照してください。

手順

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択します。
4. [Clusters] (クラスター) ページで、削除するクラスターを選択します。
5. ページの右上で、[Delete Cluster] (クラスターを削除) を選択します。

   クラスターに関連付けられているすべてのリソースを削除しなかった場合は、メッセージが表示されます。
6. 確認ボックスに [delete ***cluster name***] (削除 クラスター名) と入力してください。

Amazon ECS コンテナインスタンスの登録を解除する

> **Important**
>
> このトピックは、Amazon EC2 で作成されたコンテナインスタンスのみを対象としています。外部インスタンスの登録を解除する方法については、Amazon ECS 外部インスタンスの登録を解除する を参照してください。

Amazon EC2 でバックアップされたコンテナインスタンスの使用を終了する場合は、そのインスタンスをクラスターから登録解除できます。登録解除後、コンテナインスタンスは新しいタスクを受けることができなくなります。

登録解除するときにコンテナインスタンスでタスクが実行されている場合、インスタンスを削除するかタスクが他の手段で停止するまで、これらのタスクは実行されたままになります。ただし、これらのタスクは孤立しています (Amazon ECS によるモニタリングや情報収集の対象外になります)。コンテナインスタンス上の孤立したタスクが Amazon ECS サービスに含まれる場合、サービススケジューラは、可能であれば、別のコンテナインスタンスでそのタスクの別のコピーを開始します。Application Load Balancer ターゲットグループに登録されている、孤立したサービスタスクのコンテナは、すべてその登録が解除されます。これらはロードバランサーまたはターゲットグループの設定に従って Connection Draining が開始されます。awsvpc ネットワークモードを使用している孤立したタスク、その Elastic Network Interface は削除されます。

登録解除後に、コンテナインスタンスを別の用途に使用する予定の場合は、登録解除前に、コンテナインスタンスで実行中のすべてのタスクを停止する必要があります。これにより、孤立したタスクによってリソースが消費されなくなります。

コンテナインスタンスの登録を解除するときは、以下の考慮事項に注意してください。

- 各コンテナインスタンスには、それぞれに固有の状態情報があるため、1 つのクラスターから登録解除して別のクラスターに再登録しないでください。コンテナインスタンスリソースを再配置するには、1 つのクラスターからコンテナインスタンスを終了し、新しいクラスターで新しいコンテナインスタンスを起動することをお勧めします。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」および Amazon ECS Linux コンテナインスタンスの起動 を参照してください。
- コンテナインスタンスが Auto Scaling グループまたはAWS CloudFormationスタックで管理されている場合は、Auto Scaling グループを更新するか、AWS CloudFormationスタックでインスタンス

を終了します。それ以外の場合は、Auto Scaling グループまたはAWS CloudFormationにより、インスタンス終了後に新しいインスタンスが作成されます。

- 接続された Amazon ECS コンテナエージェントを使用して実行中のコンテナインスタンスを削除する場合は、エージェントによってクラスターからインスタンスが自動的に登録解除されます。停止したコンテナインスタンス、または切断されたエージェントがあるインスタンスは、終了時に自動的に登録解除されません。
- コンテナインスタンスを登録解除すると、インスタンスがクラスターから削除されますが、Amazon EC2 インスタンスは終了しません。インスタンスの使用を終了する場合は、必ずインスタンスを終了して課金を停止します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」を参照してください。

手順

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、外部インスタンスが存在するリージョンを選択します。
3. ナビゲーションペインで [Clusters] (クラスター) を選択し、インスタンスをホストするクラスターを選択します。
4. [Cluster : ***name***] (クラスター: 名前) のページで、[Infrastructure] (インフラストラクチャ) タブを選択します。
5. [Container instances] (コンテナインスタンス)で、登録解除するインスタンス ID を選択します。コンテナインスタンスの詳細ページにリダイレクトされます。
6. [Container Instance : ***id***] (コンテナインスタンス: id) ページで、[Deregister] (登録解除) を選択します。
7. 確認画面で [登録解除] を選択します。
8. コンテナインスタンスの使用を終了する場合は、基になる Amazon EC2 インスタンスを終了します。詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスの終了」を参照してください。

Amazon ECS コンテナインスタンスをドレインする

クラスターからコンテナインスタンスを削除する必要がある場合があります。例えば、システム更新を実行したり、クラスターキャパシティーをスケールダウンしたりする場合などです。Amazon ECS では、コンテナインスタンスを`DRAINING` ステータスに遷移する能力を提供します。これ

は、コンテナインスタンスのドレインと呼ばれます。コンテナインスタンスを DRAINING に設定すると、Amazon ECS によって新規タスクがそのコンテナインスタンスに配置されなくなります。

サービスのドレイニング動作

PENDING 状態にあるサービスの一部であるタスクは、直ちに停止されます。クラスター内に利用可能なコンテナインスタンス容量がある場合、サービススケジューラによって置き換えタスクが開始されます。十分なコンテナインスタンス容量がない場合、問題を示すサービスイベントメッセージが送信されます。

RUNNING 状態にあるコンテナインスタンス上のサービスの一部であるタスクは、STOPPED 状態に移行します。サービススケジューラは、サービスのデプロイタイプ、デプロイ設定パラメータ、minimumHealthyPercent および maximumPercent に従って、タスクを置き換えようとします。詳細については、Amazon ECS サービスおよびAmazon ECS サービス定義パラメータを参照してください。

- minimumHealthyPercent が 100% を下回っている場合、タスクの代替中、スケジューラは一時的に desiredCount を無視できます。例えば、desiredCount が 4 つのタスクの場合、最小値 50% でスケジューラは 2 つの既存タスクを停止してから 2 つの新規タスクを開始できます。最小が 100% の場合、サービススケジューラは、代替タスクが正常な状態と見なされるまで既存タスクを削除できません。ロードバランサーを使用しないサービスのタスクが RUNNING 状態にある場合、正常な状態と見なされます。ロードバランサーを使用するサービスのタスクは、RUNNING 状態にあり、そのタスクをホストするコンテナインスタンスがロードバランサーによって正常と報告された場合に、正常であると見なされます。

  > **Important**
  >
  > スポットインスタンスを使用していて、minimumHealthyPercent が 100% 以上の場合、サービスには、スポットインスタンスが終了する前にタスクを置き換えるための十分な時間がありません。

- maximumPercent パラメータは、タスクの置き換え中に実行できるタスク数の上限を表します。これは、置き換えのバッチサイズを定義するために使用できます。例えば、desiredCount が 4 つのタスクで、最大が 200% であればドレインされる 4 つのタスクを停止する前に 4 つの新規タスクを開始できます (これを行うために必要なクラスターリソースを使用できる場合)。最大が 100% の場合、代替タスクは、ドレインするタスクが停止するまで開始できません。

> **Important**
>
> `minimumHealthyPercent` と `maximumPercent` の両方が 100% の場合、サービスは既存のタスクを削除できず、代替タスクを開始することもできません。これにより、コンテナインスタンスのドレインの成功を防止し、新たなデプロイが防止されます。

スタンドアロンタスクのドレイニング動作

`PENDING` または `RUNNING` 状態のスタンドアロンタスクは影響を受けません。自分で停止するか、手動で停止するまで待つ必要があります。コンテナインスタンスは `DRAINING` ステータスのままです。

インスタンスで実行されているすべてのタスクが `STOPPED` 状態に移行すると、コンテナインスタンスのドレインが完了します。コンテナインスタンスは、再びアクティブ化または削除されるまで、`DRAINING` 状態のままです。コンテナインスタンス上のタスクの状態を確認するには、ListTasks オペレーションを `containerInstance` パラメータと共に使用して、インスタンス上のタスクのリストを取得した後、各 Amazon リソースネーム (ARN) または各タスクの ID で DescribeTasks オペレーションを実行して、タスクの状態を確認します。

コンテナインスタンスがタスクのホスティングを再開する準備ができたら、コンテナインスタンスの状態を `DRAINING` から `ACTIVE` に変更します。Amazon ECS サービススケジューラは、コンテナインスタンスを再度検討してタスクを配置します。

手順

次の手順に従って、新しい AWS Management Console を使用してコンテナインスタンスをドレインする設定ができます。

また、UpdateContainerInstancesState API アクションまたは update-container-instances-state コマンドを使用して、コンテナインスタンスのステータスを `DRAINING` に変更することも可能です。

AWS Management Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、インスタンスをホストするクラスターを選択します。

4. [Cluster : ***name***] (クラスター: 名前) のページで、[Infrastructure] (インフラストラクチャ) タブを選択します。次に、[Container instances] (コンテナインスタンス) タブを選択し、ドレインしたい各コンテナインスタンスのチェックボックスをオンにします。
5. [アクション]、[ドレイン] の順に選択します。

Amazon ECS コンテナエージェント

Amazon ECS エージェントは、クラスターに登録されているすべてのコンテナインスタンスで実行されるプロセスです。これにより、コンテナインスタンスと Amazon ECS の間の通信が容易になります。

> **Note**
>
> Linux コンテナインスタンスでは、エージェントコンテナは `/lib`、`/lib64`、`/proc` などの最上位ディレクトリをマウントします。これは、Amazon EBS ボリューム、`awsvpc` ネットワークモード、Amazon ECS Service Connect、FireLens – Amazon ECS といった、ECS の様々な機能を利用するために必要です。

Amazon ECSコンテナエージェントの各バージョンは、異なる機能セットをサポートし、以前のバージョンのバグ修正を提供します。可能であれば、最新バージョンの Amazon ECSコンテナエージェントを使用することを常にお勧めします。コンテナエージェントを最新バージョンに更新するには、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

どの機能と拡張が各エージェントリリースに含まれているか確認するには、https://github.com/aws/amazon-ecs-agent/releases を参照してください。

> **Important**
>
> 信頼できるメトリクスの最小 Docker バージョンは、Amazon ECS 最適化 AMI `20220607` 以降に含まれる Docker バージョン `v20.10.13` 以降です。
> バージョン `1.20.0` 以降のAmazon ECSエージェントでは、`1.9.0` より前のバージョンの Docker のサポートが廃止されました。

ライフサイクル

Amazon ECS コンテナエージェントが Amazon EC2 インスタンスをクラスターに登録すると、Amazon EC2 インスタンスのステータスは、ACTIVE として、エージェントの接続ステータスは、TRUE としてレポートされます。このコンテナインスタンスはタスクの実行リクエストを受けることができます。

コンテナインスタンスを (終了ではなく) 停止した場合、ステータスは ACTIVE のままになりますが、エージェント接続ステータスは数分以内に FALSE になります。コンテナインスタンスで実行されていたタスクはすべて停止します。コンテナインスタンスを再び開始すると、コンテナエージェントは、Amazon ECS サービスと再接続し、インスタンスでタスクを再実行できるようになります。

> **Important**
>
> コンテナインスタンスを停止して開始するか、再起動した場合、Amazon ECS コンテナエージェントの以前の一部のバージョンは、元のコンテナインスタンス ID を登録解除せずに、そのインスタンスを再登録します。この場合、 Amazon ECS では、クラスター内のコンテナインスタンスが実際の数より多く一覧表示されます。(同じ Amazon EC2 インスタンス ID に対してコンテナインスタンス ID が重複している場合は、重複しているコンテナインスタンスのうち、インスタンスのステータスが ACTIVE でエージェントの接続ステータスが FALSE になっているものを安全に登録解除できます。) この問題は、最新のバージョンの Amazon ECS コンテナエージェントで修正されています。最新バージョンへの更新の詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

コンテナインスタンスのステータスを DRAINING に変更すると、新しいタスクはそのコンテナインスタンスに配置されません。そのコンテナインスタンスで実行されているサービスタスクは、可能な場合は削除され、システム更新を実行できるようになります。詳細については、「Amazon ECS コンテナインスタンスをドレインする」を参照してください。

コンテナインスタンスを登録解除または終了した場合、コンテナインスタンスのステータスは直ちに INACTIVE に変わり、コンテナインスタンスを一覧表示しても、そのコンテナインスタンスはレポートされなくなります。ただし、終了後 1 時間は、コンテナインスタンスの内容を表示できます。1 時間後、インスタンスの内容は表示できなくなります。

> **Important**
>
> インスタンスを手動でドレインさせるか、Auto Scaling グループのライフサイクルフックを構築して、インスタンスの状態を DRAINING にさせます。Auto Scaling ライフサイクルフックの詳細については、「Amazon EC2 Auto Scaling ライフサイクルフック」を参照してください。

Amazon ECS に最適化された AMI

Amazon ECS に最適化された AMI の Linux バリアントは、Amazon Linux 2 AMI をベースとして使用しています。各バリアントの Amazon Linux 2 ソース AMI 名を取得するには、Systems Manager Parameter Store API をクエリします。詳細については、「Amazon ECS に最適化された Linux AMI メタデータを取得する」を参照してください。Amazon ECS に最適化された最新の Amazon Linux 2 AMI からコンテナインスタンスを起動すると、現行バージョンのコンテナエージェントを取得できます。最新の Amazon ECS 対応 Amazon Linux 2 AMI を使用してコンテナインスタンスを起動するには、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

追加情報

次のページでは、変更に関する追加情報を説明します。

- GitHub の Amazon ECS Agent の変更ログ
- `ecs-init` アプリケーションのソースコード、エージェントをパッケージ化するためのスクリプトと構成は、エージェントリポジトリの一部になりました。`ecs-init` の古いバージョンおよびパッケージについては、GitHub で「Amazon ecs-init の変更ログ」を参照してください。
- Amazon Linux 2 リリースノート。
- Docker ドキュメントの「Docker Engine リリースノート」
- NVIDIA ドキュメントの「NVIDIA ドライバードキュメント」

Amazon ECS コンテナエージェントの設定

適用対象: EC2 インスタンス

Amazon ECS コンテナエージェントでは、多数の設定オプションがサポートされており、そのほとんどは環境変数を介して設定します。

コンテナインスタンスが Amazon ECS に最適化されたAMIの Linux バリアントを使用して起動された場合は、これらの環境変数を /etc/ecs/ecs.config ファイルに設定してからエージェントを再び開始できます。起動時に Amazon EC2 ユーザーデータを使用して、コンテナインスタンスにこれらの設定変数を作成することもできます。詳細については、「Amazon ECS Linux コンテナインスタンスをブートストラップしてデータを渡す」を参照してください。

コンテナインスタンスが Amazon ECS に最適化された AMI の Windows バリアントを使用して起動された場合は、PowerShell SetEnvironmentVariable コマンドを使用して、これらの環境変数を設定してからエージェントを再び開始できます。詳細については、「Amazon EC2 ユーザーガイド」の「ユーザーデータ入力を使用して EC2 インスタンスを起動するときにコマンドを実行する」および「the section called “コンテナインスタンスのブートストラップ”」を参照してください。

Amazon ECS コンテナエージェントを手動で開始する場合 (Amazon ECSに最適化されていない AMI い場合)、これらの環境変数は、エージェントの起動に使用する docker run コマンドで使用できます。これらの変数は構文 --env=*VARIABLE_NAME*=*VARIABLE_VALUE* で使用します。プライベートリポジトリの認証情報など、機密性の高い情報の場合は、エージェントの環境変数をファイルに保存し、--env-file *path_to_env_file* オプションを使用して、それらすべてを一度に渡す必要があります。以下のコマンドを使用して変数を追加できます。

```
sudo systemctl stop ecs
sudo vi /etc/ecs/ecs.config
# And add the environment variables with VARIABLE_NAME=VARIABLE_VALUE format.
sudo systemctl start ecs
```

使用できるパラメータ

使用可能な Amazon ECS コンテナエージェントの設定パラメータについては、GitHub の「Amazon ECS コンテナエージェント」を参照してください。

Amazon S3 に Amazon ECS コンテナインスタンスの設定を保存する

Amazon ECS コンテナエージェントの設定は、環境変数によって制御されます。Amazon ECS に最適化されたAMIの Linux バリアントは、コンテナエージェントの起動時に /etc/ecs/ecs.config でこれらの変数を検索し、見つかった変数に応じてエージェントを設定します。ECS_CLUSTER などの機密性の低い環境変数は、Amazon EC2 のユーザーデータを経由して起動時にコンテナインスタンスに渡され、そのままこのファイルに書き込まれます。ただし、AWS 認証情報や ECS_ENGINE_AUTH_DATA 変数など機密性の高い情報は、ユーザーデータでインスタンスに渡したり、.bash_history ファイルに表示される可能性のある方法で /etc/ecs/ecs.config に書き込んだりしないでください。

設定情報を Amazon S3 のプライベートバケットに保存し、コンテナインスタンスの IAM ロールに読み取り専用アクセス権限を付与するのが、コンテナインスタンスの起動時に設定を許可する安全で便利な方法です。`ecs.config` ファイルのコピーはプライベートバケットに保存できます。その後、AWS CLI Amazon EC2 ユーザーデータを使用してをインストールし、インスタンスの起動時に設定情報を `/etc/ecs/ecs.config` にコピーできます。

`ecs.config` Amazon S3 のファイルを保存するには

1. コンテナインスタンスロール (ecsInstanceRole) に、Amazon S3 への読み取り専用アクセス権を持つ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、AmazonS3ReadOnlyAccess を `ecsInstanceRole` ロールに割り当てます。ポリシーをロールにアタッチする方法については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。
2. 次の形式を使用して、有効な Amazon ECS エージェントの設定変数を含む `ecs.config` ファイルを作成します。この例では、プライベートレジストリ認証を設定しています。詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

   ```
   ECS_ENGINE_AUTH_TYPE=dockercfg
   ECS_ENGINE_AUTH_DATA={"https://index.docker.io/v1/":
   {"auth":"zq212MzEXAMPLE7o6T25Dk0i","email":"email@example.com"}}
   ```

   > **Note**
   >
   > 利用可能な Amazon ECS エージェントの設定変数の完全なリストについては、GitHub の「Amazon ECS コンテナエージェント」を参照してください。

3. 設定ファイルを保存するには、Amazon S3 内にプライベートバケットを作成します。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「バケットの作成」を参照してください。
4. `ecs.config` ファイルを S3 バケットにアップロードします。詳細については、Amazon Simple Storage Service 開発者ガイドの「オブジェクトのアップロード」を参照してください。

起動時に **`ecs.config`** ファイルを Amazon S3 からロードするには

1. このセクションの上記の手順を完了して、読み取り専用 Amazon S3 アクセス権限をコンテナインスタンスに許可し、 `ecs.config` ファイルをプライベート S3 バケットに保存します。

2. 新しいコンテナインスタンスを起動し、EC2 ユーザーデータで次のサンプルスクリプトを使用します。このスクリプトは AWS CLI をインストールし、設定ファイルを `/etc/ecs/ecs.config` にコピーします。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

```
#!/bin/bash
yum install -y aws-cli
aws s3 cp s3://your_bucket_name/ecs.config /etc/ecs/ecs.config
```

Amazon ECS コンテナエージェントをインストールする

Amazon ECS クラスターに Amazon EC2 インスタンスを登録する必要があり、そのインスタンスが Amazon ECS に最適化された AMI に基づく AMI を使用していない場合は、次の手順を使用して Amazon ECS コンテナエージェントを手動でインストールできます。これを行うには、リージョンの Amazon S3 バケットのいずれかから、または Amazon Elastic Container Registry Public からエージェントをダウンロードできます。リージョンの Amazon S3 バケットのいずれかからダウンロードする場合は、必要に応じて、PGP 署名を使用してコンテナエージェントファイルの有効性を検証できます。

> **Note**
>
> Amazon ECS と Docker サービスの両方の `systemd` ユニットには、両方のサービスを開始する前に `cloud-init` が終了するのを待つディレクティブがあります。Amazon EC2ユーザーデータの実行が終了するまで、`cloud-init` プロセスは終了したと見なされません。したがって、Amazon EC2 ユーザーデータを介して Amazon ECS または Docker を起動すると、デッドロックが発生する可能性があります。Amazon EC2 ユーザーデータを使用してコンテナエージェントを起動するには、`systemctl enable --now --no-block ecs.service` を使用できます。

非 Amazon Linux EC2 インスタンスに Amazon ECS コンテナエージェントをインストールする

Amazon EC2 インスタンスに Amazon ECS コンテナエージェントをインストールするには、リージョンの Amazon S3 バケットのいずれかからエージェントをダウンロードしてインストールできます。

> **Note**
>
> Amazon Linux AMI 以外を使用する場合、Amazon ECS エージェントがタスクレベルのリソース制限をサポートするためには、Amazon EC2 インスタンスは `cgroup` ドライバーの `cgroupfs` サポートが必要です。詳細については、GitHub で Amazon ECS エージェントについて参照してください。

各システムアーキテクチャの最新 Amazon ECS コンテナエージェントファイルは、リージョン別に参考として以下に示します。

リージョン	リージョン名	Amazon ECS init deb ファイル	Amazon ECS init rpm ファイル
us-east-2	米国東部 (オハイオ)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
us-east-1	米国東部 (バージニア北部)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
us-west-1	米国西部 (北カリフォルニア)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
us-west-2	米国西部 (オレゴン)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)

リージョン	リージョン名	Amazon ECS init deb ファイル	Amazon ECS init rpm ファイル
ap-east-1	アジアパシフィック (香港)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
ap-northeast-1	アジアパシフィック (東京)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
ap-northeast-2	アジアパシフィック (ソウル)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
ap-south-1	アジアパシフィック (ムンバイ)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
ap-southeast-1	アジアパシフィック (シンガポール)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
ap-southeast-2	アジアパシフィック (シドニー)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)

リージョン	リージョン名	Amazon ECS init deb ファイル	Amazon ECS init rpm ファイル
ca-central-1	カナダ (中部)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
eu-central-1	欧州 (フランクフルト)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
eu-west-1	欧州 (アイルランド)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
eu-west-2	欧州 (ロンドン)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
eu-west-3	欧州 (パリ)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
sa-east-1	南米 (サンパウロ)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 Amazon ECS init aarch64 (aarch64)

リージョン	リージョン名	Amazon ECS init deb ファイル	Amazon ECS init rpm ファイル
us-gov-east-1	AWS GovCloud (米国東部)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)
us-gov-west-1	AWS GovCloud (米国西部)	Amazon ECS init amd64 (amd64) Amazon ECS init arm64 (arm64)	Amazon ECS init x86_64 (x86_64) Amazon ECS init aarch64 (aarch64)

非 Amazon Linux AMI を使用した Amazon EC2 インスタンスに Amazon ECS コンテナエージェントをインストールするには

1. Amazon ECSへのアクセスを許可する IAM; ロールを使用して Amazon EC2インスタンスを起動します。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。
2. インスタンスに接続します。
3. 最新バージョンの Docker をインスタンスにインストールします。
4. Docker のバージョンをチェックして、システムがバージョンの最小要件を満たしていることを確認します。

> **Note**
>
> 信頼できるメトリクスの最小 Docker バージョンは、Amazon ECS 最適化 AMI 20220607 以降に含まれる Docker バージョン v20.10.13 以降です。
> バージョン 1.20.0 以降のAmazon ECSエージェントでは、1.9.0 より前のバージョンの Docker のサポートが廃止されました。

```
docker --version
```

5. オペレーティングシステムとシステムアーキテクチャ用の適切な Amazon ECS エージェントファイルをダウンロードし、インストールします。

   deb アーキテクチャの場合:

   ```
   ubuntu:~$ curl -O https://s3.us-west-2.amazonaws.com/amazon-ecs-agent-us-west-2/amazon-ecs-init-latest.amd64.deb
   ubuntu:~$ sudo dpkg -i amazon-ecs-init-latest.amd64.deb
   ```

   rpm アーキテクチャの場合:

   ```
   fedora:~$ curl -O https://s3.us-west-2.amazonaws.com/amazon-ecs-agent-us-west-2/amazon-ecs-init-latest.x86_64.rpm
   fedora:~$ sudo yum localinstall -y amazon-ecs-init-latest.x86_64.rpm
   ```

6. /lib/systemd/system/ecs.service ファイルを編集し、[Unit] セクションの最後に次の行を追加します。

   ```
   After=cloud-final.service
   ```

7. (オプション) インスタンスを default クラスター以外のクラスターに登録するには、/etc/ecs/ecs.config ファイルを編集して以下の内容を追加します。次の例は MyCluster クラスターを指定します。

   ```
   ECS_CLUSTER=MyCluster
   ```

   これらや他のエージェントランタイムオプションの詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

   > **Note**
   >
   > オプションで、エージェント環境変数を Amazon S3 に保存できます (これらの環境変数は、Amazon EC2 ユーザーデータを使用して、起動時にコンテナインスタンスにダウンロードできます)。これは、プライベートリポジトリの認証情報のような機密情報の場合に推奨されます。詳細については、Amazon S3 に Amazon ECS コンテナインスタンスの設定を保存するおよびAmazon ECS での AWS 以外のコンテナイメージの使用を参照してください。

8. ecs サービスを開始します。

```
ubuntu:~$ sudo systemctl start ecs
```

ホストネットワークモードで Amazon ECS エージェントを実行する

Amazon ECSコンテナエージェントを実行している場合、ecs-init は host ネットワークモードでコンテナエージェントのコンテナを作成します。これは、コンテナエージェントのコンテナでサポートされている唯一のネットワークモードです。

これにより、コンテナエージェントにより開始されたコンテナの Amazon EC2 インスタンスのメタデータサービスエンドポイント (http://169.254.169.254) へのアクセスをブロックできます。これにより、コンテナはコンテナインスタンスプロファイルから IAM ロール認証情報にアクセスできなくなります。また、タスクでは IAM タスクロールの認証情報のみが使用されます。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

また、コンテナエージェントが docker0 ブリッジ上の接続とネットワークトラフィックで競合しないようにもできます。

Amazon ECS コンテナエージェントのログ設定パラメータ

Amazon ECS コンテナエージェントは、コンテナインスタンスのログを保存します。

コンテナエージェントバージョン 1.36.0 以降の場合、デフォルトでは、ログは Linux インスタンスの /var/log/ecs/ecs-agent.log および Windows インスタンスの C:\ProgramData\Amazon\ECS\log\ecs-agent.log にあります。

コンテナエージェントバージョン 1.35.0 以前の場合、デフォルトでは、ログは Linux インスタンスの /var/log/ecs/ecs-agent.log.*timestamp* および Windows インスタンスの C:\ProgramData\Amazon\ECS\log\ecs-agent.log.*timestamp* にあります。

デフォルトでは、エージェントログは 1 時間ごとにローテーションされ、最大 24 個のログが保存されます。

以下のコンテナエージェントの設定変数は、エージェントのデフォルトのログ記録動作を変更するために使用できます。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

ECS_LOGFILE

値の例: /ecs-agent.log

Linux のデフォルト値: Null

Windows のデフォルト値: Null

エージェントログを書き込む場所。Amazon ECS-最適化 AMI を使用する際のデフォルトの方法である ecs-init 経由でエージェントを実行している場合、コンテナ内のパスは、/log になり、ecs-init はホスト上の /var/log/ecs/ にマウントします。

ECS_LOGLEVEL

値の例:crit 、error、warn、info、debug

Linux のデフォルト値: info

Windows のデフォルト値: info

ログに記録する詳細レベル。

ECS_LOGLEVEL_ON_INSTANCE

値の例:none、 crit、 error、 warn、 info、 debug

Linux のデフォルト値:noneに明確に空でない値が設定されている場合はECS_LOG_DRIVER、それ以外の場合はECS_LOGLEVELと同じ値

Windows のデフォルト値:noneに明確に空ではない値が設定されている場合はECS_LOG_DRIVER、それ以外の場合はECS_LOGLEVELと同じ値

ECS_LOGLEVELをオーバーライドして、ロギングドライバーに記録されるレベルとは別に、オンインスタンスのログファイルに記録される必要のある詳細レベルを設定するために使用できます。ロギングドライバが明確に設定されている場合、インスタンス上のログはデフォルトでオフになります。この変数で再び有効にできます。

ECS_LOG_DRIVER

値の例: awslogs、fluentd、gelf、json-file、journald、logentries、syslog、splunk

Linux のデフォルト値: json-file

Windows のデフォルト値: 該当しません

エージェントコンテナが使用するロギングドライバを決定します。

ECS_LOG_ROLLOVER_TYPE

値の例: size、hourly

Linux のデフォルト値: hourly

Windows のデフォルト値: hourly

コンテナエージェントのログファイルを 1 時間ごとに更新するか、サイズに基づいて更新するかを決定します。デフォルトでは、エージェントのログファイルは 1 時間ごとに更新されます。

ECS_LOG_OUTPUT_FORMAT

値の例: logfmt、json

Linux のデフォルト値: logfmt

Windows のデフォルト値: logfmt

ログ出力形式を決定します。json 形式を使用すると、ログの各行は構造化された JSON マップになります。

ECS_LOG_MAX_FILE_SIZE_MB

値の例: 10

Linux のデフォルト値: 10

Windows のデフォルト値: 10

ECS_LOG_ROLLOVER_TYPE 変数を size に設定すると、この変数は、更新前のログファイルの最大サイズ (MB 単位) を決定します。ロールオーバータイプを hourly に設定すると、この変数は無視されます。

ECS_LOG_MAX_ROLL_COUNT

値の例: 24

Linux のデフォルト値: 24

Windows のデフォルト値: 24

更新済みログファイルを保持する数を決定します。この制限に達すると、より古いログファイルは削除されます。

コンテナエージェントバージョン 1.36.0 以降では、logfmt 形式を使用した場合のログファイルは以下の例のようになります。

```
level=info time=2019-12-12T23:43:29Z msg="Loading configuration" module=agent.go
```

```
level=info time=2019-12-12T23:43:29Z msg="Image excluded from cleanup: amazon/amazon-
ecs-agent:latest" module=parse.go
level=info time=2019-12-12T23:43:29Z msg="Image excluded from cleanup: amazon/amazon-
ecs-pause:0.1.0" module=parse.go
level=info time=2019-12-12T23:43:29Z msg="Amazon ECS agent Version: 1.36.0, Commit:
 ca640387" module=agent.go
level=info time=2019-12-12T23:43:29Z msg="Creating root ecs cgroup: /ecs"
 module=init_linux.go
level=info time=2019-12-12T23:43:29Z msg="Creating cgroup /ecs"
 module=cgroup_controller_linux.go
level=info time=2019-12-12T23:43:29Z msg="Loading state!" module=statemanager.go
level=info time=2019-12-12T23:43:29Z msg="Event stream ContainerChange start
 listening..." module=eventstream.go
level=info time=2019-12-12T23:43:29Z msg="Restored cluster 'auto-robc'" module=agent.go
level=info time=2019-12-12T23:43:29Z msg="Restored from checkpoint file. I
 am running as 'arn:aws:ecs:us-west-2:0123456789:container-instance/auto-
robc/3330a8a91d15464ea30662d5840164cd' in cluster 'auto-robc'" module=agent.go
```

JSON 形式を使用した場合のログファイルは以下の例のようになります。

```
{"time": "2019-11-07T22:52:02Z", "level": "info", "msg": "Starting Amazon Elastic
 Container Service Agent", "module": "engine.go"}
```

コンテナエージェントバージョン 1.35.0 以前では、ログファイルの形式は以下のようになります。

```
2016-08-15T15:54:41Z [INFO] Starting Agent: Amazon ECS Agent - v1.12.0 (895f3c1)
2016-08-15T15:54:41Z [INFO] Loading configuration
2016-08-15T15:54:41Z [WARN] Invalid value for task cleanup duration, will be overridden
 to 3h0m0s, parsed value 0, minimum threshold 1m0s
2016-08-15T15:54:41Z [INFO] Checkpointing is enabled. Attempting to load state
2016-08-15T15:54:41Z [INFO] Loading state! module="statemanager"
2016-08-15T15:54:41Z [INFO] Detected Docker versions [1.17 1.18 1.19 1.20 1.21 1.22]
2016-08-15T15:54:41Z [INFO] Registering Instance with ECS
2016-08-15T15:54:41Z [INFO] Registered! module="api client"
```

プライベート Docker イメージ用の Amazon ECS コンテナインスタンスを設定する

Amazon ECS コンテナエージェントは、基本認証を使用してプライベートレジストリで認証できます。プライベートレジストリ認証を有効にすると、タスク定義のプライベート Docker イメージを使用できます。この機能は、EC2 起動タイプを使用するタスクでのみサポートされています。

プライベートレジストリ認証を有効にする別の方法では、AWS Secrets Manager を使用して、プライベートレジストリ認証情報を安全に保存してから、コンテナの定義で参照します。これにより、プライベートリポジトリのイメージをタスクで使用できるようになります。このメソッドは、EC2 または Fargate 起動タイプのいずれかを使用するタスクをサポートします。詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。

Amazon ECS コンテナエージェントでは、起動時に次の 2 つの環境変数を検索します。

- `ECS_ENGINE_AUTH_TYPE`。送信する認証データのタイプを指定します。
- `ECS_ENGINE_AUTH_DATA`。実際の認証情報が含まれます。

Amazon ECSに最適化されたAMIのLinuxバリアントは、コンテナインスタンスの起動時、およびサービスが開始されるたびに (sudo start ecs コマンドを使用して)、`/etc/ecs/ecs.config` ファイルをスキャンしてこれらの変数を探します。Amazon ECSに最適化されていないAMIは、これらの環境変数をファイルに保存し、`--env-file` *`path_to_env_file`*オプションを付けてコンテナエージェントを起動するdocker runコマンドに渡す必要があります。

> **Important**
>
> これらの認証環境変数を、 Amazon EC2 ユーザーデータを使用してインスタンス起動時に挿入することや、`--env` オプションを使用して docker run コマンドに渡すことはお勧めしません。これらの方法は、認証情報などの機密データには適していません。認証情報をコンテナインスタンスに安全に追加する方法については、「Amazon S3 に Amazon ECS コンテナインスタンスの設定を保存する」を参照してください。

認証形式

プライベートレジストリ認証には、`dockercfg` と `docker` の 2 つの形式を使用できます。

dockercfg 認証形式

`dockercfg` 形式は、docker login コマンドの実行時に作成した設定ファイルに保存されている認証情報を使用します。このファイルを作成するには、ローカルシステムで docker login を実行し、レジストリのユーザー名、パスワード、および E メールアドレスを入力します。コンテナインスタンスにログインして、そこでコマンドを実行することもできます。Docker のバージョンによって、ファイルは `~/.dockercfg` または `~/.docker/config.json` として保存されます。

```
cat ~/.docker/config.json
```

出力:

```
{
  "auths": {
    "https://index.docker.io/v1/": {
      "auth": "zq212MzEXAMPLE7o6T25Dk0i"
    }
  }
}
```

> **Important**
>
> Docker の新しいバージョンは、外部 auths オブジェクトを使用して、上に示したような設定ファイルを作成します。Amazon ECS エージェントは、auths オブジェクトを持たない、以下の形式の dockercfg 認証データのみをサポートします。jq ユーティリティをインストール済みである場合、このデータは cat ~/.docker/config.json | jq .auths コマンドを使用して抽出できます。

```
cat ~/.docker/config.json | jq .auths
```

出力:

```
{
  "https://index.docker.io/v1/": {
    "auth": "zq212MzEXAMPLE7o6T25Dk0i",
    "email": "email@example.com"
  }
}
```

上記の例では、以下の環境変数を、Amazon ECS コンテナエージェントが実行時にロードする環境変数ファイル (/etc/ecs/ecs.config Amazon ECSに最適化された AMI の場合は) に追加しなければなりません。Amazon ECS に最適化された AMI を使用せず、 docker run を使用して手動でエージェントを開始する場合は、エージェント開始時に --env-file *path_to_env_file* オプションを使用して環境変数ファイルを指定します。

```
ECS_ENGINE_AUTH_TYPE=dockercfg
```

```
ECS_ENGINE_AUTH_DATA={"https://index.docker.io/v1/":
{"auth":"zq212MzEXAMPLE7o6T25Dk0i","email":"email@example.com"}}
```

次の構文を使用して複数のプライベートレジストリを設定できます。

```
ECS_ENGINE_AUTH_TYPE=dockercfg
ECS_ENGINE_AUTH_DATA={"repo.example-01.com":
{"auth":"zq212MzEXAMPLE7o6T25Dk0i","email":"email@example-01.com"},"repo.example-02.com":
{"auth":"fQ172MzEXAMPLEoF7225DU0j","email":"email@example-02.com"}}
```

docker 認証形式

docker 形式は、エージェントが認証する必要があるレジストリサーバーの JSON 表現を使用します。また、そのレジストリに必要な認証パラメータ (ユーザー名、パスワード、およびそのアカウントの E メールアドレスなど) も含まれます。Docker Hub アカウントの場合、JSON 表現は次のようになります。

```
{
  "https://index.docker.io/v1/": {
    "username": "my_name",
    "password": "my_password",
    "email": "email@example.com"
  }
}
```

この例では、以下の環境変数を、Amazon ECS コンテナエージェントが実行時にロードする環境変数ファイル (/etc/ecs/ecs.config Amazon ECSに最適化された AMI の場合は) に追加する必要があります。Amazon ECS に最適化された AMI を使用せず、 docker run を使用して手動でエージェントを開始する場合は、エージェント開始時に `--env-file` *path_to_env_file* オプションを使用して環境変数ファイルを指定します。

```
ECS_ENGINE_AUTH_TYPE=docker
ECS_ENGINE_AUTH_DATA={"https://index.docker.io/v1/":
{"username":"my_name","password":"my_password","email":"email@example.com"}}
```

次の構文を使用して複数のプライベートレジストリを設定できます。

```
ECS_ENGINE_AUTH_TYPE=docker
```

```
ECS_ENGINE_AUTH_DATA={"repo.example-01.com":
{"username":"my_name","password":"my_password","email":"email@example-01.com"},"repo.example-02
{"username":"another_name","password":"another_password","email":"email@example-02.com"}}
```

手順

以下の手順を使用して、コンテナインスタンスのプライベートレジストリをオン状態にします。

Amazon ECS に最適化された AMI のプライベートレジストリを有効にするには

1. SSH を使用してコンテナインスタンスにログインします。
2. /etc/ecs/ecs.config ファイルを開いて、レジストリとアカウントの ECS_ENGINE_AUTH_TYPE 値と ECS_ENGINE_AUTH_DATA 値を追加します。

   ```
   sudo vi /etc/ecs/ecs.config
   ```

   この例では Docker Hub のユーザーアカウントが認証されます。

   ```
   ECS_ENGINE_AUTH_TYPE=docker
   ECS_ENGINE_AUTH_DATA={"https://index.docker.io/v1/":
   {"username":"my_name","password":"my_password","email":"email@example.com"}}
   ```

3. エージェントが ECS_DATADIR 環境変数を使用して状態を保存しているかどうかを確認します。

   ```
   docker inspect ecs-agent | grep ECS_DATADIR
   ```

   出力:

   ```
   "ECS_DATADIR=/data",
   ```

   > **Important**
   >
   > 前のコマンドで ECS_DATADIR 環境変数が返されない場合は、エージェントを停止する前に、このコンテナインスタンスで実行されているタスクをすべて停止する必要があります。より新しいエージェントは ECS_DATADIR 環境変数を使用して状態を保存するため、タスクが実行中でも問題なく停止および起動できます。詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

4. ecs サービスを停止します。

```
sudo stop ecs
```

出力:

```
ecs stop/waiting
```

5. ecs サービスを再起動します。

- Amazon ECS に最適化された Amazon Linux 2 AMI の場合:

```
sudo systemctl restart ecs
```

- Amazon ECS に最適化された Amazon Linux AMI の場合:

```
sudo stop ecs && sudo start ecs
```

6. (オプション) エージェント詳細分析 API オペレーションをクエリして、エージェントが実行されていることを確認し、新しいコンテナインスタンスに関する情報の一部を表示できます。詳細については、「the section called “コンテナの詳細分析”」を参照してください。

```
curl http://localhost:51678/v1/metadata
```

Amazon ECS タスクとイメージの自動クリーンアップ

タスクがコンテナインスタンスに配置されるたびに、Amazon ECS コンテナエージェントによって、タスクが参照するイメージがリポジトリの指定されたタグの最新版であるかどうかが確認されます。そうでない場合、デフォルトの動作では、エージェントがそれぞれのリポジトリからイメージを取得します。タスクやサービスで頻繁にイメージを更新する場合は、コンテナインスタンスのストレージが、もう使用しておらず、今後使用する予定もない Docker イメージですぐにいっぱいになってしまいます。例えば、継続的な統合や継続的なデプロイ (CI/CD) パイプラインを使用している場合です。

> **Note**
>
> Amazon ECS エージェントイメージのプル動作は、ECS_IMAGE_PULL_BEHAVIOR パラメータを使用してカスタマイズできます。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

同様に、停止したタスクに属するコンテナも、ログ情報、データボリューム、その他の生成物でコンテナインスタンスストレージを消費します。これらの生成物は、コンテナが予期せずに停止した場合のデバッグには役に立ちますが、このストレージのほとんどが一定期間後は安全に解放できます。

デフォルトでは、Amazon ECS コンテナエージェントによって、停止したタスクとコンテナインスタンスのどのタスクでも使用されていない Docker イメージがクリーンアップされます。

> **Note**
>
> 自動イメージクリーンアップ機能には、Amazon ECS コンテナエージェントのバージョン 1.13.0 以上が必要です。エージェントを最新バージョンに更新するには、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

以下のエージェント設定変数を使用して、タスクとイメージの自動クリーンアップの使い勝手を調整できます。コンテナインスタンスでこれらの変数を設定する方法の詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

`ECS_ENGINE_TASK_CLEANUP_WAIT_DURATION`

この変数は、停止されたタスクに属するコンテナを削除するまでの待機時間を指定します。イメージクリーンアッププロセスは、そのイメージを参照するコンテナがある限りイメージを削除できません。イメージがコンテナ (停止または実行中) から参照されなくなり、そのイメージがクリーンアップの対象になります。デフォルトでは、このパラメータは 3 時間に設定されていますが、アプリケーションでの必要に応じて、最短で 1 秒まで短縮できます。値を 1 秒未満に設定した場合、パラメータは無視されます。

`ECS_DISABLE_IMAGE_CLEANUP`

この変数を `true` に設定した場合は、コンテナインスタンスでのイメージの自動クリーンアップはオフになり、イメージの自動的な削除は実行されません。

ECS_IMAGE_CLEANUP_INTERVAL

この変数は、イメージの自動クリーンアッププロセスが削除するイメージをチェックする頻度を指定します。デフォルトでは 30 分ごとですが、より頻繁にイメージを削除するには最短で 10 分まで短くできます。

ECS_IMAGE_MINIMUM_CLEANUP_AGE

この変数は、イメージが取得されてから、削除の対象になるまでの期間の最短時間を指定します。これは、取得されたばかりのイメージがクリーンアップされるのを防ぐために使用されます。デフォルトは 1 時間です。

ECS_NUM_IMAGES_DELETE_PER_CYCLE

この変数は、1 つのクリーンアップサイクルで削除するイメージの数を指定します。デフォルトは 5 で、最小は 1 です。

Amazon ECS コンテナエージェントが実行中でありイメージの自動クリーンアップがオフになっていない場合、エージェントは ECS_IMAGE_CLEANUP_INTERVAL 変数で決定された頻度で、実行中または停止されたコンテナから参照されていない Docker イメージをチェックします。使用されていないイメージが見つかり、それらが ECS_IMAGE_MINIMUM_CLEANUP_AGE 変数で指定された最短クリーンアップ時間よりも古い場合、エージェントは ECS_NUM_IMAGES_DELETE_PER_CYCLE 変数で指定された最大数までイメージを削除します。最後に参照された日時が最も古いイメージから順に削除されます。イメージが削除されると、エージェントは次の間隔まで待ってから、再度プロセスを繰り返します。

Amazon ECS でコンテナをスケジュールする

Amazon Elastic Container Service (Amazon ECS) は、コンテナ化されたワークロードに柔軟なスケジューリング機能を提供する共有状態のオプティミスティックな並列システムです。Amazon ECS スケジューラはAmazon ECS API と同じクラスターの状態情報を利用して、適切な配置を決定します。

Amazon ECS は、長時間実行されるタスクおよびアプリケーションにサービススケジューラを提供します。バッチジョブまたは単一実行タスクに対してスタンドアロンタスクまたはスケジュールされたタスクを手動で実行することもできます。ニーズに最適なタスクを実行するためのタスク配置戦略や制約を指定できます。例えば、タスクを複数のアベイラビリティーゾーンにまたがって実行するか、単一のアベイラビリティーゾーン内で実行するかを指定できます。さらに、オプションとして、独自のカスタムまたはサードパーティーのスケジューラでタスクを統合することもできます。

オプション	どのようなときに使うか	詳細情報
サービス	サービススケジューラは、長期実行するステートレスサービスやアプリケーションに適しています。サービススケジューラはオプションで、タスクがElastic Load Balancing ロードバランサーに登録されていることも確認します。サービススケジューラで維持されているサービスを更新できます。これには、新しいタスク定義のデプロイや、実行中のタスクの必要数の変更が含まれる場合があります。デフォルトでは、サービススケジューラによってタスクは複数のアベイラビリティーゾーン間で分散されます。ただし、タスク配置戦略と制約を	Amazon ECS サービス

オプション	どのようなときに使うか	詳細情報
	使用すると、タスク配置の決定をカスタマイズできます。	
スタンドアロンのタスク	スタンドアロンタスクは、作業を実行してから停止するバッチジョブなどのプロセスに適しています。例えば、キューに作業が入ったときに RunTask を呼び出す処理を入れることができます。タスクはキューから作業を引き出し、作業を実行して、その後終了します。RunTaskを使用すると、デフォルトのタスク配置戦略でクラスター全体にタスクをランダムに分散させることができます。これにより、単一のインスタンスが不均衡な数のタスクを取得する可能性を最小限に抑えることができます。	Amazon ECS スタンドアロンタスク

オプション	どのようなときに使うか	詳細情報
スケジュールされたタスク	スケジュールされたタスクは、クラスター内で設定された間隔で実行するタスクがある場合に適しており、EventBridge Scheduler を使用してスケジュールを作成できます。バックアップ操作またはログスキャンのタスクを実行できます。作成する EventBridge Scheduler のスケジュールは、指定した時間にクラスター内の 1 つ以上のタスクを実行できます。スケジュールされたイベントは、特定の間隔 (*N* 分、時間または日ごとに実行されます) に設定できます。それ以外の場合、より複雑なスケジューリングには、`cron` 表現を使用できます。	Amazon EventBridge スケジューラを使用して Amazon ECS タスクをスケジュールする

コンピューティングオプション

Amazon ECS では、タスクまたはサービスを実行するインフラストラクチャを指定できます。キャパシティープロバイダー戦略または起動タイプを使用できます。

Fargate の場合、キャパシティープロバイダーは Fargate と Fargate Spot です。EC2 の場合、キャパシティープロバイダーは登録されたコンテナインスタンスを持つ Auto Scaling グループです。

キャパシティープロバイダー戦略は、クラスターに関連付けられたキャパシティープロバイダー全体にタスクを分散します。

キャパシティプロバイダー戦略では、クラスターに既に関連付けられており、`ACTIVE` または `UPDATING` ステータスを持つキャパシティプロバイダーのみを使用できます。クラスターの作成時に、キャパシティプロバイダーをクラスターに関連付けることができます。

キャパシティプロバイダー戦略では、オプションのベース値は、指定されたキャパシティプロバイダーで実行されるタスクの最小限の数を指定します。キャパシティープロバイダー戦略では、ベースを定義できるキャパシティープロバイダーは 1 つだけです。

ウェイト値は、指定したキャパシティプロバイダーを使用する起動済みタスクの総数に対する相対的な割合を決定します。次の例を考えます。2 つのキャパシティプロバイダーを含む戦略があり、両方の重みが 1 であるとします。ベースの割合が達すると、タスクは 2 つのキャパシティプロバイダー間で均等に分割されます。同じロジックを使用して、capacityProviderA に 1 の重みを指定し、capacityProviderB に 4 の重みを指定するとします。そして、capacityProviderA を使うタスクが 1 つ実行されるごとに、capacityProviderB を使うタスクが 4 つ実行されることになります。

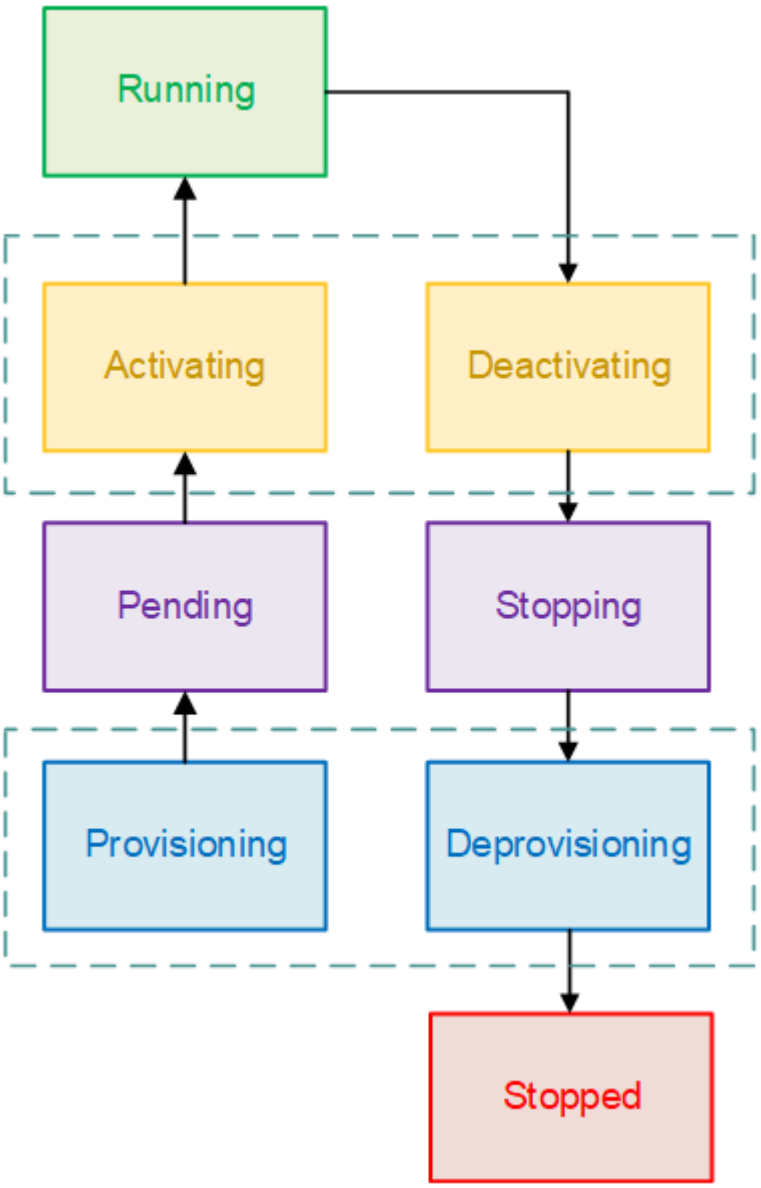
起動タイプでは、Fargate またはクラスターに手動で登録した Amazon EC2 インスタンスでタスクを直接起動します。

Amazon ECS タスクライフサイクル

タスクが手動またはサービスの一部として開始されると、自己終了するか手動で停止されるまでに、複数の状態を経由します。バッチジョブとして実行され、PENDING から RUNNING、その後 STOPPED と自然に進行するタスクもあります。他のタスクの場合は、サービスの一部であることもありますが、無制限に実行され続けるか、必要に応じてスケールアップまたはスケールダウンします。

タスクの停止や、スケールアップまたはスケールダウンのためのサービスの必要数の更新など、タスクのステータスの変更がリクエストされた場合、Amazon ECS コンテナエージェントはこれらの変更をタスクの最後の既知のステータス (lastStatus) およびタスクの目的のステータス (desiredStatus) として追跡します。タスクの最後の既知のステータスと目的のステータスの両方が、コンソールでまたは API あるいは AWS CLI でタスクを記述することにより、表示できます。

以下のフローチャートは、タスクのライフサイクルのフローを示しています。



ライフサイクル状態

それぞれのタスクのライフサイクル状態の説明は、以下のとおりです。

PROVISIONING

Amazon ECS は、タスクを起動する前に追加のステップを実行する必要があります。例えば、awsvpc ネットワークモードを使用するタスクの場合、Elastic Network Interface をプロビジョニングする必要があります。

保留中

これは、Amazon ECS が他の操作を実行するためにコンテナエージェントで待機している遷移状態です。タスクは、そのタスクに利用可能なリソースがあるまで保留状態のままです。

アクティブ化中

これは、タスクが起動された後で、タスクが RUNNING 状態に移行する前に、Amazon ECS が追加の手順を実行する必要がある移行状態です。これは、Amazon ECS がコンテナイメージをプルし、コンテナを作成し、タスクネットワークを設定し、ロードバランサーのターゲットグループを登録し、サービス検出を設定する状態です。

RUNNING

タスクを正常に実行中です。

非アクティブ化中

これは、タスクを停止する前に Amazon ECS が追加のステップを実行する必要がある移行状態です。例えば、Elastic Load Balancings ターゲットグループを使用するように設定されたサービスの一部であるタスクの場合、この状態でターゲットグループの登録解除が行われます。

停止中

これは、Amazon ECS が他の操作を実行するためにコンテナエージェントで待機している遷移状態です。

Linux コンテナの場合、コンテナエージェントは、アプリケーションを終了してシャットダウンする必要があることを通知する SIGTERM シグナルを送信し、タスク定義で設定された StopTimeout 期間を待機した後に SIGKILL を送信します。

プロビジョン解除中

Amazon ECS は、タスクが停止された後で、タスクが STOPPED 状態に移行する前に、追加の手順を実行する必要があります。例えば、awsvpc ネットワークモードを使用するタスクの場合、Elastic Network Interface をデタッチして削除する必要があります。

停止

タスクは正常に停止しました。

エラーが原因でタスクが停止した場合は、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

DELETED

これは、タスクが停止したときの移行状態です。この状態はコンソールには表示されませんが、`describe-tasks` に表示されます。

Amazon ECS がタスクをコンテナインスタンスに配置する方法

タスク配置を使用して、アベイラビリティーゾーンやインスタンスタイプなど、特定の基準を満たすコンテナインスタンスにタスクを配置するように Amazon ECS を設定できます。

以下はタスク配置のコンポーネントです。

- タスク配置戦略 - タスク配置またはタスクの終了でコンテナインスタンスを選択するためのアルゴリズムです。例えば、Amazon ECS でランダムにコンテナインスタンスを選択することも、インスタンスのグループ間に均等に分散されているタスクを持つコンテナインスタンスを選択することもできます。
- タスクグループ - データベースタスクなどの関連タスクのグループ。
- タスク配置制約事項 - コンテナインスタンスにタスクを配置するために満たす必要があるルールです。この制約が満たされない場合、タスクは配置されず、`PENDING` 状態のままになります。たとえば、制約を使用して、特定のインスタンスタイプにのみタスクを割り当てることができます。

Amazon ECS には、起動タイプごとに異なるアルゴリズムがあります。

EC2 起動タイプ

EC2 起動タイプを使用するタスクには、Amazon ECS ではタスク定義で指定されている CPU やメモリなどの要件に基づいてタスクを配置する場所を決定する必要があります。同様に、タスク数を減らすときも、Amazon ECS でどのタスクを終了させるか決定する必要があります。タスク配置の戦略と制約を適用することで、Amazon ECS がタスクを配置および終了する方法をカスタマイズできます。

デフォルトのタスク配置戦略は、タスクを手動 (スタンドアロンタスク) で実行するのか、それともサービス内で実行するのかによって異なります。Amazon ECS サービスの一部として実行されるタスクの場合、タスク配置戦略は `attribute:ecs.availability-zone` を使用した `spread` です。サービス内にないタスクには、デフォルトのタスク配置の制約はありません。詳細については、「Amazon ECS でコンテナをスケジュールする」を参照してください。

> **Note**
>
> タスク配置戦略はベストエフォートです。Amazon ECSは、最適な配置オプションが利用できない場合でも、タスクの配置を試みます。ただし、タスク配置の制約が有効な場合、タスクを配置できないことがあります。

タスク配置戦略と制約は併用できます。例えば、タスク配置戦略とタスク配置制約を使用して、アベイラビリティーゾーン間でタスクを分散し、各アベイラビリティーゾーン内のメモリに基づいてビンパックタスクを分散できます。ただし、G2 インスタンスのみです。

Amazon ECSがタスクを配置する際は、以下のプロセスでコンテナインスタンスを選択します。

1. タスク定義の CPU、GPU、メモリ、ポートの要件を満たすコンテナインスタンスを識別します。
2. タスク配置の制約事項を満たすコンテナインスタンスを識別します。
3. タスク配置戦略を満たすコンテナインスタンスを識別します。
4. タスクを配置するコンテナインスタンスを選択します。

Fargate 起動タイプ

タスク配置戦略および制約事項は、Fargate 起動タイプを使用しているタスクをサポートしていません。Fargate は、アクセス可能なアベイラビリティーゾーンにタスクを分散するよう最善を尽くします。キャパシティープロバイダーに Fargate と Fargate Spot の両方が含まれている場合、スプレッドの動作はキャパシティープロバイダーごとに異なります。

戦略を使用して Amazon ECS タスク配置を定義する

EC2 起動タイプを使用するタスクには、Amazon ECS ではタスク定義で指定されている CPU やメモリなどの要件に基づいてタスクを配置する場所を決定する必要があります。同様に、タスク数を減らすときも、Amazon ECS でどのタスクを終了させるか決定する必要があります。タスク配置の戦略と制約を適用することで、Amazon ECS がタスクを配置および終了する方法をカスタマイズできます。

デフォルトのタスク配置戦略は、タスクを手動 (スタンドアロンタスク) で実行するのか、それともサービス内で実行するのかによって異なります。Amazon ECS サービスの一部として実行されるタスクの場合、タスク配置戦略は `attribute:ecs.availability-zone` を使用した `spread` です。サービス内にないタスクには、デフォルトのタスク配置の制約はありません。詳細については、「Amazon ECS でコンテナをスケジュールする」を参照してください。

> **Note**
>
> タスク配置戦略はベストエフォートです。Amazon ECSは、最適な配置オプションが利用できない場合でも、タスクの配置を試みます。ただし、タスク配置の制約が有効な場合、タスクを配置できないことがあります。

タスク配置戦略と制約は併用できます。例えば、タスク配置戦略とタスク配置制約を使用して、アベイラビリティーゾーン間でタスクを分散し、各アベイラビリティーゾーン内のメモリに基づいてビンパックタスクを分散できます。ただし、G2 インスタンスのみです。

Amazon ECSがタスクを配置する際は、以下のプロセスでコンテナインスタンスを選択します。

1. タスク定義の CPU、GPU、メモリ、ポートの要件を満たすコンテナインスタンスを識別します。
2. タスク配置の制約事項を満たすコンテナインスタンスを識別します。
3. タスク配置戦略を満たすコンテナインスタンスを識別します。
4. タスクを配置するコンテナインスタンスを選択します。

タスク配置戦略は、サービス定義または `placementStrategy` パラメータを使用したタスク定義で指定できます。

```
"placementStrategy": [
    {
        "field": "The field to apply the placement strategy against",
        "type": "The placement strategy to use"
    }
]
```

タスクを実行するとき (RunTask)、新しいサービスを作成するとき (CreateService)、または既存のサービスを更新するとき (UpdateService) に戦略を指定できます。

次の表は利用可能なタイプとフィールドを説明しています。

type	有効なフィールド値	
`binpack`	• cpu • メモリ	

type	有効なフィールド値	
タスクはコンテナインスタンスに配置され、未使用の CPU またはメモリを最小にします。この戦略は、使用中のコンテナインスタンスの数を最小限に抑えます。 この戦略が使用されてスケールインアクションが実行されると、Amazon ECS はタスクを終了します。タスクが終了した後にコンテナインスタンスに残されたリソース量に基づいてこれが実行されます。タスクの終了後に利用可能なリソースが最も多く残るコンテナインスタンスが、そのタスクを終了されます。		
`random` タスクはランダムに配置されます。	使用されていない	

type	有効なフィールド値	
`spread` タスクは指定された値に基づいて均等に配置されます。サービスタスクはそのサービスからのタスクに基づいて分散されます。スタンドアロンタスクは、同じタスクグループからのタスクに基づいて分散されます。タスクグループの詳細については、「Amazon ECS タスクをグループ化する」を参照してください。 `spread` 戦略が使用されてスケールインアクションが実行されると、Amazon ECS は、アベイラビリティーゾーン間のバランスを維持するタスクを選択して終了します。アベイラビリティーゾーン内では、タスクはランダムに選択されます。	• `instanceId` (または同じ効果のある `host`) • `attribute:ecs.availability-zone` のようなコンテナインスタンスに適用される任意のプラットフォームまたはカスタム属性	

タスク配置の戦略は、既存のサービスに対しても更新できます。詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

実行する順序で戦略の配列を作成することで、複数の戦略を使用するタスク配置戦略を作成できます。例えば、複数のアベイラビリティーゾーンにタスクを分散し、各アベイラビリティーゾーン内のメモリに基づいてタスクをビンパックする場合、アベイラビリティーゾーン戦略を指定し、その後にメモリ戦略を指定します。戦略の例については、「Amazon ECS タスク配置戦略の例」を参照してください。

Amazon ECS タスク配置戦略の例

次のアクションを使用してタスク配置戦略を指定できます。CreateService、UpdateService、および RunTask。

例

- 複数のアベイラビリティーゾーンでタスクを均等に分散する
- すべてのインスタンスでタスクを均等に分散する
- メモリに基づいてタスクをビンパックする
- タスクをランダムに配置します。
- 複数のアベイラビリティーゾーンでタスクを均等に分散し、各アベイラビリティーゾーン内で複数のインスタンスでタスクを均等に分散する
- 複数のアベイラビリティーゾーンでタスクを均等に分散し、各アベイラビリティーゾーン内でメモリに基づいてタスクをビンパックする
- 複数のインスタンスでタスクを均等に分散し、メモリに基づいてタスクをビンパックする

複数のアベイラビリティーゾーンでタスクを均等に分散する

次の戦略は、アベイラビリティーゾーン間でタスクを均等に分散します。

```
"placementStrategy": [
    {
        "field": "attribute:ecs.availability-zone",
        "type": "spread"
    }
]
```

すべてのインスタンスでタスクを均等に分散する

次の戦略は、すべてのインスタンス間でタスクを均等に分散します。

```
"placementStrategy": [
    {
        "field": "instanceId",
        "type": "spread"
    }
]
```

メモリに基づいてタスクをビンパックする

次の戦略はメモリに基づいてタスクをビンパックします。

```
"placementStrategy": [
    {
        "field": "memory",
        "type": "binpack"
    }
]
```

タスクをランダムに配置します。

次の戦略はタスクをランダムに配置します。

```
"placementStrategy": [
    {
        "type": "random"
    }
]
```

複数のアベイラビリティーゾーンでタスクを均等に分散し、各アベイラビリティーゾーン内で複数のインスタンスでタスクを均等に分散する

次の戦略は、アベイラビリティーゾーン間でタスクを均等に分散し、次に各アベイラビリティーゾーン内でインスタンスを均等に分散します。

```
"placementStrategy": [
    {
        "field": "attribute:ecs.availability-zone",
        "type": "spread"
    },
    {
        "field": "instanceId",
        "type": "spread"
    }
]
```

複数のアベイラビリティーゾーンでタスクを均等に分散し、各アベイラビリティーゾーン内でメモリに基づいてタスクをビンパックする

次の戦略は、アベイラビリティーゾーン間でタスクを均等に分散し、次に各アベイラビリティーゾーン内でメモリに基づいてタスクをビンパックします。

```
"placementStrategy": [
    {
        "field": "attribute:ecs.availability-zone",
        "type": "spread"
    },
    {
        "field": "memory",
        "type": "binpack"
    }
]
```

複数のインスタンスでタスクを均等に分散し、メモリに基づいてタスクをビンパックする

次の戦略は、すべてのインスタンスでタスクを均等に分散し、各インスタンス内のメモリに基づいてタスクをビンパックします。

```
"placementStrategy": [
    {
        "field": "instanceId",
        "type": "spread"
    },
    {
        "field": "memory",
        "type": "binpack"
    }
]
```

Amazon ECS タスクをグループ化する

一連の関連するタスクを識別してタスクグループで配置できます。同じタスクグループ名のすべてのタスクは、spreadタスクの配置戦略の使用時に、セットとして見なされます。例えば、データベースおよびウェブサーバーなど、1 つのクラスターで異なるアプリケーションを実行していることを想定します。データベースを確実にアベイラビリティーゾーン間に均等に分散するには、それらのデータベースをdatabasesという名前のタスクグループに追加し、spreadタスク配置戦略を使用し

ます。詳細については、「戦略を使用して Amazon ECS タスク配置を定義する」を参照してください。

タスクグループはタスク配置の制約にも使用できます。memberOf 制約でタスクグループを指定したとき、タスクは指定されたタスクグループ内のコンテナインスタンスにのみ送信されます。例については、「Amazon ECS タスク配置の制約事項の例」を参照してください。

デフォルトでは、カスタムタスクグループ名が指定されていない場合、スタンドアロンタスクはタスク定義ファミリ名 (例えば family:my-task-definition) をタスクグループ名として使用します。サービスの一部として起動されたタスクは、サービス名をタスクグループ名として使用し、変更することはできません。

タスクグループには次の要件が適用されます。

- タスクグループ名は 255 文字以下である必要があります。
- 各タスクを 1 つのグループと同一にできます。
- タスクを起動後、タスクグループを変更することはできません。

Amazon ECS がタスクに使用するコンテナインスタンスを定義する

タスク配置の制約事項は、Amazon ECS がインスタンス上でタスクを実行できるかどうかを判断するために使用するコンテナインスタンスに関するルールです。少なくとも 1 つのコンテナインスタンスが制約に一致する必要があります。制約に一致するインスタンスがない場合、タスクは PENDING 状態のままになります。新しいサービスを作成するか、既存のサービスを更新するときに、サービスのタスク用にタスク配置制約を指定できます。

placementConstraint パラメータを使用して、サービス定義、タスク定義、またはタスクでタスク配置制約事項を指定できます。

```
"placementConstraints": [
    {
        "expression": "The expression that defines the task placement constraints",
        "type": "The placement constraint type to use"
    }
]
```

次の表は、パラメータの使用法の説明です。

[Constraint type (制約タイプ)]	次の場合に指定できます。	
`distinctInstance` それぞれのアクティブタスクを別々のコンテナインスタンスに配置します。 Amazon ECS は、タスク配置におけるタスクの目的のステータスを確認します。例えば、既存のタスクの目的のステータスが `STOPPED` の場合 (ただし、最後のステータスが目的のステータスではない場合)、`distinctInstance` 配置の制約事項にもかかわらず、新しい受信タスクを同じインスタンスに配置することができます。したがって、同じインスタンスで最後のステータスが `RUNNING` のタスクが 2 つ表示される場合があります。 **Important** タスクの強力な分離を求めているお客様には、Fargate を使用することをお勧めします。Fargate はハードウェア仮想化環境で各タスクを実行します。これにより、これらのコンテナ化されたワークロードがネットワー	• タスク RunTask を実行する • 新しいサービス CreateService の作成、	

[Constraint type (制約タイプ)]	次の場合に指定できます。	
クインターフェイス、Fargate の一時ストレージ、CPU、またはメモリを他のタスクと共有しないことが保証されます。詳細については、「AWS Fargate のセキュリティの概要」をご参照ください。		
`memberOf` 式を満たすコンテナインスタンスにタスクを配置します。	• タスク RunTask を実行する • 新しいサービス CreateService の作成、 • 新しいタスク定義 RegisterTaskDefinition の作成 • タスク定義 RegisterTaskDefinition の新しいバージョンの作成 • サービス UpdateService の更新	

`memberOf` 制約事項タイプを使用すると、Amazon ECS がタスクを配置できるコンテナインスタンスを定義するクラスタークエリ言語を使用して式を作成できます。この式は、コンテナインスタンスを属性別にグループ化する方法です。この式は、`placementConstraint` の `expression` パラメータに含まれます。

Amazon ECS コンテナインスタンス属性

コンテナインスタンスに属性と呼ばれるカスタムメタデータを追加できます。各属性には名前とオプションの文字列値があります。Amazon ECSが提供する組み込み属性を使用することも、カスタム属性を定義することもできます。

次のセクションでは、組み込み型、オプション型、カスタム型属性のサンプルが含まれています。

組み込み属性

Amazon ECSは次の属性を自動的にコンテナインスタンスに適用します。

`ecs.ami-id`

インスタンスの起動に使用される AMI の ID。この属性の値の例は「`ami-1234abcd`」です。

`ecs.availability-zone`

インスタンスのアベイラビリティーゾーン。この属性の値の例は「`us-east-1a`」です。

`ecs.instance-type`

インスタンスのインスタンスタイプ。この属性の値の例は「`g2.2xlarge`」です。

`ecs.os-type`

インスタンスのオペレーティングシステム。この属性に指定できる値は `linux` と `windows` です。

`ecs.os-family`

インスタンスのオペレーティングシステムのバージョン。

Linux インスタンスの場合、有効な値は `LINUX` です。Windows インスタンスの場合、ECS は値を `WINDOWS_SERVER_<OS_Release>_<FULL or CORE>` 形式で設定します。有効な値は、`WINDOWS_SERVER_2022_FULL`、`WINDOWS_SERVER_2022_CORE`、`WINDOWS_SERVER_20H2_COR` および `WINDOWS_SERVER_2016_FULL` です。

これは、Windows コンテナおよび Windows containers on AWS Fargate にとって重要です。なぜなら、すべての Windows コンテナの OS バージョンがホストのそれと一致する必要があるからです。コンテナイメージの Windows バージョンがホストと異なる場合、コンテナは起動しません。詳細については、マイクロソフトのドキュメント Web サイトの「Windows コンテナバージョンの互換性」を参照してください。

クラスターが複数の Windows バージョンを実行している場合、次の配置制約を使用して、同じバージョンで実行されている EC2 インスタンスにタスクが配置されるようにすることができます: `memberOf(attribute:ecs.os-family == WINDOWS_SERVER_<OS_Release>_<FULL or CORE>)`。詳細については、「the section called “Amazon ECS に最適化された Windows AMI メタデータを取得する”」を参照してください。

`ecs.cpu-architecture`

インスタンスの CPU アーキテクチャ。この属性の値の例は`x86_64` と `arm64` です。

`ecs.vpc-id`

インスタンスが起動された VPC。この属性の値の例は「`vpc-1234abcd`」です。

`ecs.subnet-id`

インスタンスが使用しているサブネット。この属性の値の例は「`subnet-1234abcd`」です。

オプションの属性

Amazon ECS では、コンテナインスタンスに次の属性を追加することができます。

`ecs.awsvpc-trunk-id`

この属性が存在する場合、インスタンスにトランクネットワークインターフェイスがあります。詳細については、「Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす」を参照してください。

`ecs.outpost-arn`

この属性が存在する場合は、Outpost の Amazon Resource Name (ARN) が含まれます。詳細については、「the section called “AWS OutpostsのAmazon Elastic Container Service”」を参照してください。

`ecs.capability.external`

この属性が存在する場合、インスタンスは外部インスタンスとして識別されます。詳細については、「外部起動タイプ用の Amazon ECS クラスター」を参照してください。

カスタム属性

コンテナインスタンスに、カスタム属性を適用できます。例えば、「stack」という名前で「prod」という値の属性を定義できます。

カスタム属性を指定するとき、次の点を考慮する必要があります。

- `name` は、1 ~ 128 文字で指定する必要があります。文字 (大文字と小文字)、数字、ハイフン、アンダースコア、スラッシュ、バックスラッシュ、ピリオドを使用できます。
- `value` は、1 ~ 128 文字で指定する必要があります。文字 (大文字と小文字)、数字、ハイフン、アンダースコア、ピリオド、アットマーク (@)、スラッシュ、バックスラッシュ、コロン、またはスペースを使用できます。値の先頭または末尾にホワイトスペースを含めることはできません。

Amazon ECS タスク用のコンテナインスタンスを定義する式を作成する

クラスタークエリは、オブジェクトをグループ化できる式です。例えば、アベイラビリティーゾーン、インスタンスタイプ、カスタムメタデータなどの属性でコンテナインスタンスをグループ化できます。詳細については、「Amazon ECS コンテナインスタンス属性」を参照してください。

コンテナインスタンスのグループを定義した後、グループに基づいてコンテナインスタンスのタスクを配置するように Amazon ECS をカスタマイズできます。詳細については「Amazon ECS タスクとしてのアプリケーションの実行」および「コンソールを使用した Amazon ECS サービスの作成」を参照してください。また、コンテナインスタンスをリスト表示する際にグループフィルタを適用できます。

式の構文

式の構文は次のとおりです。

```
subject operator [argument]
```

件名

評価する属性またはフィールド。

`agentConnected`

Amazon ECS コンテナエージェント接続ステータスでコンテナインスタンスを選択します。このフィルタを使用して、切断されたコンテナエージェントでインスタンスを検索します。

有効な演算子: equals (==)、not_equals (!=)、in、not_in (!in)、matches (=~)、not_matches (!~)

`agentVersion`

Amazon ECS コンテナエージェントバージョンでコンテナインスタンスを選択します。このフィルタを使用して、Amazon ECS コンテナエージェントの古くなったバージョンを実行しているインスタンスを検索します。

有効な演算子: equals (==)、not_equals (!=)、greater_than (>)、greater_than_equal (>=)、less_than (<)、less_than_equal (<=)

`attribute:`*`attribute-name`*

属性でコンテナインスタンスを選択します。詳細については、「Amazon ECS コンテナインスタンス属性」を参照してください。

`ec2InstanceId`

Amazon EC2 インスタンス ID で、コンテナインスタンスを選択します。

有効な演算子: equals (==)、not_equals (!=)、in、not_in (!in)、matches (=~)、not_matches (!~)

`registeredAt`

コンテナインスタンス登録日で、コンテナインスタンスを選択します。このフィルタを使用して、新しく登録されたインスタンスまたは古いインスタンスを検索します。

有効な演算子: equals (==)、not_equals (!=)、greater_than (>)、greater_than_equal (>=)、less_than (<)、less_than_equal (<=)

有効な日付形式: 2018-06-18T22:28:28+00:00、2018-06-18T22:28:28Z、2018-06-18T22:28:28、2018-06-18

`runningTasksCount`

実行中のタスクの数でコンテナインスタンスを選択します。このフィルタを使用して、空またはほぼ空 (実行中のタスクがほぼない) のインスタンスを検索します。

有効な演算子: equals (==)、not_equals (!=)、greater_than (>)、greater_than_equal (>=)、less_than (<)、less_than_equal (<=)

`task:group`

コンテナインスタンスをタスクグループで選択します。詳細については、「Amazon ECS タスクをグループ化する」を参照してください。

演算子

比較演算子。以下の演算子がサポートされています。

演算子	説明
==, が	文字列が等価
!=、not_equals	文字列が不等価
>、greater_than	以上
>=、greater_than_equal	以上

演算子	説明
<、less_than	未満
<=、less_than_equal	以下
exists	対象が存在
!exists、not_exists	サブジェクトが存在しません
in	引数リストの値
!in、not_in	引数リストにない値
=~、matches	パターンが一致
!~、not_matches	パターンが不一致

> **Note**
>
> 1 つの式に括弧を含めることはできません。ただし、複合式で優先順位を指定するために括弧を使用できます。

引数

多くの演算子は、引数がリテラル値です。

in および not_in 演算子は、引数として引数リストを想定しています。次のように引数リストを指定します。

```
[argument1, argument2, ..., argumentN]
```

matches と not_matches 演算子は、Java の正規表現構文に準拠する引数を想定しています。詳細については、java.util.regex.Pattern を参照してください。

複合式

次のブール演算子を使用して式を結合できます。

- &&, および
- ||, または
- !, 先頭の文字に

括弧を使用して、優先度を指定できます。

```
(expression1 or expression2) and expression3
```

式の例

以下に式の例を示します。

例: 文字列が等価

次の式は指定されたインスタンスタイプのインスタンスを選択します。

```
attribute:ecs.instance-type == t2.small
```

例: 引数リスト

次の式は、アベイラビリティーゾーンが us-east-1a または us-east-1b のインスタンスを選択します。

```
attribute:ecs.availability-zone in [us-east-1a, us-east-1b]
```

例: 複合式

次の表現は、us-east-1d アベイラビリティーゾーンにはない G2 インスタンスを選択します。

```
attribute:ecs.instance-type =~ g2.* and attribute:ecs.availability-zone != us-east-1d
```

例: タスクのアフィニティ

次の式は、service:production グループのタスクをホストするインスタンスを選択します。

```
task:group == service:production
```

例: タスクのアンチアフィニティ

次の表現は、データベースグループでタスクをホストしないインスタンスを選択します。

```
not(task:group == database)
```

例: 実行中のタスクの数

次の式は、1 つのタスクのみを実行しているインスタンスを選択します。

```
runningTasksCount == 1
```

Amazon ECS コンテナエージェントバージョン

次の式は、コンテナエージェントバージョン 1.14.5 より前のバージョンを実行しているインスタンスを選択します。

```
agentVersion < 1.14.5
```

例: インスタンス登録時

次の式は、2018 年 2 月 13 日以前に登録されているインスタンスを選択します。

```
registeredAt < 2018-02-13
```

例: Amazon EC2 インスタンス ID

次の式は、以下の Amazon EC2 インスタンス ID のインスタンスを選択します。

```
ec2InstanceId in ['i-abcd1234', 'i-wxyx7890']
```

Amazon ECS タスク配置の制約事項の例

以下はタスク配置の制約事項の例です。

この例では、memberOf 制約を使用して T2 インスタンスにタスクを配置します。次のアクションを使用して指定できます。CreateService、UpdateService、RegisterTaskDefinition、および RunTask。

```
"placementConstraints": [
    {
        "expression": "attribute:ecs.instance-type =~ t2.*",
        "type": "memberOf"
```

```
    }
]
```

この例では、memberOf 制約を使用して、指定されたタスク配置方法に従って、daemon-service タスクグループ内のデーモンサービスタスクを持つインスタンスに、レプリカタスクを配置します。この制約により、デーモンサービスタスクはレプリカサービスタスクよりも前に EC2 インスタンスに配置されます。

daemon-service を デーモンサービスの名前に置き換えます。

```
"placementConstraints": [
    {
        "expression": "task:group == service:daemon-service",
        "type": "memberOf"
    }
]
```

この例では、memberOf 制約を使用して、指定されたタスク配置方法に従って、databases タスクグループ内の他のタスクとともにインスタンスにタスクを配置します。タスクグループの詳細については、「Amazon ECS タスクをグループ化する 」を参照してください。次のアクションを使用して指定できます。CreateService、UpdateService、RegisterTaskDefinition、および RunTask。

```
"placementConstraints": [
    {
        "expression": "task:group == databases",
        "type": "memberOf"
    }
]
```

distinctInstance 制約は、グループ内の各タスクを別のインスタンスに配置します。次のアクションを使用して指定できます。CreateService、UpdateService、および RunTask。

Amazon ECS は、タスク配置におけるタスクの目的のステータスを確認します。例えば、既存のタスクの目的のステータスが STOPPED の場合 (ただし、最後のステータスが目的のステータスではない場合)、distinctInstance 配置の制約事項にもかかわらず、新しい受信タスクを同じインスタンスに配置することができます。したがって、同じインスタンスで最後のステータスが RUNNING のタスクが 2 つ表示される場合があります。

```
"placementConstraints": [
    {
```

```
        "type": "distinctInstance"
    }
]
```

Amazon ECS スタンドアロンタスク

バッチプロセスなど、何らかの処理を実行した後に停止するアプリケーションがある場合、アプリケーションをタスクとして実行できます。タスクを 1 回実行する場合は、コンソール、AWS CLI、API または SDK を使用できます。

レートベース、cron ベース、または 1 回限りのスケジュールでアプリケーションを実行する必要がある場合は、EventBridge Scheduler を使用してスケジュールを作成できます。

タスクワークフロー

Amazon ECS タスク (スタンドアロンタスクまたは Amazon ECS サービス) を起動すると、タスクが作成され、最初に PROVISIONING 状態に移行されます。タスクが PROVISIONING 状態になると、Amazon ECS はタスクを配置するためのコンピューティング能力を見つける必要があるため、タスクもコンテナも存在しません。

Amazon ECS は、起動タイプまたはキャパシティプロバイダーの設定に基づいて、タスクに適したコンピューティング性能を選択します。Fargate と Amazon EC2 の両方の起動タイプで、キャパシティプロバイダーおよびキャパシティプロバイダー戦略を使用できます。Fargate を使用すると、クラスター容量のプロビジョニング、設定、スケーリングについて心配する必要はありません。Fargate は、お客様のタスクに必要なすべてのインフラストラクチャ管理を行います。EC2 起動タイプの場合、Amazon EC2 インスタンスをクラスターに登録してクラスター容量を管理するか、クラスターの自動スケーリングを使用してコンピューティングキャパシティ管理を簡素化することができます。クラスター自動スケーリングは、クラスター容量を動的にスケーリングするため、ユーザーは実行中のタスクに集中できます。Amazon ECS は、タスク定義で指定した要件 (CPU やメモリなど)、および配置の制約事項と戦略に基づいて、タスクを配置する場所を決定します。詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

マネージドスケーリングが有効になっているキャパシティープロバイダーを使用すると、コンピューティングキャパシティーの不足が原因で開始できないタスクは、すぐに失敗するのではなく、PROVISIONING 状態に移行されます。タスクを配置する容量が決まったら、Amazon ECS は必要なアタッチメント (awsvpc モード内のタスク用の Elastic Network Interface (ENI) など) をプロビジョニングします。Amazon ECS コンテナエージェントを使用してコンテナイメージをプルし、コンテナを起動します。プロビジョニングが完了し、関連するコンテナが起動すると、Amazon ECS

はタスクを RUNNING 状態に移行します。タスクの状態の詳細については、「Amazon ECS タスクライフサイクル」を参照してください。

Amazon ECS タスクの起動時間を最適化する

タスク起動をスピードアップするために、以下の推奨事項を考慮してください。

- コンテナイメージと binpack インスタンスをキャッシュします。

  EC2 起動タイプを使用する場合、Amazon ECS コンテナエージェントのプル動作を ECS_IMAGE_PULL_BEHAVIOR: prefer-cached のように設定できます。キャッシュされたイメージがない場合に、リモートでイメージがプルされます。それ以外の場合は、インスタンスにキャッシュされたイメージが使用されます。キャッシュされたイメージが削除されないように、そのコンテナの自動イメージクリーンアップはオフになっています。これにより、次回起動時のイメージのプルタイムが短縮されます。コンテナインスタンスのタスク密度が高い場合、キャッシュの効果はさらに大きくなります。コンテナインスタンスは binpack 配置戦略を使用して設定できます。コンテナイメージのキャッシュは、通常はコンテナイメージのサイズが大きい Windows ベースのワークロード (数十 GB) に特に役立ちます。binpack 配置戦略を使用する場合は、Elastic Network Interface (ENI) トランキングを使用して、各コンテナインスタンスに awsvpc ネットワークモードでより多くのタスクを配置することを検討することもできます。ENI トランキングを使用すると、awsvpc モードで実行できるタスク数が増加します。たとえば、同時に 2 つのタスクしか実行できない c5.large インスタンスの場合、ENI トランキングでは最大 10 のタスクを実行できます。
- 最適なネットワークモードを選択する

  awsvpc ネットワークモードが理想的な例は多数ありますが、このネットワークモードは本質的にタスク起動レイテンシーを増加させる可能性があります。これは、awsvpc モード内の各タスクについて、Amazon EC2 API を呼び出して ENI をプロビジョニングしてアタッチする必要があるため、タスク起動に数秒のオーバーヘッドが追加されるためです。対照的に、awsvpc ネットワークモードを使用する主な利点は、各タスクにトラフィックを許可または拒否するセキュリティグループがあることです。つまり、タスクとサービス間の通信をよりきめ細かく制御できる柔軟性が増します。デプロイ速度を優先する場合は、bridge モードを使用してタスクの起動をスピードアップすることを検討してください。詳細については、「the section called “AWSVPC ネットワークモード”」を参照してください。
- タスク起動のライフサイクルを追跡して、最適化の機会を見つけます。

  多くの場合、アプリケーションが起動するまでにかかる時間を知ることは困難です。アプリケーションの起動時に、コンテナイメージの起動、起動スクリプトの実行、その他の設定を行うと、

驚くほど時間がかかることがあります。タスクメタデータエンドポイントを使用してメトリクスを投稿し、ContainerStartTime からアプリケーションがトラフィックを処理できるようになるまでのアプリケーションの起動時間を追跡できます。このデータにより、アプリケーションが起動時間全体にどのような影響を与えているかを把握し、アプリケーション固有の不要なオーバーヘッドを減らし、コンテナイメージを最適化できる領域を見つけることができます。詳細については、「Amazon ECS のキャパシティーと可用性の最適化」を参照してください。

- 最適なインスタンスタイプを選択する (EC2 起動タイプの場合)

  適切なインスタンスタイプは、タスクに設定したリソース予約 (CPU、メモリなど) に基づいて選択します。したがって、インスタンスのサイズを決定する際には、1 つのインスタンスに配置できるタスクの数を計算できます。適切に配置されたタスクの簡単な例は、m5.large インスタンス (2 vCPU と 8 GB のメモリをサポート) で 0.5 vCPU と 2 GB のメモリ予約を必要とする 4 つのタスクをホストすることです。このタスク定義の予約は、インスタンスのリソースを最大限に活用します。

Amazon ECS タスクとしてのアプリケーションの実行

1 回限りのプロセス用のタスクは AWS Management Console を使用して作成できます。

スタンドアロンタスクを作成するには (AWS Management Console)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. Amazon ECS コンソールでは、クラスターの詳細ページまたはタスク定義リビジョンリストからスタンドアロンタスクを作成できます。選択したリソースページに応じて、次の手順を使用してスタンドアロンタスクを作成します。

サービスの起動元	ステップ
クラスター詳細ページ...	a. [Clusters] ページで、サービスを作成するクラスターを選択します。 b. Tasksタブで、Run new taskを選択します。
タスク定義のリビジョンページ...	a. [タスク定義] ページで、タスク定義ファミリを選択して、そのファミリー

サービスの起動元	ステップ
	のリビジョンを表示します。 b. 使用するリビジョンを選択します。 c. [デプロイ] メニューから、[タスクの実行] を選択します。

3. (オプション) [コンピューティング設定 (詳細)] セクションでは、タスクの分散方法を選択します。[キャパシティープロバイダー戦略] または [起動タイプ] のいずれかを選択できます。キャパシティプロバイダー戦略を使用するには、キャパシティプロバイダーをクラスターレベルで設定する必要があります。キャパシティプロバイダーを使用するようにクラスターを構成していない場合は、代わりに起動タイプを使用してください。

ディストリビューションの方法	ステップ
キャパシティープロバイダー戦略	a. [Compute options] (コンピューティングオプション) セクションで、[Capacity provider strategy] (キャパシティープロバイダー戦略) を選択します。 b. 戦略を選択: • デフォルトのキャパシティープロバイダー戦略を使用するには、[Use cluster default] (デフォルトのクラスターを使用) を選択します。 • クラスターにデフォルトのキャパシティ

ディストリビューションの方法	ステップ
	ープロバイダー戦略がない場合、またはカスタム戦略を使用する場合は、[Use custom] (カスタムを使用)、[Add capacity provider strategy] (キャパシティプロバイダー戦略の追加)を選択し、[Base] (ベース)、[Capacity provider] (キャパシティープロバイダー)、[Weight] (ウェイト) を指定して、カスタムキャパシティープロバイダー戦略を定義します。 **Note** 戦略でキャパシティープロバイダーを使用するには、キャパシティープロバイダーをクラスターに関連付ける必要があります。

ディストリビューションの方法	ステップ
起動タイプ	a. [Compute options] (コンピューティングオプション) セクションで、[Launch type] (起動タイプ) を選択します。 b. [Launch type] (起動タイプ) で、起動タイプを選択します。 c. (オプション) Fargate 起動タイプが指定されている場合、Platform version(プラットフォームのバージョン)で、使用するプラットフォームのバージョンを指定します。プラットフォームバージョンが指定されない場合、LATEST プラットフォームバージョンが使用されます。

4. Application type(アプリケーションの種類)で、Task(タスク)を選択します。
5. [タスク定義] の場合、タスク定義ファミリーとリビジョンを選択します。

> **Important**
>
> コンソールは、選択を検証し、選択したタスク定義ファミリーおよびリビジョンが、定義されたコンピューティング設定と互換性があることを確認します。

6. [Desired tasks] (必要なタスク) で、起動するタスクの数を入力します。
7. タスク定義で awsvpc ネットワークモードを使用している場合、[Networking] (ネットワーク) を展開します。カスタム設定を指定するには、次のステップを実行します。

   a. VPC の場合、使用する VPC を選択します。

b. [Subnets] (サブネット) で、タスクスケジューラがタスクを配置するときに考慮する VPC 内のサブネットを 1 つ以上選択します。

> **Important**
>
> awsvpc ネットワークモードではプライベートサブネットだけがサポートされます。タスクはパブリック IP アドレスを受信しません。したがって、アウトバウンドのインターネットアクセスには NAT ゲートウェイが必要であり、またインバウンドのインターネットトラフィックは、ロードバランサーを経由します。

c. [セキュリティグループ] で、既存のセキュリティグループを選択することも、新しいセキュリティグループを作成することもできます。既存のセキュリティグループを使用するには、セキュリティグループを選択し、次のステップに進みます。新しいセキュリティグループを作成するには、[Create a new security group (新しいセキュリティグループの作成)] を選択します。セキュリティグループの名前、説明を指定してから、セキュリティグループのインバウンドルールを 1 つ以上追加する必要があります。

d. [Public IP] (パブリック IP) では、タスクの Elastic Network Interface (ENI) にパブリック IP アドレスを自動的に割り当てるかどうかを選択します。

   AWS Fargate タスクをパブリックサブネットで実行するときに、そのタスクにパブリック IP アドレスを割り当てて、インターネットへのルートを持つようにすることができます。このフィールドを使用して EC2 タスクにパブリック IP を割り当てることはできません。詳細については、「Fargate 起動タイプの Amazon ECS タスクネットワーキングオプション」および「Amazon ECS タスクへのネットワークインターフェイスの割り当て」を参照してください。

8. デプロイ時の設定と互換性のあるデータボリュームをタスクで使用する場合は、[ボリューム] を拡張してボリュームを設定できます。

   ボリューム名とボリュームタイプはタスク定義リビジョンの作成時に設定され、スタンドアロンタスクの実行時には変更できません。ボリューム名とタイプを更新するには、新しいタスク定義リビジョンを作成し、その新しいリビジョンを使用してタスクを実行する必要があります。

このボリュームタイプを設定するには	この操作を行います	
Amazon EBS	a. [EBS ボリュームタイプ] には、タスクにアタッチ	

このボリュームタイプを設定するには	この操作を行います	
	する EBS ボリュームのタイプを選択します。 b. [サイズ (GiB)] には、ボリュームサイズの有効な値をギビバイト (GiB) 単位で入力します。最小で 1 GiB、最大で 16,384 GiB のボリュームサイズを指定できます。スナップショット ID を指定しない限り、この値は必須です。 c. [IOPS] には、ボリュームが提供する入力/出力オペレーションの数 (IOPS) の最大数を入力します。この値は `io1`、`io2`、および `gp3` ボリュームタイプでのみ設定できます。 d. [スループット (MiB/秒)] には、ボリュームが提供すべきスループットをメビバイト/秒 (MiBps または MiB/s) で入力します。この値は `gp3` ボリュームタイプでのみ設定できます。 e. [スナップショット ID] には、既存の Amazon EBS ボリュームスナップショットを選択するか、スナップショットからボリュームを作成する場合	

このボリュームタイプを設定するには	この操作を行います	
	はスナップショットの ARN を入力します。新しい空のボリュームは、スナップショット ID を選択または入力しないで作成することもできます。 f. タスクの終了後にタスクに接続するように構成されたボリュームを保持する場合は、[終了ポリシー] のチェックボックスを選択解除します。デフォルトでは、タスクにアタッチされている EBS ボリュームは、タスクが終了すると削除されます。 g. [ファイルシステムのタイプ] では、ボリューム上のデータストレージおよび取得に使用するファイルシステムの種類を選択します。オペレーティングシステムのデフォルトまたは特定のファイルシステムタイプのいずれかを選択できます。Linux のデフォルトは XFS です。スナップショットから作成されたボリュームでは、スナップショットの作成時にボリュームが使用していたのと同じファイルシステムタイプを指定す	

このボリュームタイプを設定するには	この操作を行います	
	る必要があります。ファイルシステムのタイプが一致しない場合、タスクは開始できません。 h. [インフラストラクチャロール] には、Amazon ECS がタスクの Amazon EBS ボリュームを管理できるようにするために必要な権限を持つ IAM ロールを選択します。`AmazonECSInfrastructureRolePolicyForVolumes` 管理ポリシーをロールにアタッチすることも、このポリシーをガイドとして使用して、特定のニーズを満たすアクセス権限を持つ独自のポリシーを作成してアタッチすることもできます。必要なアクセス権限の詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。 i. デフォルト設定で Amazon EBS 暗号化を使用する場合は、[暗号化] で [デフォルト] を選択します。アカウン	

このボリュームタイプを設定するには	この操作を行います	
	トにデフォルトで暗号化が設定されている場合、ボリュームは設定で指定されている AWS Key Management Service (AWS KMS) キーで暗号化されます。[デフォルト] を選択し、Amazon EBS のデフォルト暗号化がオンになっていない場合、ボリュームは暗号化されません。 [カスタム] を選択した場合は、ボリューム暗号化に任意の AWS KMS key を指定できます。 [なし] を選択すると、デフォルトで暗号化が設定されている場合や、暗号化されたスナップショットからボリュームを作成した場合を除き、ボリュームは暗号化されません。 j. [暗号化] に [カスタム] を選択した場合は、使用する AWS KMS key を指定する必要があります。[KMS キー] には、AWS KMS key を選択するか、キーの ARN を入力します。対称型のカスタマー管理キーを使用	

このボリュームタイプを設定するには	この操作を行います	
	してボリュームを暗号化する場合は、AWS KMS key ポリシーに適切な権限が定義されていることを確認してください。詳細については、「Amazon EBS ボリュームのデータ暗号化」を参照してください。 k. (オプション) [タグ] では、タスク定義からタグを伝達するか、独自のタグを指定することで、Amazon EBS ボリュームにタグを追加できます。 タスク定義からタグを伝達する場合は、[タグの伝播元] で [タスク定義] を選択します。[伝播しない] を選択した場合、または値を選択しなかった場合、タグは伝播されません。 独自のタグを指定する場合は、[タグの追加] を選択し、追加する各タグのキーと値を指定します。 Amazon EBS ボリュームのタグ付けの詳細については、「Amazon EBS ボリュームのタグ付け」を参照してください。	

9. (オプション) デフォルト以外のタスク配置戦略を使用するには、[Task Placement] (タスクの配置) を展開し、以下のオプションから選択します。

   詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

   - [AZ バランススプレッド] - アベイラビリティーゾーン間およびアベイラビリティーゾーン内のコンテナインスタンス間でタスクを分散します。
   - [AZ Balanced BinPack] - 利用可能な最小メモリでアベイラビリティーゾーン間およびコンテナインスタンス間でタスクを分散します。
   - [ビンパック] - CPU またはメモリの最小利用可能量に基づいてタスクを配置します。
   - [ホストごとに 1 つのタスク] - 各コンテナインスタンスのサービスから最大 1 タスクを配置します。
   - [カスタム] - 独自のタスク配置戦略を定義します。

   [Custom] (カスタム) を選択した場合、タスクを配置するアルゴリズムと、タスク配置時に考慮されるルールを定義します。

   - [Strategy] (方針) にとって [Type] (タイプ) そして [Field] (フィールド) で、アルゴリズムとアルゴリズムに使用するエンティティを選択します。

     最大 5 個の戦略を入力できます。
   - [制約] の [タイプ] および [式] で、制約のルールと属性を選択します。

     例えば、T2 インスタンスにタスクを配置する制約を設定するには、[Expression] (表現) で、[attribute:ecs.instance-type =~ t2.*] と入力します。

     最大 10 個の制約を入力できます。

10. (オプション) タスク IAM ロール、またはタスク定義で定義されているタスク実行ロールをオーバーライドするには、[Task overrides] (タスクのの上書き) を展開し、以下のステップを実行します。

    a. [タスクロール] で、このタスクの IAM ロールを選択します。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

       `ecs-tasks.amazonaws.com`信頼関係を持つロールのみが表示されます。タスクの IAM ロールを作成する方法については、「タスクの IAM ロールを作成する」を参照してください。

b. [タスク実行ロール] で、タスク実行ロールを選択します。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

11. (オプション) コンテナコマンドと環境変数をオーバーライドするには、[Container Overrides] (コンテナの上書き) を展開し、コンテナを展開します。

- タスク定義コマンド以外のコンテナにコマンドを送信するには、[コマンドの上書き] で Docker コマンドを入力します。
- [Add Environment Variable] (環境変数の追加) で、環境変数を追加します。Keyに、環境変数の名前を入力します。Value(値) で、(文字列を囲む二重引用符 (" ") なしで) 環境値の文字列値を入力します。

  AWS は文字列を二重引用符 (" ") で囲み、次の形式で文字列をコンテナに渡します。

```
MY_ENV_VAR="This variable contains a string."
```

12. (オプション) タスクを識別しやすくするには、[Tags] (タグ) セクションを展開し、タグを設定します。

    Amazon ECS で、新しく起動されたすべてのタスクに、クラスター名とタスク定義のタグで自動でタグ付けするには、[Turn on Amazon ECS managed tags] (Amazon ECS で管理されたタグを有効にする) を選択し、[Task definition] (タスク定義) を選択します。

    タグを追加または削除します。

- [タグを追加] [Add tag] (タグを追加) を選択し、以下を実行します。
  - [キー] にはキー名を入力します。
  - [値] にキー値を入力します。
- [タグの削除] タグの横にある [タグの削除] を選択します。

13. [Create] (作成) を選択します。

Amazon EventBridge スケジューラを使用して Amazon ECS タスクをスケジュールする

EventBridge スケジューラーはサーバーレススケジューラであり、一元化されたマネージドサービスからタスクを作成、実行、管理できます。イベントバスやルールに依存しない、1 回限りの定期的なスケジューリング機能を提供します。EventBridge スケジューラは高度にカスタマイズ可能で、EventBridge のスケジュールルールよりもスケーラビリティが高く、ターゲット API 操作と

AWS サービスの範囲が広がります。EventBridge スケジューラには、EventBridge スケジューラコンソールでタスクに設定できる以下のスケジュールが用意されています。

- レートベース
- cron ベース

  cron ベースのスケジュールはどのタイムゾーンでも設定できます。
- 1 回限りのスケジュール

  1 回限りのスケジュールはどのタイムゾーンでも設定できます。

Amazon ECS は Amazon EventBridge スケジューラを使用してスケジュールできます。

Amazon ECS コンソールでスケジュールされたタスクを作成できますが、現在、EventBridge Scheduler コンソールではさらに多くの機能を提供しています。

タスクをスケジュールする前に、次のステップを完了します。

1. タスクが実行されるサブネット ID とサブネットのセキュリティグループ ID を取得するには、VPC コンソールを使用します。詳細については、「VPC のサブネット」と「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 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。
2. EventBridge スケジューラの実行ロールを設定します。詳細については、「Amazon EventBridge スケジューラユーザーガイド」の「実行ロールを設定する」を参照してください。

コンソールを使用して新しいスケジュールを作成するには

1. Amazon EventBridge スケジューラコンソール (https://console.aws.amazon.com/scheduler/home) を開きます。
2. [スケジュール] ページで、[スケジュールを作成] を選択します。
3. [スケジュールの詳細を指定] ページの [スケジュールの名前と説明] セクションで、次を実行します。

   a. [スケジュール名] で、スケジュールの名前を入力します。例えば、**MyTestSchedule** と指定します。

   b. (オプション) [説明] で、スケジュールの説明を入力します。例えば、**TestSchedule** と指定します。

c. [スケジュールグループ] で、スケジュールグループを選択します。グループがない場合は、[デフォルト] を選択します。スケジュールグループを作成するには、[独自のスケジュールを作成] を選択します。

スケジュールグループを使用して、スケジュールのグループにタグを追加します。

4. スケジュールオプションを選択します。

頻度	手順	
[1 回限りのスケジュール] 1 回限りのスケジュールは、指定した日時に 1 回だけターゲットを呼び出します。	[日付と時刻] で、次を実行します。 • 有効な日付を YYYY/MM/DD 形式で入力します。 • タイムスタンプを 24 時間 (hh:mm) 形式で入力します。 • [タイムゾーン] で、タイムゾーンを選択します。	
[繰り返しのスケジュール] 繰り返しのスケジュールは、cron 式またはレート式を使用して指定したレートでターゲットを呼び出します。	a. [スケジュールの種類] では、次のいずれかを実行します。 • Cron 式を使用してスケジュールを定義するには、[cron ベースのスケジュール] を選択して Cron 式を入力します。 • Rate 式を使用してスケジュールを定義するには、[rate ベースのスケジュール] を選択して Rate 式を入力します。 cron およびレート式の詳細については、「A	

頻度	手順	
	mazon EventBridge スケジューラユーザーガイド」の「EventBridge スケジューラのスケジュールタイプ」を参照してください。 b. [フレックスタイムウィンドウ] で、[オフ] を選択してオプションをオフにするか、事前定義された時間枠のいずれかを選択します。例えば、[15 分] を選択し、1 時間に 1 回ターゲットを呼び出す繰り返しのスケジュールを設定した場合、スケジュールは毎時の開始後 15 分以内に実行されます。	

5. (オプション) 前のステップで [定期的なスケジュール] を選択した場合は、[時間枠] セクションで次を実行します。

   a. [タイムゾーン] で、タイムゾーンを選択します。

   b. [開始日時] で、有効な日付を YYYY/MM/DD 形式で入力してから、タイムスタンプを 24 時間 (hh:mm) 形式で指定します。

   c. [終了日時] で、有効な日付を YYYY/MM/DD 形式で入力してから、タイムスタンプを 24 時間 (hh:mm) 形式で指定します。

6. [Next] を選択します。

7. [ターゲットを選択] ページで、次の操作を行います。

   a. [すべての API] を選択し、検索ボックスで ECS と入力します。

   b. [Amazon ECS] を選択します。

   c. 検索ボックスで RunTask と入力し、[RunTask] を選択します。

d. [ECS クラスター] で、クラスターを選択します。

e. [ECS タスク] で、タスクに使用するタスク定義を選択します。

f. 起動タイプを使用するには、[コンピューティングオプション] を展開し、[起動タイプ] を選択します。その後、起動タイプを選択します。

Fargate 起動タイプが指定される場合、[プラットフォームバージョン] で、使用するプラットフォームバージョンを入力します。プラットフォームが指定されていない場合は、LATEST プラットフォームバージョンが使用されます。

g. [サブネット] で、タスクを実行するサブネット ID を入力します。

h. [セキュリティグループ] で、サブネットのセキュリティグループ ID を入力します。

i. (オプション) デフォルト以外のタスク配置戦略を使用するには、[配置制約] を展開し、制約を入力します。

詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

j. (オプション) タスクを識別しやすくするために、[タグ] でタグを設定します。

新しく起動されたすべてのタスクに対して、Amazon ECS がタスク定義タグを自動的にタグ付けするようにするには、[Amazon ECS マネージドタグを有効にする] を選択します。

8. [Next] を選択します。

9. [Settings] (設定) ページで、以下の操作を行います。

a. スケジュールをオンにするには、[スケジュールの状態] で [スケジュールを有効にする] をオンに切り替えます。

b. スケジュールの再試行ポリシーを設定するには、[再試行ポリシーとデッドレターキュー (DLQ)] で次を実行します。

- [再試行] を切り替えてオンにします。
- [イベントの最大保持時間] で、EventBridge スケジューラが未処理のイベントを保持しなければならない最大の [時間] と [分] を入力します。
- 最大 24 時間です。
- [最大再試行回数] で、ターゲットがエラーを返した場合に EventBridge スケジューラがスケジュールを再試行する最大回数を入力します。

再試行の最大値は 185 です。

再試行ポリシーを使用すると、スケジュールがそのターゲットの呼び出しに失敗した場合、EventBridge スケジューラはスケジュールを再実行します。設定されている場合は、スケジュールの最大保持時間と再試行を設定する必要があります。

c. EventBridge スケジューラが未配信のイベントを保存する場所を選択します。

[デッドレターキュー (DLQ)] オプション	手順	
保存しない	[None] を選択します。	
スケジュールを作成しようとしている同じ AWS アカウント にイベントを保存する	a. [自分の AWS アカウント の Amazon SQS キューを DLQ として選択] を選択します。 b. Amazon SQS キューの Amazon リソースネーム (ARN) を選択します。	
スケジュールを作成しようとしているのとは別の AWS アカウント にイベントを保存する	a. [他の AWS アカウント の Amazon SQS キューを DLQ として指定] を選択します。 b. Amazon SQS キューの Amazon リソースネーム (ARN) を入力します。	

d. カスタマーマネージドキーを使用してターゲットの入力を暗号化するには、[暗号化] で [暗号化設定をカスタマイズする (高度)] を選択します。

このオプションを選択した場合は、既存の KMS キー ARN を入力するか、[AWS KMS key を作成] を選択して AWS KMS コンソールに移動します。EventBridge スケジューラが保管中のデータを暗号化する方法の詳細については、「Amazon EventBridge スケジューラユーザーガイド」の「保管中の暗号化」を参照してください。

e. [許可] で、[既存のロールを使用] を選択してから、ロールを選択します。

EventBridge スケジューラに新しい実行ロールを作成させるには、[このスケジュールの新しいロールを作成] を選択します。その後、[ロール名] で名前を入力します。このオプションを選択すると、EventBridge スケジューラは、テンプレート化されたターゲットに必要な許可をロールにアタッチします。

10. [Next] を選択します。
11. [スケジュールの確認と作成] ページで、スケジュールの詳細を確認します。各セクションで、そのステップに戻って詳細を編集するには、[編集] を選択します。
12. [スケジュールを作成] を選択します。

    [スケジュール] ページで、新規および既存のスケジュールのリストを表示できます。[ステータス] 列で、新しいスケジュールが [有効] になっていることを確認します。

次のステップ

EventBridge スケジューラコンソールまたは AWS CLI を使用し、スケジュールを管理できます。詳細については、「Amazon EventBridge スケジューラユーザーガイド」の「Managing a schedule」を参照してください。

Amazon ECS タスクの停止

スタンドアロンタスクを実行し続ける必要がなくなった場合は、タスクを停止できます。Amazon ECS コンソールでは、1 つ以上のタスクを簡単に停止できます。

スタンドアロンの停止したタスクは、再起動できません。

サービスを停止したい場合は、「コンソールを使用して Amazon ECS サービスの削除」を参照してください。

スタンドアロンタスクを停止するには (AWS Management Console)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [クラスター] ページで、クラスターを選択してクラスターの詳細ページに移動します。
4. クラスターの詳細ページで、[タスク] タブを選択します。
5. [起動タイプのフィルター] リストを使用して、起動タイプごとにタスクをフィルターできます。

停止するタスク	ステップ
1 つ以上	a. タスクを選択し、[停止]、[選択したものを停止] を選択します。 b. [タスク停止確認ページ] で [停止] を選択します。
すべて	**Important** コンソールを使用してすべてのタスクを停止することを選択した場合、Amazon ECS はすべてのスタンドアロンタスクとサービスの一部であるタスクを停止します。したがって、このオプションを使用する場合は注意が必要です。 a. [停止]、[すべてを停止] の順に選択します。 b. [タスク停止確認ページ] で、[すべてのタスクを停止] を入力してから、[停止] を選択します。

Amazon ECS サービス

Amazon ECS サービスを使用すると、Amazon ECS クラスター内で、タスク定義の指定した数のインスタンスを同時に実行して維持できます。タスクの 1 つが失敗または停止した場合、Amazon

ECS サービススケジューラはタスク定義の別のインスタンスを起動してそれを置き換えます。これは、サービスで必要な数のタスクを維持するのに役立ちます。

オプションで、ロードバランサーの背後でサービスを実行することもできます。ロードバランサーは、サービスに関連付けられたタスク間でトラフィックを分散させます。

長時間実行されるステートレスサービスおよびアプリケーションには、サービススケジューラを使用することをお勧めします。サービススケジューラにより、指定したスケジューリング戦略が順守され、タスクが失敗したときに タスクが再スケジュールされます。例えば、基盤となるインフラストラクチャに障害が発生した場合、サービススケジューラはタスクを再スケジュールします。タスク配置の戦略と制約を使用して、スケジューラがタスクを配置および終了する方法をカスタマイズできます。サービス内のタスクが停止すると、スケジューラはタスクを置き換えるために新しいタスクを起動します。このプロセスは、サービスが使用するスケジュール戦略に基づいて、サービスがタスクの必要数に達するまで続行されます。サービスのスケジューリング戦略は、サービスタイプとも呼ばれます。

また、コンテナのヘルスチェックまたはロードバランサーのターゲットグループのヘルスチェックが失敗すると、サービススケジューラーによって、異常であると判断されたタスクが置き換えられます。この置き換え動作は、maximumPercent および desiredCount のサービス定義パラメータによって異なります。タスクが異常とマークされた場合、サービススケジューラーによってまず置き換えタスクが開始されます。次に以下が発生します。

- 置き換えタスクのヘルスステータスが HEALTHY になると、サービススケジューラーが異常のあるタスクを停止します。
- 置き換えタスクのヘルスステータスが UNHEALTHY の場合、スケジューラーは異常のある置き換えタスクまたは既存の異常タスクのいずれかを停止して、タスク総数が desiredCount と等しくなるようにします。

maximumPercent パラメーターによって、置き換えタスクを先に開始できないようにスケジューラーが制限されている場合、スケジューラーは異常のあるタスクをランダムに 1 つずつ停止して容量を解放してから置き換えタスクを開始します。異常のあるタスクがすべて正常なタスクに置き換えられるまで、起動と停止のプロセスが続きます。異常なタスクがすべて置き換えられ、正常なタスクだけが実行中になると、合計タスク数が desiredCount を超える場合、タスク数が desiredCount になるまで、正常なタスクが無作為に停止されます。maximumPercent および desiredCount の詳細については、「サービス定義パラメータ」を参照してください。

サービススケジューラには、タスクが繰り返し起動に失敗した場合にタスクを再起動する頻度を調整するロジックが含まれています。RUNNING 状態にならずにタスクが停止すると、サービススケ

ジューラは起動の試行の速度を遅くし始め、サービスイベントメッセージを送信します。この動作により、問題を解決する前に、失敗したタスクに不要なリソースが使用されるのを防ぐことができます。サービスが更新されると、サービススケジューラは正常なスケジューリング動作を再開します。詳細については、Amazon ECS サービスのスロットルロジックおよびAmazon ECS のサービスイベントメッセージを表示するを参照してください。

利用できる 2 つのサービススケジューラ戦略があります。

- REPLICA - レプリカスケジュール戦略では、クラスター全体で必要数のタスクを配置して維持します。デフォルトでは、サービススケジューラによってタスクはアベイラビリティーゾーン間に分散されます。タスク配置の戦略と制約を使用すると、タスク配置の決定をカスタマイズできます。詳細については、「レプリカ戦略」を参照してください。
- DAEMON - デーモンのスケジュール戦略では、指定したすべてのタスク配置制約を満たすクラスター内のアクティブなコンテナインスタンスごとに、1 つのタスクのみをデプロイします。この戦略を使用する場合、タスクの必要数や配置戦略、サービスの自動スケーリングポリシーを指定する必要はありません。詳細については、「デーモン戦略」を参照してください。

> **Note**
>
> Fargate タスクは DAEMON スケジュール戦略をサポートしていません。

デーモン戦略

デーモンのスケジュール戦略では、指定したすべてのタスク配置制約を満たすクラスター内のアクティブなコンテナインスタンスごとに、1 つのタスクのみをデプロイします。サービススケジューラは、実行中のタスクのタスク配置の制約事項を評価し、配置制約を満たさないタスクを停止します。この戦略を使用する場合、タスクの必要数や配置戦略を指定したり、サービス自動スケーリングポリシーを使用したりする必要はありません。

Amazon ECS は、CPU、メモリ、およびネットワークインターフェイスを含むコンテナインスタンスのコンピューティングリソースをデーモンタスク用に予約します。他のレプリカサービスを使用してクラスターでデーモンサービスを起動すると、Amazon ECS はデーモンタスクを優先します。これは、デーモンタスクがインスタンス上で起動する最初のタスクであり、すべてのレプリカタスクが停止した後に停止する最後のタスクであることを意味します。この戦略により、保留中のレプリカ・タスクでリソースが使用されず、デーモンタスクでリソースを使用できるようになります。

デーモンサービススケジューラは DRAINING ステータスのインスタンスにはタスクを配置しません。コンテナインスタンスが DRAINING ステータスに移行すると、そのインスタンス上のデーモンタスクは停止します。サービススケジューラはまた、新しいコンテナインスタンスがいつクラスターに追加されるかをモニタリングし、追加されたらそれらのインスタンスにデーモンタスクを追加します。

デプロイメント設定を指定する場合、maximumPercent パラメータの値は 100 (パーセンテージとして指定) である必要があります。これは、設定されていない場合に使用されるデフォルト値です。minimumHealthyPercent パラメータのデフォルト値は 0 (パーセンテージで指定) です。

デーモンサービスの配置制約を変更するには、サービスを再起動する必要があります。Amazon ECS は、デーモンタスクの対象となるインスタンスに予約されているリソースを動的に更新します。既存のインスタンスの場合、スケジューラはインスタンスにタスクを配置しようとします。

タスク定義でタスクサイズまたはコンテナリソースの予約が変更されると、新しいデプロイが開始されます。新しいデプロイは、サービスを更新したり、タスク定義の異なるリビジョンを設定したりするときにも開始されます。Amazon ECS は、デーモンの更新された CPU およびメモリ予約をピックアップし、デーモンのタスクでその容量をブロックします。

上記のいずれかの場合に十分なリソースがない場合、次のことが起こります。

- タスクの配置が失敗します。
- CloudWatch イベントが生成されます。
- Amazon ECS は、リソースが使用可能になるのを待って、インスタンスでタスクのスケジュールを試行します。
- Amazon ECS は、配置制約基準を満たさなくなったリザーブドインスタンスを解放し、対応するデーモンタスクを停止します。

デーモンのスケジューリング戦略は、次の場合に使用できます。

- アプリケーションコンテナの実行
- ログ記録、モニタリング、トレースタスク用のサポートコンテナの実行

Fargate 起動タイプ、 CODE_DEPLOY または EXTERNALデプロイメントコントローラータイプを使用するタスクは、スケジューリング戦略をサポートしません。

サービススケジューラがタスクの実行を停止する場合、アベイラビリティーゾーン間のクラスターの負荷バランスを維持します。スケジューラは、次のロジックを使用します。

- 配置戦略が定義されている場合、その戦略を使用して終了するタスクを選択します。例えば、サービスにアベイラビリティーゾーンの spread 戦略が定義されている場合、1 つのタスクが選択され、残りのタスクは最適に分散されたまま残ります。
- 配置戦略が定義されていない場合は、次のロジックを使用してクラスター内のアベイラビリティーゾーン全体への配分を維持します。
  - 有効なコンテナインスタンスをソートします。それぞれのアベイラビリティーゾーンで、このサービスの実行中のタスクの数が最も多いインスタンスを優先します。例えば、実行中のサービスタスクがゾーン A には 1 つ、ゾーン B とゾーン C にはそれぞれ 2 つずつある場合、ゾーン B またはゾーン C のいずれかのコンテナインスタンスが終了に最適と見なされます。
  - 前のステップに基づいて、最適なアベイラビリティーゾーン内のコンテナインスタンスで、タスクを停止します。このサービスで実行中のタスク数が最も多いコンテナインスタンスを優先します。

レプリカ戦略

レプリカスケジュール戦略では、クラスターに必要数のタスクを配置して維持します。

Fargate でタスクを実行するサービスについては、サービススケジューラは、新しいタスクの起動時や実行中タスクの停止時に、アベイラビリティーゾーン間の負荷バランスを維持するよう最大限試みます。タスク置き換え戦略や制約を指定する必要はありません。

EC2 インスタンスでタスクを実行するサービスを作成する場合、オプションでタスク配置戦略と制約を指定して、タスク配置に関する決定をカスタマイズできます。タスク配置戦略または制約が指定されていない場合、デフォルトでは、サービススケジューラはタスクをアベイラビリティーゾーン全体に分散します。サービススケジューラは、次のロジックを使用します。

- クラスター内のどのコンテナインスタンスがサービスのタスク定義をサポートできるか (必要な CPU、メモリ、ポート、コンテナインスタンス属性がなど) を判断します。
- サービスに定義された配置の制約を満たすコンテナインスタンスを特定します。
- デーモンサービスに依存するレプリカサービス (たとえば、タスクがログを使用する前に実行する必要があるデーモンログルータスクなど) がある場合は、デーモンサービスタスクがレプリカサービスタスクよりも前に EC2 インスタンスに配置されるようにするタスク置き換え制約を作成します。詳細については、「Amazon ECS タスク配置の制約事項の例」を参照してください。
- 配置戦略が定義されている場合は、その戦略を使用して残りの候補からインスタンスを選択します。

- 定義された配置戦略がない場合は、次のロジックを使用してクラスター内のアベイラビリティーゾーン全体にタスクが配分されます。
  - 有効なコンテナインスタンスをソートします。それぞれのアベイラビリティーゾーンで、このサービスの実行中のタスクの数が最も少ないインスタンスを優先します。例えば、ゾーン A に実行中のサービスタスクが 1 つあり、ゾーン B と C に実行中のサービスタスクがない場合、ゾーン B または C のいずれかの有効なコンテナインスタンスが配置に最適と見なされます。
  - 前のステップに基づいて、新しいサービスタスクを最適なアベイラビリティーゾーン内の有効なコンテナインスタンスに配置します。このサービスで実行中のタスク数が最も少ないコンテナインスタンスを優先します。

REPLICA 戦略を使用する際は、サービスの高可用性を確保するのに役立つため、サービスの再調整機能を使用することをお勧めします。

アベイラビリティーゾーン間での Amazon ECS サービスの調整

アプリケーションの高可用性を実現するために、マルチタスクサービスを複数のアベイラビリティーゾーンで実行するように設定することをお勧めします。最初の配置戦略をアベイラビリティーゾーンに分散するように指定するサービスの場合、AWS は可能な限り、使用可能なアベイラビリティーゾーン間でサービスタスクを均等に分散します。ただし、アベイラビリティーゾーンの中断後など、あるアベイラビリティーゾーンで実行されているタスク数が、他のアベイラビリティーゾーンで実行されているタスク数と同じではない場合があります。このタスクの不均衡に対処するには、アベイラビリティーゾーンの再調整機能を有効にします。アベイラビリティーゾーンの再調整により、Amazon ECS は各サービスのアベイラビリティーゾーン間のタスクの分散を継続的にモニタリングします。Amazon ECS は、不均等なタスク分散を検出すると、アベイラビリティーゾーン間でワークロードを再調整するアクションを自動的に実行します。これには、タスクが最も少ないアベイラビリティーゾーンで新しいタスクを起動し、オーバーロードされたアベイラビリティーゾーンでタスクを終了することが含まれます。この再分散により、単一のアベイラビリティーゾーンが障害点になることがなくなり、コンテナ化されたアプリケーションの全体的な可用性を維持できます。自動再調整プロセスにより、手動による介入が不要になり、イベント後の復旧までの時間が短縮されます。

アベイラビリティーゾーンの再調整プロセスの概要を次に示します。

1. Amazon ECS は、サービスが定常状態に達した後にモニタリングを開始し、各アベイラビリティーゾーンで実行されているタスク数を調べます。
2. Amazon ECS は、各アベイラビリティーゾーンで実行されているタスク数の不均衡を検出すると、次のオペレーションを実行します。

- アベイラビリティーゾーンの再調整が開始されていることを示すサービスイベントを送信します。
- 実行中のタスク数が最も少ないアベイラビリティーゾーンのタスクを開始します
- 実行中のタスク数が最も多いアベイラビリティーゾーンのタスクを停止します。
- スケジューラは、新しく開始されたタスクが HEALTHY および RUNNING になるのを待ってから、オーバースケーリングされたアベイラビリティーゾーンのタスクを停止します。
- アベイラビリティーゾーンの再調整結果を含むサービスイベントを送信します。

アベイラビリティーゾーンの再調整は、Fargate および EC2 起動タイプをサポートします。Fargate の場合、Amazon ECS はバランスを維持するために、使用可能なアベイラビリティーゾーン間でタスクを自動的に再分散します。EC2 起動タイプの場合、Amazon ECS は、定義された配置戦略と制約を考慮して、ベストエフォートベースで既存のコンテナインスタンス間でタスクを再調整します。ただし、Amazon ECS は再調整プロセスの一環として使用率の低いアベイラビリティーゾーンで新しいインスタンスを起動することができないため、再調整は既存のコンテナインスタンスに制限されます。

アベイラビリティーゾーンの再調整は、次の設定で機能します。

- `Replica` 戦略を使用するサービス
- アベイラビリティーゾーン分散を最初のタスク配置戦略として指定するサービス、または配置戦略を指定しないサービス。

アベイラビリティーゾーンの再調整は、次のいずれかの条件を満たすサービスでは使用できません。

- `Daemon` 戦略を使用する
- `EXTERNAL` 起動タイプ (ECS Anywhere) を使用する
- `maximumPercent` 値に 100% を使用する
- Classic Load Balancer を使用する
- `attribute:ecs.availability-zone` をタスク配置の制約として使用する

アベイラビリティーゾーンの再調整による配置戦略と配置制約

配置戦略により、Amazon ECS がタスク配置を終了するためのコンテナインスタンスとアベイラビリティーゾーンを選択する方法が決まります。タスク配置の制約は、タスクを特定のコンテナインスタンスで実行できるかどうかを決定するルールです。EC2 起動タイプでは、アベイラビリティー

ゾーンの再調整と組み合わせて配置戦略と配置制約を使用できます。ただし、アベイラビリティーゾーンの再調整が機能するには、アベイラビリティーゾーン分散配置戦略が最初に指定される戦略である必要があります。アベイラビリティーゾーンの再調整は、さまざまな配置戦略の組み合わせと互換性があります。例えば、最初にタスクをアベイラビリティーゾーン間で均等に分散し、次に各アベイラビリティーゾーン内のメモリに基づいてタスクをビンパックする戦略を作成できます。この場合、アベイラビリティーゾーンの分散戦略が最初に指定されているため、アベイラビリティーゾーンの再調整は機能します。配置戦略配列の最初の戦略がアベイラビリティーゾーン分散コンポーネントではない場合、アベイラビリティーゾーンの再調整は機能しないことに注意してください。この要件により、タスク分散の主な焦点は、高可用性にとって重要なアベイラビリティーゾーン間のバランスを維持することです。タスク配置の戦略と制約の詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

次の戦略例は、アベイラビリティーゾーン間でタスクを均等に分散し、次に各アベイラビリティーゾーン内でメモリに基づいてタスクをビンパックします。spread 戦略が最初に行われるため、アベイラビリティーゾーンの再調整はサービスと互換性があります。

```
"placementStrategy": [
    {
        "field": "attribute:ecs.availability-zone",
        "type": "spread"
    },
    {
        "field": "memory",
        "type": "binpack"
    }
]
```

アベイラビリティーゾーンの再調整を有効にする

新規および既存のサービスに対してアベイラビリティーゾーンの再調整を有効にする必要があります。

コンソール、API、または AWS CLI を使用して、アベイラビリティーゾーンの再調整を有効または無効にできます。

サービスタイプ	API	コンソール	CLI
既存	UpdateService	コンソールを使用した Amazon ECS サービスの更新	update-service
新	CreateService	コンソールを使用した Amazon ECS サービスの作成	サービスの作成

Amazon ECS アベイラビリティーゾーンの再調整を追跡する

アベイラビリティーゾーンの再調整がサービスに対して有効になっているかどうかは、コンソールで確認するか、`describe-services` を呼び出して確認できます。次の例を使用して、CLI でステータスを確認できます。

レスポンスは `ENABLED` または `DISABLED` のいずれかになります。

```
aws ecs describe-services \
    --services service-name \
    --cluster cluster-name \
    --query services[0].availabilityZoneRebalancing
```

サービスイベント

Amazon ECS は、アベイラビリティーゾーンの再調整ライフサイクルを理解するのに役立つサービスアクションイベントを送信します。

イベント	シナリオ	タイプ	詳細はこちら
SERVICE_REBALANCING_STARTED	Amazon ECS がアベイラビリティーゾーンの再調整オペレーションを開始	INFO	サービス *(service-name)* は、*Availability Zone 1* の *number-tasks* タスク、*Availability Zone 2* の

イベント	シナリオ	タイプ	詳細はこちら
			number-tasks タスク、*Availability Zone 3* の *number-tasks* タスクで AZ が調整されていません。AZ の再調整は進行中です。
SERVICE_REBALANCING_COMPLETED	アベイラビリティーゾーンの再調整オペレーションが完了	INFO	サービス (*service-name*) は、*Availability Zone 1* の *number-tasks* タスク、*Availability Zone 2* の *number-tasks* タスク、*Availability Zone 3* の *number-tasks* タスクで AZ が調整されています。
TASKS_STARTED	Amazon ECS がアベイラビリティーゾーンの再調整オペレーションの一環としてタスクを正常に開始	INFO	*service-name* は、AZ の再調整のために *Availability Zone* の *number-tasks* タスクを開始しました: *task-ids*。

イベント	シナリオ	タイプ	詳細はこちら
TASKS_STOPPED	Amazon ECS がアベイラビリティーゾーンの再調整オペレーションの一環としてタスクを正常に停止	INFO	*service-name* は、AZ の再調整のために *Availability Zone* の実行中の *number-tasks* タスクを停止しました: *task-ids*。
SERVICE_TASK_PLACEMENT_FAILURE	Amazon ECS がアベイラビリティーゾーンの再調整オペレーションの一環としてタスクを開始することに失敗	ERROR	EC2 起動タイプについては、「サービス (*service-name*) で、すべての要件を満たしたコンテナインスタンスがないため、*Availability Zone* にタスクを配置できません。」を参照してください Fargate 起動タイプについては、「サービス (*service-name*) で、*Availability Zone* にタスクを配置できません。」を参照してください
TASKSET_SCALE_IN_FAILURE_BY_TASK_PROTECTION	タスク保護が使用されているため、アベイラビリティーゾーンの再調整オペレーションはブロックされます。	INFO	サービス (*service-name*) で、*task-set-name* が *reason* によりスケールインできなかったため、AZ を再調整できませんでした。

イベント	シナリオ	タイプ	詳細はこちら
SERVICE_REBALANCING_STOPPED	アベイラビリティーゾーンの再調整オペレーションが停止。Amazon ECS は、詳細情報を提供する追加のイベントを送信します。	INFO	サービス (*service-name*) が AZ の再調整を停止しました。

タスク状態変更イベント

Amazon ECS は、再調整プロセスの一環として開始されるタスクごとに、タスク状態変更イベント (START) を送信します。

Amazon ECS は、再調整プロセスの一環として停止するタスクごとに、タスク状態変更イベント (STOPPED) イベントを送信します。理由は `Availability Zone rebalancing initiated by (deployment ecs-svc/`*deployment-id*`)` に設定されています。

イベントの詳細については、「Amazon ECS タスク状態変更イベント」を参照してください。

コンソールを使用した Amazon ECS サービスの作成

タスク定義の指定された数のインスタンスをクラスター内で同時に実行して維持するサービスを作成します。タスクの 1 つが失敗または停止した場合、Amazon ECS サービススケジューラはタスク定義の別のインスタンスを起動してそれを置き換えます。これは、サービスで必要な数のタスクを維持するのに役立ちます。

サービスを作成する前に、次の設定パラメータを決定します。

- タスクを分散するコンピューティングオプションが 2 つあります。
  - [capacity provider strategy] (キャパシティープロバイダー戦略) により、Amazon ECS がタスクを 1 つまたは複数のキャパシティプロバイダーに分散させます。
  - [起動タイプ] により、Amazon ECS は Fargate またはクラスターに登録された EC2 インスタンスのいずれかでタスクを直接起動します。
- `awsvpc` ネットワークモードを使用するタスク定義、またはロードバランサーを使用するように設定されたサービスには、ネットワーク設定が必要です。デフォルトでは、コンソールは、デフォル

トAmazon VPC 内のすべてのサブネットおよびデフォルトセキュリティグループとともにデフォルトのAmazon VPC を選択します。

- 配置戦略、デフォルトのタスク配置戦略は、アベイラビリティーゾーン間でタスクを均等に分散します。

  サービスの高可用性を確保するために、アベイラビリティーゾーンの再調整を使用することをお勧めします。詳細については、「アベイラビリティーゾーン間での Amazon ECS サービスの調整」を参照してください。

- サービスデプロイに [Launch Type] (起動タイプ) を使用するバージョン、デフォルトではクラスター VPC のサブネットでサービスが開始されます。
- [capacity provider strategy] (キャパシティープロバイダー戦略) では、コンソールはデフォルトでコンピューティングオプションを選択します。次に、コンソールがデフォルトを選択するときに使用する順序について説明します。
  - クラスターにデフォルトのキャパシティープロバイダー戦略が定義されている場合は、その戦略が選択されます。
  - クラスターにデフォルトのキャパシティープロバイダー戦略が定義されていないが、Fargate キャパシティープロバイダーをクラスターに追加している場合は、キャパシティープロバイダーを使用するカスタム FARGATE キャパシティープロバイダー戦略が選択されます。
  - クラスターにデフォルトのキャパシティープロバイダー戦略が定義されていないが、クラスターに 1 つ以上の Auto Scaling グループキャパシティープロバイダーが追加されている場合は、[Use custom (アドバンスト)] オプションが選択され、戦略を手動で定義する必要があります。
  - クラスターにデフォルトのキャパシティープロバイダー戦略が定義されておらず、クラスターにキャパシティープロバイダーが追加されていない場合は、Fargate起動タイプが選択されます。
- デプロイの失敗が検出された場合のデフォルトのオプションでは、[Amazon ECS デプロイサーキットブレーカー] オプションと [失敗時のロールバック] オプションを使用します。

  詳細については、「 Amazon ECS デプロイサーキットブレーカーが障害を検出する方法」を参照してください。

- ブルー/グリーンデプロイオプションを使用する場合は、CodeDeploy でアプリケーションをどのように移動させるかを決めてください。以下のオプションが利用できます。
  - [CodeDeployDefault.ECSAllAtOnce]: すべてのトラフィックを同時に更新済みの Amazon ECS コンテナに移行します。
  - CodeDeployDefault.ECSLinear10PercentEvery1Minutes: すべてのトラフィックがシフトされるまで、1 分ごとにトラフィックの 10 パーセントをシフトします。

  - CodeDeployDefault.ECSLinear10PercentEvery3Minutes: すべてのトラフィックがシフトされるまで、3 分ごとにトラフィックの 10 パーセントをシフトします。
  - [CodeDeployDefault.ECSCanary10Percent5Minutes]: 最初の増分で 10 パーセントのトラフィックをシフトします。残りの 90 パーセントは 5 分後にデプロイされます。
  - [CodeDeployDefault.ECSCanary10percent15Minutes]: 最初の増分で 10 パーセントのトラフィックをシフトします。残りの 90 パーセントは 15 分後にデプロイされます。
- Amazon ECS でサービス内の必要なタスク数を自動的に増減するかどうかを決定します。詳細については、「Amazon ECS サービスを自動的にスケールする」を参照してください。
- Amazon ECS 内で実行される他のアプリケーションにアプリケーションを接続する必要がある場合、アーキテクチャに適したオプションを決定してください。詳細については、「Amazon ECS サービスを相互接続する」を参照してください。
- Amazon ECS サーキットブレーカーを使用するサービスを作成すると、Amazon ECS はサービスデプロイとサービスリビジョンを作成します。これらのリソースを使用すると、サービス履歴に関する詳細情報を表示できます。詳細については、「Amazon ECS サービスデプロイを使用してサービス履歴を表示する」を参照してください。

  AWS CLI を使用してサービスを作成する方法については、「AWS Command Line Interface リファレンス」の「create-service」を参照してください。

  AWS CloudFormation を使用してサービスを作成する方法については、「AWS CloudFormation ユーザーガイド」の「AWS::ECS::Service」を参照してください。

デフォルトのオプションを使用してサービスを作成する

コンソールを使用すると、サービスをすばやく作成してデプロイできます。サービスには次の設定があります。

- クラスターに関連する VPC およびサブネットにデプロイします
- タスクを 1 つ展開します
- ローリングデプロイを使用します
- デフォルトのキャパシティプロバイダーでキャパシティプロバイダー戦略を使用します
- デプロイサーキットブレーカーを使用して障害を検出し、障害時にデプロイを自動的にロールバックするオプションを設定します。

デフォルトパラメータを使用してサービスをデプロイするには、次の手順に従います。

サービスを作成するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションページで、[クラスター] を選択します。
3. [クラスター] ページで、サービスを作成するクラスターを選択します。
4. [Services] (サービス) タブから、[Create] (作成) を選択します。
5. [Deployment configure] (デプロイ設定) で、アプリケーションのデプロイ方法を指定します。
   a. [Application type] (アプリケーションの種類) で、[Service] (サービス) を選択します。
   b. [Task definition] (タスク定義) の場合、使用するタスク定義ファミリーとリビジョンを選択します。
   c. [Service name] (サービス名) でサービスの名前を入力します。
   d. [Desired tasks] (必要なタスク) で、サービス内で起動および維持するタスクの数を入力します。
6. （オプション）サービスとタスクを識別しやすくするには、[Tags] (タグ) セクションを展開し、タグを設定します。

   Amazon ECS で、新しく起動されたすべてのタスクに、クラスター名とタスク定義のタグで自動でタグ付けするには、[Turn on Amazon ECS managed tags] (Amazon ECS で管理されたタグを有効にする) を選択し、[Task definition] (タスク定義) を選択します。

   Amazon ECS で、新しく起動されたすべてのタスクに、クラスター名とサービスタグを自動でタグ付けするには、[Turn on Amazon ECS managed tags] (Amazon ECS で管理されたタグを有効にする) を選択し、[Service] (サービス) を選択します。

   タグを追加または削除します。

   - [タグを追加] [Add tag] (タグを追加) を選択し、以下を実行します。
     - [キー] にはキー名を入力します。
     - [値] にキー値を入力します。
   - [タグの削除] タグの横にある [タグの削除] を選択します。

定義済みのパラメータを使用したサービスの作成

定義済みのパラメータを使用してサービスを作成するには、次の手順に従います。

サービスを作成するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. サービスを起動するリソースを決定します。

サービスの起動元	ステップ
クラスター	a. [Clusters] ページで、サービスを作成するクラスターを選択します。 b. [Services] (サービス) タブから、[Create] (作成) を選択します。
起動タイプ	a. [タスク定義] ページで、タスク定義の横にあるオプションボタンを選択します。 b. [デプロイ] メニューで [サービスを作成] を選択します。

3. (オプション) クラスターのインフラストラクチャ全体にタスクを分散する方法を選択します。[Compute configuration] (コンピュート設定) を展開し、オプションを選択します。

ディストリビューションの方法	ステップ
キャパシティープロバイダー戦略	a. [コンピューティングオプション] で、[キャパシティープロバイダー戦略] を選択します。 b. 戦略を選択: • デフォルトのキャパシティープロバイダー戦略を使用するに

ディストリビューションの方法	ステップ
	は、[Use cluster default] (デフォルトのクラスターを使用) を選択します。 • クラスターにデフォルトのキャパシティプロバイダー戦略がない場合、またはカスタム戦略を使用する場合は、[カスタムを使用]、[キャパシティプロバイダー戦略を追加] を選択し、[ベース]、[キャパシティプロバイダー]、[重み] を指定して、カスタムキャパシティプロバイダー戦略を定義します。 **Note** 戦略でキャパシティープロバイダーを使用するには、キャパシティープロバイダーをクラスターに関連付ける必要があります。

ディストリビューションの方法	ステップ	
起動タイプ	a. [Compute options] (コンピューティングオプション) セクションで、[Launch type] (起動タイプ) を選択します。 b. [Launch type] (起動タイプ) で、起動タイプを選択します。 c. (オプション) Fargate 起動タイプが指定されている場合、Platform version(プラットフォームのバージョン)で、使用するプラットフォームのバージョンを指定します。プラットフォームバージョンが指定されない場合、LATEST プラットフォームバージョンが使用されます。	

4. サービスのデプロイ方法を指定するには、[デプロイ設定] に移動してから、オプションを選択します。

   a. [アプリケーションタイプ] では、[サービス] が選択されたままにします。

   b. [Task definition] (タスク定義) と [Revision] (リビジョン) の場合、使用するタスク定義ファミリーとリビジョンを選択します。

   c. [Service name] (サービス名) でサービスの名前を入力します。

   d. [Service type] (サービスタイプ) で、サービススケジューリング戦略を選択します。

      - タスク配置の制約をすべて満たすアクティブなコンテナインスタンスに、スケジューラが正確に 1 つのタスクをデプロイするには、[Daemon] (デーモン) を選択します。

- スケジューラがクラスターに必要数のタスクを配置して維持するためには、[Replica] (レプリカ) を選択します。

e. [Replica] (レプリカ) を使用した場合、[Desired tasks] (必要なタスク) に、サービス内で起動および維持するタスクの数を入力します。

f. [レプリカ] を選択した場合、Amazon ECS がアベイラビリティーゾーン間のタスクの分散をモニタリングし、不均衡が発生したときにタスクを再分散させるには、[アベイラビリティーゾーンのサービス再調整] で、[アベイラビリティーゾーンのサービス再調整] を選択します。

g. サービスのデプロイタイプを決定してください。[デプロイオプション] を展開し、次のパラメータを指定します。

デプロイタイプ	ステップ	
ローリング更新	a. [Min running tasks] (実行中のタスクの最小化) の場合、デプロイ時に RUNNING の状態に保つ必要のあるサービス内のタスクの下限数をタスクの必要数のパーセント値 (最も近い整数に切り上げ) で入力します。詳細については、[Deployment configuration] (デプロイ設定) を参照してください。 b. [Max running tasks] (実行中のタスクの最大化)) には、デプロイ時に RUNNING または PENDING 状態にできるサービスのタスクの上限数を必要数のタスクのパーセント値 (最も近い整数に切り下げ) で入力します。	

デプロイタイプ	ステップ	
ブルー/グリーンデプロイ	a. デプロイ構成 には、CodeDeployがデプロイ中に本番トラフィックを置き換えタスクセットにルーティングする方法を選択します。 b. [CodeDeploy のサービスロール] では、承認された AWS のサービス に API リクエストを行うためにサービスが使用する IAM ロールを選択します。	

h. Amazon ECS がデプロイの障害を検出して処理する方法を設定するには、[Deployment failure detection] (デプロイ障害検出) を展開し、オプションを選択します。

i. タスクを開始できない場合にデプロイを停止するには、[Use the Amazon ECS deployment circuit breaker] (Amazon ECS デプロイサーキットブレーカーを使用する) を選択します。

デプロイサーキットブレーカーによってデプロイが失敗状態に設定されたときに、ソフトウェアがデプロイを最後に完了したデプロイ状態に自動的にロールバックするようにするには、[失敗時のロールバック] を選択します。

ii. アプリケーションメトリクスに基づいてデプロイを停止するには、[CloudWatch アラームを使用する] を選択します。次に、[CloudWatch アラーム名] からアラームを選択します。新しいアラームを作成するには、CloudWatch コンソールに移動します。

CloudWatch アラームによってデプロイが失敗状態に設定されたときに、ソフトウェアがデプロイを最後に完了したデプロイ状態に自動的にロールバックするようにするには、[失敗時のロールバック] を選択します。

5. (オプション) Service Connect を使用するには、[Turn on Service Connect] (Service Connect をオンにする) を選択し、以下を指定します。

a. [Service Connect configuration] (Service Connect 設定) で、クライアントモードを指定します。

- サービスが名前空間内の他のサービスへの接続のみを必要とするネットワーククライアントアプリケーションを実行している場合は、[クライアント側のみ] を選択します。
- サービスがネットワークまたは Web サービスアプリケーションを実行していて、このサービスにエンドポイントを提供し、名前空間内の他のサービスに接続する必要がある場合は、[Client and server] (クライアントとサーバー) を選択します。

b. デフォルトのクラスター名前空間ではない名前空間を使用するには、[Namespace] (名前空間) でサービス名前空間を選択します。

c. (オプション) [Use log collection] (ログコレクションを使用) を選択し、ログ構成を指定します。使用可能なログドライバーごとに、指定するログドライバーオプションがあります。デフォルトのオプションでは、コンテナログを CloudWatch Logs に送信します。その他のログドライバオプションは、AWS FireLens を使用して構成されます。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。

以下では、各コンテナログの送信先について詳しく説明します。

- Amazon CloudWatch — コンテナログを CloudWatch Logs に送信するようにタスクを設定します。デフォルトのログドライバーオプションが提供され、ユーザーに代わり CloudWatch ロググループを作成します。別のロググループ名を指定するには、ドライバーオプションの値を変更します。
- [Amazon Data Firehose] — Firehose にコンテナログを送信するようタスクを設定します。Firehose 配信ストリームにログを送信するデフォルトのログドライバーオプションが提供されています。別の配信ストリーム名を指定するには、ドライバーオプションの値を変更します。
- Amazon Kinesis Data Streams — Kinesis Data Streams にコンテナログを送信するようタスクを設定します。Kinesis Data Streams のストリームにログを送信するデフォルトのログドライバーオプションが提供されています。別のストリーム名を指定するには、ドライバーオプションの値を変更します。
- Amazon OpenSearch Service — コンテナログを OpenSearch Service ドメインに送信するようタスクを設定します。ログドライバーオプションを提供する必要があります。
- Amazon S3 — Amazon S3 バケットにコンテナログを送信するようタスクを設定します。デフォルトのログドライバーオプションが提供されていますが、有効な Amazon S3 バケット名を指定する必要があります。

6. (オプション) サービス検出を使用するには、[サービス検出を使用] を選択し、以下を指定します。

a. 新しい名前空間を使用するには、[名前空間の設定] で [新しい名前空間の作成] を選択し、名前空間の名前と説明を入力します。既存の名前空間を使用するには、[既存の名前空間を選択] を選択し、使用する名前空間を選択します。

b. サービスの名前や説明などのサービス検出サービス情報を入力します。

c. Amazon ECS にコンテナレベルのヘルスチェックを定期的に実行させるには、[Amazon ECS タスク状態の伝達の有効化] を選択します。

d. [DNS record type (DNS レコード型)] で、サービスに作成する DNS レコード型を選択します。Amazon ECS サービス検出は、タスク定義で指定されたネットワークモードに応じて、[A] レコードおよび [SRV] レコードのみをサポートします。これらのレコードタイプの詳細については、Amazon Route 53 デベロッパーガイドのサポートされているDNSレコードタイプを参照してください。

- サービスタスクで指定されたタスク定義が `bridge` または `host` ネットワークモードを使用する場合、SRV タイプのレコードのみがサポートされます。レコードに関連付けるコンテナ名とポートの組み合わせを選択します。
- サービスタスクで指定されたタスク定義が `awsvpc` ネットワークモードを使用する場合、A または SRV レコードタイプのいずれかを選択します。[A] を選択した場合は、次の手順をスキップします。[SRV] を選択する場合は、サービスを検出できるポートまたはレコードに関連付けるコンテナ名とポートの組み合わせを指定します。

TTL には、レコードセットが DNS リゾルバーおよびウェブブラウザによってキャッシュされる時間を秒単位で入力します。

7. (オプション) サービスのロードバランサーを設定するには、[Load Balancing] (負荷分散) セクションを展開します。

ロードバランサーを選択します。

このロードバランサーを使用するには	この操作を行います
Application Load Balancer	a. [Load balancer type] で、[Application Load Balancer] を選択します。 b. 選択新しいロードバランサーを作成するをクリッ

このロードバランサーを使用するには	この操作を行います	
	クして新しいApplication Load Balancer を作成するか、既存のロードバランサーを使用する既存のApplication Load Balancer を選択します。 c. [Load balancer name] (ロードバランサー名) では、一意な名前を入力します。 d. [Choose container to load balance] (負荷分散するコンテナを選択) で、サービスをホストするコンテナを選択します。 e. [Listener] (リスナー) で、Application Load Balancer が接続リクエストをリッスンするポートとプロトコルを入力します。デフォルトでは、ロードバランサーはポート 80 と HTTP を使用するように設定されます。 f. [Target group name] (ターゲットグループ名) では、Application Load Balancer がリクエストをルーティングするターゲットグループの名前とプロトコルを入力します。デフォルトでは、ターゲットグループは、タス	

このロードバランサーを使用するには	この操作を行います	
	ク定義で定義されている最初のコンテナにリクエストをルーティングします。 g. [登録の遅延] には、ロードバランサーがターゲットの状態を UNUSED に変更するまでの秒数を入力します。デフォルトは 300 秒です。 h. [Health check path] (ヘルスチェックパス) では、Application Load Balancer とコンテナ間の接続の正常性を検証するために、Application Load Balancer が定期的にリクエストを送信するコンテナ内に存在するパスを入力します。デフォルトはルートディレクトリ (/)。 i. [Health check grace period] (ヘルスチェックの猶予期間) では、サービススケジューラが不健全な Elastic Load Balancing ターゲットヘルスチェックを無視する時間 (秒単位) を入力します。	

このロードバランサーを使用するには	この操作を行います
Network Load Balancer	a. [Load balancer type] (ロードバランサータイプ) では、[Network Load Balancer] を選択します。 b. [Load Balancer] (ロードバランサー) では、既存の Network Load Balancer を選択します。 c. [Choose container to load balance] (負荷分散するコンテナを選択) で、サービスをホストするコンテナを選択します。 d. [Target group name] (ターゲットグループ名) では、Network Load Balancer がリクエストをルーティングするターゲットグループの名前とプロトコルを入力します。デフォルトでは、ターゲットグループは、タスク定義で定義されている最初のコンテナにリクエストをルーティングします。 e. [登録の遅延] には、ロードバランサーがターゲットの状態を UNUSED に変更するまでの秒数を入力します。デフォルトは 300 秒です。

このロードバランサーを使用するには	この操作を行います	
	f. [Health check path] (ヘルスチェックパス) では、Application Load Balancer とコンテナ間の接続の正常性を検証するために、Network Load Balancer が定期的にリクエストを送信するコンテナ内に存在するパスを入力します。デフォルトはルートディレクトリ (/)。 g. [Health check grace period] (ヘルスチェックの猶予期間) では、サービススケジューラが不健全な Elastic Load Balancing ターゲットヘルスチェックを無視する時間 (秒単位) を入力します。	

8. (オプション) VPC Lattice を使用するには、[VPC Lattice を有効にする] を選択し、次に以下を指定します。

   a. インフラストラクチャロール については、インフラストラクチャロールを選択します。

      ロールを作成していない場合は、[インフラストラクチャロールの作成] を選択します。

   b. [ターゲットグループ] で、1 つまたは複数のターゲットグループを選択します。少なくとも 1 つのターゲットグループを選択する必要があります。最大 5 つのターゲットグループを選択できます。追加のターゲットグループを追加するには、[ターゲットグループの追加] を選択します。選択した各ターゲットグループの [ポート名]、[プロトコル]、および [ポート] を選択します。

      ターゲットグループを削除するには、[削除] を選択します。

> **Note**
>
> - 既存のターゲットグループを追加する場合は、AWS CLI を使用する必要があります。AWS CLI を使用してターゲットグループを追加する方法については、「AWS Command Line Interface リファレンス」の「register-targets」を参照してください。
> - VPC Lattice サービスは複数のターゲットグループを持つことができますが、各ターゲットグループは 1 つのサービスにのみ追加できます。

c. VPC Lattice 設定を完了するには、リスナーのデフォルトアクションに新しいターゲットグループを含めるか、VPC Lattice コンソール内の既存の VPC Lattice サービスのルールに新しいターゲットグループを含めます。詳細については、「Listener rules for your VPC Lattice service」を参照してください。

9. (オプション) サービスの Auto Scaling を設定するには、[サービスの自動スケーリング] を展開し、次のパラメータを指定します。

   a. サービスの自動スケーリングを使用するには、[Service auto scaling] (サービスの自動スケーリング) を選択します。

   b. [タスクの最小数] に、サービスの自動スケーリングで使用するタスクの下限数を入力します。必要な数がこの数を下回ることはありません。

   c. [タスクの最大数] に、サービスの自動スケーリングで使用するタスクの上限数を入力します。必要な数がこの数を超えることはありません。

   d. ポリシータイプを選択します。[スケーリングポリシータイプ] で、次のいずれかのオプションを選択します。

使用するポリシータイプ	この操作を行います	
ターゲット追跡	a. [スケーリングポリシータイプ] で [ターゲットの追跡] を選択します。 b. [Policy Name] (ポリシー名) にこのポリシーの名前を入力します。	

使用するポリシータイプ	この操作を行います	
	c. [ECS サービスメトリクス] で次のいずれかのメトリクスを選択します。 • [ECSServiceAverageCPUUtilization] — サービスの平均 CPU 使用率。 • [ECSServiceAverageMemoryUtilization] — サービスのメモリ平均使用率。 • [ALBRequestCountPerTarget] - Application Load Balancer ターゲットグループ内のターゲットごとに完了したリクエストの数。 d. [Target value] (ターゲット値) には、選択したメトリックに対してサービスが保持する値を入力します。 e. [スケールアウトのクールダウン期間] には、スケールインアクティビティが完了してから別のスケールアウトアクティビティが開始されるまでの時間 (秒) を入力します。 f. [スケールインのクールダウン期間] には、スケールインアクティビ	

使用するポリシータイプ	この操作を行います	
	ティが完了してから別のスケールインアクティビティが開始されるまでの時間 (秒) を入力します。 g. ポリシーがスケールインアクティビティを実行しないようにするには、[Turn off scale-in] (スケールインをオフにする) を選択します。 h. • (オプション) トラフィックの増加に合わせてスケーリングポリシーをスケールアウトさせたいが、トラフィックが減少してもスケールインする必要がない場合は、[スケールインをオフにする] を選択します。	

使用するポリシータイプ	この操作を行います	
ステップスケーリング	a. [スケーリングポリシータイプ] で [ステップスケーリング] を選択します。 b. [ポリシー名] で、このポリシー名を入力します。 c. [アラーム名] に、アラームの一意の名前を入力します。 d. [Amazon ECS サービスメトリクス] で、アラームに使用するサービスメトリクスを選択します。 e. [統計] で、アラーム統計を選択します。 f. [期間] で、アラームの期間を選択します。 g. [アラーム条件] で、選択したメトリクスを定義されたしきい値と比較する方法を選択します。 h. [メトリクスを比較するためのしきい値] と [アラームを開始する評価期間] に、アラームに使用するしきい値としきい値を評価する期間を入力します。 i. [スケーリングアクション]で、次の手順を実行します。 • [アクション] には、サービスに対してタス	

使用するポリシータイプ	この操作を行います	
	クを追加する、削除する、または特定の必要数を設定するかを選択します。 • タスクの追加または削除を選択した場合は、スケーリングアクションの開始時に追加または削除するタスクの数 (または既存のタスクの割合) を [値] に入力します。希望の数を設定することを選択した場合は、タスクの数を入力します。[タイプ] で、[値] が整数であるか、既存の必要なカウントのパーセント値であるかを選択します。 • [下限] と [上限] に、ステップスケーリング調整の下限と上限を入力します。デフォルトでは、[ポリシーを追加] の下限はアラームしきい値であり、上限は正 (+) の無限大です。デフォルトでは、[ポリシーを削除] の上限はアラームしきい値であり、下限は負 (-) の無限大です。	

使用するポリシータイプ	この操作を行います	
	• (オプション) さらにスケーリングオプションを追加します。[新しいスケーリングアクションの追加] を選択し、[アクションのスケーリング] の手順を繰り返します。 • [クールダウン期間] には、前回のスケーリングアクティビティが有効になるまで待機する時間を秒単位で入力します。追加ポリシーの場合、スケールアウトアクティビティの終了後、スケーリングポリシーによってスケールインアクティビティがブロックされ、一度にスケールアウトできるタスクの数が制限されます。削除ポリシーの場合、これはスケールインアクティビティの後、別のスケールインアクティビティが開始されるまでに経過する必要がある時間です。	

10. (オプション) デフォルト以外のタスク配置戦略を使用するには、[Task Placement] (タスクの配置) を展開し、以下のオプションから選択します。

    詳細については、「Amazon ECS がタスクをコンテナインスタンスに配置する方法」を参照してください。

- [AZ バランススプレッド] - アベイラビリティーゾーン間およびアベイラビリティーゾーン内のコンテナインスタンス間でタスクを分散します。
- [AZ Balanced BinPack] - 利用可能な最小メモリでアベイラビリティーゾーン間およびコンテナインスタンス間でタスクを分散します。
- [ビンパック] - CPU またはメモリの最小利用可能量に基づいてタスクを配置します。
- [ホストごとに 1 つのタスク] - 各コンテナインスタンスのサービスから最大 1 タスクを配置します。
- [カスタム] - 独自のタスク配置戦略を定義します。

[Custom] (カスタム) を選択した場合、タスクを配置するアルゴリズムと、タスク配置時に考慮されるルールを定義します。

- [Strategy] (方針) にとって [Type] (タイプ) そして [Field] (フィールド) で、アルゴリズムとアルゴリズムに使用するエンティティを選択します。

  最大 5 個の戦略を入力できます。
- [制約] の [タイプ] および [式] で、制約のルールと属性を選択します。

  例えば、T2 インスタンスにタスクを配置する制約を設定するには、[Expression] (表現) で、[attribute:ecs.instance-type =~ t2.*] と入力します。

  最大 10 個の制約を入力できます。

11. タスク定義で awsvpc ネットワークモードを使用している場合、[Networking] (ネットワーク) を展開します。カスタム設定を指定するには、次のステップを実行します。

    a. VPC の場合、使用する VPC を選択します。

    b. [Subnets] (サブネット) で、タスクスケジューラがタスクを配置するときに考慮する VPC 内のサブネットを 1 つ以上選択します。

    > **Important**
    >
    > awsvpc ネットワークモードではプライベートサブネットだけがサポートされます。タスクはパブリック IP アドレスを受信しません。したがって、アウトバウンドのインターネットアクセスには NAT ゲートウェイが必要であり、またインバウンドのインターネットトラフィックは、ロードバランサーを経由します。

c. [Security groups] (セキュリティグループ) で、既存のセキュリティグループを選択することも、新しいセキュリティグループを作成することもできます。既存のセキュリティグループを使用するには、セキュリティグループを選択し、次のステップに進みます。新しいセキュリティグループを作成するには、[Create a new security group (新しいセキュリティグループの作成)] を選択します。セキュリティグループの名前、説明を指定してから、セキュリティグループのインバウンドルールを 1 つ以上追加する必要があります。

d. [Public IP] (パブリック IP) では、タスクの Elastic Network Interface (ENI) にパブリック IP アドレスを自動的に割り当てるかどうかを選択します。

   AWS Fargate タスクをパブリックサブネットで実行するときに、そのタスクにパブリック IP アドレスを割り当てて、インターネットへのルートを持つようにすることができます。このフィールドを使用して EC2 タスクにパブリック IP を割り当てることはできません。詳細については、「Fargate 起動タイプの Amazon ECS タスクネットワーキングオプション」および「Amazon ECS タスクへのネットワークインターフェイスの割り当て」を参照してください。

12. デプロイ時の設定と互換性のあるデータボリュームをタスクで使用する場合は、[ボリューム] を拡張してボリュームを設定できます。

    ボリューム名とボリュームタイプはタスク定義リビジョンを作成するときに設定され、サービスの作成時には変更できません。ボリューム名とタイプを更新するには、新しいタスク定義リビジョンを作成し、その新しいリビジョンを使用してサービスを作成する必要があります。

このボリュームタイプを設定するには	この操作を行います	
Amazon EBS	a. [EBS ボリュームタイプ] には、タスクにアタッチする EBS ボリュームのタイプを選択します。 b. [サイズ (GiB)] には、ボリュームサイズの有効な値をギビバイト (GiB) 単位で入力します。最小で 1 GiB、最大で 16,384 GiB のボリュームサイズを指定できます。スナッ	

このボリュームタイプを設定するには	この操作を行います	
	プショット ID を指定しない限り、この値は必須です。 c. [IOPS] には、ボリュームが提供する入力/出力オペレーションの数 (IOPS) の最大数を入力します。この値は io1、io2、および gp3 ボリュームタイプでのみ設定できます。 d. [スループット (MiB/秒)] には、ボリュームが提供すべきスループットをメビバイト/秒 (MiBps または MiB/s) で入力します。この値は gp3 ボリュームタイプでのみ設定できます。 e. [スナップショット ID] には、既存の Amazon EBS ボリュームスナップショットを選択するか、スナップショットからボリュームを作成する場合はスナップショットの ARN を入力します。新しい空のボリュームは、スナップショット ID を選択または入力しないで作成できます。 f. [ファイルシステムのタイプ] では、ボリューム上のデータストレージおよび	

このボリュームタイプを設定するには	この操作を行います	
	取得に使用するファイルシステムの種類を選択します。オペレーティングシステムのデフォルトまたは特定のファイルシステムタイプのいずれかを選択できます。Linux のデフォルトは XFS です。スナップショットから作成されたボリュームでは、スナップショットの作成時にボリュームが使用していたのと同じファイルシステムタイプを指定する必要があります。ファイルシステムのタイプが一致しない場合、タスクは開始できません。 g. [インフラストラクチャロール] には、Amazon ECS がタスクの Amazon EBS ボリュームを管理できるようにするために必要な権限を持つ IAM ロールを選択します。AmazonECSInfrastructureRolePolicyForVolumes 管理ポリシーをロールにアタッチすることも、このポリシーをガイドとして使用して、特定のニーズを満たすアクセス権限	

このボリュームタイプを設定するには	この操作を行います	
	を持つ独自のポリシーを作成してアタッチすることもできます。必要なアクセス権限の詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。 h. デフォルト設定で Amazon EBS 暗号化を使用する場合は、[暗号化] で [デフォルト] を選択します。アカウントにデフォルトで暗号化が設定されている場合、ボリュームは設定で指定されている AWS Key Management Service (AWS KMS) キーで暗号化されます。[デフォルト] を選択し、Amazon EBS のデフォルト暗号化がオンになっていない場合、ボリュームは暗号化されません。 [カスタム] を選択した場合は、ボリューム暗号化に任意の AWS KMS key を指定できます。 [なし] を選択すると、デフォルトで暗号化が設定されている場合や、暗号化	

このボリュームタイプを設定するには	この操作を行います	
	されたスナップショットからボリュームを作成した場合を除き、ボリュームは暗号化されません。 i. [暗号化] に [カスタム] を選択した場合は、使用する AWS KMS key を指定する必要があります。[KMS キー] には、AWS KMS key を選択するか、キーの ARN を入力します。対称型のカスタマー管理キーを使用してボリュームを暗号化する場合は、AWS KMS key ポリシーに適切な権限が定義されていることを確認してください。詳細については、「Amazon EBS ボリュームのデータ暗号化」を参照してください。 j. (オプション) [タグ] では、タスク定義またはサービスからタグを伝達するか、独自のタグを指定することで、Amazon EBS ボリュームにタグを追加できます。 タスク定義からタグを伝達する場合は、[タグの伝播元] で [タスク定義] を選択します。サー	

このボリュームタイプを設定するには	この操作を行います	
	ビスからタグを伝達する場合は、[タグの伝播元] で [サービス] を選択します。[伝播しない] を選択した場合、または値を選択しなかった場合、タグは伝播されません。 独自のタグを指定する場合は、[タグの追加] を選択し、追加する各タグのキーと値を指定します。 Amazon EBS ボリュームのタグ付けの詳細については、「Amazon EBS ボリュームのタグ付け」を参照してください。	

13. （オプション）サービスとタスクを識別しやすくするには、[Tags] (タグ) セクションを展開し、タグを設定します。

    新しく起動したすべてのタスクに対して、Amazon ECS がクラスター名とタスク定義タグで自動的にタグ付けするようにするには、[Amazon ECS マネージドタグを有効にする] を選択し、[タグの伝播元] で [タスク定義] を選択します。

    新しく起動したすべてのタスクに対して、Amazon ECS がクラスター名とサービスタグで自動的にタグ付けするようにするには、[Amazon ECS マネージドタグを有効にする] を選択し、[タグの伝播元] で [サービス] を選択します。

    タグを追加または削除します。

    - [タグを追加] [Add tag] (タグを追加) を選択し、以下を実行します。
      - [キー] にはキー名を入力します。
      - [値] にキー値を入力します。
    - [タグの削除] タグの横にある [タグの削除] を選択します。

14. [Create] (作成) を選択します。

次のステップ

Amazon ECS サーキットブレーカーのサービスのデプロイを追跡し、サービス履歴を表示します。詳細については、「Amazon ECS サービスデプロイを使用してサービス履歴を表示する」を参照してください。

コンソールを使用した Amazon ECS サービスの更新

タスク定義、必要なタスク数、キャパシティプロバイダー戦略、プラットフォームバージョン、デプロイ設定、またはこれらの組み合わせを更新できます。現在のサービス設定はあらかじめ入力されます。

ブルー/グリーンデプロイ設定の更新方法については、「コンソールを使用した Amazon ECS ブルー/グリーンデプロイの更新」を参照してください。

コンソールを使用する際には、以下の点を考慮してください。

サービスを一時的に停止したい場合は、[必要なタスク]を 0 に設定します。次に、サービスを開始する準備ができたら、サービスを元の [必要なタスク] 数で更新します。

コンソールを使用する際には、以下の点を考慮してください。

- 次のいずれかのパラメータを使用するサービスを更新するには、AWS Command Line Interface を使用する必要があります。
  - Blue/Green デプロイ
  - サービス検出 – サービス検出では、設定内容のみを表示できます。
  - カスタムメトリクスによるトラッキングポリシー
  - サービスを更新 – awsvpc のネットワーク設定とヘルスチェックの猶予期間は更新できません。

  AWS CLI を使用してサービスを更新する方法の詳細については、「AWS Command Line Interface リファレンス」の「update-service」を参照してください。
- タスク定義でコンテナが使用するポートを変更する場合は、更新後のポートを使用するようにコンテナインスタンスのセキュリティグループを更新する必要がある場合があります。
- Amazon ECS は、Elastic Load Balancing ロードバランサーまたは Amazon ECS コンテナインスタンスに関連付けられたセキュリティグループを自動的には更新しません。

- サービスでロードバランサーを使用する場合、コンソールを使用してサービスの作成時に定義したロードバランサー設定は変更できません。代わりに AWS CLI または SDK を使用して、ロードバランサーの設定を変更します。設定の変更方法の詳細については、「Amazon Elastic Containers サービス API リファレンス」の「UpdateService」を参照してください。
- サービスのタスク定義を更新する場合は、ロードバランサー設定で指定されたコンテナ名とコンテナポートはタスク定義のままにしておく必要があります。

実行中のサービスを更新することで、サービスが維持するタスク数、タスクがどのタスク定義を使用するか、また、タスクで Fargate 起動タイプを使用している場合には、サービスが使用するプラットフォームバージョンなど、一部のサービス設定パラメータを変更できます。Linux プラットフォームのバージョンを使用するサービスは、Windows プラットフォームのバージョンを更新できません。その逆も同様です。さらに容量が必要なアプリケーションがある場合には、サービスのスケール調整ができます。スケールダウンする未使用のキャパシティーがある場合は、サービスのタスクの必要数を減らし、リソースを解放できます。

コンテナイメージのプル動作は、起動タイプによって異なります。詳細については、以下のいずれかを参照してください。

- Amazon ECS の Fargate 起動タイプ
- Amazon ECS の EC2 起動タイプ
- Amazon ECS の外部 (Amazon ECS Anywhere) 起動タイプ

サービススケジューラは、最小ヘルス率と最大ヘルス率のパラメータ (サービスのデプロイ設定) を使用して、デプロイ戦略を判断します。

サービスでローリング更新 (ECS) のデプロイタイプが使用されている場合、最小ヘルス率は、デプロイ時に RUNNING 状態に保つ必要のあるサービスのタスクの下限数をサービスのタスクの必要数のパーセント値 (最も近い整数に切り上げ) で表します。サービスに EC2 起動タイプを使用するタスクが含まれている場合、DRAINING 状態のコンテナインスタンスがある間は、パラメータも適用されます。追加のクラスターキャパシティーを使用しないデプロイのために、このパラメータを使用します。例えば、サービスで必要数が 4 タスク、最小ヘルス率が 50% とすると、スケジューラは 2 つの新しいタスクを開始する前に、2 つの既存のタスクを停止してクラスターのキャパシティーを解放できます。ロードバランサーを使用しないサービスのタスクは、RUNNING 状態にある場合正常な状態と見なされます。ロードバランサーを使用するサービスのタスクは、RUNNING 状態にあり、ロードバランサーによって正常と報告された場合に、正常であると見なされます。最小ヘルス率のデフォルト値は 100% です。

サービスでローリング更新 (ECS) のデプロイタイプが使用されている場合、maximum percent パラメータは、デプロイ時に PENDING 、RUNNING、または STOPPING 状態で使用できるサービスのタスクの上限数をそれらのタスク数の適切なパーセント値 (最も近い整数に切り下げ) として表します。サービスに EC2 起動タイプを使用するタスクが含まれている場合、DRAINING 状態のコンテナインスタンスがある間は、パラメータも適用されます。このパラメータは、デプロイのバッチサイズを定義するために使用します。例えば、サービスで必要数が 4 タスク、最大ヘルス率の値が 200% とすると、スケジューラは 4 つの古いタスクを停止する前に、4 つの新しいタスクを開始できます。そのために必要なクラスターリソースを使用できることが前提です。最大ヘルス率のデフォルト値は 200% です。

更新中にサービススケジューラがタスクを置き換えるとき、サービスはまずロードバランサーからタスクを削除し (使用されている場合)、接続のドレインが完了するのを待ちます。その後、タスクで実行されているコンテナに docker stop と同等のコマンドが発行されます。この結果、SIGTERM 信号と 30 秒のタイムアウトが発生し、その後に SIGKILL が送信され、コンテナが強制的に停止されます。コンテナが SIGTERM 信号を正常に処理し、その受信時から 30 秒以内に終了する場合、SIGKILL 信号は送信されません。サービススケジューラは、最小ヘルス率と最大ヘルス率の設定で定義されているとおりに、タスクを開始および停止します。

また、コンテナのヘルスチェックまたはロードバランサーのターゲットグループのヘルスチェックが失敗すると、サービススケジューラーによって、異常であると判断されたタスクが置き換えられます。この置き換え動作は、maximumPercent および desiredCount のサービス定義パラメータによって異なります。タスクが異常とマークされた場合、サービススケジューラーによってまず置き換えタスクが開始されます。次に以下が発生します。

- 置き換えタスクのヘルスステータスが HEALTHY になると、サービススケジューラーが異常のあるタスクを停止します。
- 置き換えタスクのヘルスステータスが UNHEALTHY の場合、スケジューラーは異常のある置き換えタスクまたは既存の異常タスクのいずれかを停止して、タスク総数が desiredCount と等しくなるようにします。

maximumPercent パラメーターによって、置き換えタスクを先に開始できないようにスケジューラーが制限されている場合、スケジューラーは異常のあるタスクをランダムに 1 つずつ停止して容量を解放してから置き換えタスクを開始します。異常のあるタスクがすべて正常なタスクに置き換えられるまで、起動と停止のプロセスが続きます。異常なタスクがすべて置き換えられ、正常なタスクだけが実行中になると、合計タスク数が desiredCount を超える場合、タスク数が desiredCount になるまで、正常なタスクが無作為に停止されます。maximumPercent および desiredCount の詳細については、「サービス定義パラメータ」を参照してください。

> **Important**
>
> タスク定義でコンテナが使用するポートを変更する場合は、更新後のポートを使用するようにコンテナインスタンスのセキュリティグループを更新する必要がある場合があります。サービスのタスク定義を更新する場合、サービスの作成時に指定したコンテナ名とコンテナポートは、タスク定義のままにしておく必要があります。
> Amazon ECS は、Elastic Load Balancing ロードバランサーまたは Amazon ECS コンテナインスタンスに関連付けられたセキュリティグループを自動的には更新しません。

Amazon ECS サーキットブレーカーを使用するサービスを更新すると、Amazon ECS はサービスデプロイとサービスリビジョンを作成します。これらのリソースを使用すると、サービス履歴に関する詳細情報を表示できます。詳細については、「Amazon ECS サービスデプロイを使用してサービス履歴を表示する」を参照してください。

手順

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. クラスターの詳細ページの [サービス] セクションで、サービスの横にあるチェックボックスを選択し、[更新] を選択します。
4. サービスで新しいデプロイを開始するには、[Force new deployment] (新しいデプロイの強制) を選択します。
5. [タスク定義] の場合、タスク定義ファミリーとリビジョンを選択します。

   > **Important**
   >
   > コンソールは、選択したタスク定義ファミリーおよびリビジョンが、定義されたコンピューティング設定と互換性があることを確認します。警告が表示された場合は、タスク定義の互換性と、選択したコンピューティング設定の両方を確認します。

6. [Replica] (レプリカ) を使用した場合、[Desired tasks] (必要なタスク) に、サービス内で起動および維持するタスクの数を入力します。
7. [レプリカ] を選択した場合、Amazon ECS がアベイラビリティーゾーン間のタスクの分散をモニタリングし、不均衡が発生したときにタスクを再分散させるには、[アベイラビリティーゾーンのサービス再調整] で、[アベイラビリティーゾーンのサービス再調整] を選択します。

8. [Min running tasks] (実行中のタスクの最小化) の場合、デプロイ時に RUNNING の状態に保つ必要のあるサービス内のタスクの下限数をタスクの必要数のパーセント値 (最も近い整数に切り上げ) で入力します。詳細については、[Deployment configuration] (デプロイ設定) を参照してください。
9. [Max running tasks] (実行中のタスクの最大化)) には、デプロイ時に RUNNING または PENDING 状態にできるサービスのタスクの上限数を必要数のタスクのパーセント値 (最も近い整数に切り下げ) で入力します。
10. Amazon ECS がデプロイの障害を検出して処理する方法を設定するには、[Deployment failure detection] (デプロイ障害検出) を展開し、オプションを選択します。

    a. タスクを開始できない場合にデプロイを停止するには、[Use the Amazon ECS deployment circuit breaker] (Amazon ECS デプロイサーキットブレーカーを使用する) を選択します。

       デプロイサーキットブレーカーによってデプロイが失敗状態に設定されたときに、ソフトウェアがデプロイを最後に完了したデプロイ状態に自動的にロールバックするようにするには、[失敗時のロールバック] を選択します。

    b. アプリケーションメトリクスに基づいてデプロイを停止するには、[CloudWatch アラームを使用する] を選択します。次に、[CloudWatch アラーム名] からアラームを選択します。新しいアラームを作成するには、CloudWatch コンソールに移動します。

       CloudWatch アラームによってデプロイが失敗状態に設定されたときに、ソフトウェアがデプロイを最後に完了したデプロイ状態に自動的にロールバックするようにするには、[失敗時のロールバック] を選択します。
11. 計算オプションを変更するには、[コンピュート構成] を展開してから以下の操作を実行します。

    a. AWS Fargate のサービスにとって、[Platform version] (プラットフォームのバージョン) で、新しいバージョンを選択します。

    b. キャパシティプロバイダー戦略を使用するサービスの場合、[キャパシティプロバイダー戦略] で、次を実行します。

       - キャパシティプロバイダーをさらに追加するには、[さらに追加] を選択します。その後、[キャパシティプロバイダー] で、キャパシティプロバイダーを選択します。
       - キャパシティプロバイダーを削除するには、キャパシティプロバイダーの右側にある [削除] を選択します。

       Auto Scaling グループキャパシティープロバイダーを使用するサービスは、Fargate キャパシティープロバイダーを使用するように更新することはできません。Fargate キャパシティ

プロバイダーを使用するサービスは、Auto Scaling グループキャパシティプロバイダーを使用するように更新できません。

12. (オプション) サービスの Auto Scaling を設定するには、[サービスの自動スケーリング] を展開し、次のパラメータを指定します。

    a. サービスの自動スケーリングを使用するには、[Service auto scaling] (サービスの自動スケーリング) を選択します。

    b. [タスクの最小数] に、サービスの自動スケーリングで使用するタスクの下限数を入力します。必要な数がこの数を下回ることはありません。

    c. [タスクの最大数] に、サービスの自動スケーリングで使用するタスクの上限数を入力します。必要な数がこの数を超えることはありません。

    d. ポリシータイプを選択します。[スケーリングポリシータイプ] で、次のいずれかのオプションを選択します。

使用するポリシータイプ	この操作を行います
ターゲット追跡	a. [スケーリングポリシータイプ] で [ターゲットの追跡] を選択します。 b. [Policy Name] (ポリシー名) にこのポリシーの名前を入力します。 c. [ECS サービスメトリクス] で次のいずれかのメトリクスを選択します。 • [ECSServiceAverageCPUUtilization] — サービスの平均 CPU 使用率。 • [ECSServiceAverageMemoryUtilization] — サービスのメモリ平均使用率。 • [ALBRequestCountPerTarget] - Application

使用するポリシータイプ	この操作を行います	
	Load Balancer ターゲットグループ内のターゲットごとに完了したリクエストの数。 d. [Target value] (ターゲット値) には、選択したメトリックに対してサービスが保持する値を入力します。 e. [スケールアウトのクールダウン期間] には、スケールインアクティビティが完了してから別のスケールアウトアクティビティが開始されるまでの時間 (秒) を入力します。 f. [スケールインのクールダウン期間] には、スケールインアクティビティが完了してから別のスケールインアクティビティが開始されるまでの時間 (秒) を入力します。 g. ポリシーがスケールインアクティビティを実行しないようにするには、[Turn off scale-in] (スケールインをオフにする) を選択します。 h. • (オプション) トラフィックの増加に合わせてスケーリングポリ	

使用するポリシータイプ	この操作を行います	
	シーをスケールアウトさせたいが、トラフィックが減少してもスケールインする必要がない場合は、[スケールインをオフにする] を選択します。	

使用するポリシータイプ	この操作を行います	
ステップスケーリング	a. [スケーリングポリシータイプ] で [ステップスケーリング] を選択します。 b. [ポリシー名] で、このポリシー名を入力します。 c. [アラーム名] に、アラームの一意の名前を入力します。 d. [Amazon ECS サービスメトリクス] で、アラームに使用するサービスメトリクスを選択します。 e. [統計] で、アラーム統計を選択します。 f. [期間] で、アラームの期間を選択します。 g. [アラーム条件] で、選択したメトリクスを定義されたしきい値と比較する方法を選択します。 h. [メトリクスを比較するためのしきい値] と [アラームを開始する評価期間] に、アラームに使用するしきい値としきい値を評価する期間を入力します。 i. [スケーリングアクション]で、次の手順を実行します。 • [アクション] には、サービスに対してタス	

使用するポリシータイプ	この操作を行います	
	クを追加する、削除する、または特定の必要数を設定するかを選択します。 • タスクの追加または削除を選択した場合は、スケーリングアクションの開始時に追加または削除するタスクの数 (または既存のタスクの割合) を [値] に入力します。希望の数を設定することを選択した場合は、タスクの数を入力します。[タイプ] で、[値] が整数であるか、既存の必要なカウントのパーセント値であるかを選択します。 • [下限] と [上限] に、ステップスケーリング調整の下限と上限を入力します。デフォルトでは、[ポリシーを追加] の下限はアラームしきい値であり、上限は正 (+) の無限大です。デフォルトでは、[ポリシーを削除] の上限はアラームしきい値であり、下限は負 (-) の無限大です。	

使用するポリシータイプ	この操作を行います	
	• (オプション) さらにスケーリングオプションを追加します。[新しいスケーリングアクションの追加] を選択し、[アクションのスケーリング] の手順を繰り返します。 • [クールダウン期間] には、前回のスケーリングアクティビティが有効になるまで待機する時間を秒単位で入力します。追加ポリシーの場合、スケールアウトアクティビティの終了後、スケーリングポリシーによってスケールインアクティビティがブロックされ、一度にスケールアウトできるタスクの数が制限されます。削除ポリシーの場合、これはスケールインアクティビティの後、別のスケールインアクティビティが開始されるまでに経過する必要がある時間です。	

13. (オプション) Service Connect を使用するには、[Turn on Service Connect] (Service Connect をオンにする) を選択し、以下を指定します。

    a. [Service Connect configuration] (Service Connect 設定) で、クライアントモードを指定します。

- サービスが名前空間内の他のサービスへの接続のみを必要とするネットワーククライアントアプリケーションを実行している場合は、[Client side only] (クライアント側のみ) を選択します。
- サービスがネットワークまたは Web サービスアプリケーションを実行していて、このサービスにエンドポイントを提供し、名前空間内の他のサービスに接続する必要がある場合は、[Client and server] (クライアントとサーバー) を選択します。

b. デフォルトのクラスター名前空間ではない名前空間を使用するには、[Namespace] (名前空間) でサービス名前空間を選択します。

14. デプロイ時の設定と互換性のあるデータボリュームをタスクで使用する場合は、[ボリューム] を拡張してボリュームを設定できます。

ボリューム名とボリュームタイプはタスク定義リビジョンを作成するときに設定され、サービスの更新時には変更できません。ボリューム名とタイプを更新するには、新しいタスク定義リビジョンを作成し、新しいリビジョンを使用してサービスを更新する必要があります。

このボリュームタイプを設定するには	この操作を行います
Amazon EBS	a. [EBS ボリュームタイプ] には、タスクにアタッチする EBS ボリュームのタイプを選択します。 b. [サイズ (GiB)] には、ボリュームサイズの有効な値をギビバイト (GiB) 単位で入力します。最小で 1 GiB、最大で 16,384 GiB のボリュームサイズを指定できます。スナップショット ID を指定しない限り、この値は必須です。 c. [IOPS] には、ボリュームが提供する入力/出力オペレーションの数 (IOPS) の

このボリュームタイプを設定するには	この操作を行います	
	最大数を入力します。この値は io1、io2、および gp3 ボリュームタイプでのみ設定できます。 d. [スループット (MiB/秒)] には、ボリュームが提供すべきスループットをメビバイト/秒 (MiBps または MiB/s) で入力します。この値は gp3 ボリュームタイプでのみ設定できます。 e. [スナップショット ID] には、既存の Amazon EBS ボリュームスナップショットを選択するか、スナップショットからボリュームを作成する場合はスナップショットの ARN を入力します。新しい空のボリュームは、スナップショット ID を選択または入力しないで作成できます。 f. [ファイルシステムのタイプ] では、ボリューム上のデータストレージおよび取得に使用するファイルシステムの種類を選択します。オペレーティングシステムのデフォルトまたは特定のファイルシステムタイプのいずれかを	

このボリュームタイプを設定するには	この操作を行います	
	選択できます。Linux のデフォルトは XFS です。スナップショットから作成されたボリュームでは、スナップショットの作成時にボリュームが使用していたのと同じファイルシステムタイプを指定する必要があります。ファイルシステムのタイプが一致しない場合、タスクは開始できません。 g. [インフラストラクチャロール] には、Amazon ECS がタスクの Amazon EBS ボリュームを管理できるようにするために必要な権限を持つ IAM ロールを選択します。`AmazonECSInfrastructureRolePolicyForVolumes` 管理ポリシーをロールにアタッチすることも、このポリシーをガイドとして使用して、特定のニーズを満たすアクセス権限を持つ独自のポリシーを作成してアタッチすることもできます。必要なアクセス権限の詳細については、「Amazon ECS インフラストラクチャ IAM	

このボリュームタイプを設定するには	この操作を行います	
	ロール」を参照してください。 h. デフォルト設定で Amazon EBS 暗号化を使用する場合は、[暗号化] で [デフォルト] を選択します。アカウントにデフォルトで暗号化が設定されている場合、ボリュームは設定で指定されている AWS Key Management Service (AWS KMS) キーで暗号化されます。[デフォルト] を選択し、Amazon EBS のデフォルト暗号化がオンになっていない場合、ボリュームは暗号化されません。 [カスタム] を選択した場合は、ボリューム暗号化に任意の AWS KMS key を指定できます。 [なし] を選択すると、デフォルトで暗号化が設定されている場合や、暗号化されたスナップショットからボリュームを作成した場合を除き、ボリュームは暗号化されません。 i. [暗号化] に [カスタム] を選択した場合は、使	

このボリュームタイプを設定するには	この操作を行います	
	用する AWS KMS key を指定する必要があります。[KMS キー] には、AWS KMS key を選択するか、キーの ARN を入力します。対称型のカスタマー管理キーを使用してボリュームを暗号化する場合は、AWS KMS key ポリシーに適切な権限が定義されていることを確認してください。詳細については、「Amazon EBS ボリュームのデータ暗号化」を参照してください。 j. (オプション) [タグ] では、タスク定義またはサービスからタグを伝達するか、独自のタグを指定することで、Amazon EBS ボリュームにタグを追加できます。 タスク定義からタグを伝達する場合は、[タグの伝播元] で [タスク定義] を選択します。サービスからタグを伝達する場合は、[タグの伝播元] で [サービス] を選択します。[伝播しない] を選択した場合、または値を選択	

このボリュームタイプを設定するには	この操作を行います	
	しなかった場合、タグは伝播されません。 独自のタグを指定する場合は、[タグの追加] を選択し、追加する各タグのキーと値を指定します。 Amazon EBS ボリュームのタグ付けの詳細については、「Amazon EBS ボリュームのタグ付け」を参照してください。	

15. (オプション) サービスを識別しやすくするには、[Tags] (タグ) セクションを展開し、タグを設定します。

    - [タグの追加] [タグの追加] を選択して、以下を実行します。
      - [キー] にはキー名を入力します。
      - [値] にキー値を入力します。
    - [タグの削除] タグの横にある [タグの削除] を選択します。

16. [Update] (更新) を選択します。

次のステップ

Amazon ECS サーキットブレーカーのサービスのデプロイを追跡し、サービス履歴を表示します。詳細については、「Amazon ECS サービスデプロイを使用してサービス履歴を表示する」を参照してください。

コンソールを使用した Amazon ECS ブルー/グリーンデプロイの更新

Amazon ECS コンソールを使用してブルー/グリーンデプロイ設定を更新できます。ブルー/グリーンデプロイ設定は、そのままの状態で事前入力されています。以下のブルー/グリーンデプロイオプションを更新できます。

- デプロイグループ名 - CodeDeploy デプロイ設定
- アプリケーション名 - CodeDeploy のデプロイグループ
- デプロイメント構成 - CodeDeployがデプロイメント中に本番トラフィックを置換タスクセットへルーティングする方法
- ロードバランサーのテストリスナー - CodeDeploy は、デプロイ時にテストトラフィックを置換タスクセットにルーティングするためにテストリスナーを使用します

設定を更新する前に、新しいオプションを設定する必要があります。

ブルー/グリーンデプロイ構成を更新するには (Amazon ECS コンソール)

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [Cluster overview] (クラスターの概要ページ) で、サービスを選択し、[Update] (更新) を選択します。
4. [デプロイオプション - Powered by CodeDeploy] を展開し、更新するオプションを選択します。
   - CodeDeploy デプロイグループを変更するには、[アプリケーション名] でデプロイグループを選択します。
   - CodeDeploy デプロイセッティングを変更するには、[デプロイグループ名] でグループを選択します。
   - CodeDeploy がデプロイ中に本番トラフィックを置換タスクセットにルーティングする方法を変更するには、[デプロイ設定]で、オプションを選択します。
5. サービスのデプロイメントの新しいリビジョンの一部として実行するデプロイライフサイクルイベントフックと関連する Lambda 関数を選択します。使用できるライフサイクルフックは次のとおりです。
   - BeforeInstall – 置き換えタスクセットが作成される前に、このデプロイライフサイクルイベントフックを使用して Lambda 関数を呼び出します。このライフサイクルイベントでの Lambda 関数の結果は、ロールバックを開始しません。
   - AfterInstall – 置き換えタスクセットが作成された後に、このデプロイライフサイクルイベントフックを使用して Lambda 関数を呼び出します。このライフサイクルイベントでの Lambda 関数の結果は、ロールバックを開始することができます。
   - BeforeAllowTraffic – 本稼働トラフィックが置き換えタスクセットに再ルーティングされる前に、このデプロイライフサイクルイベントフックを使用して Lambda 関数を呼び出します。

このライフサイクルイベントでの Lambda 関数の結果は、ロールバックを開始することができます。

- BeforeAllowTraffic – 本稼働トラフィックが置き換えタスクセットに再ルーティングされる前に、このデプロイライフサイクルイベントフックを使用して Lambda 関数を呼び出します。このライフサイクルイベントでの Lambda 関数の結果は、ロールバックを開始することができます。

6. テストリスナーを変更するには、[負荷分散] を展開し、次に [CodeDeploy デプロイ用のテストリスナー] でテストリスナーを選択します。
7. [Update] (更新) を選択します。

コンソールを使用して Amazon ECS サービスの削除

サービスを削除する理由としては、次のようなものがあります。

- アプリケーションが不要になった
- サービスを新しい環境に移行する
- アプリケーションがアクティブに使用されていない
- アプリケーションが必要以上のリソースを使用しているため、コストを最適化しようとしている

削除する前に、このサービスは自動的に 0 までスケールダウンされます。サービスに関連付けられているロードバランサーリソース、またはサービス検出リソースは、サービスの削除による影響を受けません。Elastic Load Balancing リソースを削除するには、ロードバランサーのタイプに応じて、次のいずれかのトピックを参照してください。「Application Load Balancer の削除」または「Network Load Balancer の削除」。

サービスを削除すると、Amazon ECS はそのサービスのすべてのサービスデプロイとサービスリビジョンを削除します。

サービスを削除するときに、クリーンアップが必要なタスクがまだ実行中の場合、サービスは `ACTIVE` から `DRAINING` ステータスに移行し、そのサービスステータスはコンソールまたは `ListServices` API オペレーションで表示されなくなります。すべてのタスクが `STOPPING` または `STOPPED` ステータスに以降されたら、サービスステータスは `DRAINING` から `INACTIVE` になります。`DRAINING` または `INACTIVE` ステータスのサービスは、`DescribeServices` API オペレーションで引き続き表示できます。

> **Important**
>
> ACTIVE または DRAINING ステータスの既存のサービスと同じ名前で新しいサービスを作成しようとすると、エラーが表示されます。

手順

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、サービスに使用するクラスターを選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [Cluster: ***name***] (クラスター: 名前) ページで、[Services] (サービス) タブを選択します。
5. サービスを選択して、[Delete] (削除) を選択します。
6. タスクがゼロになっていなくてもサービスを削除するには、[Force delete service] (サービスの強制削除) を選択します。
7. 確認プロンプトで、[削除] と入力し、[削除] を選択します。

タスクを置き換えて Amazon ECS サービスをデプロイする

ローリング更新 (ECS) デプロイタイプを使用するサービスを作成すると、Amazon ECS サービススケジューラは現在実行中のタスクを新しいタスクに置き換えます。ローリング更新中にサービスに対して Amazon ECS が追加または削除するタスク数は、サービスデプロイ設定により制御されます。

Amazon ECS は、次のパラメータを使用してタスク数を決定します。

- `minimumHealthyPercent` は、デプロイメント中またはコンテナインスタンスがドレインしているときに、サービスに対して実行する必要があるタスク数の下限を、サービスに必要なタスク数の割合 (%) として表します。この値は切り上げられます。例えば、最小正常率が `50` で、必要なタスク数が 4 の場合、スケジューラは 2 つの新しいタスクを開始する前に既存のタスクを 2 つ停止できます。同様に、最小正常率が 75% で、必要なタスク数が 2 の場合、結果の値も 2 であるため、スケジューラはタスクを停止できません。

  タスクに異常が発生すると、Amazon ECS サービススケジューラは最初に置換タスクを開始し、置換タスクが正常になるまで `minimumHealthyPercent` のタスクを維持します。置き換えタスクが起動して正常になると、異常なタスクは段階的に停止します。

- `maximumPercent` は、デプロイメント中またはコンテナインスタンスがドレインしているときに、サービスに対して実行する必要があるタスク数の上限を、サービスに必要なタスク数の割合 (%) として表します。この値は切り捨てられます。例えば、最大パーセンテージが `200` で、目的のタスク数が 4 の場合、スケジューラは既存のタスクを 4 つ停止する前に 4 つの新しいタスクを開始できます。同様に、最大比率が 125 で、必要なタスク数が 3 の場合、結果の値も 3 であるため、スケジューラはタスクを開始できません。

> **Important**
>
> 最小正常率または最大正常率を設定するときは、デプロイが開始されたときにスケジューラが 1 つ以上のタスクを停止または開始できることを確認する必要があります。無効なデプロイメント構成が原因でサービスのデプロイメントが停止している場合、サービスイベントメッセージが送信されます。詳細については、「サービス (*service-name*) は、サービスデプロイメント構成のため、デプロイメント中にタスクを停止または開始できませんでした。minimumHealthyPercent または maximumPercent の値を更新してから、もう一度試してください。」を参照してください。

ローリングデプロイには 2 つの方法があり、サービスデプロイが失敗したタイミングをすばやく特定できます。

- the section called " デプロイサーキットブレーカーが障害を検出する方法"
- the section called "CloudWatch アラームがデプロイ障害を検出する方法"

これらの方法は個別に使用することも、一緒に使用することもできます。両方の方法を使用する場合、失敗に対するいずれかの方法の失敗の基準が満たされ次第、デプロイは失敗に設定されます。

使用するメソッドを決定する際は、以下のガイドラインを参考にします。

- サーキットブレーカー - タスクが開始できないときにデプロイを停止する場合は、このメソッドを使用します。
- CloudWatch アラーム - アプリケーションメトリクスに基づきデプロイを停止する場合は、このメソッドを使用します。

どちらの方法も、以前のサービスリビジョンへのロールバックをサポートしています。

コンテナイメージの解決

デフォルトでは、Amazon ECS はタスク定義で指定されたコンテナイメージタグをコンテナイメージダイジェストに解決します。単一のタスクを実行および維持するサービスを作成すると、そのタスクはタスク内のコンテナイメージダイジェストを確立するために使用されます。複数のタスクを実行および維持するサービスを作成すると、デプロイ中にサービススケジューラによって開始された最初のタスクを使用して、タスク内のコンテナイメージダイジェストを確立します。

コンテナイメージダイジェストの確立を 3 回以上試行しても失敗した場合、デプロイはイメージダイジェストの解決なしで続行されます。デプロイサーキットブレーカーが有効になっている場合、デプロイも失敗し、ロールバックされます。

コンテナイメージダイジェストが確立されると、Amazon ECS はこのダイジェストを、他の対象タスクの開始や、その後のサービスの更新に使用します。この結果、サービス内のすべてのタスクで常に同じコンテナイメージが実行され、ソフトウェアのバージョン整合性が得られます。

この動作は、コンテナ定義の `versionConsistency` パラメータを使用して、タスク内のコンテナごとに設定できます。詳細については、「`versionConsistency`」を参照してください。

> **Note**
>
> - `1.31.0` より前のバージョンの Amazon ECS エージェントは、イメージダイジェストの解決をサポートしていません。エージェントバージョン `1.31.0` ~ `1.69.0` では、Amazon ECR リポジトリにプッシュされたイメージに対してのみイメージダイジェストの解決がサポートされています。エージェントバージョン `1.70.0` 以降では、すべてのイメージに対してイメージダイジェストの解決がサポートされています。
> - イメージダイジェスト解決に対応した Fargate Linux プラットフォームの最低バージョンは `1.3.0` です。イメージダイジェスト解決に対応した Fargate Windows プラットフォームの最低バージョンは `1.0.0` です。
> - Amazon ECS は、Amazon GuardDuty セキュリティエージェントや Service Connect プロキシなど、Amazon ECS によって管理されるサイドカーコンテナのダイジェストをキャプチャしません。
> - 複数のタスクがあるサービスでコンテナイメージの解決に関連する潜在的なレイテンシーを減らすには、EC2 コンテナインスタンスで Amazon ECS エージェントバージョン `1.83.0` 以降を実行してください。潜在的なレイテンシーを回避するには、タスク定義でコンテナイメージダイジェストを指定します。

- タスク数が 0 のサービスを作成した場合、タスク数が 0 よりも大きいサービスの別のデプロイをトリガーするまで Amazon ECS はコンテナダイジェストを確立できません。
- 更新されたイメージダイジェストを確立するために、新しいデプロイを強制できます。更新されたダイジェストは新しいタスクの開始に使用され、既に実行中のタスクには影響しません。新しいデプロイの強制の詳細については、「Amazon ECS API リファレンス」の「forceNewDeployment」を参照してください。

Amazon ECS デプロイサーキットブレーカーが障害を検出する方法

デプロイサーキットブレーカーは、タスクが定常状態に到達したかどうかを判断する、ローリング更新メカニズムです。デプロイサーキットブレーカーには、デプロイが失敗した場合に、 COMPLETED 状態のデプロイに自動的にロールバックするオプションがあります。

サービスデプロイの状態が変わったとき、Amazon ECS はサービスデプロイ状態変更イベントを EventBridge に送信します。これにより、サービスデプロイの状態を監視するためのプログラムによる方法がもたらされます。詳細については、「Amazon ECS サービスデプロイ状態変更イベント」を参照してください。デプロイを開始するための手動アクションを実行できるように、eventName が SERVICE_DEPLOYMENT_FAILED の EventBridge ルールをを使用して作成および監視することをお勧めします。詳細については、「Amazon EventBridge ユーザーガイド」の「Getting started with EventBridge」を参照してください。

デプロイサーキットブレーカーは、デプロイが失敗したと判断すると、COMPLETED 状態にある最新のデプロイを探します。このデプロイをロールバックデプロイとして使用します。ロールバックが開始されると、デプロイは COMPLETED から IN_PROGRESS に変わります。つまり、デプロイは COMPLETED 状態になるまで次のロールバックの対象にはなりません。デプロイサーキットブレーカーが COMPLETED 状態のデプロイを見つけられない場合、サーキットブレーカーは新しいタスクを起動せず、デプロイは停止します。

サービスを作成すると、スケジューラーは起動に失敗したタスクを 2 段階で追跡します。

- ステージ 1 - スケジューラーはタスクが RUNNING 状態に移行するかどうかを監視します。
  - 成功 - RUNNING 状態に移行したタスクが複数あるため、デプロイメントが COMPLETED 状態に移行する可能性があります。障害基準はスキップされ、サーキットブレーカーはステージ 2 に移行します。
  - 失敗 - RUNNING 状態に移行しなかったタスクが連続して発生し、デプロイが FAILED 状態に移行する可能性があります。

- ステージ 2 - RUNNING 状態のタスクが 1 つ以上あると、デプロイメントはこの段階に入ります。サーキットブレーカーは、評価対象の現在のデプロイのタスクのヘルスチェックをチェックします。検証済みのヘルスチェックは、Elastic Load Balancing、AWS Cloud Map サービスヘルスチェック、コンテナヘルスチェックです。
  - 成功 - ヘルスチェックに合格した実行状態のタスクが少なくとも 1 つあります。
  - 失敗 - ヘルスチェックに失敗したために置き換えられたタスクが失敗のしきい値に達しました。

サービスでデプロイサーキットブレーカーメソッドを使用する際には、以下を考慮してください。EventBridge がルールを生成します。

- この `DescribeServices` レスポンスは、デプロイの状態、`rolloutState` および `rolloutStateReason` についての洞察を提供します。新しいデプロイが開始されると、ロールアウトの状態は `IN_PROGRESS` 状態から始まります。サービスが定常状態になると、ロールアウトの状態は `COMPLETED` に移行します。サービスが定常状態にならず、サーキットブレーカーがオンになっている場合、デプロイは `FAILED` 状態に移行します。`FAILED` 状態のデプロイでは、新しいタスクは起動されません。
- 開始および完了したデプロイに対して送信されるサービスデプロイの状態変更イベントに加えて、Amazon ECS はサーキットブレーカーがオンになったデプロイが失敗した場合にもイベントを送信します。これらのイベントは、デプロイが失敗した理由やロールバックのためにデプロイが開始されたかどうかについての詳細情報を提供します。詳細については、「Amazon ECS サービスデプロイ状態変更イベント」を参照してください。
- 以前のデプロイが失敗し、ロールバックが発生したために新しいデプロイが開始された場合、サービスデプロイ状態変更イベントの `reason` フィールドには、ロールバックのためにデプロイが開始されたことが示されます。
- デプロイサーキットブレーカーは、ローリング更新 (ECS) デプロイコントローラーを使用する Amazon ECS サービスでのみサポートされています。
- Amazon ECS コンソールを使用するか、CloudWatch オプションと共にデプロイサーキットブレーカーを使用する場合は AWS CLI を使用する必要があります。詳細については、「AWS Command Line Interface リファレンス」の「the section called “定義済みのパラメータを使用したサービスの作成”」および「create-service」を参照してください。

以下の `create-service` AWS CLI の例は、デプロイサーキットブレーカーと共にロールバックオプションが使用されている場合の Linux サービスの作成方法を示しています。

```
aws ecs create-service \
```

```
    --service-name MyService \
    --deployment-controller type=ECS \
    --desired-count 3 \
    --deployment-configuration "deploymentCircuitBreaker={enable=true,rollback=true}"
\
    --task-definition sample-fargate:1 \
    --launch-type FARGATE \
    --platform-family LINUX \
    --platform-version 1.4.0 \
    --network-configuration
"awsvpcConfiguration={subnets=[subnet-12344321],securityGroups=[sg-12344321],assignPublicIp=EN
```

例:

デプロイ 1 は COMPLETED 状態にあります。

デプロイ 2 は起動できないため、サーキットブレーカーはデプロイ 1 にロールバックされます。デプロイ 1 は IN_PROGRESS 状態に移行します。

デプロイ 3 が開始され、COMPLETED 状態のデプロイがないため、デプロイ 3 はロールバックやタスクの起動ができません。

失敗しきい値

デプロイサーキットブレーカはしきい値を計算し、その値を使用してデプロイを FAILED 状態に移行するタイミングを判断します。

デプロイサーキットブレーカの最小しきい値は 3 であり、最大しきい値は 200 です。値を次の式に使用してデプロイの失敗を判断します。

```
Minimum threshold <= 0.5 * desired task count => maximum threshold
```

計算結果が最低値の 3 より大きく、最大値の 200 より小さい場合、障害のしきい値は計算されたしきい値 (切り上げ) に設定されます。

> **Note**
>
> しきい値のどちらも変更できません。

デプロイステータスチェックには 2 つの段階があります。

1. デプロイサーキットブレーカは、デプロイの一部であるタスクを監視して RUNNING 状態のタスクを確認します。スケジューラは、現在のデプロイのタスクが RUNNING 状態のときに失敗条件を無視して次のステージに進みます。タスク RUNNING 状態に到達できなかった場合、デプロイサーキットブレーカは故障数を 1 つ増やします。障害カウントがしきい値に等しい場合、デプロイは FAILED としてマークされます。
2. RUNNING 状態のタスクが 1 つ以上ある場合、このステージが開始されます。デプロイサーキットブレーカは、現在のデプロイのタスクの次のリソースにヘルスチェックを実行します。
   - Elastic Load Balancing ロードバランサー
   - AWS Cloud Map サービス
   - Amazon ECS コンテナヘルスチェック

   タスクのヘルスチェックが失敗した場合、デプロイサーキットブレーカーは障害数を 1 つ増やします。障害カウントがしきい値に等しい場合、デプロイは FAILED としてマークされます。

例をいくつか、次のテーブルに示します。

希望タスク数	計算	Threshold
1	`3 <= 0.5 * 1 => 200`	3 (計算値は最小値より小さい)
25	`3 <= 0.5 * 25 => 200`	13 (値は切り上げられます)
400	`3 <= 0.5 * 400 => 200`	200
800	`3 <= 0.5 * 800 => 200`	200 (計算値は最大値を超えています)

たとえば、しきい値が 3 の場合、サーキットブレーカーは故障回数が 0 に設定された状態で起動します。タスクが RUNNING 状態に到達できなかった場合、デプロイサーキットブレーカは故障数を 1 つ増やします。障害カウントが 3 である場合、デプロイは FAILED としてマークされます。

ロールバックオプションの使用方法に関するその他の例については、「Amazon ECS デプロイサーキットブレーカーのお知らせ」を参照してください。

CloudWatch アラームが Amazon ECS のデプロイ障害を検出する方法

指定された CloudWatch アラームが ALARM 状態になったことを検出したとき、デプロイが失敗に設定されるように Amazon ECS を設定できます。

オプションとして、失敗したデプロイを最後に完了したデプロイにロールバックするように設定できます。

以下の `create-service` AWS CLI の例は、デプロイアラームと共にロールバックオプションが使用されている場合の Linux サービスの作成方法を示しています。

```
aws ecs create-service \
     --service-name MyService \
     --deployment-controller type=ECS \
     --desired-count 3 \
     --deployment-configuration
 "alarms={alarmNames=[alarm1Name,alarm2Name],enable=true,rollback=true}" \
     --task-definition sample-fargate:1 \
     --launch-type FARGATE \
     --platform-family LINUX \
     --platform-version 1.4.0 \
     --network-configuration
 "awsvpcConfiguration={subnets=[subnet-12344321],securityGroups=[sg-12344321],assignPublicIp=EN
```

サービスで Amazon CloudWatch アラームメソッドを使用する場合は、以下を考慮してください。

- ベイク時間は、新しいサービスバージョンがスケールアウトされ、古いサービスバージョンがスケールインされた後の期間で、その間 Amazon ECS はデプロイに関連するアラームを監視し続けます。Amazon ECS は、デプロイに関連するアラーム設定に基づいてこの期間を計算します。この値は設定できません。
- `deploymentConfiguration` リクエストパラメータには `alarms` のデータ型が含まれるようになっています。アラーム名、メソッド使用の有無、アラームがデプロイの失敗を示したときのロールバック開始の有無について指定できます。詳細については、「Amazon Elastic Container Service API リファレンス」の「CreateService」を参照してください。
- この `DescribeServices` レスポンスは、デプロイの状態、`rolloutState` および `rolloutStateReason` についての洞察を提供します。新しいデプロイが開始されると、ロールアウトの状態は `IN_PROGRESS` 状態から始まります。サービスが定常状態になりベイク時間が完了すると、ロールアウトの状態は `COMPLETED` に移行します。サービスが定常状態にならず、アラームが `ALARM` 状態になった場合、デプロイは `FAILED` 状態に移行します。`FAILED` 状態のデプロイでは、新しいタスクは起動されません。

- 開始および完了したデプロイに対して Amazon ECS から送信されるサービスデプロイの状態変更イベントに加えて、Amazon ECS はアラームを使用するデプロイが失敗した場合にもイベントを送信します。これらのイベントは、デプロイが失敗した理由やロールバックのためにデプロイが開始されたかどうかについての詳細情報を提供します。詳細については、「Amazon ECS サービスデプロイ状態変更イベント」を参照してください。
- 以前のデプロイが失敗し、ロールバックがオンになったために新しいデプロイが開始された場合、サービスデプロイ状態変更イベントの `reason` フィールドには、ロールバックのためにデプロイが開始されたことが示されます。
- 障害検出にデプロイサーキットブレーカーと Amazon CloudWatch アラームを使用する場合、どちらかのメソッドの基準が満たされ次第、どちらかがデプロイの失敗を開始します。デプロイの失敗を開始したメソッドでロールバックオプションが使用されている場合は、ロールバックが発生します。
- Amazon CloudWatch アラームは、ローリング更新 (ECS) デプロイコントローラーを使用する Amazon ECS サービスでのみサポートされています。
- このオプションは、Amazon ECS コンソールまたは AWS CLI を使用して設定できます。詳細については、「AWS Command Line Interface リファレンス」の「the section called “定義済みのパラメータを使用したサービスの作成”」および「create-service」を参照してください。
- デプロイステータスが長時間 `IN_PROGRESS` のままになっていると気付くことがあるかもしれません。これは、アクティブなデプロイを削除し終えるまで Amazon ECS のステータスは変化せず、また、ベイク時間が過ぎるまでは、このステータスが変更されることがないためです。アラームの設定によっては、デプロイにアラームを使用しない場合よりも数分長くかかるように思える場合もあります (新しいプライマリタスクセットがスケールアップされ、古いデプロイがスケールダウンされる場合であってもです)。CloudFormation タイムアウトを使用する場合は、タイムアウトを増やすことを検討してください。詳細については、「AWS CloudFormation ユーザーガイド」の「テンプレートでの待機条件の作成」を参照してください。
- Amazon ECS は `DescribeAlarms` を呼び出してアラームをポーリングします。`DescribeAlarms` の呼び出しはアカウントに関連付けられた CloudWatch の Service Quotas にカウントされます。`DescribeAlarms` を呼び出す AWS サービスが他にもある場合は、アラームをポーリングする際に Amazon ECS に影響が及ぶ可能性があります。例えば、別のサービスがクォータに達するだけの `DescribeAlarms` 呼び出しを行うと、そのサービスがスロットリングされると共に Amazon ECS もスロットリングされ、アラームをポーリングできなくなります。スロットリング期間中にアラームが生成されると、Amazon ECS はアラームを見逃してロールバックが行われない可能性があります。デプロイに他の影響はありません。CloudWatch の Service Quotas の詳細については、「CloudWatch ユーザーガイド」の「CloudWatch Service Quotas」を参照してください。

- デプロイの開始時にアラームの状態が ALARM である場合、Amazon ECS はそのデプロイ中はアラームの監視を行いません (Amazon ECS はアラーム設定を無視します)。この動作により、初期デプロイの失敗を修正するために、新たなデプロイを開始する場合に対応しています。

推奨アラーム

次のアラームメトリクスを使用することをお勧めします。

- Application Load Balancer を使用する場合は、HTTPCode_ELB_5XX_Count および HTTPCode_ELB_4XX_Count の Application Load Balancer メトリクスを使用します。これらのメトリクスは HTTP スパイクをチェックします。Application Load Balancer メトリクスの詳細については、「Application Load Balancer のユーザーガイド」の「Application Load Balancer の CloudWatch メトリクス」を参照してください。
- 既存のアプリケーションがある場合は、CPUUtilization および MemoryUtilization のメトリクスを使用します。これらのメトリクスは、クラスターまたはサービスが使用する CPU とメモリの割合をチェックします。詳細については、「the section called “考慮事項”」を参照してください。
- タスクで Amazon Simple Queue Service キューを使用する場合は、ApproximateNumberOfMessagesNotVisible Amazon SQS メトリクスを使用します。このメトリクスは、遅延の発生によりすぐに読み取ることのできない、キュー内のメッセージ数をチェックします。Amazon SQS メトリクスの詳細については、「Amazon Simple Queue Service デベロッパーガイド」の「Amazon SQS で使用できる CloudWatch メトリクス」を参照してください。

Amazon ECS サービスパラメータのベストプラクティス

アプリケーションのダウンタイムを発生させないためのデプロイプロセスは次のとおりです。

1. 既存のコンテナを実行したまま、新しいアプリケーションコンテナを起動します。
2. 新しいコンテナが正常であることを確認します。
3. 古いコンテナを停止します。

デプロイメント構成とクラスター内の予約されていない空きスペースの量によっては、すべての古いタスクを新しいタスクに置き換えるまでに、これを複数回行う必要がある場合があります。

数を変更するのに使用できるサービス設定オプションは 2 つあります。

- minimumHealthyPercent: 100% (デフォルト)

  デプロイ中にサービスが RUNNING 状態を維持する必要があるタスクの数の下限を入力します。これは、最も近い整数に切り上げられた desiredCount のパーセンテージです。このパラメータにより、追加のクラスターキャパシティーを使用せずにデプロイできます。

- maximumPercent: 200% (デフォルト)

  デプロイ中に RUNNING または PENDING 状態で許可されるサービスのタスク数の上限。これは、最も近い整数に切り捨てられた desiredCount のパーセンテージ (%) です。

例: デフォルト設定オプション

タスクが 6 つある次のサービスが、合計 8 つのタスクを処理できるクラスターにデプロイされているとします。デフォルトのサービス設定オプションでは、デプロイは 6 つの対象タスクの 100% を下回ることはありません。

デプロイの手順は次のとおりです。

1. 目標は 6 つのタスクを置き換えることです。
2. デフォルト設定では実行中のタスクが 6 つ必要なため、スケジューラは新しいタスクを 2 つ開始します。

   現在、既存のタスクが 6 つあり、新しいタスクが 2 つあります。
3. スケジューラは既存のタスクのうちの 2 つを停止します。

   現在、既存のタスクが 4 つあり、新しいタスクが 2 つあります。
4. スケジューラはさらに新しいタスクを 2 つ開始します。

   現在、既存のタスクが 4 つあり、新しいタスクが 4 つあります。
5. スケジューラは既存のタスクのうちの 2 つをシャットダウンします。

   現在、既存のタスクが 2 つあり、新しいタスクが 4 つあります。
6. スケジューラはさらに新しいタスクを 2 つ開始します。

   現在、既存のタスクが 2 つあり、新しいタスクが 6 つあります。
7. スケジューラは最後の 2 つの既存のタスクをシャットダウンします。

   現在、新しいタスクが 6 つあります。

上記の例では、オプションにデフォルト値を使用すると、新しいタスクが開始されるたびに 2.5 分待たされます。さらに、ロードバランサーは古いタスクが停止するまで 5 分間待たなければならない場合があります。

例: **minimumHealthyPercent** の変更

minimumHealthyPercent 値を 50% に設定すると、デプロイをスピードアップできます。

タスクが 6 つある次のサービスが、合計 8 つのタスクを処理できるクラスターにデプロイされているとします。デプロイの手順は次のとおりです。

1. 目標は 6 つのタスクを置き換えることです。
2. スケジューラは既存のタスクのうちの 3 つを停止します。

   minimumHealthyPercent 値を満たす既存のタスクがまだ 3 つ実行されています。
3. スケジューラは新しいタスクを 5 つ開始します。

   既存のタスクが 3 つあり、新しいタスクが 5 つあります。
4. スケジューラは残りの 3 つの既存のタスクを停止します。

   新しいタスクが 5 つあります。
5. スケジューラは最後の新しいタスクを開始します。

   新しいタスクが 6 つあります。

例: クラスターの空き容量を変更する

追加のタスクを実行できるように、空き容量を増やすこともできます。

タスクが 6 つある次のサービスが、合計 10 個のタスクを処理できるクラスターにデプロイされているとします。デプロイの手順は次のとおりです。

1. 目標は既存のタスクを置き換えることです。
2. スケジューラは既存のタスクのうちの 3 つを停止します。

   既存のタスクが 3 つあります。
3. スケジューラは新しいタスクを 6 つ開始します。

   既存のタスクと 6 つの新しいタスクがあります。
4. スケジューラは既存のタスク 3 つを停止します。

新しいタスクが 6 つあります。

レコメンデーション

タスクがしばらくアイドル状態で、使用率が高くない場合は、サービス設定オプションで次の値を使用してください。

- `minimumHealthyPercent`: 50%
- `maximumPercent`: 200%

Amazon ECS サービスデプロイを使用してサービス履歴を表示する

サービスデプロイは、デプロイの包括的なビューを提供します。サービスデプロイでは、サービスに関する次の情報が提供されます。

- 現在デプロイされているワークロード設定 (ソースサービスリビジョン)
- デプロイ中のワークロード設定 (ターゲットサービスリビジョン)
- デプロイステータス
- サーキットブレークが検出された失敗したタスク数
- アラーム状態になっている CloudWatch アラーム
- サービスデプロイが開始および完了した日時
- ロールバックの詳細 (発生した場合)

サービスデプロイプロパティの詳細については、「Amazon ECS サービスデプロイに含まれるプロパティ」を参照してください。

サービスデプロイは読み取り専用で、それぞれに一意の ID があります。

サービスデプロイには 3 つのステージがあります。

ステージ	定義	関連付けられた状態
保留中	サービスデプロイが作成されたが、開始されていない	保留中
継続的	サービスデプロイが進行中	• IN_PROGRESS

ステージ	定義	関連付けられた状態
		• STOP_REQUESTED • ROLLBACK_IN_PROGRESS
完了	サービスデプロイが完了 (成功または失敗)	• SUCCESSFUL • 停止 • ROLLBACK_SUCCESSFUL • ROLLBACK_FAILED

サービスデプロイを使用して、サービスのライフサイクルを理解し、実行する必要があるアクションがあるかどうかを判断します。例えば、ロールバックが発生した場合は、サービスデプロイを調査し、サービスイベントを確認する必要がある場合があります。

コンソール、API、および AWS CLI を使用して、2024 年 10 月 25 日以降に作成されたデプロイの最新の 90 日間の履歴を表示できます。

サービスデプロイのライフサイクル

Amazon ECS は、次のいずれかのアクションが発生すると、新しいサービスデプロイを自動的に作成します。

- ユーザーがサービスを作成した。
- ユーザーがサービスを更新し、[新しいデプロイの強制] オプションを使用した。
- ユーザーが、デプロイを必要とする 1 つ以上のサービスプロパティを更新した。

Amazon ECS は、デプロイの実行時にサービスデプロイの進行状況を反映するために次のサービスデプロイプロパティを更新します。

- ステータス
- 実行中のタスク数

  サービスリビジョンに示されている実行中のタスク数が、実際に実行されているタスク数と等しくない場合があります。この数は、デプロイが完了したときに実行されているタスク数を表します。例えば、サービスデプロイとは関係なくタスクを起動した場合、それらのタスクはサービスリビジョンの実行タスク数に含まれません。

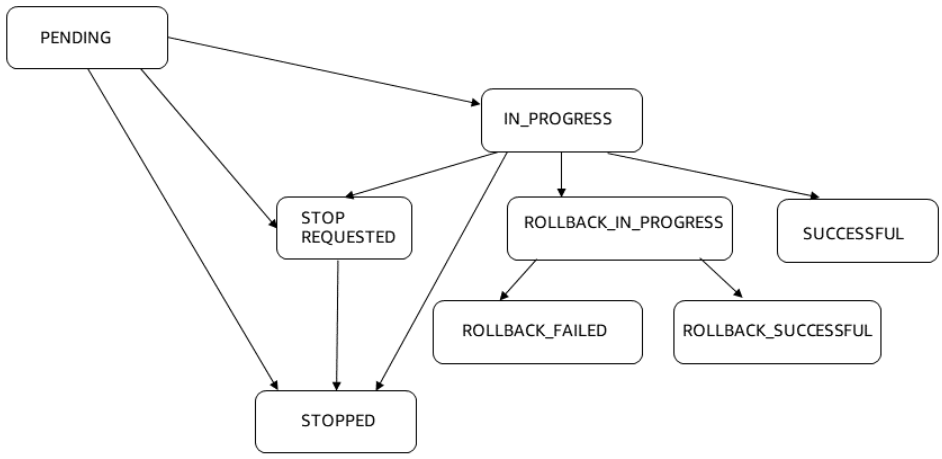
- サーキットブレーカーの障害検出:
  - 開始に失敗したタスク数
- CloudWatch アラームの障害検出
  - アクティブなアラーム
- ロールバック情報:
  - 開始時刻
  - ロールバックの理由
  - ロールバックに使用されるサービスリビジョンの ARN
- ステータスの理由

サービスを削除すると、Amazon ECS はサービスデプロイを削除します。

サービスデプロイの状態

サービスデプロイは PENDING 状態で開始されます。

次の図は、PENDING 状態の後に発生する可能性のあるサービスデプロイの状態を示しています: IN_PROGRESS、SUCCESSFUL、STOP_REQUESTED、ROLLBACK_IN_PROGRESSS、ROLLBACK_FAILED、R



以下の情報は、サービスデプロイの状態に関する詳細を提供します。

- PENDING - サービスデプロイは作成されましたが、開始されていません。

  状態は、IN_PROGRESS、STOP_REQUESTED、または STOPPED に移行する可能性があります。
- IN_PROGRESS - サービスデプロイが進行中です。

  状態は、SUCCESSFUL、STOP_REQUESTED、ROLLBACK_IN_PROGRESS または STOPPED に移行する可能性があります。
- STOP_REQUESTED - 次のいずれかが発生すると、サービスデプロイの状態は STOP_REQUESTED に移行します。
  - ユーザーが新しいサービスデプロイを開始した。
  - ロールバックオプションが障害検出メカニズム (サーキットブレーカーまたはアラームベース) に使用されていないため、サービスが SUCCESSFUL 状態に達しない。

  状態は STOPPED に移行します。
- SUCCESSFUL - サービスデプロイが正常に完了すると、サービスデプロイの状態は SUCCESSFUL に移行します。
- ROLLBACK_IN_PROGRESS - ロールバックオプションが障害検出メカニズム (サーキットブレーカーまたはアラームベース) に使用されていて、サービスが失敗すると、サービスデプロイの状態は ROLLBACK_IN_PROGRESS に移行します。

  状態は ROLLBACK_SUCCESSFUL または ROLLBACK_FAILED に移行します。

Amazon ECS サービスデプロイに含まれるプロパティ

サービスデプロイには、次のプロパティが含まれます。

プロパティ	説明	
サービスデプロイ ARN	サービスデプロイの ARN。	
サービス ARN	このサービスデプロイのサービスの ARN。	
クラスター ARN	サービスをホストするクラスターの ARN。	

プロパティ	説明
サービスデプロイの作成時刻	サービスデプロイが作成された時刻。
サービスデプロイの開始時刻	サービスデプロイが開始された時刻。
サービスデプロイの終了時刻	サービスデプロイが終了した時刻。
サービスデプロイの停止時刻	サービスデプロイが停止した時刻。
サービスデプロイの更新時刻	サービスデプロイが最後に更新された時刻。
ソースサービスリビジョン	現在実行中のサービスリビジョン。 含まれるプロパティについては、「Amazon ECS サービスリビジョンに含まれるプロパティ」を参照してください。

プロパティ	説明
デプロイ設定	サーキットブレーカー設定、決定するアラームを含むデプロイパラメータ。 • デプロイ中またはコンテナインスタンスのドレイン中に、サービスに対して実行する必要があるタスク数の下限 (サービスに必要なタスク数の割合)。 • デプロイ中またはコンテナインスタンスのドレイン中に、サービスに対して実行する必要があるタスク数の上限 (サービスに必要なタスク数の割合)。 • サーキットブレーカーの設定。 • 障害検出に使用されるアラーム。
ターゲットサービスリビジョン	デプロイするサービスリビジョン。 デプロイが正常に完了すると、ターゲットサービスリビジョンは実行中のサービスリビジョンになります。

プロパティ	説明	
サービスデプロイの状態	サービスデプロイの状態。 有効な値は、PENDING、SUCCESSFUL、STOPPED、STOP_REQUESTED、STOP_IN_PROGRESS、IN_PROGRESS、ROLLBACK_IN_PROGRESS、ROLLBACK_SUCCESSFUL、および ROLLBACK_FAILED です。	
サービスデプロイ状態の情報	サービスデプロイが現在の状態である理由に関する情報。例えば、サーキットブレーカーが障害を検出したなど。	
ロールバック情報	デプロイが失敗したときにサービスデプロイが使用するロールバックオプション。	
サービスデプロイサーキットブレーカーオプション	サービスデプロイが失敗したと判断するサーキットブレーカー。	
サービスデプロイの CloudWatch アラーム	サービスデプロイがいつ失敗したかを判断する CloudWatch アラーム。	

Amazon ECS サービスデプロイを表示するために必要なアクセス許可

最小権限のベストプラクティスに従うと、コンソールでサービスデプロイを表示するには、アクセス許可を追加する必要があります。

次のアクションへのアクセスが必要です。

- ListServiceDeployments

- DescribeServiceDeployments
- DescribeServiceRevisions

次のリソースへのアクセスが必要です。

- サービス
- サービスデプロイ
- サービスリビジョン

次のポリシー例には必要なアクセス許可が含まれており、アクションは指定されたサービスに限定されます。

account、cluster-name、および service-name を独自の値に置き換えます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
            "Action": [
              "ecs:ListServiceDeployments",
              "ecs:DescribeServiceDeployments",
              "ecs:DescribeServiceRevisions"
            ],
            "Resource": [
             "arn:aws:ecs:us-east-1:123456789012:service/cluster-name/service-name",
             "arn:aws:ecs:us-east-1:123456789012:service-deployment/cluster-name/
service-name/*",
             "arn:aws:ecs:us-east-1:123456789012:service-revision/cluster-name/service-
name/*"
            ]
        }
    ]
}
```

Amazon ECS サービスデプロイの表示

2024 年 10 月 25 日以降に作成されたデプロイの最新の 90 日間の履歴を確認できます。サービスデプロイは、次のいずれかの状態になります。

- 進行中

- 保留中
- 完了

この情報を使用して、サービスのデプロイ方法やサービスリビジョンを更新する必要があるかどうかを判断できます。含まれるプロパティについては、「Amazon ECS サービスデプロイに含まれるプロパティ」を参照してください。

開始する前に、サービスデプロイを表示するために必要なアクセス許可を設定します。詳細については、「Amazon ECS サービスデプロイを表示するために必要なアクセス許可」を参照してください。

Amazon ECS Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービスの詳細] ページが表示されます。
4. [サービスの詳細] ページで、[デプロイ] を選択します。
5. 表示するサービスデプロイを選択します。

このデプロイタイプのサービスデプロイを表示するには	この操作を行います	
進行中のデプロイ	[進行中のデプロイ] で、[デプロイ ID] を選択します。	
最後のデプロイ	[最後のデプロイ] で、[デプロイ ID] を選択します。	
完了したデプロイ	[サービスデプロイ] で、[デプロイ ID] を選択します。	

   [サービスデプロイの詳細] ページが表示されます。
6. (オプション) サービスリビジョンを比較して、相違点を確認します。

[サービスリビジョン] で、[リビジョンの比較] を選択し、比較するリビジョンを 2 つ選択します。

サービスリビジョンは並行して表示され、相違点が強調表示されます。

AWS CLI

1. `list-service-deployments` を実行して、サービスデプロイ ARN を取得します。

   変数を実際の値に置き換えます。

   ```
   aws ecs list-service-deployments --cluster cluster-name --service service-name
   ```

   表示するデプロイの serviceDeploymentArn を書き留めます。

   ```
   {
       "serviceDeployments": [
           {
               "serviceDeploymentArn": "arn:aws:ecs:us-west-2:123456789012:service-
   deployment/example/sd-example/NCWGC2ZR-taawPAYrIaU5",
               "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/example/
   sd-example",
               "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/example",
               "targetServiceRevisionArn": "arn:aws:ecs:us-
   west-2:123456789012:service-revision/example/sd-example/4980306466373577095",
               "status": "SUCCESSFUL"
           }
       ]
   }
   ```

2. `describe-service-deployments` を実行します。`list-service-deployments` から返された `serviceDeploymentArn` を使用します。

   変数を実際の値に置き換えます。

   ```
   aws ecs describe-service-deployments --service-deployment-arns
    arn:aws:ecs:region:123456789012:service-deployment/cluster-name/service-
   name/NCWGC2ZR-taawPAYrIaU5
   ```

次のステップ

デプロイのサービスリビジョンの詳細を表示できます。詳細については、「Amazon ECS サービスリビジョンの詳細の表示」を参照してください。

Amazon ECS サービスリビジョン

サービスリビジョンには、Amazon ECS がデプロイしようとしているワークロード設定のレコードが含まれています。サービスを作成またはデプロイするたびに、Amazon ECS はサービスリビジョンでデプロイしようとしている設定を自動的に作成してキャプチャします。

サービスリビジョンは読み取り専用で、一意の識別子があります。含まれるプロパティについては、「Amazon ECS サービスリビジョンに含まれるプロパティ」を参照してください。

サービスリビジョンには次の利点があります。

- サービスデプロイ中に、現在デプロイされているサービスリビジョン (ソース) とデプロイ中のサービスリビジョン (ターゲット) を比較できます。
- サービスデプロイにロールバックオプションを使用すると、Amazon ECS はサービスデプロイを最後に正常にデプロイされたサービスリビジョンに自動的にロールバックします。
- サービスリビジョンには、1 つのリソースにおけるワークロード設定のレコードが含まれます。

サービスリビジョンのライフサイクル

Amazon ECS は、サービスの作成時、またはデプロイを開始するサービスプロパティの更新時に、新しいサービスリビジョンを自動的に作成します。

Amazon ECS は、ロールバックオペレーションの新しいサービスリビジョンを作成しません。Amazon ECS は、最後に成功したサービスリビジョンをロールバックに使用します。

サービスリビジョンはイミュータブルです。

サービスを削除すると、Amazon ECS はサービスリビジョンを削除します。

2024 年 10 月 25 日以降に作成されたサービスリビジョンは、コンソール、API、および CLI を使用して表示できます。

Amazon ECS サービスリビジョンに含まれるプロパティ

サービスリビジョンには、次のプロパティが含まれます。

リソース	説明
サービス ARN	クライアントを識別する ARN。
クラスター ARN	サービスをホストするクラスターの ARN。
タスク定義 ARN	サービスタスクに使用されるタスク定義の ARN。
サービスレジストリ	サービス検出に使用されるサービスレジストリの詳細。 • コンテナ名 サービス検出サービスに使用されるコンテナ名の値。 • コンテナポート サービス検出サービスに使用されるポートの値。この値は、タスク定義でも指定されます。 • ポート サービス検出サービスが SRV レコードを指定した場合に使用されるポート値。 • レジストリ ARN サービスレジストリの Amazon リソースネーム (ARN)。
キャパシティープロバイダー	キャパシティプロバイダー戦略の詳細。

リソース	説明	
	• キャパシティプロバイダーの名前 サービスに使用されるキャパシティプロバイダー名。 • キャパシティプロバイダーの重み 指定されたキャパシティプロバイダーを使用する必要がある起動済みタスクの総数の相対的な割合。 • キャパシティプロバイダーベース 指定されたキャパシティプロバイダーで実行する最小タスク数。	
コンテナイメージ	コンテナイメージに関する詳細。 • コンテナ名 • イメージダイジェスト • コンテナイメージ	

リソース	説明
ネットワーク	サービスのネットワーク構成。 • パブリック IP アドレスがあるかどうか • タスクが実行されるサブネット • サービストラフィックを制御するセキュリティグループ
起動タイプ	サービスに使用される起動タイプ。

Fargate 固有のプロパティ	起動タイプが Fargate の場合、これは Fargate バージョンに関する情報になります。
	• プラットフォームバージョンとプラットフォームファミリー
	• エフェメラルストレージ
	  • デプロイに割り当てるエフェメラルストレージの量。
	  • ストレージの暗号化に使用する KMS キー。

リソース	説明	
デプロイ時に設定される Amazon EBS ボリューム	起動時に設定されるボリュームとしてタスク定義で指定されたボリュームの設定。 • 暗号化された ボリュームが暗号化されているかどうかを示します。 • ファイルシステムのタイプ ボリュームの Linux ファイルシステムタイプ。 • IOPS 1 秒あたりの I/O 操作の数 (IOPS)。 • KMS キー • IAM ロール このボリュームに関連付けられている IAM ロールの ARN。 • サイズ ボリュームのサイズ (GiB 単位)。 • スナップショット ID ボリュームスナップショット ID。 • タグ仕様 ボリュームのタグ設定。 • スループット	

リソース	説明
	ボリュームにプロビジョニングされたスループット。 • ボリュームタイプ ボリュームタイプ。
Service Connect	Service Connect の設定。 • Service Connect が使用中かどうかの表示 • 名前空間 • 相互接続されたサービスのリスト • Service Connect のログ記録設定
サービスロードバランサー	サービストラフィックをルーティングするロードバランサー。 • 名前 • コンテナ名 • コンテナポート • ターゲットグループ ARN
Runtime Monitoring	Runtime Monitoring がオンになっているかどうかを示します。
作成日	サービスリビジョンが作成された日付。
VPC Lattice	サービスリビジョンの VPC Lattice 設定。

Amazon ECS サービスリビジョンの詳細の表示

2024 年 10 月 25 日以降に作成された以下のサービスリビジョンタイプに関する情報を表示できます。

- ソース - 現在デプロイされているワークロード設定
- ターゲット - デプロイ中のワークロード設定

Amazon ECS Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービスの詳細] ページが表示されます。
4. [サービスの詳細] ページで、[デプロイ] を選択します。
5. 表示するサービスリビジョンを選択します。

このデプロイタイプのサービスリビジョンを表示するには	この操作を行います	
進行中のデプロイ	[進行中のデプロイ] で、次の操作を行います。 • ソースサービスリビジョンを表示するには、[サービスリビジョン] で、ソース [リビジョンタイプ] のサービスリビジョン ID を選択します。 • ターゲットサービスリビジョンを表示するには、[サービスリビジョン] で、ターゲット [リビジョンタイプ] のサービ	

このデプロイタイプのサービスリビジョンを表示するには	この操作を行います	
	スリビジョン ID を選択します。	
最後のデプロイ	[最後のデプロイ] で、[ターゲットサービスリビジョン] を選択します。	
完了したデプロイ	[サービスデプロイ] で、次の操作を行います。 • [ターゲットサービスリビジョン] で、ID を選択します。	

AWS CLI

1. describe-service-deployments を実行して、サービスリビジョン ARN を取得します。

   変数を実際の値に置き換えます。

   ```
   aws ecs describe-service-deployments --service-deployment-arns
    arn:aws:ecs:region:account-id:service/cluster-name/service-name/NCWGC2ZR-taawPAYrIaU5
   ```

   sourceServiceRevisions または targetServiceRevisions の arn を書き留めます。

   ```
   {
       "serviceDeployments": [
           {
               "serviceDeploymentArn": "arn:aws:ecs:us-west-2:123456789012:service-deployment/example/sd-example/NCWGC2ZR-taawPAYrIaU5",
               "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/example/sd-example",
   ```

```
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/example",
            "updatedAt": "2024-09-10T16:49:35.572000+00:00",
            "sourceServiceRevision": {
                "arn": "arn:aws:ecs:us-west-2:123456789012:service-revision/
example/sd-example/4980306466373578954",
                "requestedTaskCount": 0,
                "runningTaskCount": 0,
                "pendingTaskCount": 0
            },
            "targetServiceRevision": {
                "arn": "arn:aws:ecs:us-west-2:123456789012:service-revision/
example/sd-example/4980306466373577095",
                "requestedTaskCount": 0,
                "runningTaskCount": 0,
                "pendingTaskCount": 0
            },
            "status": "IN_PROGRESS",
            "deploymentConfiguration": {
                "deploymentCircuitBreaker": {
                    "enable": false,
                    "rollback": false
                },
                "maximumPercent": 200,
                "minimumHealthyPercent": 100
            }
        }
    ],
    "failures": []
}
```

2. describe-service-revisions を実行します。describe-service-deployments から返された arn を使用します。

   変数を実際の値に置き換えます。

```
aws ecs describe-service-revisions --service-revision-arns
 arn:aws:ecs:region:123456789012:service-revision/cluster-name/service-
name/4980306466373577095
```

デプロイ前に Amazon ECS サービスの状態を検証する

ブルー/グリーンデプロイタイプでは、CodeDeploy によって制御される ブルー/グリーンデプロイモデルを使用します。このデプロイタイプは、本番稼働用トラフィックを送信する前にサービスの新しいデプロイを検証するために使用します。詳細については、「AWS CodeDeploy ユーザーガイド」の「What Is CodeDeploy」を参照してください。デプロイ前に Amazon ECS サービスの状態を検証します。

ブルー/グリーンデプロイ中にトラフィックを移行するには、次の 3 つの方法があります。

- Canary - トラフィックは 2 つの増分で移行されます。事前定義された複数の Canary オプションから選択し、最初の増分および間隔でトラフィックを更新済みタスクセットに移行する割合 (%) を分単位で指定できます。次に 2 回目の増分で残りのトラフィックを移行します。
- Linear - トラフィックは等しい増分で移行され、増分間の間隔 (分) も同じです。事前定義された複数の線形オプションから選択し、増分ごとに移行するトラフィックの割合 (%) と増分間の間隔 (分) を指定できます。
- 一括 - すべてのトラフィックを元のタスクセットから更新済みタスクセットに同時に移行します。

以下に示しているのは、サービスが Blue/Green デプロイタイプを使用するときに Amazon ECS が使用する CodeDeploy のコンポーネントです。

CodeDeploy アプリケーション

CodeDeploy リソースのコレクションです。これは 1 つ以上のデプロイグループで構成されます。

CodeDeploy デプロイグループ

デプロイ設定。これには以下の構成要素があります。

- Amazon ECS クラスターとサービス
- ロードバランサーのターゲットグループとリスナー情報
- デプロイメントロールバック戦略
- トラフィックルーティング設定
- 元のリビジョンの終了設定
- デプロイ設定
- デプロイメントを停止するために設定できる CloudWatch アラームの設定
- 通知用の SNS または CloudWatch Eventsの設定

詳細については、AWS CodeDeployユーザーガイドの「デプロイグループの操作」を参照してください。

CodeDeploy デプロイ構成

デプロイメント中に本番トラフィックを置換タスクに CodeDeploy がルーティングする方法を指定します。次の事前定義された線形および Canary デプロイ設定を使用できます。また、カスタム定義の線形および Canary デプロイを作成することもできます。詳細については、AWS CodeDeploy ユーザーガイドの「デプロイ構成の操作」を参照してください。

- [CodeDeployDefault.ECSAllAtOnce]: すべてのトラフィックを同時に更新済みの Amazon ECS コンテナに移行します。
- CodeDeployDefault.ECSLinear10PercentEvery1Minutes: すべてのトラフィックがシフトされるまで、1 分ごとにトラフィックの 10 パーセントをシフトします。
- CodeDeployDefault.ECSLinear10PercentEvery3Minutes: すべてのトラフィックがシフトされるまで、3 分ごとにトラフィックの 10 パーセントをシフトします。
- [CodeDeployDefault.ECSCanary10Percent5Minutes]: 最初の増分で 10 パーセントのトラフィックをシフトします。残りの 90 パーセントは 5 分後にデプロイされます。
- [CodeDeployDefault.ECSCanary10percent15Minutes]: 最初の増分で 10 パーセントのトラフィックをシフトします。残りの 90 パーセントは 15 分後にデプロイされます。

リビジョン

リビジョンは、CodeDeploy アプリケーション仕様ファイル (AppSpec ファイル) です。AppSpec ファイルでは、タスク定義の完全な ARN と置換タスクセットのコンテナとポートを指定し、新しいデプロイが作成時にトラフィックがルーティングされるようにします。コンテナ名は、タスク定義内で参照されているコンテナ名のいずれかに設定する必要があります。ネットワーク設定またはプラットフォームのバージョンがサービス定義で更新された場合は、AppSpec ファイルでその詳細についても指定する必要があります。また、デプロイメントライフサイクルイベント中に実行する Lambda 関数も指定できます。Lambda 関数を使用することで、デプロイメント中にテストを実行し、メトリクスを返すことができます。詳細については、AWS CodeDeployユーザーガイドで「AppSpec ファイルリファレンス」を参照してください。

考慮事項

ブルー/グリーンデプロイタイプを使用するときは、以下の点を考慮します。

- Blue/Green デプロイタイプを使用して、Amazon ECS サービスが最初に作成されたとき、Amazon ECS タスクセットが作成されます。

- Application Load Balancer または Network Load Balancer の使用にサービスを設定する必要があります。ロードバランサーの要件は以下のとおりです。
  - 本番稼働用リスナーをロードバランサーに追加する必要があります。これは本番トラフィックをルーティングするために使用されます。
  - オプションテストリスナーをロードバランサーに追加することができます。これはテストトラフィックをルーティングするために使用されます。テストリスナーを指定する場合、CodeDeploy はデプロイメント中にテストトラフィックを置換タスクセットにルーティングします。
  - 本番稼働用とテストリスナーの両方が同じロードバランサーに属している必要があります。
  - ロードバランサーに対してターゲットグループを定義する必要があります。ターゲットグループは本番稼働用リスナーを通じてトラフィックをサービスの元のタスクセットにルーティングします。
  - Network Load Balancer を使用する場合、`CodeDeployDefault.ECSAllAtOnce` デプロイメント構成のみがサポートされます。
- サービスの自動スケーリングと ブルー/グリーンデプロイタイプを使用するように設定されたサービスでは、自動スケーリングはデプロイ中にブロックされませんが、状況によってはデプロイが失敗する場合があります。以下では、この動作について詳しく説明します。
  - サービスがスケーリング中の状態でデプロイが開始されると、グリーンタスクセットが作成され、CodeDeploy は Green タスクセットが定常状態になるまで最大 1 時間待機し、完了するまでトラフィックをシフトしません。
  - サービスが ブルー/グリーンデプロイのプロセス中で、スケーリングイベントが発生した場合、トラフィックは 5 分間シフトし続けます。サービスが 5 分以内に定常状態にならない場合、CodeDeploy はデプロイを停止し、失敗としてマークします。
  - サービスが青/緑でのデプロイのプロセス中でスケーリングイベントが発生した場合、必要タスクカウントが予期しない値に設定される場合があります。これは実行中のタスク数を現在の容量と見なすことで自動スケーリングによって発生します。これは必要タスク数の計算で使用される適切なタスク数の 2 倍です。
- Fargate 起動タイプ、`CODE_DEPLOY` またはデプロイメントコントローラータイプを使用するタスクは、`DAEMON` スケジューリング戦略をサポートしません。
- 最初に CodeDeploy アプリケーションおよびデプロイグループを作成する際に、以下を指定する必要があります。
  - ロードバランサーに対して 2 つのターゲットグループを定義する必要があります。1 つのターゲットグループは、Amazon ECS サービスの作成時に、ロードバランサーに対して定義された

最初のターゲットグループです。2 番目のターゲットグループの唯一の要件は、サービスが使用するものとは別のロードバランサーに関連付けることはできないということです。

- Amazon ECS サービスに対して CodeDeploy デプロイを作成すると、CodeDeploy は置換タスクセット (または Green タスクセット) をデプロイで作成します。テストリスナーをロードバランサーに追加した場合、CodeDeploy はテストトラフィックを置換タスクセットにルーティングします。この時点で検証テストを実行できます。次に、CodeDeploy は本番稼働用トラフィックを元のタスクセットから置換タスクセットに再ルーティングします。このときデプロイグループへのトラフィックの再ルーティング設定に従います。

必要な IAM 許可

ブルー/グリーンデプロイは、Amazon ECS と CodeDeploy API の組み合わせによって実現されています。ユーザーは、Amazon ECS ブルー/グリーンデプロイを使用するためには、これらのサービスに対する適切なアクセス権限が必要です。AWS Management Consoleまたは AWS CLI または SDK を使用します。

サービスの作成や更新に使用するデフォルトの IAM アクセス権限に加えて、Amazon ECS には次のアクセス権限が必要です。`AmazonECS_FullAccess` IAM ポリシーには、次の許可が追加されています。詳細については、「AmazonECS_FullAccess」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "codedeploy:CreateApplication",
                "codedeploy:CreateDeployment",
                "codedeploy:CreateDeploymentGroup",
                "codedeploy:GetApplication",
                "codedeploy:GetDeployment",
                "codedeploy:GetDeploymentGroup",
                "codedeploy:ListApplications",
                "codedeploy:ListDeploymentGroups",
                "codedeploy:ListDeployments",
                "codedeploy:StopDeployment",
                "codedeploy:GetDeploymentTarget",
                "codedeploy:ListDeploymentTargets",
                "codedeploy:GetDeploymentConfig",
                "codedeploy:GetApplicationRevision",
```

```
                "codedeploy:RegisterApplicationRevision",
                "codedeploy:BatchGetApplicationRevisions",
                "codedeploy:BatchGetDeploymentGroups",
                "codedeploy:BatchGetDeployments",
                "codedeploy:BatchGetApplications",
                "codedeploy:ListApplicationRevisions",
                "codedeploy:ListDeploymentConfigs",
                "codedeploy:ContinueDeployment",
                "sns:ListTopics",
                "cloudwatch:DescribeAlarms",
                "lambda:ListFunctions"
            ],
            "Resource": ["*"]
        }
    ]
}
```

> **Note**
>
> タスクおよびサービスを実行するために必要な標準の Amazon ECS アクセス権限を付与するだけでなく、ユーザーにはタスクの IAM ロールを使用する `iam:PassRole` アクセス権限も必要です。

CodeDeploy には、Amazon ECS API の呼び出し、Elastic Load Balancing の変更、Lambda 関数の起動、CloudWatch アラームの記述のアクセス権限が必要です。また、ユーザーの代わりにサービスの必要数を変更するためのアクセス許可も必要です。Blue/Green デプロイタイプを使用する Amazon ECS サービスを作成する前に、IAM ロール (`ecsCodeDeployRole`) を作成する必要があります。詳細については、「Amazon ECS CodeDeploy IAM ロール」を参照してください。

「Amazon ECS サービス作成の例」および「Amazon ECS サービス更新の例」の IAM ポリシー例に、ユーザーが AWS Management Consoleで Amazon ECS ブルー/グリーンデプロイを使用するためのアクセス許可が示されています。

ブルー/グリーンデプロイを使用した Amazon ECS サービスのデプロイ

AWS CLI でブルー/グリーンデプロイタイプを使用する Fargate タスクを含む、Amazon ECS サービスを作成する方法について説明します。

> **Note**
>
> ブルー/グリーンデプロイを実行するためのサポートが AWS CloudFormation に追加されています。詳細については、[AWS CloudFormationユーザーガイド]の[AWS CloudFormationを使用した CodeDeploy による Perform Amazon ECS ブルー/グリーンデプロイの実行]を参照してください。

前提条件

このチュートリアルでは、以下の前提条件をすでに満たしているものとします。

- AWS CLI の最新バージョンがインストールされ、設定されていること。AWS CLI のインストールまたはアップグレードについては、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。
- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- VPC およびセキュリティグループが使用できるように作成されていること。詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。
- Amazon ECS CodeDeploy IAM ロールが作成されます。詳細については、「Amazon ECS CodeDeploy IAM ロール」を参照してください。

ステップ 1: Application Load Balancer の作成

ブルー/グリーンデプロイタイプを使用する Amazon ECS サービスは、Application Load Balancer または Network Load Balancer のいずれかを使用する必要があります。このチュートリアルでは、Application Load Balancer を使用します。

Application Load Balancer を作成するには

1. [ロードバランサーの作成]コマンドを使用して、Application Load Balancer を作成します。異なるアベイラビリティーゾーンにある 2 つのサブネット、およびセキュリティグループを指定します。

```
aws elbv2 create-load-balancer \
     --name bluegreen-alb \
```

```
    --subnets subnet-abcd1234 subnet-abcd5678 \
    --security-groups sg-abcd1234 \
    --region us-east-1
```

出力には、次の形式でロードバランサーの Amazon リソースネーム (ARN) が含まれます。

```
arn:aws:elasticloadbalancing:region:aws_account_id:loadbalancer/app/bluegreen-alb/
e5ba62739c16e642
```

2. ターゲットグループを作成するには、create-target-group コマンドを使用します。このターゲットグループは、サービスで設定されている元のタスクにトラフィックをルーティングします。

```
aws elbv2 create-target-group \
    --name bluegreentarget1 \
    --protocol HTTP \
    --port 80 \
    --target-type ip \
    --vpc-id vpc-abcd1234 \
    --region us-east-1
```

出力には、以下の形式でターゲットグループの ARN が含まれます。

```
arn:aws:elasticloadbalancing:region:aws_account_id:targetgroup/
bluegreentarget1/209a844cd01825a4
```

3. ターゲットグループにリクエストを転送するデフォルトルールが関連付けられた、ロードバランサーのリスナーを作成するには、create-listener コマンドを使用します。

```
aws elbv2 create-listener \
    --load-balancer-arn
 arn:aws:elasticloadbalancing:region:aws_account_id:loadbalancer/app/bluegreen-alb/
e5ba62739c16e642 \
    --protocol HTTP \
    --port 80 \
    --default-actions
 Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:region:aws_account_id:targetgroup
bluegreentarget1/209a844cd01825a4 \
    --region us-east-1
```

出力には、以下の形式でリスナーの ARN が含まれます。

```
arn:aws:elasticloadbalancing:region:aws_account_id:listener/app/bluegreen-alb/
e5ba62739c16e642/665750bec1b03bd4
```

ステップ 2: Amazon ECS クラスターを作成する

[create-cluster]コマンドを使用して、使用するtutorial-bluegreen-clusterという名前のクラスターを作成します。

```
aws ecs create-cluster \
     --cluster-name tutorial-bluegreen-cluster \
     --region us-east-1
```

出力には、以下の形式でクラスターの ARN が含まれます。

```
arn:aws:ecs:region:aws_account_id:cluster/tutorial-bluegreen-cluster
```

ステップ 3: タスク定義を登録する

登録-タスク-定義コマンドを使用して、Fargate と互換性のあるタスク定義を登録します。これには、awsvpc ネットワークモードを使用する必要があります。このチュートリアルで使用するタスク定義の例を以下に示します。

まず、以下の内容で fargate-task.json というファイルを作成します。タスク実行ロールの ARN を使用していることを確認します。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

```
{
    "family": "sample-fargate",
    "networkMode": "awsvpc",
    "containerDefinitions": [
        {
            "name": "sample-app",
            "image": "public.ecr.aws/docker/library/httpd:latest",
            "portMappings": [
                {
                    "containerPort": 80,
                    "hostPort": 80,
                    "protocol": "tcp"
```

```
                }
            ],
            "essential": true,
            "entryPoint": [
                "sh",
  "-c"
            ],
            "command": [
                "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample
 App</title> <style>body {margin-top: 40px; background-color: #333;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
 <h2>Congratulations!</h2> <p>Your application is now running on a container in Amazon
 ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html && httpd-
foreground\""
            ]
        }
    ],
    "requiresCompatibilities": [
        "FARGATE"
    ],
    "cpu": "256",
    "memory": "512"
}
```

次に、作成した fargate-task.json ファイルを使用して、タスク定義を登録します。

```
aws ecs register-task-definition \
     --cli-input-json file://fargate-task.json \
     --region us-east-1
```

ステップ 4: Amazon ECS サービスを作成する

サービスを作成するには、create-service コマンドを使用します。

まず、以下の内容で service-bluegreen.json というファイルを作成します。

```
{
    "cluster": "tutorial-bluegreen-cluster",
    "serviceName": "service-bluegreen",
    "taskDefinition": "tutorial-task-def",
    "loadBalancers": [
        {
```

```
            "targetGroupArn":
 "arn:aws:elasticloadbalancing:region:aws_account_id:targetgroup/
bluegreentarget1/209a844cd01825a4",
            "containerName": "sample-app",
            "containerPort": 80
        }
    ],
    "launchType": "FARGATE",
    "schedulingStrategy": "REPLICA",
    "deploymentController": {
        "type": "CODE_DEPLOY"
    },
    "platformVersion": "LATEST",
    "networkConfiguration": {
       "awsvpcConfiguration": {
          "assignPublicIp": "ENABLED",
          "securityGroups": [ "sg-abcd1234" ],
          "subnets": [ "subnet-abcd1234", "subnet-abcd5678" ]
       }
    },
    "desiredCount": 1
}
```

次に、作成した service-bluegreen.json ファイルを使用してサービスを作成します。

```
aws ecs create-service \
     --cli-input-json file://service-bluegreen.json \
     --region us-east-1
```

出力には、以下の形式でサービスの ARN が含まれます。

```
arn:aws:ecs:region:aws_account_id:service/service-bluegreen
```

次のコマンドを使用し、ロードバランサーの DNS 名を取得します。

```
 aws elbv2 describe-load-balancers --name bluegreen-alb  --query
 'LoadBalancers[*].DNSName'
```

Web ブラウザに DNS 名を入力すると、サンプルアプリが青色の背景で表示された Web ページが表示されます。

ステップ 5: AWS CodeDeploy リソースを作成する

次のステップに従って、CodeDeploy アプリケーション、CodeDeploy デプロイグループの Application Load Balancer ターゲットグループ、および CodeDeploy デプロイグループを作成します。

CodeDeploy リソースを作成するには

1. [アプリケーションの作成]コマンドを使用して、CodeDeploy アプリケーションを作成します。ECS コンピューティングプラットフォームを指定します。

```
aws deploy create-application \
     --application-name tutorial-bluegreen-app \
     --compute-platform ECS \
     --region us-east-1
```

出力には、以下の形式でアプリケーションの ID が含まれます。

```
{
    "applicationId": "b8e9c1ef-3048-424e-9174-885d7dc9dc11"
}
```

2. [ターゲットグループの作成]コマンドを使用して、CodeDeploy デプロイ グループの作成時に使用される 2 つ目のApplication Load Balancer ターゲットグループを作成します。

```
aws elbv2 create-target-group \
     --name bluegreentarget2 \
     --protocol HTTP \
     --port 80 \
     --target-type ip \
     --vpc-id "vpc-0b6dd82c67d8012a1" \
     --region us-east-1
```

出力には、以下の形式でターゲットグループの ARN が含まれます。

```
arn:aws:elasticloadbalancing:region:aws_account_id:targetgroup/
bluegreentarget2/708d384187a3cfdc
```

3. [デプロイ-グループの作成]コマンドを使用して CodeDeploy デプロイ グループを作成します。

まず、以下の内容で tutorial-deployment-group.json というファイルを作成します。この例では、作成したリソースを使用します。serviceRoleArn には、Amazon ECS CodeDeploy IAM ロールの ARN を指定します。詳細については、「Amazon ECS CodeDeploy IAM ロール」を参照してください。

```
{
   "applicationName": "tutorial-bluegreen-app",
   "autoRollbackConfiguration": {
      "enabled": true,
      "events": [ "DEPLOYMENT_FAILURE" ]
   },
   "blueGreenDeploymentConfiguration": {
      "deploymentReadyOption": {
         "actionOnTimeout": "CONTINUE_DEPLOYMENT",
         "waitTimeInMinutes": 0
      },
      "terminateBlueInstancesOnDeploymentSuccess": {
         "action": "TERMINATE",
         "terminationWaitTimeInMinutes": 5
      }
   },
   "deploymentGroupName": "tutorial-bluegreen-dg",
   "deploymentStyle": {
      "deploymentOption": "WITH_TRAFFIC_CONTROL",
      "deploymentType": "BLUE_GREEN"
   },
   "loadBalancerInfo": {
      "targetGroupPairInfoList": [
        {
          "targetGroups": [
             {
                 "name": "bluegreentarget1"
             },
             {
                 "name": "bluegreentarget2"
             }
          ],
          "prodTrafficRoute": {
              "listenerArns": [
                  "arn:aws:elasticloadbalancing:region:aws_account_id:listener/
app/bluegreen-alb/e5ba62739c16e642/665750bec1b03bd4"
              ]
```

```
          }
        }
      ]
   },
   "serviceRoleArn": "arn:aws:iam::aws_account_id:role/ecsCodeDeployRole",
   "ecsServices": [
       {
           "serviceName": "service-bluegreen",
           "clusterName": "tutorial-bluegreen-cluster"
       }
   ]
}
```

次に、CodeDeploy デプロイ グループを作成します。

```
aws deploy create-deployment-group \
     --cli-input-json file://tutorial-deployment-group.json \
     --region us-east-1
```

出力には、以下の形式でデプロイグループの ID が含まれます。

```
{
    "deploymentGroupId": "6fd9bdc6-dc51-4af5-ba5a-0a4a72431c88"
}
```

ステップ 6: CodeDeploy デプロイを作成およびモニタリングする

CodeDeploy デプロイを作成する前に、次のように fargate-task.json のタスク定義 command を更新し、サンプルアプリの背景色を緑色に変更します。

```
{
    ...
        "containerDefinitions": [
            {
                ...
                "command": [
                    "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample
 App</title> <style>body {margin-top: 40px; background-color: #097969;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
 <h2>Congratulations!</h2> <p>Your application is now running on a container in Amazon
```

```
 ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html && httpd-
foreground\""
                ]
            }
        ],
        ...
}
```

次のコマンドを使用し、更新されたタスク定義を登録します。

```
aws ecs register-task-definition \
     --cli-input-json file://fargate-task.json \
     --region us-east-1
```

以下のステップを従い、アプリケーション仕様ファイル (AppSpec ファイル) と CodeDeploy デプロイを作成してアップロードします。

CodeDeploy デプロイを作成してモニタリングするには

1. 以下の手順を使用して、AppSpec ファイルを作成してアップロードします。

   a. CodeDeploy デプロイグループの内容で appspec.yaml というファイルを作成します。この例では、更新されたタスク定義を使用しています。

   ```
   version: 0.0
   Resources:
     - TargetService:
         Type: AWS::ECS::Service
         Properties:
           TaskDefinition: "arn:aws:ecs:region:aws_account_id:task-
   definition/tutorial-task-def:2"
           LoadBalancerInfo:
             ContainerName: "sample-app"
             ContainerPort: 80
           PlatformVersion: "LATEST"
   ```

   b. 「s3 mb」コマンドを使用して、AppSpec ファイルの Amazon S3 バケットを作成します。

   ```
   aws s3 mb s3://tutorial-bluegreen-bucket
   ```

   c. 「s3 cp」コマンドを使用して、AppSpec ファイルを Amazon S3 バケットにアップロードします。

```
aws s3 cp ./appspec.yaml s3://tutorial-bluegreen-bucket/appspec.yaml
```

2. 以下のステップを使用して、CodeDeploy デプロイを作成します。

   a. CodeDeploy デプロイの内容で create-deployment.json というファイルを作成します。この例では、チュートリアルの前半で作成したリソースを使用します。

```
{
    "applicationName": "tutorial-bluegreen-app",
    "deploymentGroupName": "tutorial-bluegreen-dg",
    "revision": {
        "revisionType": "S3",
        "s3Location": {
            "bucket": "tutorial-bluegreen-bucket",
            "key": "appspec.yaml",
            "bundleType": "YAML"
        }
    }
}
```

   b. デプロイを作成するには、create-deployment コマンドを使用します。

```
aws deploy create-deployment \
     --cli-input-json file://create-deployment.json \
     --region us-east-1
```

   出力には、以下の形式でデプロイの ID が含まれます。

```
{
    "deploymentId": "d-RPCR1U3TW"
}
```

3. デプロイの詳細を取得するには、get-deployment-target コマンドで、前の出力からの deploymentId を指定します。

```
aws deploy get-deployment-target \
--deployment-id "d-IMJU3A8TW" \
--target-id tutorial-bluegreen-cluster:service-bluegreen \
--region us-east-1
```

初期では、デプロイの状態は InProgress です。トラフィックは、BLUE の taskSetLabel、PRIMARY の状態、100.0 の trafficWeight である元のタスクセットに送信されます。置換タスクセットには、GREEN の taskSetLabel、ACTIVE の状態、0.0 の trafficWeight があります。DNS 名を入力した Web ブラウザには、引き続き青い背景のサンプルアプリが表示されます。

```
{
"deploymentTarget": {
"deploymentTargetType": "ECSTarget",
"ecsTarget": {
    "deploymentId": "d-RPCR1U3TW",
    "targetId": "tutorial-bluegreen-cluster:service-bluegreen",
    "targetArn": "arn:aws:ecs:region:aws_account_id:service/service-bluegreen",
    "lastUpdatedAt": "2023-08-10T12:07:24.797000-05:00",
    "lifecycleEvents": [
        {
            "lifecycleEventName": "BeforeInstall",
            "startTime": "2023-08-10T12:06:22.493000-05:00",
            "endTime": "2023-08-10T12:06:22.790000-05:00",
            "status": "Succeeded"
        },
        {
            "lifecycleEventName": "Install",
            "startTime": "2023-08-10T12:06:22.936000-05:00",
            "status": "InProgress"
        },
        {
            "lifecycleEventName": "AfterInstall",
            "status": "Pending"
        },
        {
            "lifecycleEventName": "BeforeAllowTraffic",
            "status": "Pending"
        },
        {
            "lifecycleEventName": "AllowTraffic",
            "status": "Pending"
        },
        {
            "lifecycleEventName": "AfterAllowTraffic",
            "status": "Pending"
        }
```

```
    ],
    "status": "InProgress",
    "taskSetsInfo": [
        {
            "identifer": "ecs-svc/9223370493423413672",
            "desiredCount": 1,
            "pendingCount": 0,
            "runningCount": 1,
            "status": "ACTIVE",
            "trafficWeight": 0.0,
            "targetGroup": {
                "name": "bluegreentarget2"
            },
            "taskSetLabel": "Green"
        },
        {
            "identifer": "ecs-svc/9223370493425779968",
            "desiredCount": 1,
            "pendingCount": 0,
            "runningCount": 1,
            "status": "PRIMARY",
            "trafficWeight": 100.0,
            "targetGroup": {
                "name": "bluegreentarget1"
            },
            "taskSetLabel": "Blue"
        }
    ]
}
}
}
```

以下の出力に示すように、デプロイメントのステータスが Succeeded になるまで、コマンドを使用してデプロイメントの詳細の取得を続けます。これで、トラフィックは置換タスクセットにリダイレクトされ、PRIMARY の状態および 100.0 の trafficWeight になりました。ロードバランサーの DNS 名を入力したウェブブラウザを更新すると、背景が緑色のサンプルアプリが表示されます。

```
{
"deploymentTarget": {
"deploymentTargetType": "ECSTarget",
"ecsTarget": {
```

```
    "deploymentId": "d-RPCR1U3TW",
    "targetId": "tutorial-bluegreen-cluster:service-bluegreen",
    "targetArn": "arn:aws:ecs:region:aws_account_id:service/service-bluegreen",
    "lastUpdatedAt": "2023-08-10T12:07:24.797000-05:00",
    "lifecycleEvents": [
        {
            "lifecycleEventName": "BeforeInstall",
            "startTime": "2023-08-10T12:06:22.493000-05:00",
            "endTime": "2023-08-10T12:06:22.790000-05:00",
            "status": "Succeeded"
        },
        {
            "lifecycleEventName": "Install",
            "startTime": "2023-08-10T12:06:22.936000-05:00",
            "endTime": "2023-08-10T12:08:25.939000-05:00",
            "status": "Succeeded"
        },
        {
            "lifecycleEventName": "AfterInstall",
            "startTime": "2023-08-10T12:08:26.089000-05:00",
            "endTime":  "2023-08-10T12:08:26.403000-05:00",
            "status": "Succeeded"
        },
        {
            "lifecycleEventName": "BeforeAllowTraffic",
            "startTime": "2023-08-10T12:08:26.926000-05:00",
            "endTime":  "2023-08-10T12:08:27.256000-05:00",
            "status": "Succeeded"
        },
        {
            "lifecycleEventName": "AllowTraffic",
            "startTime": "2023-08-10T12:08:27.416000-05:00",
            "endTime": "2023-08-10T12:08:28.195000-05:00",
            "status": "Succeeded"
        },
        {
            "lifecycleEventName": "AfterAllowTraffic",
            "startTime": "2023-08-10T12:08:28.715000-05:00",
            "endTime":  "2023-08-10T12:08:28.994000-05:00",
            "status": "Succeeded"
        }
    ],
    "status": "Succeeded",
    "taskSetsInfo": [
```

```
        {
            "identifer": "ecs-svc/9223370493425779968",
            "desiredCount": 1,
            "pendingCount": 0,
            "runningCount": 1,
            "status": "ACTIVE",
            "trafficWeight": 0.0,
            "targetGroup": {
                "name": "bluegreentarget1"
            },
            "taskSetLabel": "Blue"
        },
        {
            "identifer": "ecs-svc/9223370493423413672",
            "desiredCount": 1,
            "pendingCount": 0,
            "runningCount": 1,
            "status": "PRIMARY",
            "trafficWeight": 100.0,
            "targetGroup": {
                "name": "bluegreentarget2"
            },
            "taskSetLabel": "Green"
        }
    ]
}
}
}
```

ステップ 7: クリーンアップする

このチュートリアルが終了したら、使用していないリソースに対する料金が発生しないように、チュートリアルに関連付けられたリソースをクリーンアップします。

チュートリアルに関連付けられたリソースのクリーンアップ

1. [デプロイグループの削除]コマンドを使用して、CodeDeploy デプロイグループを削除します。

```
aws deploy delete-deployment-group \
     --application-name tutorial-bluegreen-app \
     --deployment-group-name tutorial-bluegreen-dg \
     --region us-east-1
```

2. [アプリケーションの削除]コマンドを使用して、 CodeDeploy アプリケーションを削除します。

```
aws deploy delete-application \
     --application-name tutorial-bluegreen-app \
     --region us-east-1
```

3. [削除サービス]コマンドを使用して、Amazon ECS サービスを削除します。`--force` フラグを使用すると、タスクがゼロになっていなくてもサービスを削除できます。

```
aws ecs delete-service \
     --service arn:aws:ecs:region:aws_account_id:service/service-bluegreen \
     --force \
     --region us-east-1
```

4. [delete-cluster] コマンドを使用して、Amazon ECS クラスターを削除します。

```
aws ecs delete-cluster \
     --cluster tutorial-bluegreen-cluster \
     --region us-east-1
```

5. [s3 rm]コマンドを使用して、Amazon S3 バケットから AppSpec ファイルを削除します。

```
aws s3 rm s3://tutorial-bluegreen-bucket/appspec.yaml
```

6. [s3 rb]コマンドを使用して、 Amazon S3 バケットを削除します。

```
aws s3 rb s3://tutorial-bluegreen-bucket
```

7. [delete-load-balancer] コマンドを使用して、Application Load Balancerを削除します。

```
aws elbv2 delete-load-balancer \
     --load-balancer-arn
 arn:aws:elasticloadbalancing:region:aws_account_id:loadbalancer/app/bluegreen-alb/
e5ba62739c16e642 \
     --region us-east-1
```

8. [delete-target-group]コマンドを使用して、2 つのApplication Load Balancer ターゲットグループを削除します。

```
aws elbv2 delete-target-group \
```

```
    --target-group-arn
 arn:aws:elasticloadbalancing:region:aws_account_id:targetgroup/
bluegreentarget1/209a844cd01825a4 \
    --region us-east-1
```

```
aws elbv2 delete-target-group \
    --target-group-arn
 arn:aws:elasticloadbalancing:region:aws_account_id:targetgroup/
bluegreentarget2/708d384187a3cfdc \
    --region us-east-1
```

サードパーティーのコントローラーを使用して Amazon ECS サービスをデプロイする

この外部デプロイタイプでは、Amazon ECS サービスのデプロイプロセスを完全に制御するために、すべてのサードパーティーのデプロイコントローラーを使用できます。サービスの詳細はサービス管理 API アクション (CreateService、UpdateService、DeleteService) または タスク設定管理 API アクション (CreateTaskSet、UpdateTaskSet、UpdateServicePrimaryTaskSet、DeleteTaskSet) のいずれかにより管理されます。各 API アクションは、サービス定義パラメータのサブセットを管理します。

UpdateService API アクションは、サービスの必要数およびヘルスチェック猶予期間パラメータを更新します。起動タイプ、プラットフォームバージョン、ロードバランサーの詳細、ネットワーク構成、またはタスク定義を更新する必要がある場合、新しいタスクセットを作成する必要があります。

UpdateTaskSet API アクションは、タスクセットのスケールパラメータのみを更新します。

UpdateServicePrimaryTaskSet API アクションは、サービス内のどのタスクセットをプライマリタスクセットであるかを変更します。DescribeServices API アクションを呼び出すと、プライマリタスクセットに指定されたすべてのフィールドが返されます。サービスのプライマリタスクセットが更新されると、サービスの新しいプライマリタスクセットに存在し、古いプライマリタスクセットとは異なるタスクセットのパラメータ値はどれでも、新しいプライマリタスクセットが定義されるときに新しい値に更新されます。サービスにプライマリタスクセットが定義されていない場合にサービスを定義するとき、タスクセットフィールドは null になります。

外部デプロイに関する考慮事項

外部デプロイタイプを使用するときは、以下の点を考慮します。

- サポートされているロードバランサーのタイプは、Application Load Balancer または Network Load Balancer です。
- Fargate 起動タイプ、または EXTERNAL デプロイコントローラータイプは、DAEMON スケジューリング戦略をサポートしません。

外部デプロイワークフロー

以下に示しているのは、Amazon ECS で外部デプロイを管理する基本的なワークフローです。

外部デプロイコントローラーを使用して Amazon ECS サービスを管理するには

1. Amazon ECS サービスを作成する 必須のパラメータは、サービス名のみです。サービスを作成するときに、外部デプロイコントローラーを使用して以下のパラメータを指定できます。その他すべてのサービスパラメータは、サービス内でタスクセットが作成されるときに指定されます。

   `serviceName`

   タイプ: 文字列

   必須: はい

   サービスの名前。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコアを使用できます。サービス名は同じクラスター内で一意になるようにしてください。ただし、リージョン内の複数のクラスター間や複数のリージョンにまたがるクラスター間では、同様の名前のサービスがあっても構いません。

   `desiredCount`

   指定したタスクセットのタスク定義のインスタンスをサービス内で実行状態に保つ数を設定します。

   `deploymentConfiguration`

   デプロイ時に実行されるタスクの数と、タスクの停止および開始の順序を制御するオプションのデプロイパラメータ。

   `tags`

   タイプ: オブジェクトの配列

   必須: いいえ

サービスに適用し、サービスの分類と整理に役立つメタデータ。タグはそれぞれ、1 つのキーとオプションの 1 つの値で設定されており、どちらもお客様側が定義します。サービスが削除されると、タグも削除されます。サービスには最大 50 個のタグを適用できます。詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。

`key`

タイプ: 文字列

長さの制限: 最小長は 1 です。最大長は 128 です。

必須: いいえ

タグを構成するキーと値のペアの一部。キーは、より具体的なタグ値のカテゴリのように動作する、一般的なラベルです。

`value`

タイプ: 文字列

長さの制約: 最小長は 0 です。最大長は 256 です。

必須: いいえ

タグを構成するキーと値のペアのオプションの一部。値はタグカテゴリ (キー) の記述子として機能します。

`enableECSManagedTags`

サービス内のタスクに Amazon ECS マネージドタグを使用するか否かを指定します。詳細については、「請求にタグを使用する」を参照してください。

`propagateTags`

タイプ: 文字列

有効な値: `TASK_DEFINITION` | `SERVICE`

必須: いいえ

タグをタスク定義またはサービスからサービスのタスクへコピーするかどうかを指定します。値を指定しない場合、タグはコピーされません。タグは、サービス作成中のサービス内

のタスクにのみコピーすることができます。タグをサービス作成後またはタスク作成後のタスクに追加するには、TagResource API アクションを使用します。

schedulingStrategy

使用するスケジュール戦略。外部デプロイコントローラーを使用するサービスは、REPLICA スケジューリング戦略のみをサポートします。

placementConstraints

サービスのタスクに使用する、配置制約オブジェクトの配列。タスクごとに最大 10 個の制約を指定できます (この制限数には、タスク定義内の制約と、実行時に指定される制約が含まれます)。Fargate 起動タイプを使用している場合、タスク配置の制約事項はサポートされません。

placementStrategy

サービスのタスクで使用する配置戦略オブジェクト。サービスごとに最大 4 つの戦略ルールを指定できます。

次の例は、外部デプロイコントローラーを使用するサービスを作成するためのサービス定義です。

```
{
    "cluster": "",
    "serviceName": "",
    "desiredCount": 0,
    "role": "",
    "deploymentConfiguration": {
        "maximumPercent": 0,
        "minimumHealthyPercent": 0
    },
    "placementConstraints": [
        {
            "type": "distinctInstance",
            "expression": ""
        }
    ],
    "placementStrategy": [
        {
            "type": "binpack",
            "field": ""
        }
```

```
    ],
    "schedulingStrategy": "REPLICA",
    "deploymentController": {
        "type": "EXTERNAL"
    },
    "tags": [
        {
            "key": "",
            "value": ""
        }
    ],
    "enableECSManagedTags": true,
    "propagateTags": "TASK_DEFINITION"
}
```

2. 最初のタスクセットを作成します。タスクセットには、サービスに関する次の詳細が含まれています。

   `taskDefinition`

   使用するタスクセットのタスクのタスク定義。

   `launchType`

   タイプ: 文字列

   有効な値: EC2 | FARGATE | EXTERNAL

   必須: いいえ

   サービスを実行する起動タイプ。起動タイプを指定しない場合は、デフォルトで `capacityProviderStrategy` が使用されます。詳しくは、「Amazon ECS 起動タイプ」を参照してください。

   `launchType` を指定した場合、`capacityProviderStrategy` パラメータを省略する必要があります。

   `platformVersion`

   タイプ: 文字列

   必須: いいえ

サービス内のタスクが実行されているプラットフォームのバージョン。プラットフォームのバージョンは、Fargate 起動タイプを使用するタスクに対してのみ指定されています。指定されない場合、デフォルトで最新バージョン (LATEST) が使用されます。

AWS Fargate プラットフォームのバージョンを使って、Fargate タスクインフラストラクチャの特定のランタイム環境を参照できます。プラットフォームのバージョンに LATEST を指定してタスクを実行またはサービスを作成すると、プラットフォームの最新バージョンをタスクで利用できるようになります。サービスをスケールアップする場合は、これらのタスクには、サービスの最新のデプロイで指定されたプラットフォームのバージョンが提供されます。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。

> **Note**
>
> プラットフォームのバージョンは、EC2 起動タイプを使用するタスクには指定されません。

`loadBalancers`

サービスで使用するロードバランサーを表すロードバランサーオブジェクト。外部デプロイコントローラーを使用する場合、Application Load Balancer と Network Load Balancer のみがサポートされます。Application Load Balancer を使用している場合、タスクセットあたり 1 つの Application Load Balancer ターゲットグループのみが許可されます。

次のスニペットは、使用する `loadBalancer` オブジェクトの例を示しています。

```
"loadBalancers": [
        {
            "targetGroupArn": "",
            "containerName": "",
            "containerPort": 0
        }
]
```

> **Note**
>
> loadBalancer オブジェクトを指定する場合は、targetGroupArn を指定し、loadBalancerName パラメータを省略する必要があります。

networkConfiguration

サービスのネットワーク構成。このパラメータは awsvpc ネットワークモードを使用して独自の Elastic Network Interface を受け取るタスク定義の場合に必要です。その他のネットワークモードではサポートされていません。Fargate 起動タイプのネットワークの詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。

serviceRegistries

このサービスに割り当てるサービス検出レジストリの詳細。詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。

scale

タスクセットに配置して実行し続けるために必要なタスク数の浮動小数点パーセンテージ。この値は、サービスの desiredCount の割合 (%) の合計として指定されます。許容値は 0 から 100 までの数字です。

外部デプロイコントローラー用のタスクセットを作成するための JSON の例を次に示します。

```
{
    "service": "",
    "cluster": "",
    "externalId": "",
    "taskDefinition": "",
    "networkConfiguration": {
        "awsvpcConfiguration": {
            "subnets": [
                ""
            ],
            "securityGroups": [
                ""
            ],
```

```
            "assignPublicIp": "DISABLED"
        }
    },
    "loadBalancers": [
        {
            "targetGroupArn": "",
            "containerName": "",
            "containerPort": 0
        }
    ],
    "serviceRegistries": [
        {
            "registryArn": "",
            "port": 0,
            "containerName": "",
            "containerPort": 0
        }
    ],
    "launchType": "EC2",
    "capacityProviderStrategy": [
        {
            "capacityProvider": "",
            "weight": 0,
            "base": 0
        }
    ],
    "platformVersion": "",
    "scale": {
        "value": null,
        "unit": "PERCENT"
    },
    "clientToken": ""
}
```

3. サービスの変更が必要な場合、更新するパラメータに応じて UpdateService、UpdateTaskSet、または CreateTaskSet のいずれかの API アクションを使用します。タスクセットを作成した場合は、サービスの各タスクセットに scale パラメータを使用して、サービス内で継続して実行するタスクの数を決定します。例えば、tasksetA を含むサービスがあり tasksetB を作成した場合、本番トラフィックを移行する前に tasksetB の有効性をテストする場合があります。両方のタスクの scale を 100 に設定し、すべての本番トラフィックを tasksetB に移行する準備が整ったときに、tasksetA の scale を 0 に更新して、スケールダウンすることもできます。

ロードバランサーを使用して Amazon ECS サービストラフィックを分散する

サービスは、オプションで Elastic Load Balancing を使用して、サービスのタスク間でトラフィックを均等に分散するように設定できます。

> **Note**
>
> タスクセットを使用するとき、セット内のすべてのタスクが Elastic Load Balancing を使用するように設定、または Elastic Load Balancing を使用しないように設定する必要があります。

AWS Fargate でホストされている Amazon ECS サービスでは、Application Load Balancer、Network Load Balancer、および Gateway Load Balancer がサポートされています。次の表を使用して、使用するロードバランサーのタイプを確認してください。

ロードバランサーのタイプ	以下の場合に使用	
Application Load Balancer	HTTP/HTTPS (またはレイヤー 7) トラフィックをルーティングします。 Amazon Load Balancer は Amazon ECS サービスでの使用に便利な複数の機能を提供しています。 • 各サービスは、複数のロードバランサーからトラフィックを送信し、複数のターゲットグループを指定することにより複数のロードバランシングポートを公開できます。 • バインドマウントは、Fargate インスタンスと	

ロードバランサーのタイプ	以下の場合に使用	
	Amazon EC2 インスタンスの両方でホストされているタスクでサポートされています。 • Application Load Balancer により、コンテナが動的ホストポートマッピングを使用できるようになります (同じサービスから複数のタスクがコンテナインスタンスごとに許可するため)。 • Application Load Balancer では、パスベースのルーティングと優先ルールをサポートしています (複数のサービスが 1 つの Application Load Balancer で同じリスナーポートを使用するため)。	
Network Load Balancer	TCP または UDP (またはレイヤー 4) トラフィックをルーティングします。	
Gateway Load Balancer	TCP または UDP (またはレイヤー 4) トラフィックをルーティングします。 ファイアウォール、侵入検知および防止システム、ディープパケットインスペクションシステムなどの仮想アプライアンスを使用します。	

サービスで Network Load Balancer または Gateway Load Balancer でのみ使用できる機能が必要な場合を除き、最新の機能を利用できるように、Amazon ECS サービスで Application Load Balancer を使用することをお勧めします。これらのロードバランサーの違いについては、「Elastic Load Balancing ユーザーガイド」の「Elastic Load Balancing とは」を参照してください。

ロードバランサーについては、お客様が利用された分のみのお支払いとなります。詳細については、Elastic Load Balancing の料金表を参照してください。

Amazon ECS のロードバランサーのヘルスチェックパラメータを最適化する

ロードバランサーは、ロードバランサーに対して有効になっているアベイラビリティーゾーンの正常なターゲットにのみ、リクエストをルーティングします。各ターゲットはターゲットグループに登録されます。ロードバランサーは、ターゲットグループのヘルスチェック設定を使用して、各ターゲットの状態を確認します。ターゲットは、登録後に正常と見なされるためには、1 つのヘルスチェックに合格する必要があります。Amazon ECS はロードバランサーをモニタリングします。ロードバランサーは Amazon ECS コンテナに定期的にヘルスチェックを送信します。Amazon ECS エージェントはモニタリングし、ロードバランサーがコンテナの状態を報告するのを待ちます。この処理は、コンテナが正常状態にあると見なされる前に行われます。

Elastic Load Balancing の次の 2 つのヘルスチェックパラメータがデプロイ速度に影響します。

- ヘルスチェック間隔: 個々のコンテナのヘルスチェック間のおおよその時間を秒単位で決定します。デフォルトでは、ロードバランサーは 30 秒ごとにチェックします。

  このパラメータは以下の名前です。

  - Elastic Load Balancing API の `HealthCheckIntervalSeconds`
  - Amazon EC2 コンソールでの [インターバル]
- 正常性しきい値: 異常なコンテナが正常であると判断されるまでに必要なヘルスチェックの連続成功回数を決定します。デフォルトでは、ロードバランサーはターゲットコンテナが正常であると報告する前に 5 回のヘルスチェックに合格する必要があります。

  このパラメータは以下の名前です。

  - Elastic Load Balancing API の `HealthyThresholdCount`
  - Amazon EC2 コンソールの [正常なしきい値]

デフォルト設定では、コンテナの状態を判断するための合計時間は 2 分 30 秒 (`30 seconds * 5 = 150 seconds`) です。

サービスが 10 秒以内に起動して安定すれば、ヘルスチェックプロセスをスピードアップできます。プロセスをスピードアップするには、ヘルスチェックの回数とチェックの間隔を減らしてください。

- `HealthCheckIntervalSeconds` (Elastic Load Balancing API 名) または [インターバル] (Amazon EC2 コンソール名): 5
- `HealthyThresholdCount` (Elastic Load Balancing API 名) または [正常なしきい値] (Amazon EC2 コンソール名): 2

この設定では、ヘルスチェックの処理にデフォルトの 2 分 30 秒かかるのに対し、10 秒かかります。

Elastic Load Balancing ヘルスチェックパラメータの詳細については、「Elastic Load Balancing ユーザーガイド」の「ターゲットグループのヘルスチェック」を参照してください。

Amazon ECS のロードバランサー Connection Draining パラメータを最適化する

最適化を可能にするために、クライアントはコンテナサービスへのキープアライブ接続を維持します。これにより、そのクライアントからの後続のリクエストが既存の接続を再利用できるようにします。コンテナへのトラフィックを停止したいときは、ロードバランサーに通知します。ロードバランサーはクライアントがキープアライブ接続を閉じたかどうかを定期的に確認します。Amazon ECS エージェントはロードバランサーを監視し、キープアライブ接続が閉じられた (ターゲットが `UNUSED` の状態にある) ことをロードバランサーが報告するのを待ちます。

ロードバランサーがターゲットを `UNUSED` 状態へと移行するまで待機する時間の長さが登録解除の遅延です。以下のロードバランサーパラメータを設定して、デプロイをスピードアップできます。

- `deregistration_delay.timeout_seconds`: 300 (デフォルト)

レスポンス時間が 1 秒未満のサービスの場合は、パラメータを次の値に設定して、クライアントとバックエンドサービスとの間の接続を切断するまでロードバランサーが 5 秒だけ待機するようにします。

- `deregistration_delay.timeout_seconds`: 5

> **Note**
>
> ファイルのアップロードやストリーミング接続が遅いなど、リクエストの有効期間が長いサービスの場合は、この値を 5 秒に設定しないでください。

SIGTERM 応答性

Amazon ECS は、まず SIGTERM シグナルをそのタスクに送信し、アプリケーションを終了してシャットダウンする必要があることを通知します。次に、Amazon ECS は SIGKILL メッセージを送信します。アプリケーションが SIGTERM を無視する場合、Amazon ECS サービスはプロセスを終了する SIGKILL シグナルの送信を待つ必要があります。

Amazon ECS が SIGKILL メッセージの送信を待つ時間は、次の Amazon ECS エージェントオプションによって決まります。

- `ECS_CONTAINER_STOP_TIMEOUT`: 30 (デフォルト)

  コンテナエージェントパラメータの詳細については、GitHub の「Amazon ECS コンテナエージェント」を参照してください。

待機時間を短縮するには、Amazon ECS エージェントパラメータを次の値に設定します。

- `ECS_CONTAINER_STOP_TIMEOUT`: 2

  アプリケーションに 1 秒以上かかる場合は、値に 2 を掛けて、その数値を値として使用します。

この場合、Amazon ECS はコンテナがシャットダウンされるまで 2 秒間待機し、アプリケーションが停止しなかったときに Amazon ECS は SIGKILL メッセージを送信します。

SIGTERM シグナルをトラップして反応するようにアプリケーションコードを変更することもできます。JavaScript の例を次に示します。

```
process.on('SIGTERM', function() {
  server.close();
})
```

このコードにより、HTTP サーバーは新しいリクエストのリッスンを停止し、処理中のリクエストへの応答を終了します。イベントループは何も行わないため Node.js プロセスが終了します。これを考

慮すると、プロセスが実行中のリクエストを完了するのに 500 ミリ秒しかかからない場合、プロセスは停止タイムアウトを待って SIGKILL を送信する必要がなく、早期に終了します。

Amazon ECS 用の Application Load Balancer を使用する

Application Load Balancer では、アプリケーションレイヤー (HTTP/HTTPS) でルーティング決定を行い、パスベースのルーティングをサポートします。また、クラスター内の各コンテナインスタンスの 1 つまたは複数のポートにリクエストをルーティングできます。Application Load Balancer では、動的ホストポートマッピングをサポートしています。たとえば、タスクコンテナ定義で NGINX コンテナポートのポート 80、ホストポートのポート 0 を指定した場合、ホストポートはコンテナインスタンスの一時ポート範囲から動的に選択されます (最新の Amazon ECS に最適化された AMI の 32768 ~ 61000 など)。タスクの起動時に、NGINX コンテナは、インスタンス ID およびポートの組み合わせとして Application Load Balancer で登録されます。トラフィックは、コンテナに対応するインスタンス ID およびポートに分散されます。この動的なマッピングにより、同じコンテナインスタンスの単一のサービスから複数のタスクを持つことができます。詳細については、「Application Load Balancer ユーザーガイド」を参照してください。

デプロイを高速化するためのパラメータ設定のベストプラクティスについては、以下を参照してください。

- Amazon ECS のロードバランサーのヘルスチェックパラメータを最適化する
- Amazon ECS のロードバランサー Connection Draining パラメータを最適化する

Amazon ECS で Application Load Balancer を使用する場合は、次の点を考慮してください。

- Amazon ECS には、タスクの作成時および停止時に、ロードバランサーへのターゲットの登録および登録解除に必要なアクセス許可を提供するサービスリンク IAM ロールが必要です。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。
- ターゲットグループでは、IP アドレスタイプを IPv4 に設定する必要があります。
- awsvpc ネットワークモードを使用するタスクを含むサービスの場合、サービスのターゲットグループを作成するときに、instance ではなく、ip をターゲットタイプとして選択する必要があります 。これは、awsvpc ネットワークモードを使用するタスクは、Amazon EC2 インスタンスではなく、Elastic Network Interface に関連付けられているためです。
- サービスが HTTP/HTTPS サービスのポート 80 やポート 443 など、複数の負荷分散されたポートにアクセスする必要がある場合は、2 つのリスナーを設定できます。1 つのリスナーは、リクエストをサービスに転送する HTTPS を担当し、別のリスナーは HTTP リクエストを適切な HTTPS

ポートへのリダイレクトを担当します。詳細については、Application Load Balancer ユーザーガイドの「Application Load Balancer のアクセスログ」を参照してください。

- ロードバランサーのサブネット設定には、コンテナインスタンスが存在するアベイラビリティーゾーンすべてを含める必要があります。
- サービスの作成後にロードバランサーの設定を AWS Management Console から変更することはできません。AWS Copilot、AWS CloudFormation、AWS CLI、SDK のいずれかを使用して、AWS CodeDeploy ブルー/グリーンまたは外部ではなく、ECS ローリングデプロイコントローラのみのロードバランサー設定を変更できます。ロードバランサー設定を追加、更新、削除すると、Amazon ECS は、更新された Elastic Load Balancing 設定で新しいデプロイを開始します。これにより、タスクがロードバランサーに登録およびロードバランサーから登録解除されます。Elastic Load Balancing 設定を更新する前に、テスト環境でこれを検証することをお勧めします。設定の変更方法の詳細については、「Amazon Elastic Containers サービス API リファレンス」の UpdateService を参照してください。
- サービスタスクがロードバランサーのヘルスチェック条件を満たさない場合、タスクは停止され、再起動されます。このプロセスは、サービスが実行中のタスクの必要数に達するまで続行されます。
- ロードバランサーで有効にされているサービスに問題がある場合は、「Amazon ECS のサービスロードバランサーのトラブルシューティング」を参照してください。
- タスクとロードバランサーは、同じ VPC 内にある必要があります。
- 各サービスに固有のターゲットグループを使用します。

  複数のサービスに同じターゲットグループを使用すると、サービスのデプロイ時に問題が発生する可能性があります。

Application Load Balancer の作成方法については、「Application Load Balancer」の「Application Load Balancer の作成」を参照してください。

Amazon ECS 用の Network Load Balancer を使用する

Network Load Balancer により、トランスポートレイヤー (TCP/SSL) でルーティングの決定が行われます。毎秒数百万のリクエストを処理できます。ロードバランサーは、接続を受信すると、フローハッシュルーティングアルゴリズムを使用してデフォルトルールのターゲットグループからターゲットを選択します。リスナー構成で指定されたポート上の選択したターゲットへの TCP 接続を開こうとします。ヘッダーを変更せずにリクエストを転送します。Network Load Balancer では、動的ホストポートマッピングをサポートしています。たとえば、タスクコンテナ定義で NGINX コンテナポートのポート 80、ホストポートのポート 0 を指定した場合、ホストポートはコンテナインスタン

スの一時ポート範囲から動的に選択されます (最新の Amazon ECS に最適化された AMI の 32768 ~ 61000 など)。タスクの起動時に、NGINX コンテナは、インスタンス ID およびポートの組み合わせとして Network Load Balancer で登録されます。トラフィックは、コンテナに対応するインスタンス ID およびポートに分散されます。この動的なマッピングにより、同じコンテナインスタンスの単一のサービスから複数のタスクを持つことができます。Network Load Balancer の詳細については、「https://docs.aws.amazon.com/elasticloadbalancing/latest/network/ のユーザーガイド」を参照してください。

デプロイを高速化するためのパラメータ設定のベストプラクティスについては、以下を参照してください。

- Amazon ECS のロードバランサーのヘルスチェックパラメータを最適化する
- Amazon ECS のロードバランサー Connection Draining パラメータを最適化する

Amazon ECS で Network Load Balancer を使用する場合は、次の点を考慮してください。

- Amazon ECS には、タスクの作成時および停止時に、ロードバランサーへのターゲットの登録および登録解除に必要なアクセス許可を提供するサービスリンク IAM ロールが必要です。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。
- 1 つのサービスに 5 つ以上のターゲットグループをアタッチすることはできません。
- `awsvpc` ネットワークモードを使用するタスクを含むサービスの場合、サービスのターゲットグループを作成するときに、`instance` ではなく、`ip` をターゲットタイプとして選択する必要があります 。これは、`awsvpc` ネットワークモードを使用するタスクは、Amazon EC2インスタンスではなく、Elastic Network Interface に関連付けられているためです。
- ロードバランサーのサブネット設定には、コンテナインスタンスが存在するアベイラビリティーゾーンすべてを含める必要があります。
- サービスの作成後にロードバランサーの設定を AWS Management Console から変更することはできません。AWS Copilot、AWS CloudFormation、AWS CLI、SDK のいずれかを使用して、AWS CodeDeploy ブルー/グリーンまたは外部ではなく、ECS ローリングデプロイコントローラのみのロードバランサー設定を変更できます。ロードバランサー設定を追加、更新、削除すると、Amazon ECS は、更新された Elastic Load Balancing 設定で新しいデプロイを開始します。これにより、タスクがロードバランサーに登録およびロードバランサーから登録解除されます。Elastic Load Balancing 設定を更新する前に、テスト環境でこれを検証することをお勧めします。設定の変更方法の詳細については、「Amazon Elastic Containers サービス API リファレンス」の UpdateService を参照してください。

- サービスタスクがロードバランサーのヘルスチェック条件を満たさない場合、タスクは停止され、再起動されます。このプロセスは、サービスが実行中のタスクの必要数に達するまで続行されます。
- IP アドレスをターゲットとして設定し、クライアント IP の保持をオフにした Gateway Load Balancer を使用する場合、リクエストは Gateway Load Balancer のプライベート IP アドレスから送信されたと見なされます。これは、ターゲットのセキュリティグループで受信リクエストとヘルスチェックを許可するとすぐに、Gateway Load Balancer の背後にあるサービスが世界中からアクセス可能になることを意味します。
- Fargate タスクでは、プラットフォームバージョン `1.4.0` (Linux) または `1.0.0` (Windows) を使用する必要があります。
- ロードバランサーで有効にされているサービスに問題がある場合は、「Amazon ECS のサービスロードバランサーのトラブルシューティング」を参照してください。
- タスクとロードバランサーは、同じ VPC 内にある必要があります。
- Network Load Balancer のクライアント IP アドレスの保存は Fargate ターゲットと互換性があります。
- 各サービスに固有のターゲットグループを使用します。

  複数のサービスに同じターゲットグループを使用すると、サービスのデプロイ時に問題が発生する可能性があります。

Network Load Balancer を作成する方法については、「Network Load Balance」での「Network Load Balancer の作成」を参照してください。

> **Important**
>
> サービスのタスク定義で、`awsvpc` ネットワークモード (起動タイプが Fargate の場合に必要) が使用されている場合は、`instance` ではなく、`ip` をターゲットタイプとして選択する必要があります。これは、`awsvpc` ネットワークモードを使用するタスクは、Amazon EC2 インスタンスではなく、Elastic Network Interface に関連付けられているためです。
> インスタンス ID が
> C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3、および T1 のインスタンス ID でインスタンスを登録することはできません。IP アドレスで、これらの種類のインスタンスを登録することができます。

Amazon ECS 用の Gateway Load Balancer を使用する

ゲートウェイロードバランサーは、開放型システム間相互接続 (OSI) モデルの第 3 層 (ネットワークレイヤー) で機能します。すべてのポートですべての IP パケットをリッスンし、リスナールールで指定されたターゲットグループにトラフィックを転送します。5 タプル (TCP/UDP フローの場合) または 3 タプル (非 TCP/UDP フローの場合) を使用して、特定のターゲットアプライアンスへのフローのスティッキ状態を維持します。たとえば、タスクコンテナ定義で NGINX コンテナポートのポート 80、ホストポートのポート 0 を指定した場合、ホストポートはコンテナインスタンスの一時ポート範囲から動的に選択されます (最新の Amazon ECS に最適化された AMI の 32768 ~ 61000 など)。タスクの起動時に、NGINX コンテナは、インスタンス ID およびポートの組み合わせとして Gateway Load Balancer で登録されます。トラフィックは、コンテナに対応するインスタンス ID およびポートに分散されます。この動的なマッピングにより、同じコンテナインスタンスの単一のサービスから複数のタスクを持つことができます。詳細については、「Gateway Load Balancers」の「What is a Gateway Load Balancer」を参照してください。

デプロイを高速化するためのパラメータ設定のベストプラクティスについては、以下を参照してください。

- Amazon ECS のロードバランサーのヘルスチェックパラメータを最適化する
- Amazon ECS のロードバランサー Connection Draining パラメータを最適化する

Amazon ECS で Gateway Load Balancer を使用する場合は、次の点を考慮してください。

- Amazon ECS には、タスクの作成時および停止時に、ロードバランサーへのターゲットの登録および登録解除に必要なアクセス許可を提供するサービスリンク IAM ロールが必要です。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。
- `awsvpc` ネットワークモードを使用するタスクを含むサービスの場合、サービスのターゲットグループを作成するときに、`instance` ではなく、`ip` をターゲットタイプとして選択する必要があります 。これは、`awsvpc` ネットワークモードを使用するタスクは、Amazon EC2インスタンスではなく、Elastic Network Interface に関連付けられているためです。
- ロードバランサーのサブネット設定には、コンテナインスタンスが存在するアベイラビリティーゾーンすべてを含める必要があります。
- サービスの作成後にロードバランサーの設定を AWS Management Console から変更することはできません。AWS Copilot、AWS CloudFormation、AWS CLI、SDK のいずれかを使用して、AWS CodeDeploy ブルー/グリーンまたは外部ではなく、ECS ローリングデプロイコントローラのみのロードバランサー設定を変更できます。ロードバランサー設定を追加、更新、削除すると、Amazon ECS は、更新された Elastic Load Balancing 設定で新しいデプロイを開始しま

す。これにより、タスクがロードバランサーに登録およびロードバランサーから登録解除されます。Elastic Load Balancing 設定を更新する前に、テスト環境でこれを検証することをお勧めします。設定の変更方法の詳細については、「Amazon Elastic Containers サービス API リファレンス」の UpdateService を参照してください。

- サービスタスクがロードバランサーのヘルスチェック条件を満たさない場合、タスクは停止され、再起動されます。このプロセスは、サービスが実行中のタスクの必要数に達するまで続行されます。
- IP アドレスをターゲットとして設定した Gateway Load Balancer を使用する場合、リクエストは Gateway Load Balancer のプライベート IP アドレスから送信されたと見なされます。これは、ターゲットのセキュリティグループで受信リクエストとヘルスチェックを許可するとすぐに、Gateway Load Balancer の背後にあるサービスが世界中からアクセス可能になることを意味します。
- Fargate タスクでは、プラットフォームバージョン `1.4.0` (Linux) または `1.0.0` (Windows) を使用する必要があります。
- ロードバランサーで有効にされているサービスに問題がある場合は、「Amazon ECS のサービスロードバランサーのトラブルシューティング」を参照してください。
- タスクとロードバランサーは、同じ VPC 内にある必要があります。
- 各サービスに固有のターゲットグループを使用します。

  複数のサービスに同じターゲットグループを使用すると、サービスのデプロイ時に問題が発生する可能性があります。

Gateway Load Balancer を作成する方法については、「Gateway Load Balancer」の「Gateway Load Balancer の使用開始方法」を参照してください。

> **Important**
>
> サービスのタスク定義で、`awsvpc` ネットワークモード (起動タイプが Fargate の場合に必要) が使用されている場合は、`instance` ではなく、`ip` をターゲットタイプとして選択する必要があります。これは、`awsvpc` ネットワークモードを使用するタスクは、Amazon EC2 インスタンスではなく、Elastic Network Interface に関連付けられているためです。
> インスタンス ID が
> C1、CC1、CC2、CG1、CG2、CR1、G1、G2、HI1、HS1、M1、M2、M3、および T1 のインスタンス ID でインスタンスを登録することはできません。IP アドレスで、これらの種類のインスタンスを登録することができます。

Amazon ECS サービスに複数のターゲットグループを登録する

サービス定義で複数のターゲットグループを指定すると、Amazon ECS サービスは複数のロードバランサーからのトラフィックを送信し、複数のロードバランサーポートを公開できます。

複数のターゲットグループを指定してサービスを作成するには、Amazon ECS API、SDK、AWS CLI、または AWS CloudFormation テンプレートを使用してサービスを作成する必要があります。サービスの作成後、AWS Management Console に登録されているサービスとターゲットグループを表示できます。既存サービスのロードバランサー設定を変更するには、UpdateService を使用する必要があります。

次の形式を使用して、複数のターゲットグループをサービス定義で指定できます。サービス定義の完全な構文については、「サービス定義テンプレート」を参照してください。

```
"loadBalancers":[
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_1/1234567890123456",
      "containerName":"container_name",
      "containerPort":container_port
   },
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_2/6543210987654321",
      "containerName":"container_name",
      "containerPort":container_port
   }
]
```

考慮事項

サービス定義で複数のターゲットグループを指定する際には、次の点を考慮する必要があります。

- Application Load Balancer または Network Load Balancer を使用するサービスの場合、6 個以上のターゲットグループはアタッチできません。
- サービス定義での複数のターゲットグループの指定は、次の条件でのみサポートされます。
  - サービスでは、Application Load Balancer またはNetwork Load Balancer を使用する必要があります。

  - サービスでローリング更新 (ECS) のデプロイコントローラータイプを使用する必要があります。
- Fargate と EC2 の両方の起動タイプを使用するタスクを含むサービスでは、複数のターゲットグループの指定がサポートされます。
- 複数のターゲットグループを指定するサービスを作成するときは、Amazon ECS サービスにリンクされたロールを作成する必要があります。ロールは、API リクエストの `role` パラメータを省略するか、AWS CloudFormation の `Role` プロパティを省略することによって作成されます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。

サービス定義の例

次に、サービス定義で複数のターゲットグループを指定するいくつかのユースケースの例を示します。サービス定義の完全な構文については、「サービス定義テンプレート」を参照してください。

内部トラフィックと外部トラフィックに別々のロードバランサーを使用する

次のユースケースでは、サービスは 2 つの別個のロードバランサーを使用します。1 つは内部トラフィック用、もう 1 つはインターネット向けトラフィック用で、同じコンテナとポートに対して使用します。

```
"loadBalancers":[
   //Internal ELB
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_1/1234567890123456",
      "containerName":"nginx",
      "containerPort":8080
   },
   //Internet-facing ELB
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_2/6543210987654321",
      "containerName":"nginx",
      "containerPort":8080
   }
]
```

同じコンテナの複数のポートを公開する

次のユースケースでは、サービスは 1 つのロードバランサーを使用しますが、同じコンテナから複数のポートを公開します。例えば、Jenkins コンテナは、Jenkins ウェブインターフェイス用にポート 8080 を、API 用にポート 50000 を公開する場合があります。

```
"loadBalancers":[
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_1/1234567890123456",
      "containerName":"jenkins",
      "containerPort":8080
   },
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_2/6543210987654321",
      "containerName":"jenkins",
      "containerPort":50000
   }
]
```

複数のコンテナのポートを公開する

次のユースケースでは、サービスは 1 つのロードバランサーと 2 つのターゲットグループを使用して、個別のコンテナからポートを公開します。

```
"loadBalancers":[
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_1/1234567890123456",
      "containerName":"webserver",
      "containerPort":80
   },
   {

 "targetGroupArn":"arn:aws:elasticloadbalancing:region:123456789012:targetgroup/
target_group_name_2/6543210987654321",
      "containerName":"database",
      "containerPort":3306
```

```
    }
]
```

Amazon ECS サービスを自動的にスケールする

オートスケーリング は、Amazon ECS サービスで必要なタスク数を自動的に増減する機能です。Amazon ECS は アプリケーション Auto Scaling サービスを活用してこの機能を提供します。詳細については、 ユーザーガイドの Application Auto Scaling リファレンスを参照してください。

Amazon ECS はご使用のサービスの CPU とメモリの平均使用量を含む CloudWatch メトリクスを発行します。詳細については、「Amazon ECS サービスの使用率メトリクス」を参照してください。これらおよびその他の CloudWatch メトリクスを使用して、ピーク時に高需要に対処するためにサービスをスケールアウトし (実行するタスクを増やし)、使用率の低い期間にコストを削減するためにサービスをスケールインする (実行するタスクを減らす) ことができます。

Amazon ECS Service Auto Scaling は、以下のタイプの自動スケーリングをサポートします。

- ターゲットメトリクスを使用して Amazon ECS サービスをスケールする - 特定のメトリクスのターゲット値に基づいて、サービスが実行するタスク数を増減させます。これはサーモスタットが家の温度を維持する方法に似ています。温度を選択すれば、後はサーモスタットがすべてを実行します。
- CloudWatch アラームに基づく定義済みの増分を使用して Amazon ECS サービスをスケールする - アラーム超過のサイズに応じて変動する一連のスケーリング調整値 (ステップ調整値) に基づいて、サービスが実行するタスク数を増減させます。
- スケジュールされたアクションを使用して Amazon ECS サービスをスケールする - 日付と時刻に基づいてサービスが実行するタスクの数を増減させます。
- 履歴パターンを使用して予測スケーリングで Amazon ECS サービスをスケールする — トラフィックフローの日次または週次のパターンを検出するための過去の負荷データ分析に基づいて、サービスが実行するタスク数を増減します。

考慮事項

スケーリングポリシーを使用する場合は、次の考慮事項に注意してください。

- Amazon ECSは、CloudWatch に 1 分間隔でメトリクスを送信します。クラスターとサービスが CloudWatch にメトリクスを送信するまで、メトリクスは使用できません。また、存在しないメトリクスに対して CloudWatch アラームを作成することはできません。

- スケーリングポリシーは、クールダウン期間をサポートします。これは、以前のスケーリングアクティビティが有効になるまで待機する秒数です。
  - スケールアウトイベントでは、スケールアウトが継続的に (ただし過剰になることなく) 行われます。スケーリングポリシーを使用してサービスの自動スケーリングが正常にスケールアウトすると、クールダウン時間の計算が開始されます。スケーリングポリシーは、より大きなスケールアウトが開始されるか、クールダウン期間が終了しない限り、必要な容量を再度増加させません。このスケールアウトクールダウン期間が有効な間は、スケールアウトアクティビティを開始することで追加された容量は、次のスケールアウトアクティビティに予定される容量の一部として繰り入れられます。
  - スケールインイベントでは、アプリケーションの可用性を保護するために控えめにスケールインされます。そのため、スケールインアクティビティはクールダウン期間が終了するまでブロックされます。ただし、スケールインクールダウン期間中に別のアラームがスケールアウトアクティビティを開始した場合、アプリケーションの自動スケーリングスケールによってターゲットが即座にスケールアウトされます。この場合、スケールインクールダウン期間は停止し、完了しません。
- サービススケジューラは常に必要数を優先しますが、サービスにアクティブなスケーリングポリシーとアラームがある限り、サービスの自動スケーリングはユーザーが手動で設定した必要数を変更できます。
- サービスの必要タスク数が容量最小値より小さく設定された状態で、アラームがスケールアウトアクティビティを開始したとき、サービスの自動スケーリングが必要タスク数を容量最小値までスケールアップします。その後もアラームに関連付けられたスケーリングポリシーに基づいて、必要に応じてスケーリングし続けます。ただし、必要数はすでにキャパシティーの最小値より小さいため、スケールインアクティビティでは調整されません。
- サービスの必要タスク数が容量最大値より大きく設定された状態で、アラームがスケールインアクティビティを開始したとき、Service Auto Scaling が必要タスク数を容量最大値までスケールアウトします。その後もアラームに関連付けられたスケーリングポリシーに基づいて、必要に応じてスケーリングし続けます。ただし、必要タスク数はすでに容量最大値より大きいため、スケールアウトアクティビティでは調整されません。
- スケーリングアクティビティ中、サービスで実際に実行されているタスクの数は、必要数ではなく、サービスの自動スケーリングが開始点として使用する値です。これが想定される処理能力です。これにより、例えば、追加タスクを配置するために十分なコンテナインスタンスリソースがない場合に、満たすことができない過剰な (ランナウェイ) スケーリングを防ぐことができます。後でコンテナインスタンスのキャパシティーを使用できるようになった場合、保留中の規模の拡大や縮小が続行され、クールダウン期間後にさらに規模の拡大や縮小を続行できることができます。

- 実行する作業がないときにタスク数をゼロにスケーリングするには、キャパシティーの最小値を 0 に設定します。ターゲット追跡スケーリングポリシーでは、実際の容量が 0 で、メトリクスがワークロードの需要があることを示している場合、サービスの自動スケーリングは 1 つのデータポイントの送信を待ってからスケールアウトします。この場合、開始点として可能な最小量だけスケールアウトしてから、実際の実行中のタスク数に基づいてスケーリングを再開します。
- Application Auto Scaling は、Amazon ECS デプロイの進行中にスケールインプロセスをオフにします。ただし、スケールアウトプロセスは、中断しない限り、デプロイ中に引き続き発生します。詳細については、「サービスの自動スケーリングとデプロイ」を参照してください。
- Amazon ECS タスクには、いくつかの Application Auto Scaling オプションがあります。ターゲットトラッキングは最も使いやすいモードです。これにより、CPU 平均使用率などのメトリクスの目標値を設定するだけです。次に、オートスケーラーは、その値を達成するために必要なタスクの数を自動的に管理します。ステップスケーリングを使用すると、スケーリングメトリクスの特定のしきい値と、しきい値を超えたときに追加または削除するタスクの数を定義できるため、需要の変化に迅速に対応できます。さらに重要なことは、しきい値アラームが超過する時間を最小限に抑えることで、需要の変化に非常に迅速に対応できることです。

Amazon ECS のサービス自動スケーリングを最適化する

Amazon ECS サービスは管理されたタスクのコレクションです。各サービスには、関連するタスク定義、必要なタスク数、オプションの配置戦略があります。Amazon ECS サービスの自動スケーリングは、Application Auto Scaling サービスを通じて実装されます。Application Auto Scaling は CloudWatch メトリクスをスケーリングメトリクスのソースとして使用します。また、CloudWatch アラームを使用して、サービスをスケールインまたはスケールアウトするタイミングのしきい値を設定します。スケーリングのしきい値は、メトリクスターゲットを設定して (ターゲットトラッキングスケーリング) か、しきい値を指定する (ステップスケーリング) ことで指定します。Application Auto Scaling を設定後、サービスに必要な適切なタスク数が継続的に計算されます。また、必要なタスク数を変更する必要がある場合、スケールアウトまたはスケールインによって Amazon ECS に通知します。

サービスの自動スケーリングを効果的に使用するには、適切なスケーリングメトリクスを選択する必要があります。

需要が現在の容量を超えると予測される場合は、アプリケーションをスケールアウトする必要があります。逆に、リソースが需要を上回る場合は、アプリケーションをスケールインしてコストを節約できます。

メトリックの特定

効果的にスケーリングするには、使用率または飽和度を示すメトリクスを特定することが重要です。このメトリクスがスケーリングに役立つためには、以下の特性を備えている必要があります。

- メトリクスは需要と相関している必要があります。リソースが安定していても需要が変化したら、メトリクスの値も変化させる必要があります。需要が増減すると、メトリクスも増減します。
- メトリクスの値はキャパシティに比例してスケールインする必要があります。需要が一定であれば、リソースを追加すると、メトリクスの値も比例して変化する必要があります。そのため、タスクの数を 2 倍にすると、指標は 50% 減少するはずです。

使用率メトリクスを特定する最良の方法は、ステージング環境などの実稼働前の環境で負荷テストを行うことです。商用およびオープンソースの負荷テストソリューションは広く利用可能です。これらのソリューションは通常、合成負荷を生成することも、実際のユーザートラフィックをシミュレートすることもできます。

負荷テストのプロセスを開始するには、アプリケーションの利用状況メトリクスのダッシュボードを設定します。これらのメトリクスには、CPU 使用率、メモリ使用率、I/O 操作、I/O キューの深さ、ネットワークスループットが含まれます。これらのメトリクスは Container Insights などのサービスを使用して収集できます。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。このプロセスでは、アプリケーションの応答時間や作業完了率に関するメトリクスを必ず収集してプロットしてください。

まずは小さなリクエストやジョブの挿入率から始めてください。アプリケーションがウォームアップできるように、このレートを数分間一定に保ってください。その後、速度をゆっくりと上げて、数分間一定に保ちます。アプリケーションの応答時間または完了時間が遅すぎてサービスレベル目標 (SLO) を達成できなくなるまで、このサイクルを繰り返し、その都度レートを上げていきます。

負荷テストを行う際には、各使用率メトリクスを調べてください。負荷とともに増加するメトリクスは、最適な使用率メトリクスとして役立つ最有力候補です。

次に、飽和状態に達しているリソースを特定します。同時に、使用率メトリクスを調べて、最初に高いレベルで横ばいになったものと、ピークに達して最初にアプリケーションをクラッシュさせたものを確認します。たとえば、負荷を追加するにつれて CPU 使用率が 0% から 70 ~ 80% に増加し、さらに負荷を追加してもそのレベルにとどまる場合は、CPU が飽和状態であると言っても過言ではありません。CPU アーキテクチャによっては、100% に達しない可能性があります。たとえば、負荷を追加するとメモリ使用率が増加し、タスクまたは Amazon EC2 インスタンスのメモリ制限に達するとアプリケーションが突然クラッシュしたとします。このような状況では、メモリが完全に消費

された可能性があります。アプリケーションが複数のリソースを消費する可能性があります。そのため、最初に枯渇したリソースを表すメトリクスを選択します。

最後に、タスクまたは Amazon EC2 インスタンスの数を 2 倍にしてから、負荷テストを再試行します。キーメトリクスが以前の半分の速度で、増加または減少すると仮定します。この場合、メトリクスはキャパシティに比例します。これは自動スケーリングに適した使用率メトリクスです。

次に、この架空のシナリオを考えてみましょう。アプリケーションの負荷テストを行い、1 秒あたり 100 リクエストで CPU 使用率が最終的に 80% に達したとします。負荷が増えても、CPU 使用率は上昇しなくなります。ただし、アプリケーションの応答は遅くなります。次に、負荷テストを再度実行して、タスクの数を 2 倍にしますが、速度は以前のピーク値に保たれます。CPU の平均使用率が約 40% に低下した場合、CPU 平均使用率がスケーリングメトリクスの候補として適しています。一方、タスク数を増やしても CPU 使用率が 80% のままであれば、平均 CPU 使用率は適切なスケーリング指標ではありません。その場合は、適切なメトリクスを見つけるためにさらに調査する必要があります。

一般的なアプリケーションモデルおよびスケーリングプロパティ

あらゆる種類のソフトウェアが AWS で実行されます。多くのワークロードは自社開発ですが、他のワークロードは一般的なオープンソースソフトウェアをベースにしています。その出所に関係なく、サービスの一般的なデザインパターンがいくつか確認されています。どのように効果的にスケーリングできるかは、そのパターンに大きく依存します。

効率的な CPU バウンドサーバー

効率的な CPU バウンドサーバーは、CPU とネットワークスループット以外のリソースをほとんど使用しません。各リクエストはアプリケーションだけで処理できます。リクエストはデータベースなど他のサービスには依存しません。アプリケーションは何十万もの同時リクエストを処理でき、そのために複数の CPU を効率的に活用できます。各リクエストは、メモリーオーバーヘッドの少ない専用スレッドによって処理されるか、リクエストを処理する各 CPU で実行される非同期イベントループによって処理されます。アプリケーションの各レプリカは、同じようにリクエストを処理できます。CPU が枯渇する前に枯渇する可能性のあるリソースは、ネットワーク帯域幅のみです。CPU バウンドサービスでは、ピークスループットでもメモリ使用率は、利用可能なリソースのほんの一部です。

このタイプのアプリケーションは、CPU ベースの自動スケーリングに適しています。このアプリケーションはスケーリングに関して最大限の柔軟性を備えています。より大きな Amazon EC2 インスタンスまたは Fargate vCPUs を提供することで、垂直方向にスケーリングできます。また、レプリカをさらに追加することで水平方向にスケールすることもできます。レプリカを追加したり、インスタンスサイズを 2 倍にしたりすると、容量に対する平均 CPU 使用率が半分に削減されます。

このアプリケーションに Amazon EC2 の容量を使用している場合は、c5 または c6g ファミリーなどのコンピューティング最適化インスタンスに配置することを検討してください。

効率的なメモリバウンドサーバー

効率的なメモリバウンドサーバーは、リクエストごとに大量のメモリを割り当てます。同時実行性が最大になると、必ずしもスループットが高くなるわけではありませんが、CPU リソースが使い果たされる前にメモリが使い果たされます。リクエストに関連するメモリは、リクエストが終了すると解放されます。メモリに余裕がある限り、追加のリクエストを受け付けることができます。

このタイプのアプリケーションは、メモリベースの自動スケーリングに適しています。このアプリケーションはスケーリングに関して最大限の柔軟性を備えています。より大きな Amazon EC2 または Fargate メモリリソースを提供することで、垂直方向の両方にスケーリングできます。また、レプリカをさらに追加することで水平方向にスケールすることもできます。レプリカを追加したり、インスタンスサイズを 2 倍にしたりすると、容量に対する平均メモリ使用率を半分に減らすことができます。

このアプリケーションに Amazon EC2 キャパシティを使用している場合は、r5 または r6g ファミリーなどのメモリ最適化インスタンスにキャパシティを割り当てることを検討してください。

メモリに制約のあるアプリケーションの中には、同時実行数を減らしても使用されるメモリが減らないように、リクエストの終了時にそのリクエストに関連するメモリを解放しないものがあります。このため、メモリベースのスケーリングを使用することはお勧めしません。

ワーカーベースのサーバー

ワーカーベースのサーバーは、個々のワーカースレッドごとに 1 つのリクエストを次々に処理します。ワーカースレッドは POSIX スレッドなどの軽量スレッドでもかまいません。UNIX プロセスなど、より負荷の大きいスレッドの場合もあります。どのスレッドであっても、アプリケーションがサポートできる同時実行数は常に最大です。通常、同時実行数の制限は、使用可能なメモリリソースに比例して設定されます。同時実行数の上限に達すると、追加のリクエストがバックログキューに入れられます。バックログキューがオーバーフローすると、それ以降の受信リクエストは直ちに拒否されます。このパターンに当てはまる一般的なアプリケーションには、Apache Web サーバーや Gunicorn などがあります。

このアプリケーションを拡張するには、通常、リクエストの同時実行性が最適なメトリクスです。各レプリカには同時実行数の制限があるため、平均制限に達する前にスケールアウトすることが重要です。

リクエストの同時実行メトリクスを取得する最良の方法は、アプリケーションに CloudWatch にレポートさせることです。アプリケーションの各レプリカは、同時リクエストの数をカスタムメトリ

クスとして高い頻度で公開できます。この頻度は少なくとも 1 分に 1 回に設定することをおすすめします。複数のレポートを収集したら、平均同時実行数をスケーリングメトリクスとして使用できます。このメトリクスは、同時実行数の合計をレプリカ数で割って計算されます。たとえば、同時実行数の合計が 1000 で、レプリカの数が 10 の場合、平均同時実行数は 100 です。

アプリケーションが Application Load Balancer の背後にある場合は、ロードバランサーの `ActiveConnectionCount` メトリクスをスケーリングメトリクスの要素として使用することもできます。平均値を求めるには、`ActiveConnectionCount` メトリクスをレプリカの数で割る必要があります。スケーリングには未加工のカウント値ではなく、平均値を使用する必要があります。

この設計を最適に機能させるには、リクエストレートが低い場合でも応答レイテンシの標準偏差を小さくする必要があります。需要が少ない時期には、ほとんどのリクエストに短時間で回答し、平均応答時間よりも大幅に時間がかかるリクエストは多くないことをお勧めします。平均応答時間は 95 パーセンタイル応答時間に近くなります。そうしないと、結果としてキューオーバーフローが発生する可能性があります。これはエラーにつながります。オーバーフローのリスクを軽減するために、必要に応じて追加のレプリカを提供することをお勧めします。

待機中のサーバー

待機中のサーバーはリクエストごとに何らかの処理を行いますが、機能するには 1 つ以上のダウンストリームサービスに大きく依存しています。コンテナアプリケーションは多くの場合、データベースやその他の API サービスなどのダウンストリームサービスを多用します。特に大容量または同時実行の多いシナリオでは、これらのサービスが応答するまでに時間がかかることがあります。これは、これらのアプリケーションが CPU リソースをほとんど使用せず、使用可能なメモリの観点から最大限の同時実行性を利用する傾向があるためです。

待機サービスは、アプリケーションの設計方法に応じて、メモリーバウンドのサーバーパターンとワーカーベースのサーバーパターンのどちらにも適しています。アプリケーションの同時実行がメモリによってのみ制限される場合は、平均メモリ使用率をスケーリングメトリクスとして使用する必要があります。アプリケーションの同時実行がワーカーの制限に基づいている場合は、平均同時実行数をスケーリングメトリクスとして使用する必要があります。

Java ベースのサーバー

Java ベースのサーバーが CPU に依存し、CPU リソースに比例してスケーリングする場合は、効率的な CPU バウンドのサーバーパターンに適している場合があります。その場合は、平均 CPU 使用率がスケーリングメトリクスとして適切である場合があります。ただし、多くの Java アプリケーションは CPU に依存していないため、スケーリングが困難です。

最高のパフォーマンスを得るには、Java 仮想マシン (JVM) ヒープにできるだけ多くのメモリーを割り当てることをお勧めします。Java 8 update 191 以降を含む最近のバージョンの JVM では、コンテナに収まるようにヒープサイズをできるだけ大きく自動的に設定しています。つまり、Java では、メモリー使用率がアプリケーション使用率に比例することはほとんどありません。要求率と同時実行数が増加しても、メモリ使用率は一定に保たれます。このため、メモリー使用率に基づいて Java ベースのサーバーをスケーリングすることはお勧めしません。代わりに、通常は CPU 使用率に基づいてスケーリングすることをおすすめします。

Java ベースのサーバーでは、CPU を使い果たす前にヒープが枯渇することがあります。同時実行数が多いとアプリケーションがヒープを使い果たしやすい場合は、平均接続数が最適なスケーリングメトリクスです。アプリケーションが高スループットでヒープを使い果たしやすい場合は、平均リクエストレートが最適なスケーリングメトリクスです。

ガベージコレクションされた他のランタイムを使用するサーバー

多くのサーバーアプリケーションは、.NET や Ruby などのガベージコレクションを実行するランタイムをベースにしています。これらのサーバーアプリケーションは、前述のパターンのいずれかに当てはまります。ただし、Java の場合と同様に、これらのアプリケーションの平均メモリ使用率はスループットや同時実行性と相関関係がないことが多いため、メモリに基づいてアプリケーションをスケーリングすることはお勧めしません。

このようなアプリケーションでは、アプリケーションが CPU に制約されている場合は CPU 使用率に基づいてスケールすることをおすすめします。それ以外の場合は、負荷テストの結果に基づいて、平均スループットまたは平均同時実行性を基準にスケーリングすることをお勧めします。

ジョブプロセッサ

多くのワークロードには非同期のジョブ処理が含まれます。その中には、リクエストをリアルタイムで受信せず、代わりにワークキューにサブスクライブしてジョブを受け取るアプリケーションが含まれます。この種のアプリケーションでは、ほとんどの場合、適切なスケーリング指標はキューの深さです。キューの増加は、保留中の作業が処理能力を上回っていることを示しているのに対し、キューが空の場合は、実行すべき作業よりも容量が多いことを示します。

Amazon SQS や Amazon Kinesis Data Streams などの AWS メッセージングサービスは、スケーリングに使用できる CloudWatch メトリクスを提供します。Amazon SQS では、`ApproximateNumberOfMessagesVisible` が最適なメトリクスです。Kinesis Data Streams では、Kinesis Client Library (KCL) が公開している `MillisBehindLatest` メトリクスの使用を検討してください。このメトリクスは、スケーリングに使用する前に、すべてのコンシューマで平均化する必要があります。

サービスの自動スケーリングとデプロイ

Application Auto Scaling は、Amazon ECS デプロイの進行中にスケールインプロセスをオフにします。ただし、スケールアウトプロセスは、中断しない限り、デプロイ中に引き続き発生します。デプロイの進行中にスケールアウトプロセスを中断する場合は、次の手順を実行します。

1. Application Auto Scaling のスケーラブルなターゲットに関連付けられたサービスのリソース ID (例: `service/default/sample-webapp`) を指定して describe-scalable-targets コマンドを呼び出します。出力を記録します。これは、次のコマンドを呼び出すときに必要になります。
2. リソース ID、名前空間、およびスケーラブルなディメンションを指定して register-scalable-target コマンドを呼び出します。`DynamicScalingInSuspended` と`DynamicScalingOutSuspended` の両方に `true` を指定します。
3. デプロイが完了したら、register-scalable-target コマンドを呼び出してスケーリングを再開できます。

詳細については、「Application Auto Scaling のスケーリングの中断と再開」を参照してください。

ターゲットメトリクスを使用して Amazon ECS サービスをスケールする

ターゲット追跡スケーリングポリシーで、メトリクスを選択してターゲット値を設定します。Amazon ECS サービス自動スケーリングは、スケーリングポリシーを制御する CloudWatch アラームを作成および管理し、メトリクスとターゲット値に基づいてスケーリング調整値を計算します。スケーリングポリシーは、指定されたターゲット値、またはそれに近い値にメトリクスを維持するため、必要に応じてサービスタスクを追加または削除します。ターゲットの追跡スケーリングポリシーは、メトリクスをターゲット値近くに維持することに加えて、負荷パターンの変動によるメトリクスの変動に合わせて調整し、サービスで実行されているタスク数の急速な変動を最小化します。

ターゲット追跡ポリシーにより、CloudWatch アラームとスケーリング調整を手動で定義する必要がなくなります。Amazon ECS は、設定したターゲットに基づいてこれを自動的に処理します。

ターゲット追跡ポリシーを使用する際は、以下について検討します。

- ターゲットの追跡スケーリングポリシーでは、指定されたメトリクスがターゲット値を超えている場合、スケールアウトする必要があると見なされます。指定されたメトリクスがターゲット値を下回っている場合、ターゲットの追跡スケーリングポリシーを使用してスケールアウトすることはできません。

- 指定されたメトリクスに十分なデータがない場合、ターゲットの追跡スケーリングポリシーによってスケールされません。不十分なデータは低い使用率として解釈されないため、スケールインされません。
- ターゲット値と実際のメトリクスデータポイント間にギャップが発生する場合があります。これは、Service Auto Scaling が追加または削除する容量を判断するときに、その数を切り上げまたは切り捨てることによって、常に控えめに動作するためです。これにより、不十分な容量を追加したり、必要以上に容量を削除することを防ぎます。
- アプリケーションの可用性を高めるために、サービスのスケールアウトはメトリクスに比例して可能な限り高速に行われますが、スケールインはより緩やかです。
- Application Auto Scaling は、Amazon ECS デプロイの進行中にスケールインプロセスをオフにします。ただし、スケールアウトプロセスは、中断しない限り、デプロイ中に引き続き発生します。詳細については、「サービスの自動スケーリングとデプロイ」を参照してください。
- Amazon ECS サービスに対して複数のターゲット追跡スケーリングポリシーを設定できます。ただし、各ポリシーがそれぞれ異なるメトリクスを使用している必要があります。サービスの自動スケーリングの目的は常に可用性を優先することであるため、その動作は、スケールアウトまたはスケールインに対するターゲット追跡ポリシーの準備が整っているかどうかに応じて異なります。ターゲット追跡ポリシーのいずれかでスケールアウトする準備ができると、サービスがスケールアウトされますが、すべてのターゲット追跡ポリシー (スケールイン部分がオン) でスケールインする準備ができている場合にのみスケールインされます。
- ターゲット追跡スケーリングポリシーのためにサービスの自動スケーリングが管理する CloudWatch アラームを編集または削除しないでください。スケーリングポリシーを削除するときに、サービスの自動スケーリングはアラームを自動的に削除します。
- ブルー/グリーンデプロイタイプでは、ターゲット追跡スケーリングポリシーの `ALBRequestCountPerTarget` メトリクスはサポートされません。

ターゲット追跡スケーリングポリシーの詳細については、「Application Auto Scaling ユーザーガイド」の「ターゲット追跡スケーリングポリシー」を参照してください。

Amazon ECS サービスの自動スケーリングのターゲット追跡スケーリングポリシーを作成する

ターゲット追跡スケーリングポリシーを作成して、Amazon ECS がサービスで必要なタスク数を自動的に増減するようにします。ターゲット追跡は、ターゲットメトリクス値に基づいて機能します。

コンソール

1. サービスの作成や更新に使用する標準の IAM アクセス権限に加えて、追加のアクセス権限が必要です。詳細については、「Amazon ECS のサービス自動スケーリングに必要な IAM アクセス許可」を参照してください。
2. ポリシーに使用するメトリクスを決定します。以下のメトリクスが利用可能です。

   - [ECSServiceAverageCPUUtilization] — サービスが使用する平均 CPU 使用率。
   - [ECSServiceAverageMemoryUtilization] — サービスが使用する平均メモリ使用率。
   - [ALBRequestCountPerTarget] – タスクが受信する 1 分あたりの理想的な平均リクエスト数。
3. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
4. [Clusters] (クラスター) ページで、クラスターを選択します。
5. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
6. [タスク数を設定する] を選択します。
7. [Amazon ECS サービスのタスク数] で、[自動スケーリングを使用する] を選択します。

   [タスク数セクション] が表示されます。

   a. [タスクの最小数] に、サービスの自動スケーリングで使用するタスクの下限数を入力します。必要な数がこの数を下回ることはありません。
   b. [最大] に、サービスの自動スケーリングで使用するタスクの上限数を入力します。必要な数がこの数を超えることはありません。
   c. [Save] を選択します。

      [ポリシー] ページが表示されます。
8. [スケーリングポリシーを作成する] を選択します。

   [ポリシーを作成する] ページが表示されます。
9. [スケーリングポリシータイプ] で [ターゲットの追跡] を選択します。
10. [Policy Name] (ポリシー名) にこのポリシーの名前を入力します。
11. [メトリクスのタイプ] で、オプションのリストからメトリクスを選択します。
12. [ターゲット使用率] には、Amazon ECS が維持するタスクの割合のターゲット値を入力します。サービスの自動スケーリングは、平均使用率が目標使用率になるまで、または指定した最大タスク数に達するまで、キャパシティをスケールアウトします。

13. [追加設定] で、以下を実行します。

    a. [スケールインのクールダウン期間] に、スケールインアクティビティが完了してから別のスケールインアクティビティが開始されるまでの時間を秒単位で入力します。

    b. [スケールアウトのクールダウン期間] には、前回のスケールアウトアクティビティが有効になるまで待機する時間を秒単位で入力します。

    c. スケールアウトポリシーのみを作成するには、[スケールインを無効にする] を選択します。

14. [スケーリングポリシーを作成する] を選択します。

AWS CLI

1. register-scalable-target コマンドを使用して、スケーラブルなターゲットとして Amazon ECS サービスを登録します。
2. put-scaling-policy コマンドを使用して、スケーリングポリシーを作成します。

CloudWatch アラームに基づく定義済みの増分を使用して Amazon ECS サービスをスケールする

ステップスケーリングポリシーを使用して、スケーリングプロセスを呼び出す CloudWatch アラームを作成および管理します。アラームに違反すると、Amazon ECS はそのアラームに関連付けられたスケーリングポリシーを開始します。ステップスケーリングポリシーは、ステップ調整と呼ばれる一連の調整を使用してタスクをスケールします。調整値の規模は、アラーム違反の大きさに応じて異なります。

- 違反が最初のしきい値を超えた場合、Amazon ECS は最初のステップの調整を適用します。
- 違反が 2 番目のしきい値を超えた場合、Amazon ECS は 2 番目のステップの調整を適用するというように続きます。

ターゲット追跡スケーリング ポリシーを使用して、ターゲットごとの平均 CPU 使用率や平均リクエスト数などのメトリクスに基づいてスケールすることを強くお勧めします。キャパシティーが増加すると減少し、キャパシティーが減少すると増加するメトリクスを使用すると、ターゲット追跡を使用してインスタンス数を比例的にスケールアウトしたり、タスク数を増やすことができます。これにより、Amazon ECS がアプリケーションの需要曲線に厳密に従うことが保証されます。

Amazon ECS サービスの自動スケーリングのステップスケーリングポリシーを作成する

ステップスケーリングポリシーを作成して、Amazon ECS がサービスで必要なタスク数を自動的に増減させます。ステップスケーリングは、ステップ調整と呼ばれる、超過アラームのサイズによって異なる一連のスケーリング調整値に基づいて実行されます。

コンソール

1. サービスの作成や更新に使用する標準の IAM アクセス権限に加えて、追加のアクセス権限が必要です。詳細については、「Amazon ECS のサービス自動スケーリングに必要な IAM アクセス許可」を参照してください。
2. ポリシーに使用するメトリクスを決定します。以下のメトリクスが利用可能です。
   - [ECSServiceAverageCPUUtilization] — サービスが使用する平均 CPU 使用率。
   - [ECSServiceAverageMemoryUtilization] — サービスが使用する平均メモリ使用率。
   - [ALBRequestCountPerTarget] – タスクが受信する 1 分あたりの理想的な平均リクエスト数。
3. メトリクスの CloudWatch アラームを作成します。詳細については、Amazon CloudWatch ユーザーガイドの「静的しきい値に基づいて CloudWatch アラームを作成する」を参照してください。
4. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
5. [Clusters] (クラスター) ページで、クラスターを選択します。
6. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
7. [タスク数を設定する] を選択します。
8. [Amazon ECS サービスのタスク数] で、[自動スケーリングを使用する] を選択します。

   [タスク数セクション] が表示されます。

   a. [タスクの最小数] に、サービスの自動スケーリングで使用するタスクの下限数を入力します。必要な数がこの数を下回ることはありません。
   b. [最大] に、サービスの自動スケーリングで使用するタスクの上限数を入力します。必要な数がこの数を超えることはありません。
   c. [Save] を選択します。

      [ポリシー] ページが表示されます。
9. [スケーリングポリシーを作成する] を選択します。

[ポリシーを作成する] ページが表示されます。

10. [スケーリングポリシータイプ] で [ステップスケーリング] を選択します。
11. スケールアウトプロパティを設定します。[タスクを追加するステップ] で、次を実行します。

    a. [Policy Name] (ポリシー名) にこのポリシーの名前を入力します。
    b. [CloudWatch アラーム名] で、CloudWatch アラームを選択します。
    c. [メトリクスの集計タイプ] で、選択したメトリクスを定義されたしきい値と比較する方法を選択します。
    d. [調整タイプ] で、調整がタスク数の変化に基づくか、タスクの割合の変化に基づくかを選択します。
    e. [実行するアクション] で、実行するアクションの値を入力します。

    [ステップを追加] を選択して、追加のアクションを追加します。
12. スケールインプロパティを設定します。[タスクを削除するステップ] で、次を実行します。

    a. [Policy Name] (ポリシー名) にこのポリシーの名前を入力します。
    b. [CloudWatch アラーム名] で、CloudWatch アラームを選択します。
    c. [メトリクスの集計タイプ] で、選択したメトリクスを定義されたしきい値と比較する方法を選択します。
    d. [調整タイプ] で、調整がタスク数の変化に基づくか、タスクの割合の変化に基づくかを選択します。
    e. [実行するアクション] で、実行するアクションの値を入力します。

    [ステップを追加] を選択して、追加のアクションを追加します。
13. [クールダウン期間] には、前回のスケーリングアクティビティが有効になるまで待機する時間を秒単位で入力します。追加ポリシーの場合、スケールアウトアクティビティの終了後、スケーリングポリシーによってスケールインアクティビティがブロックされ、一度にスケールアウトできるタスクの数が制限されます。削除ポリシーの場合、これはスケールインアクティビティの後、別のスケールインアクティビティが開始されるまでに経過する必要がある時間です。
14. [スケーリングポリシーを作成する] を選択します。

AWS CLI

1. register-scalable-target コマンドを使用して、スケーラブルなターゲットとして Amazon ECS サービスを登録します。

2. put-scaling-policy コマンドを使用して、スケーリングポリシーを作成します。

スケジュールされたアクションを使用して Amazon ECS サービスをスケールする

スケジュールされたスケーリングでは、特定の時間にタスク数を増減するスケジュールアクションを作成することで、予測可能な負荷の変化に基づいてアプリケーションの自動スケーリングを設定できます。これにより、予測可能な負荷の変化に合わせてアプリケーションを事前対応的にスケーリングできます。

これらのスケジュールされたスケーリングアクションにより、コストとパフォーマンスを最適化できます。アプリケーションには、週半ばのトラフィックのピークを処理するのに十分な数のタスクがありますが、それ以外の時間帯にタスクを過剰にプロビジョニングすることはありません。

スケジュールされたスケーリングとスケーリングポリシーを併用して、スケーリングに事前対応型アプローチと即応型アプローチの両方のメリットを得ることができます。スケジュールされたスケーリングアクションの実行後、スケーリングポリシーはタスクをさらにスケールするかどうかの判断を引き続き行うことができます。これは、アプリケーションの負荷を処理するために十分なタスク数を確保する上で役立ちます。アプリケーションは需要に合わせてスケールしますが、現行のキャパシティは、スケジュールされたアクションによって設定された最小タスク数と最大タスク数の範囲内に収まる必要があります。

スケジュールスケーリングは AWS CLI を使用して設定できます。スケジュールに基づくスケーリングの詳細については、「Application Auto Scaling ユーザーガイド」の「スケジュールに基づくスケーリング」を参照してください。

Amazon ECS サービスの自動スケーリングのスケジュールされたアクションを作成する

スケジュールされたアクションを作成して、Amazon ECS でサービスが実行するタスク数を日付と時刻に基づいて増減させます。

コンソール

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
4. [サービスの自動スケーリング] を選択します。

   [サービスの自動スケーリング] ページが表示されます。

5. [サービスの自動スケーリング] を設定していない場合は、[タスク数の設定] を選択します。

   Amazon ECS サービスタスク数 のセクションが表示されます。

   Amazon ECS サービスタスク数 で、[サービスの自動スケーリングを使用してサービスの必要なタスク数を調整する] を選択します。

   [タスク数セクション] が表示されます。

   a. [タスクの最小数] に、サービスの自動スケーリングで使用するタスクの下限数を入力します。必要な数がこの数を下回ることはありません。
   b. [最大] に、サービスの自動スケーリングで使用するタスクの上限数を入力します。必要な数がこの数を超えることはありません。
   c. [保存] を選択します。

      [ポリシー] ページが表示されます。
6. [スケジュールされたアクション] を選択し、[作成] を選択します。

   [スケジュールされたアクションを作成] ページが表示されます。
7. バケット名に、一意の名前を入力します。
8. [Time zone (タイムゾーン)] でタイムゾーンを選択。

   リストされているすべてのタイムゾーンは、IANA タイムゾーンデータベースから取得されます。詳細については、「List of tz database time zones」を参照してください。
9. [開始時刻] で、アクションが開始される [日付] と [時刻] を入力します。

   定期的なスケジュールを選択した場合、開始時間によって、定期的なシリーズの最初のスケジュールされたアクションが実行されるタイミングが定義されます。
10. [Recurrence (反復)] で、使用可能なオプションの 1 つを選択します。

    - 反復スケジュールに基づいてスケールするには、Amazon ECS がスケジュールされたアクションを実行する頻度を選択します。
      - [レート] で始まるオプションを選択した場合、cron 式が作成されます。
      - [Cron] を選択した場合は、いつアクションを実行するかを Cron 式を入力します。
    - 1 回だけスケールするには、[1 回] を選択します。
11. [タスク調整] で、次の操作を行います。

    - [最小] で、サービスが実行する最小タスク数を入力します。

- [最大] で、サービスが実行する最大タスク数を入力します。

12. [スケジュールされたアクションの作成] を選択してください。

CLI

次のように AWS CLI を使用して、サービスのスケジュールされたスケーリングポリシーを設定します。各*###############*を独自の情報に置き換えます。

例: 1 回のみスケールするには

次の put-scheduled-action コマンドを、`--start-time "YYYY-MM-DDThh:mm:ssZ"` と `--MinCapacity` および `--MaxCapacity` オプションのいずれかまたは両方と併用します。

```
aws application-autoscaling put-scheduled-action --service-namespace ecs \
  --resource-id service/my-cluster/my-service \
  --scheduled-action-name my-one-time-schedule \
  --start-time 2021-01-30T12:00:00 \
  --scalable-target-action MinCapacity=3,MaxCapacity=10
```

例: 定期的なスケーリングをスケジュールするには

次の put-scheduled-action コマンドを使用します。*user-input* を独自の値に置き換えます。

```
aws application-autoscaling put-scheduled-action --service-namespace ecs \
  --resource-id service/my-cluster/my-service \
  --scheduled-action-name my-recurring-action \
  --schedule "rate(5 hours)" \
  --start-time 2021-01-30T12:00:00 \
  --end-time 2021-01-31T22:00:00 \
  --scalable-target-action MinCapacity=3,MaxCapacity=10
```

指定された繰り返しスケジュールは、UTC タイムゾーンに基づいて実行されます。別のタイムゾーンを指定するには、次の例のように、`--time-zone` オプションと IANA タイムゾーンの名前を含めます。

```
--time-zone "America/New_York"
```

詳細については、「List of tz database time zones」を参照してください。

履歴パターンを使用して予測スケーリングで Amazon ECS サービスをスケールする

予測スケーリングは、トラフィックフローからの過去の負荷データを調べて、日次または週次のパターンを分析します。次に、この分析を使用して将来のニーズを予測し、必要に応じてサービスのタスクをプロアクティブに増やします。

予測自動スケーリングは、以下の状況で最も役立ちます。

- 周期的なトラフィック - 通常の営業時間にリソースの使用が増加し、夜間や週末にはリソースの使用が減少する。
- オンとオフを繰り返すワークロードパターン - バッチ処理、テスト、定期的なデータ分析など。
- 初期化に時間がかかるアプリケーション - スケールアウトイベント中のアプリケーションのパフォーマンスに影響を及ぼし、顕著なレイテンシーを引き起こす可能性がある。

アプリケーションの初期化に時間がかかり、トラフィックが規則的なパターンで増加する場合は、予測スケーリングの使用を検討する必要があります。ターゲット追跡やステップスケーリングなどの動的スケーリングポリシーを単独で使用するのではなく、予測される負荷に応じてタスク数を事前に増やすことで、より迅速にスケールできます。予測スケーリングにより、タスク数が過剰にプロビジョニングされる可能性を回避できるため、コストを削減できる場合もあります。

例えば、営業時間中の使用率が高く、夜間の使用量が少ないアプリケーションを考えてみましょう。各営業日の開始時に、予測スケーリングにより、トラフィックが最初に流入する前にタスクをスケールアウトできます。これにより、使用率の低い期間から高い使用率の期間に移行するときに、アプリケーションの高可用性とパフォーマンスを維持するのに役立ちます。トラフィックの変化に動的スケーリングが反応するのを待つ必要はありません。また、アプリケーションの負荷パターンを確認し、スケジュールされたスケーリングを使用して適切な量のタスクをスケジュールするために時間を費やす必要もありません。

内容

Amazon ECS で予測スケーリングがどのように機能するかについて説明します。

ここでは、予測スケーリングの使用に関する考慮事項、その仕組み、制限事項について説明します。

予測スケーリングを使用する際の考慮事項

- 予測スケーリングがワークロードに適していることを確認する必要があります。これを確認するには、予測専用モードでスケーリングポリシーを設定し、コンソールが推奨する内容を確認します。予測スケーリングの使用を開始する前に、予測とレコメンデーションを評価する必要があります。
- 予測スケーリングが予測を開始するには、少なくとも 24 時間以上の履歴データが必要です。使用可能な履歴データが多いほど、予測がより効果的になり、2 週間分の履歴データがあると理想的です。また、Amazon ECS サービスを削除して新しいサービスを作成する場合、予測スケーリングによって新しい予測が生成されるまで 24 時間待つ必要があります。これを高速化する 1 つの方法は、カスタムメトリクスを使用して、古い Amazon ECS サービスと新しい Amazon ECS サービス全体のメトリクスを集約することです。
- アプリケーションのすべての負荷を正確に表し、スケーリングが最も重要なアプリケーションの側面である負荷メトリクスを選択します。
- 予測スケーリングを使用した動的スケーリングにより、アプリケーションの需要に迅速に対応でき、需要が少ないときにはスケールインし、予期しないトラフィックの増加時にはスケールアウトすることができます。複数のスケーリングポリシーがアクティブな場合、各ポリシーによって希望するタスク数が個別に決定され、希望するタスク数はそれらの最大値に設定されます。
- ターゲット追跡やステップスケーリングなどの動的スケーリングポリシーと共に予測スケーリングを使用すると、リアルタイムパターンと履歴パターンの両方に基づいてアプリケーションをスケーリングできます。それ自体では、予測スケーリングはタスクをスケールインしません。
- `register-scalable-target` API を呼び出すときにカスタムロールを使用すると、予測スケーリングポリシーが SLR を有効にした場合にのみ機能することを示すエラーが表示されることがあります。この場合、role-arn なしで再度 `register-scalable-target` を呼び出す必要があります。スケーラブルターゲットを登録する際に SLR を使用し、`put-scaling-policy` API を呼び出します。

予測スケーリングの仕組み

予測スケーリングを使用するには、モニタリングおよび分析する CloudWatch メトリクスを指定する予測スケーリングポリシーを作成します。予測スケーリングが将来の値の予測を開始するには、このメトリクスに 24 時間以上のデータが必要です。

ポリシーを作成すると、予測スケーリングは最長過去 14 日間のメトリクスデータの分析を開始し、パターンを特定します。この分析は、今後 48 時間の必要量の時間ごとの予測を生成するために使用されます。最新の CloudWatch データを使用して、6 時間ごとに予測が更新されます。新しいデータを取得すると、予測スケーリングは将来の予測の正確性を継続的に向上させます。

最初に予測スケーリングを有効にしたときは、予測のみモードで実行されます。このモードでは予測を生成しますが、それらの予測に基づいて Amazon ECS サービスをスケールすることはありません。これにより、予測の正確性と適合性を評価できます。`GetPredictiveScalingForecast` API オペレーションまたは AWS Management Consoleを使用して、予測データを表示します。

予測スケーリングの使用を開始する場合は、スケーリングポリシーを予測とスケーリングモードに切り替えます。このモードでは、次のことが発生します。

Amazon ECS サービスは、デフォルトでは、その時間の予測に基づいて各時間の開始時にスケールされます。`PutScalingPolicy` API オペレーションで `SchedulingBufferTime` プロパティを使用して、早く開始することを選択できます。これにより、新しいタスクは予測される需要よりも早く起動し、トラフィックを処理する準備が整うまでの時間を確保できます。

最大タスク制限

スケーリングのために Amazon ECS サービスを登録する場合、サービスごとに起動できる最大タスク数を定義します。デフォルトでは、スケーリングポリシーが設定されている場合、タスク数をその最大制限を超えて増やすことはできません。

ただし、予測が Amazon ECS サービスの最大タスク数に近づいた場合、または超えた場合に、サービスの最大タスク数を自動的に増やすことを許可できます。

> **Warning**
>
> 最大タスク数を自動的に増やす場合は注意してください。これにより、増加した最大タスク数がモニタリングおよび管理されていない場合、意図したよりも多くのタスクが起動される可能性があります。増加した最大タスク数は、手動で更新するまで Amazon ECS サービスの新しい通常の最大タスク数になります。最大タスク数は、自動的に元の最大タスク数まで減少しません。

サポートされるリージョン

- 米国東部 (バージニア北部)

- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- カナダ (中部)
- 中国 (北京)
- 中国 (寧夏)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (ミラノ)
- ヨーロッパ (パリ)
- ヨーロッパ (ストックホルム)
- 中東 (バーレーン)
- 南米 (サンパウロ)
- AWS GovCloud (米国東部)
- AWS GovCloud (米国西部)

Amazon ECS サービスの自動スケーリングの予測スケーリングポリシーを作成する

予測スケーリングポリシーを作成して、Amazon ECS でサービスが実行するタスク数を履歴データに基づいて増減させます。

> **Note**
>
> 新しいサービスは、予測を生成する前に 24 時間以上のデータを提供する必要があります。

コンソール

1. サービスの作成や更新に使用する標準の IAM アクセス権限に加えて、追加のアクセス権限が必要です。詳細については、「Amazon ECS のサービス自動スケーリングに必要な IAM アクセス許可」を参照してください。
2. ポリシーに使用するメトリクスを決定します。以下のメトリクスが利用可能です。

   - [ECSServiceAverageCPUUtilization] — サービスが使用する平均 CPU 使用率。
   - [ECSServiceAverageMemoryUtilization] — サービスが使用する平均メモリ使用率。
   - [ALBRequestCountPerTarget] – タスクが受信する 1 分あたりの理想的な平均リクエスト数。

   または、カスタムメトリクスを使用することもできます。次の値を定義する必要があります。

   - 負荷 - アプリケーションのすべての負荷を正確に表し、スケーリングが最も重要なアプリケーションの側面であるメトリクス。

   - スケーリングメトリクス - アプリケーションにとって理想的な使用率を予測するために最適な予測子。
3. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
4. [Clusters] (クラスター) ページで、クラスターを選択します。
5. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
6. [サービスの自動スケーリング] を選択し、[タスクの数を設定] を選択します。
7. [Amazon ECS サービスのタスク数] で、[自動スケーリングを使用する] を選択します。

   [タスク数セクション] が表示されます。

   a. [タスクの最小数] に、サービスの自動スケーリングで使用するタスクの下限数を入力します。必要な数がこの数を下回ることはありません。

b. [最大] に、サービスの自動スケーリングで使用するタスクの上限数を入力します。必要な数がこの数を超えることはありません。

c. [Save] を選択します。

[ポリシー] ページが表示されます。

8. [スケーリングポリシーを作成する] を選択します。

[ポリシーを作成する] ページが表示されます。

9. [スケーリングポリシータイプ] で [予測スケーリング] を選択します。

10. [Policy Name] (ポリシー名) にこのポリシーの名前を入力します。

11. [メトリクスペア] で、オプションのリストからメトリクスを選択します。

[Application Load Balancer request count per target] (ターゲットあたりの Application Load Balancer リクエスト数) を選択した場合、[Target group] (ターゲットグループ) のターゲットグループを選択します。[ターゲットあたりの Application Load Balancer リクエスト数] は、Application Load Balancer ターゲットグループをサービスにアタッチしている場合にのみサポートされます。

[カスタムメトリクスペア] を選択した場合、[負荷のメトリクス] と [スケーリングのメトリクス] のリストから個々のメトリクスを選択します。

12. [ターゲット使用率] には、Amazon ECS が維持するタスクの割合のターゲット値を入力します。サービスの自動スケーリングは、平均使用率が目標使用率になるまで、または指定した最大タスク数に達するまで、キャパシティをスケールアウトします。

13. [スケーリングポリシーを作成する] を選択します。

AWS CLI

次のように AWS CLI を使用して、Amazon ECS サービスの予測スケーリングポリシーを設定します。各###############を独自の情報に置き換えます。

指定できる CloudWatch メトリクスの詳細については、「Amazon EC2 Auto Scaling API リファレンス」の「PredictiveScalingMetricSpecification」を参照してください。

例 1: メモリが事前定義された予測スケーリングポリシー。

以下は、メモリ設定が事前定義されたポリシーの例です。

```
cat policy.json
```

```
{
    "MetricSpecifications": [
        {
            "TargetValue": 40,
            "PredefinedMetricPairSpecification": {
                "PredefinedMetricType": "ECSServiceMemoryUtilization"
            }
        }
    ],
    "SchedulingBufferTime": 3600,
    "MaxCapacityBreachBehavior": "HonorMaxCapacity",
    "Mode": "ForecastOnly"
}
```

以下の例は、設定ファイルを指定し put-scaling-policy コマンドを実行して、ポリシーを作成する方法を示しています。

```
aws application-autoscaling put-scaling-policy \
--service-namespace ecs \
--region us-east-1 \
--policy-name predictive-scaling-policy-example \
--resource-id service/MyCluster/test \
--policy-type PredictiveScaling \
--scalable-dimension ecs:service:DesiredCount \
--predictive-scaling-policy-configuration file://policy.json
```

成功した場合、このコマンドはポリシーの ARN を返します。

```
{
    "PolicyARN": "arn:aws:autoscaling:us-
east-1:012345678912:scalingPolicy:d1d72dfe-5fd3-464f-83cf-824f16cb88b7:resource/ecs/
service/MyCluster/test:policyName/predictive-scaling-policy-example",
    "Alarms": []
}
```

例 2: CPU が事前定義された予測スケーリングポリシー。

以下は、CPU 設定が事前定義されたポリシーの例です。

```
cat policy.json
{
    "MetricSpecifications": [
```

```
        {
            "TargetValue": 0.00000004,
            "PredefinedMetricPairSpecification": {
                "PredefinedMetricType": "ECSServiceCPUUtilization"
            }
        }
    ],
    "SchedulingBufferTime": 3600,
    "MaxCapacityBreachBehavior": "HonorMaxCapacity",
    "Mode": "ForecastOnly"
}
```

以下の例は、設定ファイルを指定し put-scaling-policy コマンドを実行して、ポリシーを作成する方法を示しています。

```
aws aas put-scaling-policy \
--service-namespace ecs \
--region us-east-1 \
--policy-name predictive-scaling-policy-example \
--resource-id service/MyCluster/test \
--policy-type PredictiveScaling \
--scalable-dimension ecs:service:DesiredCount \
--predictive-scaling-policy-configuration file://policy.json
```

成功した場合、このコマンドはポリシーの ARN を返します。

```
{
    "PolicyARN": "arn:aws:autoscaling:us-
east-1:012345678912:scalingPolicy:d1d72dfe-5fd3-464f-83cf-824f16cb88b7:resource/ecs/
service/MyCluster/test:policyName/predictive-scaling-policy-example",
    "Alarms": []
}
```

Amazon ECS の予測スケーリングポリシーの評価

予測スケーリングポリシーを使用してサービスをスケールする前に、Amazon ECS コンソールでポリシーの推奨事項とその他のデータを確認します。予測が正確であることがわかるまで、予測スケーリングポリシーが実際のキャパシティをスケーリングすることが好ましくないため、これは重要です。

サービスが新しい場合は、最初の予測の作成に 24 時間かかります。

AWS が予測を作成するとき、履歴データを使用します。サービスに最新の履歴データがまだ十分にない場合、予測スケーリングは現在使用可能な履歴集計から作成された集計で予測を一時的にバックフィルすることがあります。予測は、ポリシーの作成日より最大 2 週間前にバックフィルされます。

予測スケーリングの推奨事項の表示

分析を効果的に行うには、サービスの自動スケーリングに比較対象となる予測スケーリングポリシーが少なくとも 2 つ必要です。(ただし、単一ポリシーの結果を確認することはできます) 複数のポリシーを作成するとき、1 つのメトリクスを使用するポリシーを異なるメトリクスを使用するポリシーと比較して評価できます。異なる目標値およびメトリクスの組み合わせによる影響を評価することもできます。予測スケーリングポリシーが作成された後、Amazon ECS は、どのポリシーがグループのスケーリングに適しているかについて、すぐに評価を開始します。

Amazon ECS コンソールで推奨事項を表示するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
4. [サービスの自動スケーリング] を選択します。
5. 予測スケーリングポリシーを選択し、[アクション]、[予測スケーリング]、[レコメンデーションの表示] を選択します。

   ポリシーの詳細と推奨事項を表示できます。推奨事項は、予測スケーリングポリシーを使用しない場合よりも優れた性能を発揮するかどうかについて説明します。

   予測スケーリングポリシーがグループに適切かどうかが不明な場合、[可用性への影響] 列および [コストへの影響] 列を確認し、適切なポリシーを選択してください。各列の情報は、ポリシーの影響について説明します。

   - [可用性への影響]: ポリシーを使用しない場合と比較し、ワークロードを処理するために十分なタスクをプロビジョニングすることにより、ポリシーが可用性への悪影響を回避できるかどうかについて説明します。
   - [コストへの影響]: ポリシーを使用しない場合と比較し、タスクを過剰にプロビジョニングしないことにより、ポリシーがコストへの悪影響を回避できるかどうかについて説明します。過

剰にプロビジョニングしすぎると、サービスが十分に活用されない、またはアイドル状態になり、コストへの影響が増す一方です。

複数のポリシーがある場合、より低コストで最も可用性のメリットが高いポリシーの名前の横に [最良予測] タグが表示されます。可用性への影響がより重視されます。

6. (オプション) 推奨結果の必要な期間を選択するには、[評価期間] のドロップダウンから [2 日]、[1 週間]、または [2 週間] のいずれか希望する値を選択します。デフォルトでは、評価期間は過去の 2 週間です。評価期間が長いほど、推奨結果のデータポイントが増えます。ただし、需要が非常に高い時期の後など、負荷パターンが変化した場合、データポイントを追加しても結果が改善されない可能性があります。この場合、最新のデータを見ることでより焦点を絞った推奨事項を得ることができます。

> **Note**
>
> 推奨事項は [予測のみ] モードのポリシーに対してのみ生成されます。推奨機能は、評価期間中にポリシーが [予測のみ] モードのときにより効果的に機能します。ポリシーを [予測とスケーリング] モードで開始し、後で [予測のみ] モードに切り替える場合、そのポリシーの結果に偏りが生じる可能性があります。これは、ポリシーが既に実際のキャパシティに関与しているためです。

予測スケーリングのモニタリンググラフの確認

コンソールでは、以前の日、週間、月の予測を確認し、時間の経過と共にポリシーがどの程度機能しているか視覚化できます。また、ポリシーが実際のタスク数をスケールするかどうかを決定するとき、この情報を使用して予測の精度を評価できます。

Amazon ECS コンソールで予測スケーリングのモニタリンググラフを表示するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
4. [サービスの自動スケーリング] を選択します。

5. 予測スケーリングポリシーを選択し、[アクション]、[予測スケーリング]、[グラフの表示] を選択します。
6. [モニタリング] セクションでは、ポリシーの負荷およびキャパシティに関する過去および今後の予測を実際の値と比較できます。[負荷] グラフには、選択した負荷メトリクスの負荷予測および実際の値が表示されます。[キャパシティ] グラフには、ポリシーによって予測されたタスク数が表示されます。実際に起動されたタスク数も含まれます。縦線は履歴の値と今後の予測を区切っています。これらのグラフは、ポリシーの作成後にすぐ利用できます。
7. (オプション) グラフに表示される履歴データの量を変更するには、ページ上部の [評価期間] のドロップダウンから希望する値を選択します。評価期間はこのページのデータをはいかなる方法で変換することはありません。表示される履歴データの量のみを変更します。

[負荷] グラフのデータを比較

各水平線は、1 時間間隔で報告される異なる一連のデータポイントを表しています。

1. [実際に観測された負荷] は、選択した負荷メトリクスの SUM 統計を使用し、過去の 1 時間ごとの合計負荷を表示します。
2. [ポリシーによって予測される負荷] は、1 時間ごとの負荷予測を表示します。この予測は過去 2 週間分の実際の負荷観測に基づいています。

[キャパシティ] グラフのデータの比較

各水平線は、1 時間間隔で報告される異なる一連のデータポイントを表しています。

1. [実際に観測されたタスク数] には、Amazon ECS サービスの過去の実際のキャパシティが表示されます。これは、他のスケーリングポリシーや、選択した期間に有効な最小グループサイズによって異なります。
2. [ポリシーによって予測されるキャパシティ] には、ポリシーが [予測とスケーリング] モードになっているときに各時間の開始時に予想されるベースラインキャパシティが表示されます。
3. [推定される必要タスク数] には、スケーリングメトリクスを選択したターゲット値に維持するためのサービス内の理想的なタスク数が表示されます。
4. [最小タスク数] には、サービス内の最小タスク数が表示されます。
5. [最大キャパシティ] には、サービス内の最大タスク数が表示されます。

推定される必要キャパシティを計算するため、最初は各タスクが指定された目標値で均等に使用されていると仮定します。実際には、タスク数は均等に使用されません。ただし、使用率がタスク間で均

等に分散されていると仮定することにより、必要なキャパシティの量を推定できます。次に、タスク数の要件は、予測スケーリングポリシーに使用したスケーリングメトリクスに反比例するように計算されます。つまり、タスク数が増加するにつれ、スケーリングメトリクスは同じ割合で減少します。例えば、タスク数が 2 倍になった場合、スケーリングメトリクスは半減します。

推定された必要キャパシティの計算式は、次のとおりです。

```
sum of (actualServiceUnits*scalingMetricValue)/(targetUtilization)
```

例えば、特定の時間の `actualServiceUnits` (`10`) および `scalingMetricValue` (`30`) を算出します。その後、予測スケーリングポリシー (`60`) で指定した `targetUtilization` を使用し、同じ時間に推定される必要キャパシティを計算します。これは `5` の値を返します。これは、スケーリングメトリクスの目標値とは正反比例し、キャパシティを維持するために必要なキャパシティの推定量は 5 であることを意味します。

> **Note**
>
> コスト削減およびアプリケーションの可用性を調整および改善するため、さまざまな手段が用意されています。
>
> - ベースラインキャパシティに予測スケーリングを使用し、追加のキャパシティに動的スケーリングを使用します。動的スケーリングは予測スケーリングとは独立して動作し、現在の使用率に基づいてスケールインおよびスケールアウトを行います。まず、Amazon ECS は、スケジュールされていないスケーリングポリシーごとに推奨されるタスク数を計算します。次に、最も多くのタスクを提供するポリシーに基づいてスケーリングします。
> - 負荷が減少したときにスケールインできるようにするには、サービスに、スケールイン部分を有効にした動的スケーリングポリシーが常に少なくとも 1 つ必要です。
> - 最小キャパシティおよび最大キャパシティを制限しすぎないようにすることにより、スケーリングパフォーマンスを向上させることができます。推奨されるタスク数が最小キャパシティおよび最大キャパシティの範囲に収まらないポリシーは、スケールインおよびスケールアウトができなくなります。

CloudWatch による Amazon ECS の予測スケーリングメトリクスをモニタリングする

Amazon CloudWatch を使用して、予測スケーリング用にデータをモニタリングできます。予測スケーリングポリシーは、今後の負荷を予測するために使用されるデータを収集します。収集されたデータは、定期的に CloudWatch に自動的に保存され、ポリシーが時間の経過と共にどの程度機能し

ているかを視覚化するために使用できます。また、CloudWatch アラームを作成して、パフォーマンス指標が定義した制限を超えて変化したときに通知させることもできます。

履歴予測データの視覚化

予測スケーリングポリシーの負荷予測データは CloudWatch で表示でき、他の CloudWatch メトリクスに対する予測を 1 つのグラフで視覚化する場合に役立ちます。また、より広い時間範囲を表示することで、時間の経過に伴う傾向を確認することもできます。最大 15 か月間の履歴メトリクスにアクセスして、ポリシーの動作をより的確に把握できます。

CloudWatch コンソールを使用して履歴予測データを表示する方法

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Metrics] (メトリクス)、[All metrics] (すべてのメトリクス) の順に選択します。
3. [アプリケーションの自動スケーリング] メトリクス名前空間を選択します。
4. [予測スケーリングの負荷予測] を選択します。
5. 検索フィールドに、予測スケーリングポリシー名または Amazon ECS サービスグループ名を入力し、Enter キーを押して結果をフィルタリングします。
6. メトリクスをグラフ表示するには、メトリクスの横にあるチェックボックスを選択します。グラフの名前を変更するには、鉛筆アイコンを選択します。時間範囲を変更するには、事前定義済みの値を選択するか、[custom] を選択します。詳細については、「Amazon CloudWatch ユーザーガイド」の「メトリクスのグラフ化」を参照してください。
7. 統計を変更するには、[Graphed metrics] タブを選択します。列見出しまたは個々の値を選択し、続いて各種統計を選択します。各メトリクスの任意の統計を選択できますが、すべての統計が [PredictiveScalingLoadForecast] メトリクスに有用なわけではありません。例えば、平均、最小、最大統計は有用ですが、合計統計は有用ではありません。
8. グラフに別のメトリクスを追加するには、[Browse] (参照) で [All] (すべて) を選択し、追加したいメトリクスを見つけて、その横にあるチェックボックスをオンにします。最大 10 個のメトリクスを追加できます。
9. (オプション) このグラフを CloudWatch ダッシュボードに追加するには、[Actions] (アクション)、[Add to dashboard] (ダッシュボードに追加) の順に選択します。

Metric Math を使用して精度メトリクスを作成する

Metric Math により、複数の CloudWatch メトリクスをクエリし、数式を使用して、これらのメトリクスに基づく新しい時系列を作成できます。作成された時系列を CloudWatch コンソールで可視化で

き、ダッシュボードに追加できます。Metric Math の詳細については、「Amazon CloudWatch ユーザーガイド」の「Metric Math を使用する」を参照してください。

Metric Math を使用して、サービス自動スケーリングが予測スケーリングのために生成するデータを各種の方法でグラフ化できます。これにより、ポリシーのパフォーマンスを経時的にモニタリングし、メトリクスの組み合わせを改善できるかどうかを把握することができます。

例えば、Metric Math 式を使用して、平均絶対パーセント誤差 (MAPE) をモニタリングできます。MAPE メトリクスは、予測値と、特定の予測期間中に観測された実際の値の差をモニタリングするのに役立ちます。MAPE の値の変化は、アプリケーションの性質が変化するにつれて、ポリシーのパフォーマンスが経時的に低下しているかどうかを示します。MAPE の増加は、予測値と実際の値の差が大きいことを示します。

例: Metric Math 式

このタイプのグラフを使用するには、次の例に示すような Metric Math 式を作成します。

単一のメトリクスではなく、`MetricDataQueries` 用のメトリクスデータクエリ構造の配列があります。`MetricDataQueries` の各項目は、メトリクスを取得するか、数式を実行します。最初の項目は、数式である `e1` です。指定された式は、`ReturnData` パラメータを `true` に設定し、最終的に単一の時系列を生成します。他のすべてのメトリクスで、`ReturnData` 値は `false` です。

この例では、指定された式は実際の値と予測値を入力値として使用し、新しいメトリクス (MAPE) を返します。`m1` は、実際の負荷値を含む CloudWatch メトリクスです (CPU 使用率が、`my-predictive-scaling-policy` という名前のポリシーに対して最初に指定された負荷メトリクスであると仮定)。`m2` は、予測負荷値を含む CloudWatch メトリクスです。MAPE メトリクスの計算構文は次のとおりです。

(絶対値 ((実際の値 - 予測値)/(実際の値))) の平均

精度メトリクスを視覚化してアラームを設定する

精度メトリクスデータを視覚化するには、CloudWatch コンソールの [Metrics] (メトリクス) タブをクリックします。そこからデータをグラフ化できます。詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch グラフへの数式の追加」を参照してください。

[Metrics] (メトリクス) セクションから、モニタリングしているメトリクスにアラームを設定することもできます。[Graphed metrics] (グラフ化したメトリクス) タブで、[Actions] (アクション) 列にある [Create alarm] (アラームを作成) アイコンをクリックします。[Create alarm] (アラームを作成) アイ

コンは小さなベルです。詳細および通知オプションについては、「Amazon CloudWatch ユーザーガイド」の「メトリクス数式に基づく CloudWatch アラームの作成」と「アラームの変更をユーザーに通知する」を参照してください。

GetMetricData および PutMetricAlarm を使用して、Metric Math によって計算し、その出力に基づいてアラームを作成することもできます。

スケジュールされたアクションを使用して Amazon ECS の予測値を上書きする

予測計算では考慮できない将来のアプリケーション要件に関する追加情報がある場合があります。例えば、予測の計算では、今後のマーケティングイベントに必要なタスクが過小評価される可能性があります。スケジュールされたアクションを使用して、将来の期間中の予測を一時的に上書きできます。スケジュールされたアクションは、繰り返し実行することも、1 回限りの需要変動がある特定の日時に実行することもできます。

例えば、予測される数よりも多いタスク数でスケジュールされたアクションを作成できます。実行時に、Amazon ECS はサービス内の最小タスク数を更新します。予測スケーリングはタスクの数に合わせて最適化するので、予測値を超える最小タスクの数でスケジュールされたアクションが尊重されます。これにより、タスクの数が予想を下回らないようになります。予測の上書きを停止するには、2 番目にスケジュールされたアクションを使用して、最小タスク数を元の設定に戻します。

次の手順では、将来の期間中の予測を上書きするステップを示します。

トピック

- ステップ 1: (オプション) 時系列データを分析する
- ステップ 2: 2 つのスケジュールされたアクションを作成する

> **Important**
>
> このトピックでは、予測を上書きして、予測よりも大きなキャパシティにスケールしようとしていることを前提としています。予測スケーリングポリシーの干渉なしに一時的にタスク数を減らす必要がある場合は、代わりに 予測のみ モードを使用します。予測のみモードでは、予測スケーリングは予測を生成し続けますが、自動的にタスク数を増やすことはありません。その後、リソース使用率をモニタリングし、必要に応じてタスク数を手動で減らすことができます。

ステップ 1: (オプション) 時系列データを分析する

まず、予測時系列データを分析します。これはオプションのステップですが、予測の詳細を理解したい場合に役立ちます。

1. 予測を取得する

   予測が作成されたら、予測の特定の期間をクエリできます。このクエリの目的は、特定の期間の時系列データの完全なビューを取得することです。

   クエリには、将来の予測データを最大 2 日間含めることができます。予測スケーリングをしばらく使用している場合は、過去の予測データにアクセスすることもできます。ただし、開始時刻と終了時刻の間の最大期間は 30 日間です。

   get-predictive-scaling-forecast AWS CLI コマンドを使用して予測を取得するには、コマンドに次のパラメータを指定します。

   - `resource-id` パラメータにクラスター名を入力します。
   - ポリシーの名前を `--policy-name` パラメータに入力します。
   - 開始時刻を `--start-time` パラメータに入力して、指定した時刻以降の予測データのみが返されるようにします。
   - 終了時刻を `--end-time` パラメータに入力して、指定された時刻より前の予測データのみが返されるようにします。

   ```
   aws application-autoscaling get-predictive-scaling-forecast \
       --service-namespace ecs \
       --resource-id service/MyCluster/test \
       --policy-name cpu40-predictive-scaling-policy \
       --scalable-dimension ecs:service:DesiredCount \
       --start-time "2021-05-19T17:00:00Z" \
       --end-time "2021-05-19T23:00:00Z"
   ```

   成功すると、コマンドは次の例のようなデータを返します。

   ```
   {
       "LoadForecast": [
           {
               "Timestamps": [
                   "2021-05-19T17:00:00+00:00",
   ```

```
                "2021-05-19T18:00:00+00:00",
                "2021-05-19T19:00:00+00:00",
                "2021-05-19T20:00:00+00:00",
                "2021-05-19T21:00:00+00:00",
                "2021-05-19T22:00:00+00:00",
                "2021-05-19T23:00:00+00:00"
            ],
            "Values": [
                153.0655799339254,
                128.8288551285919,
                107.1179447150675,
                197.3601844551528,
                626.4039934516954,
                596.9441277518481,
                677.9675713779869
            ],
            "MetricSpecification": {
                "TargetValue": 40.0,
                "PredefinedMetricPairSpecification": {
                    "PredefinedMetricType": "ASGCPUUtilization"
                }
            }
        }
    ],
    "CapacityForecast": {
        "Timestamps": [
            "2021-05-19T17:00:00+00:00",
            "2021-05-19T18:00:00+00:00",
            "2021-05-19T19:00:00+00:00",
            "2021-05-19T20:00:00+00:00",
            "2021-05-19T21:00:00+00:00",
            "2021-05-19T22:00:00+00:00",
            "2021-05-19T23:00:00+00:00"
        ],
        "Values": [
            2.0,
            2.0,
            2.0,
            2.0,
            4.0,
            4.0,
            4.0
        ]
    },
```

```
    "UpdateTime": "2021-05-19T01:52:50.118000+00:00"
}
```

応答には LoadForecast と CapacityForecast の 2 つの予測が含まれています。LoadForecast は、時間ごとの負荷予測を示します。CapacityForecast は、40.0 の TargetValue (平均 CPU 使用率 40%) を維持しながら予測された負荷を処理するために時間単位で必要なキャパシティーの予測値を示します。

2. ターゲット期間を特定する

   1 回限りの需要変動が発生する時間または時間範囲を特定します。予測に表示される日付と時刻は UTC であることに注意してください。

ステップ 2: 2 つのスケジュールされたアクションを作成する

次に、アプリケーションの負荷が予測を上回る特定の期間に、2 つのスケジュールされたアクションを作成します。例えば、マーケティングイベントで一時的にトラフィックがサイトに流入する場合は、1 回限りのアクションをスケジュールして、開始時に最小キャパシティーを更新できます。次に、イベント終了時に最小キャパシティーを元の設定に戻す別のアクションをスケジュールします。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [クラスターの詳細] ページの [サービス] セクションで、サービスを選択します。

   [サービス詳細] ページが表示されます。
4. [サービスの自動スケーリング] を選択します。

   [ポリシー] ページが表示されます。
5. [スケジュールされたアクション] を選択し、[作成] を選択します。

   [スケジュールアクションの作成] ページが表示されます。
6. バケット名に、一意の名前を入力します。
7. [Time zone (タイムゾーン)] でタイムゾーンを選択。

   リストされているすべてのタイムゾーンは、IANA タイムゾーンデータベースから取得されます。詳細については、「List of tz database time zones」を参照してください。
8. [開始時刻] で、アクションが開始される [日付] と [時刻] を入力します。
9. [繰り返し] で、[1 回] を選択してください。

10. [タスク調整] の [最小] には、タスクの最大数以下の値を入力します。
11. [スケジュールされたアクションの作成] を選択してください。

    [ポリシー] ページが表示されます。
12. イベントの終了時に、最小タスク数を元の設定に戻すように、2 番目にスケジュールされたアクションを設定します。予測スケーリングでは、[最小] に設定した値が予測値未満の場合のみ、タスク数をスケーリングできます。

1 回限りのイベントに対して 2 つのスケジュールされたアクションを作成するには (AWS CLI)

AWS CLI を使用してスケジュールされたアクションを作成するには、put-scheduled-update-group-action コマンドを使用します。

例えば、5 月 19 日の午後 5 時から 8 時間、最小キャパシティーを 3 インスタンスに維持するスケジュールを定義しましょう。以下のコマンドは、このシナリオを実装する方法を示しています。

最初の put-scheduled-update-group-action コマンドは、2021 年 5 月 19 日の午後 5 時 (UTC) に指定された Auto Scaling グループの最小キャパシティーを更新するように Amazon EC2 Auto Scaling に指示します。

```
aws autoscaling put-scheduled-update-group-action --scheduled-action-name my-event-
start \
  --auto-scaling-group-name my-asg --start-time "2021-05-19T17:00:00Z" --minimum-
capacity 3
```

2 番目のコマンドは、2021 年 5 月 20 日の午前 1 時 (UTC) にグループの最小キャパシティーを 1 に設定するように Amazon EC2 Auto Scaling に指示します。

```
aws autoscaling put-scheduled-update-group-action --scheduled-action-name my-event-end
 \
  --auto-scaling-group-name my-asg --start-time "2021-05-20T01:00:00Z" --minimum-
capacity 1
```

これらのスケジュールされたアクションを Auto Scaling グループに追加すると、Amazon EC2 Auto Scaling は次の処理を実行します。

- 2021 年 5 月 19 日の午後 5 時 (UTC) に、最初にスケジュールされたアクションが実行されます。グループのインスタンスが 3 未満である場合、グループは 3 インスタンスにスケールアウトさ

れます。この時刻以降の 8 時間の間、予測キャパシティーが実際のキャパシティーよりも大きい場合、または動的スケーリングポリシーが有効な場合、Amazon EC2 Auto Scaling は引き続きスケールアウトできます。

- 2021 年 5 月 20 日の午前 1 時 (UTC) に、2 番目のスケジュールされたアクションが実行されます。これにより、イベントの終了時に最小キャパシティーが元の設定に戻ります。

繰り返し起こるスケジュールに基づくスケーリング

毎週同じ期間の予測を上書きするには、2 つのスケジュールされたアクションを作成し、cron 式を使用して日時のロジックを指定します。

この cron 式のフォーマットは、スペースで区切られた 5 つのフィールド ([分] [時間] [日] [月] [曜日]) で構成されます。フィールドには、特殊文字を含む任意の許容される値を含めることができます。

例えば、次の cron 式は、毎週火曜日の午前 6:30 にアクションを実行します。アスタリスクは、フィールドのすべての値を照合するワイルドカードとして使用されます。

```
30 6 * * 2
```

関連情報

スケジュールされたアクションを管理する方法の詳細については、「スケジュールされたアクションを使用して Amazon ECS サービスをスケールする」を参照してください。

Amazon ECS のカスタムメトリクスを使用した高度な予測スケーリングポリシー

予測スケーリングポリシーで、事前定義されたメトリクスまたはカスタムメトリクスを使用できます。カスタムメトリクスは、CPU、メモリなどの事前定義されたメトリクスが、アプリケーションの負荷を十分に記述するには不十分である場合に有用です。

カスタムメトリクスを使用して予測スケーリングポリシーを作成するときは、AWS が提供するその他の CloudWatch メトリクスを指定できます。または、自分で定義して公開するメトリクスを指定することもできます。メトリクス計算を使用して既存のメトリクスを集計し、AWS が自動的に追跡しない新しい時系列に変換することもできます。例としては、新しい合計や平均を計算してデータ内の値を結合すること (集計と呼ばれます) が挙げられます。結果のデータは集計と言います。

以下のセクションには、ポリシー用の JSON 構造を構築する方法のベストプラクティスと例が記載されています。

前提条件

予測スケーリングポリシーにカスタムメトリクスを追加するには、`cloudwatch:GetMetricData` 許可が必要です。

AWS が提供するメトリクスの代わりに独自のメトリクスを指定するには、まずそのメトリクスを CloudWatch に発行する必要があります。詳細については、「Amazon CloudWatch ユーザーガイド」の「カスタムメトリクスの発行」を参照してください。

独自のメトリクスを発行するときは、少なくとも 5 分間隔の頻度でデータポイントを発行するようにしてください。データポイントは、必要な期間の長さに基づいて CloudWatch から取得されます。例えば、負荷メトリクスの指定では、時間単位のメトリクスを使用してアプリケーションの負荷を測定します。CloudWatch は、発行されたメトリクスデータを使用して、各 1 時間の期間内にタイムスタンプがあるすべてのデータポイントを集計することにより、各 1 時間の期間に対して単一のデータ値を提供します。

ベストプラクティス

次のベストプラクティスは、カスタムメトリクスをより効果的に使用するのに役立ちます。

- 負荷メトリクス仕様で最も有用なメトリクスは、Auto Scaling グループ全体の負荷を表すメトリクスです。
- スケーリングメトリクス仕様のスケールに最も有用なメトリクスは、タスクメトリクスごとの平均スループットまたは使用率です。
- ターゲット使用率は、スケーリングメトリクスのタイプと一致する必要があります。例えば、CPU 使用率を使用するポリシー設定の場合、これはパーセンテージのターゲットです。
- これらの推奨事項に従わない場合、予測される将来の時系列の値は、多くの場合、誤りになります。データが正しいことを確認するために、コンソールで予測値を表示できます。または、予測スケーリングポリシーを作成した後、GetPredictiveScalingForecast API を呼び出して返された `LoadForecast` オブジェクトを検査します。
- 予測スケーリングがアクティブスケーリングを開始する前に予測を評価できるように、予測のみモードで予測スケーリングを設定することを強くお勧めします。

制限

- 1 つのメトリクス指定で最大 10 個のメトリクスのデータポイントをクエリできます。
- この制限に関しては、1 つの式は 1 つのメトリクスとしてカウントされます。

カスタムメトリクスを使用した予測スケーリングポリシーのトラブルシューティング

カスタムメトリクスの使用中に問題が発生した場合は、次の操作を実行することをお勧めします。

- 検索式の使用中にブルー/グリーンデプロイで問題が発生した場合は、完全一致ではなく部分一致を検索する検索式を作成してください。また、クエリが特定のアプリケーションで実行されている Auto Scaling グループのみを検索していることも確認する必要があります。検索式の構文の詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch 検索式の構文」を参照してください。
- put-scaling-policy コマンドは、スケーリングポリシーの作成時に式を検証します。ただし、このコマンドでは、検出されたエラーの正確な原因を特定できない可能性があります。問題を解決するには、get-metric-data コマンドへのリクエストからの応答で受け取ったエラーをトラブルシューティングします。CloudWatch コンソールから式をトラブルシューティングすることもできます。
- `MetricDataQueries` で SUM() のような数学関数を使用せずに、独自の SEARCH() 関数を指定する場合、`ReturnData` に `false` を指定する必要があります。これは、検索式が複数の時系列を返す可能性がある一方、数式に基づくメトリクス指定は 1 つの時系列しか返すことができないためです。
- 検索式に含まれるすべてのメトリクスは、同じ解像度である必要があります。

Amazon ECS を使用した予測スケーリングカスタムメトリクス用の JSON の構築

以下のセクションには、CloudWatch からのデータをクエリするための予測スケーリングを設定する方法の例が記載されています。このオプションの設定には 2 つの異なる手法あり、予測スケーリングポリシーの JSON を構築するために使用する形式は、選択される手法の影響を受けます。メトリクス計算を使用する場合は、実行されるメトリクス計算に基づいて JSON の形式がさらに多様化します。

1. AWS が提供するその他の CloudWatch メトリクス、またはユーザーが CloudWatch に発行するメトリクスから直接データを取得するポリシーを作成するには、「AWS CLI を使用したカスタム負荷メトリクスとスケーリングメトリクスを用いた予測スケーリングポリシーの例」を参照してください。

AWS CLI を使用したカスタム負荷メトリクスとスケーリングメトリクスを用いた予測スケーリングポリシーの例

AWS CLI でカスタムロードメトリクスとスケーリングメトリクスを使用する予測スケーリングポリシーを作成するには、config.json という名前の JSON ファイルに --predictive-scaling-configuration の引数を保存します。

カスタムメトリクスの追加は、以下の例にある置き換え可能な値を独自のメトリクスとターゲット使用率に置き換えることによって開始します。

```
{
  "MetricSpecifications": [
    {
      "TargetValue": 50,
      "CustomizedScalingMetricSpecification": {
        "MetricDataQueries": [
          {
            "Id": "scaling_metric",
            "MetricStat": {
              "Metric": {
                "MetricName": "MyUtilizationMetric",
                "Namespace": "MyNameSpace",
                "Dimensions": [
                  {
                    "Name": "MyOptionalMetricDimensionName",
                    "Value": "MyOptionalMetricDimensionValue"
                  }
                ]
              },
              "Stat": "Average"
            }
          }
        ]
      },
      "CustomizedLoadMetricSpecification": {
        "MetricDataQueries": [
          {
            "Id": "load_metric",
            "MetricStat": {
              "Metric": {
                "MetricName": "MyLoadMetric",
                "Namespace": "MyNameSpace",
                "Dimensions": [
```

```
                {
                  "Name": "MyOptionalMetricDimensionName",
                  "Value": "MyOptionalMetricDimensionValue"
                }
              ]
            },
            "Stat": "Sum"
          }
        }
      ]
    }
  }
]
}
```

詳細については、「Amazon EC2 Auto Scaling API Reference」 (Amazon EC2 Auto Scaling API リファレンス) の「MetricDataQuery」を参照してください。

> **Note**
>
> 以下は、CloudWatch メトリクスのメトリクス名、名前空間、ディメンション、および統計を見つけるために役立つ追加のリソースです。
>
> - AWS のサービスで使用可能なメトリクスの詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch メトリクスを発行する AWS のサービス」を参照してください。
> - CloudWatch メトリクスの正確なメトリクス名、名前空間、ディメンション (該当する場合) を AWS CLI で取得するには、「list-metrics」を参照してください。

このポリシーを作成するには、以下の例にあるように、JSON ファイルを入力として使用して put-scaling-policy コマンドを実行します。

```
aws application-autoscaling put-scaling-policy --policy-name my-predictive-scaling-policy \
  --auto-scaling-group-name my-asg --policy-type PredictiveScaling \
  --predictive-scaling-configuration file://config.json
```

成功した場合、このコマンドはポリシーの Amazon リソースネーム (ARN) を返します。

```
{
```

```
  "PolicyARN": "arn:aws:autoscaling:region:account-id:scalingPolicy:2f4f5048-d8a8-4d14-
b13a-d1905620f345:autoScalingGroupName/my-asg:policyName/my-predictive-scaling-policy",
  "Alarms": []
}
```

Metric Math 式を使用する

以下のセクションでは、ポリシー内の予測スケーリングポリシーで Metric Math を使用する方法について説明します。

Metric Math について

既存のメトリクスデータの集計だけを行いたい場合は、CloudWatch Metric Math により、別のメトリクスを CloudWatch に発行する手間とコストを節約できます。AWS が提供するメトリクスはすべて使用できます。また、アプリケーションの一部として定義したメトリクスを使用することもできます。

詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch メトリクス数学の使用」を参照してください。

予測スケーリングポリシーで Metric Math の数式を使用する場合は、次の点を考慮してください。

- Metric Math 演算では、メトリクスのメトリクス名、名前空間、ディメンションのキーと値のペアの一意の組み合わせのデータポイントを使用します。
- 任意の算術演算子 (+ - * / ^)、統計関数 (AVG や SUM など)、または CloudWatch がサポートするその他の関数を使用できます。
- 数式の関係式では、メトリクスと他の数式の結果の両方を使用できます。
- Metric Math の数式は、さまざまな集計で構成できます。ただし、最終的な集計結果として、`Average` をスケーリングメトリクスに使用し、`Sum` を負荷メトリクスに使用するのがベストプラクティスです。
- メトリクスの指定で使用される数式はすべて、最終的に単一の時系列を返す必要があります。

Metric Math を使用するには、次の操作を実行します。

- 1 つまたは複数の CloudWatch メトリクスを選択します。次に、数式を作成します。詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch メトリクス数学の使用」を参照してください。
- CloudWatch コンソールまたは CloudWatch GetMetricData API を使用して、Metric Math の数式が有効であることを確認します。

メトリクス計算を使用してメトリクスを組み合わせる予測スケーリングポリシーの例 (AWS CLI)

場合によっては、メトリクスを直接指定するのではなく、まず何らかの方法でそのデータを処理する必要がある場合があります。例えば、Amazon SQS キューから作業を取り出すアプリケーションがあり、キュー内の項目数を予測スケーリングの基準として使用したいとします。キューにあるメッセージの数だけでは、必要なインスタンスの数は定義されません。インスタンスごとのバックログを計算するために使用できるメトリクスを作成するには、さらに多くの作業が必要です。

このシナリオの予測スケーリングポリシー例を次に示します。Amazon SQS `ApproximateNumberOfMessagesVisible` メトリクス (キューから取得可能なメッセージの数) に基づくスケーリングメトリクスおよび負荷メトリクスを指定します。Amazon EC2 Auto Scaling `GroupInServiceInstances` メトリクスと、スケーリングメトリクスのインスタンスごとのバックログを計算するための数式も使用します。

```
aws application-autoscaling put-scaling-policy --policy-name my-sqs-custom-metrics-
policy \
  --policy-type PredictiveScaling \
  --predictive-scaling-configuration file://config.json
  --service-namespace ecs \
  --resource-id service/MyCluster/test \
  "MetricSpecifications": [
    {
      "TargetValue": 100,
      "CustomizedScalingMetricSpecification": {
        "MetricDataQueries": [
          {
            "Label": "Get the queue size (the number of messages waiting to be
 processed)",
            "Id": "queue_size",
            "MetricStat": {
              "Metric": {
                "MetricName": "ApproximateNumberOfMessagesVisible",
                "Namespace": "AWS/SQS",
                "Dimensions": [
                  {
                    "Name": "QueueName",
                    "Value": "my-queue"
                  }
                ]
              },
              "Stat": "Sum"
            },
```

```
            "ReturnData": false
          },
          {
            "Label": "Get the group size (the number of running instances)",
            "Id": "running_capacity",
            "MetricStat": {
              "Metric": {
                "MetricName": "GroupInServiceInstances",
                "Namespace": "AWS/AutoScaling",
                "Dimensions": [
                  {
                    "Name": "AutoScalingGroupName",
                    "Value": "my-asg"
                  }
                ]
              },
              "Stat": "Sum"
            },
            "ReturnData": false
          },
          {
            "Label": "Calculate the backlog per instance",
            "Id": "scaling_metric",
            "Expression": "queue_size / running_capacity",
            "ReturnData": true
          }
        ]
      },
      "CustomizedLoadMetricSpecification": {
        "MetricDataQueries": [
          {
            "Id": "load_metric",
            "MetricStat": {
              "Metric": {
                "MetricName": "ApproximateNumberOfMessagesVisible",
                "Namespace": "AWS/SQS",
                "Dimensions": [
                  {
                    "Name": "QueueName",
                    "Value": "my-queue"
                  }
                ],
              },
              "Stat": "Sum"
```

```
            },
            "ReturnData": true
          }
        ]
      }
    }
  ]
}
```

この例では、ポリシーの ARN が返されます。

```
{
  "PolicyARN": "arn:aws:autoscaling:region:account-id:scalingPolicy:2f4f5048-d8a8-4d14-
b13a-d1905620f345:autoScalingGroupName/my-asg:policyName/my-sqs-custom-metrics-policy",
  "Alarms": []
}
```

Amazon ECS サービスを相互接続する

Amazon ECS タスク内で実行されるアプリケーションは、多くの場合はインターネットからの接続を受信するか、Amazon ECS サービス内で実行される他のアプリケーションに接続する必要があります。インターネットからの外部接続が必要な場合は、Elastic Load Balancing の使用をお勧めします。統合負荷分散の詳細については、「the section called “ロードバランサーを使用してサービストラフィックを分散する”」を参照してください。

Amazon ECS サービス内で実行される他のアプリケーションにアプリケーションを接続する必要がある場合、Amazon ECS にはロードバランサーを使用せずに、次の方法で行うことができます。

- Amazon ECS Service Connect

  サービス検出、接続、トラフィックモニタリング用の Amazon ECS 設定を提供する Service Connect をお勧めします。Service Connect を使用すると、アプリケーションは短縮名と標準ポートを使用して、同じクラスターや他のクラスター (同じ AWS リージョン の VPC を含む) 内の Amazon ECS サービスに接続できます。

  Service Connect を使用すると、Amazon ECS がサービス検出のすべての部分を管理します。つまり、検出可能な名前の作成、タスクの開始と終了時に各タスクのエントリを動的に管理すること、名前を検出するように設定された各タスクでのエージェントの実行などです。アプリケーションは DNS 名の標準機能を使用して接続することで名前を検索できます。アプリケーションがすでにこ

れを実行している場合、Service Connect を使用する際に、アプリケーションを変更する必要はありません。

各サービスとタスク定義内で完全な設定を行います。Amazon ECS は、デプロイ内のすべてのタスクが同じように動作するように、サービスデプロイごとにこの設定の変更を管理します。たとえば、サービス検出の DNS でよくある問題は、移行の制御です。新しい IP アドレスを指すように DNS 名を変更すると、すべてのクライアントが新しいサービスの使用を開始するまでに最大 TTL 時間がかかることがあります。Service Connect では、クライアントデプロイメントがクライアントタスクを置き換えて設定を更新します。他のデプロイと同様に、Service Connect の変更に影響するように、デプロイサーキットブレーカーやその他のデプロイ設定を設定できます。

詳細については、「Service Connect を使用して Amazon ECS サービスを短縮名で接続する」を参照してください。

- Amazon ECS サービス検出

  サービス間の通信のもう 1 つのアプローチは、サービス検出を使用する直接的な通信です。このアプローチでは、Amazon ECS との AWS Cloud Map サービス検出の統合を使用できます。Amazon ECS はサービス検出を使用して、起動されたタスクのリストを AWS Cloud Map に同期します。このホスト名は特定のサービスの 1 つ以上のタスクの内部 IP アドレスに解決される DNS ホスト名を保持します。Amazon VPC の他のサービスは、この DNS ホスト名を使用して、内部 IP アドレスを使用してトラフィックを別のコンテナに直接送信できます。

  このサービス間通信のアプローチでは、レイテンシが低くなります。コンテナ間には余分なコンポーネントはありません。トラフィックは 1 つのコンテナから別のコンテナに直接移動します。

  この方法は、各タスクに固有の IP アドレスが割り当てられる `awsvpc` ネットワークモードを使用する場合に適しています。ほとんどのソフトウェアは、IP アドレスに直接変換される DNS `A` レコードの使用のみをサポートしています。`awsvpc` ネットワークモードを使用する場合、各タスクの IP アドレスは `A` レコードになります。ただし、`bridge` ネットワークモードを使用している場合は、複数のコンテナが同じ IP アドレスを共有している可能性があります。さらに、動的ポートマッピングでは、その 1 つの IP アドレスのポート番号がコンテナにランダムに割り当てられます。この時点では、`A` レコードだけではサービス検出には不十分です。`SRV` レコードも使用する必要があります。このタイプのレコードは IP アドレスとポート番号の両方を記録できますが、アプリケーションを適切に設定する必要があります。使用するビルド済みアプリケーションの中には、`SRV` レコードをサポートしていないものもあります。

awsvpc ネットワークモードのもう 1 つの利点は、サービスごとに固有のセキュリティグループがあることです。このセキュリティ グループを設定して、そのサービスと通信する必要がある特定のアップストリームサービスからの受信接続のみを許可することができます。

サービス検出を使用するサービス間直接的な通信の主な欠点は、再試行や接続障害に対処するためのロジックを追加する必要があることです。DNS レコードには、キャッシュされる時間を制御する有効期限 (TTL) があります。DNS レコードが更新されてキャッシュが期限切れになり、アプリケーションが最新バージョンの DNS レコードを取得できるようになるまでには、ある程度の時間がかかります。そのため、アプリケーションが DNS レコードを解決して、もう存在しない別のコンテナを指すようになってしまう可能性があります。アプリケーションには再試行を処理し、不正なバックエンドを無視するロジックが必要です。

詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。

- Amazon VPC Lattice

  Amazon VPC Lattice は、Amazon ECS のお客様がコードを変更することなく、AWS コンピューティングサービス、VPC、アカウント全体で構築されたアプリケーションを観察、保護、モニタリングするために使用するマネージドアプリケーションネットワーキングサービスです。

  VPC Lattice は、コンピューティングリソースのコレクションであるターゲットグループを使用します。これらのターゲットは、アプリケーションまたはサービスを実行するものであり、Amazon EC2 インスタンス、IP アドレス、Lambda 関数、Application Load Balancer を含みます。Amazon ECS サービスを VPC Lattice ターゲットグループに関連付けることで、お客様は Amazon ECS タスクを VPC Lattice の IP ターゲットとして有効にできるようになりました。Amazon ECS は、登録されたサービスのタスクが起動されると、VPC Lattice ターゲットグループにタスクを自動的に登録します。

  詳細については、「Amazon VPC Lattice を使用して Amazon ECS サービスを接続、監視、保護する」を参照してください。

ネットワークモード互換表

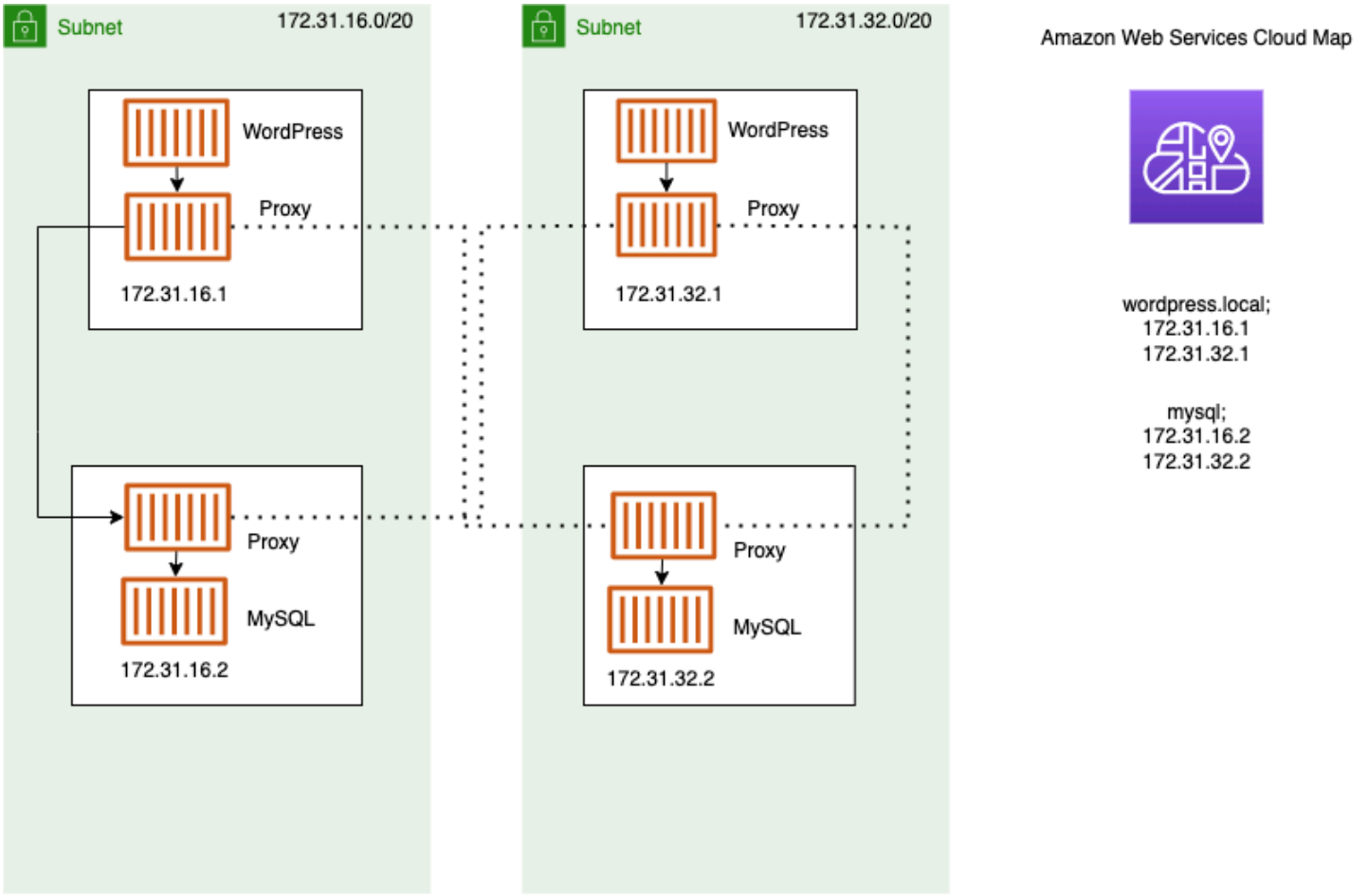
次の表は、これらのオプションとタスクネットワークモードの互換性を示すものです。この表の「クライアント」とは、Amazon ECS タスク内から接続を行うアプリケーションを指します。

相互接続オプション	ブリッジ	awsvpc	ホスト
サービス検出	はい。ただし、クライアントは hostPort を使用せず DNS の SRV レコードを認識する必要があります。	はい	はい。ただし、クライアントは hostPort を使用せず DNS の SRV レコードを認識する必要があります。
Service Connect	はい	はい	なし
VPC Lattice	はい	はい	はい

Service Connect を使用して Amazon ECS サービスを短縮名で接続する

Amazon ECS Service Connect では、Amazon ECS 設定としてサービス間通信を管理できます。Amazon ECS でサービス検出とサービスメッシュの両方を構築します。これにより、サービスのデプロイごとに管理する各サービス内の完全な設定、VPC DNS 設定に依存しない名前空間内のサービスを参照する統一された方法、すべてのアプリケーションを監視するための標準化されたメトリクスとログが提供されます。Service Connect は、サービスのみを相互接続します。

次の図は、VPC に 2 つのサブネットと 2 つのサービスを含む Service Connect ネットワークの例を示しています。各サブネットにつき 1 つのタスクで WordPress を実行するクライアントサービス。各サブネットに 1 つのタスクで MySQL を実行するサーバーサービス。どちらのサービスも、2 つのサブネットに分散された複数のタスクを実行するため、可用性が高く、タスクやアベイラビリティーゾーンの問題に対する耐性があります。実線の矢印は、WordPress から MySQL への接続を示しています。例えば、IP アドレス 172.31.16.1 が設定されたタスク内の WordPress コンテナ内から実行される mysql --host=mysql CLI コマンドなどです。このコマンドは、MySQL のデフォルトポートの短縮名 mysql を使用します。この名前とポートは、同じタスク内で Service Connect プロキシに接続します。WordPress タスクのプロキシは、ラウンドロビン負荷分散と異常値検出に対する以前の障害情報を使用して、接続する MySQL タスクを選択します。図の実線の矢印で示されているように、プロキシは IP アドレス 172.31.16.2 を使用して MySQL タスクの 2 番目のプロキシに接続します。2 番目のプロキシは、同じタスクでローカル MySQL サーバーに接続します。どちらのプロキシも接続パフォーマンスをレポートし、Amazon ECS と Amazon CloudWatch コンソールのグラフに表示されるため、あらゆる種類のアプリケーションのパフォーマンスメトリクスを同じ方法で取得できます。



Service Connect では次の用語が使用されます。

ポート名

特定のポートマッピングに名前を割り当てる Amazon ECS タスク定義設定です。この設定は Amazon ECS Service Connect でのみ使用されます。

クライアントエイリアス

エンドポイントで使用されるポート番号を割り当てる Amazon ECS サービス設定です。さらに、クライアントエイリアスはエンドポイントの DNS 名を割り当て、検出名を上書きすることができます。Amazon ECS サービスで検出名が提供されていない場合、クライアントエイリアス名がエンドポイント名としてポート名に上書きされます。エンドポイントの例については、エンドポイントの定義を参照してください。1 つの Amazon ECS サービスに複数のクライアントエイリアスを割り当てることができます。この設定は Amazon ECS Service Connect でのみ使用されます。

検出名

タスク定義から指定されたポートにオプションとして作成できる中間名。この名前は AWS Cloud Map サービスの作成に使用されます。この名前が指定されていない場合は、タスク定義からのポート名が使用されます。特定のポートおよび Amazon ECS サービスに複数の検出名を割り当てることができます。この設定は Amazon ECS Service Connect でのみ使用されます。

AWS Cloud Map サービス名は、名前空間内で一意である必要があります。この制限により、各名前空間の特定のタスク定義に対し、検出名のない Service Connect 設定は 1 つしか使用できません。

エンドポイント

API またはウェブサイトに接続するための URL です。URL にはプロトコル、DNS 名、ポートが含まれます。エンドポイント全般の詳細については、「Amazon Web Services 全般のリファレンス」の「AWS 用語集」の「エンドポイント」を参照してください。

Service Connect は、Amazon ECS サービスに接続するエンドポイントを作成すると共に、Amazon ECS サービスのタスクがエンドポイントに接続するための設定を行います。URL にはプロトコル、DNS 名、ポートが含まれます。ポートはコンテナイメージ内のアプリケーションと一致する必要があるため、プロトコルとポート名はタスク定義で選択します。サービス内では、各ポートを名前で選択し、DNS 名を割り当てることができます。Amazon ECS サービス設定で DNS 名を指定しない場合、デフォルトではタスク定義からのポート名が使用されます。例えば、Service Connect エンドポイントは `http://blog:80`、`grpc://checkout:8080`、`http://_db.production.internal:99` のいずれかになります。

Service Connect サービス

Amazon ECS サービス内の 1 つのエンドポイントの設定です。これは Service Connect 設定の一部で、コンソールの [Service Connect and discovery name configuration] (Service Connect および検出名の設定) の中の 1 行、または Amazon ECS サービスにおける JSON 設定の `services` リストの中の 1 つのオブジェクトで構成されます。この設定は Amazon ECS Service Connect でのみ使用されます。

詳細については、「Amazon Elastic Container Service API リファレンス」の「ServiceConnectService」を参照してください。

名前空間

Service Connect で使用する AWS Cloud Map 名前空間の短縮名または完全な Amazon リソースネーム (ARN)。名前空間は、Amazon ECS サービスおよびクラスターと同じ AWS リージョンに

ある必要があります。AWS Cloud Map 内の名前空間のタイプは Service Connect に影響しません。

Service Connect は、相互に対話する Amazon ECS タスクの論理グループとして AWS Cloud Map 名前空間を使用します。各 Amazon ECS サービスは 1 つの名前空間のみに属することができます。名前空間内のサービスは、同じ AWS アカウントの同じ AWS リージョン内の異なる Amazon ECS クラスターに分散できます。サービスは、任意の基準で自由に整理できます。

クライアントサービス

ネットワーククライアントアプリケーションを実行するサービスです。このサービスには名前空間が設定されている必要があります。サービス内の各タスクは、Service Connect プロキシコンテナを介して、名前空間のすべてのエンドポイントを検出して接続できます。

タスク内のいずれかのコンテナが名前空間内のサービスからエンドポイントに接続する必要がある場合は、クライアントサービスを選択します。フロントエンド、リバースプロキシ、またはロードバランサーアプリケーションが、例えば Elastic Load Balancing からなど、他の方法で外部トラフィックを受信する場合は、このタイプの Service Connect 設定を使用できます。

クライアント/サーバーサービス

ネットワークまたはウェブサービスアプリケーションを実行する Amazon ECS サービスです。このサービスには、名前空間と少なくとも 1 つのエンドポイントが設定されている必要があります。サービス内の各タスクには、エンドポイントを使用してアクセスできます。Service Connect プロキシコンテナは、エンドポイント名とポートをリッスンして、タスク内のアプリケーションコンテナにトラフィックを誘導します。

いずれかのコンテナが公開してポート上でネットワークトラフィックをリッスンする場合は、クライアント/サーバーサービスを選択してください。これらのアプリケーションは、同じ名前空間内の他のクライアント/サーバーサービスに接続する必要はありませんが、クライアント設定が必要です。バックエンド、ミドルウェア、ビジネス層、またはほとんどのマイクロサービスはこのタイプの Service Connect 設定を使用できます。フロントエンド、リバースプロキシ、またはロードバランサーアプリケーションに、同じ名前空間の Service Connect を使用して設定した他のサービスからのトラフィックを受信させる場合、これらのサービスはこのタイプの Service Connect 設定を使用する必要があります。

Service Connect 機能は関連サービスの仮想ネットワークを作成します。同じサービス設定を複数の異なる名前空間で使用することで、独立していても同一のアプリケーションセットを実行できます。Service Connect は Amazon ECS サービスのプロキシコンテナを定義します。これにより、同じタスク定義を使用して、Service Connect 設定が異なるさまざまな名前空間で同一のアプリケー

ションを実行できます。サービスが作成する各タスクは、タスク内のプロキシコンテナを実行します。

Service Connect は同じ名前空間内の Amazon ECS サービス間の接続に適しています。次のアプリケーションで Service Connect で設定された Amazon ECS サービスに接続するためには、追加の相互接続方法を使用する必要があります。

- 他の名前空間で設定されているタスク
- Service Connect 用に設定されていないタスク
- Amazon ECS の外部にあるその他のアプリケーション

これらのアプリケーションは Service Connect プロキシ経由で接続できますが、Service Connect エンドポイント名を解決することはできません。

これらのアプリケーションで Amazon ECS タスクの IP アドレスを解決するには、別の相互接続方法を使用する必要があります。

料金

- Amazon ECS Service Connect の料金は、コンテナ化されたワークロードをホストするために AWS Fargate または Amazon EC2 インフラストラクチャを使用するかどうかによって異なります。AWS Outposts で Amazon ECS を使用する場合、料金は Amazon EC2 を直接使用する場合に使われる同じモデルに従います。詳細については、Amazon ECS 料金表を参照してください。
- Amazon ECS Service Connect の使用には追加料金はかかりません。
- Service Connect が使用している場合、AWS Cloud Map の使用は完全に無料です。
- お客様は、vCPU やメモリなど、Amazon ECS Service Connect で使用されるコンピューティングリソースに対して料金を支払います。Amazon ECS Service Connect エージェントはお客様のタスク内で実行されるため、実行に追加料金はかかりません。タスクリソースは、お客様のワークロードと Amazon ECS Service Connect エージェント間で共有されます。
- AWS Private CA で Amazon ECS Service Connect トラフィック暗号化機能を使用する場合、お客様は作成するプライベート認証機関と発行される TLS 証明書ごとに料金を支払います。詳細については、「AWS Private Certificate Authority の料金」を参照してください。TLS 証明書の月額コストを見積もるには、TLS が有効になっている Amazon ECS サービスの数を把握し、それに証明書のコストを掛けて、さらに 6 を掛ける必要があります。Amazon ECS Service Connect は TLS 証明書を 5 日ごとに自動的にローテーションするため、平均して 1 か月あたり Amazon ECS サービスごとに 6 つの証明書が発行されます。

Amazon ECS Service Connect コンポーネント

Amazon ECS Service Connect を使用する場合、ネットワークリクエストを受け取るサーバーアプリケーション (クライアント/サーバーサービス) を実行するか、リクエストを行うクライアントアプリケーション (クライアントサービス) を実行するように各 Amazon ECS サービスを設定します。

Service Connect の使用を開始する準備が整ったら、クライアント/サーバーサービスから始めます。新しいサービスまたは既存のサービスに Service Connect 設定を追加できます。Amazon ECS は、名前空間に Service Connect エンドポイントを作成します。さらに、Amazon ECS は現在実行中のタスクを置き換える新しいデプロイをサービス内に作成します。

既存のタスクやその他のアプリケーションは、既存のエンドポイントや外部アプリケーションに引き続き接続できます。クライアント/サーバーサービスがスケールアウトによってタスクを追加すると、クライアントからの新しい接続はすべてのタスク間で分散されます。クライアント/サーバーサービスが更新されると、クライアントからの新しい接続は新バージョンのタスク間で分散されます。

既存のタスクを解決して新しいエンドポイントに接続することはできません。このエンドポイントを解決して接続できるのは、同じ名前空間に Service Connect 設定があり、このデプロイ後に実行を開始した新しいタスクだけです。

つまり、クライアントアプリケーションのオペレーターがアプリの設定が変更されるタイミングを決定しますが、サーバーアプリケーションのオペレーターはいつでも設定を変更できます。名前空間のエンドポイントのリストは、名前空間のサービスがデプロイされるたびに変更される可能性があります。既存のタスクと置換タスクは、最新のデプロイ後も同じように動作し続けます。

次に挙げるサンプルを参考にしてください。

まず、パブリックインターネット上で利用可能なアプリケーションを 1 つの AWS CloudFormation テンプレートと 1 つの AWS CloudFormation スタックで作成していると仮定します。AWS CloudFormation がパブリック検出と到達可能性を作成するのは、フロントエンドクライアントサービスを含めて、最後にする必要があります。フロントエンドクライアントサービスが実行されていて一般に公開されているのに、バックエンドは公開されていないという期間の発生を避けるために、サービスの作成はこの順序で行う必要があります。これにより、その期間中にエラーメッセージが一般に送信されるのを防ぐことができます。AWS CloudFormation では `dependsOn` を使用して、複数の Amazon ECS サービスを並列または同時に作成できないことを AWS CloudFormation に示す必要があります。クライアントタスクが接続するバックエンドクライアント/サーバーサービスごとに、フロントエンドクライアントサービスに `dependsOn` を追加する必要があります。

次に、フロントエンドサービスが Service Connect 設定なしで存在すると仮定します。タスクは既存のバックエンドサービスに接続しています。まず、フロントエンドが使用する DNS または `clientAlias` と同じ名前を使用して、バックエンドサービスにクライアント/サーバー Service Connect 設定を追加します。これにより、新しいデプロイが作成されると共に、すべてのデプロイのロールバック検出や、AWS Management Console、AWS CLI、AWS SDK などの、バックエンドサービスをロールバックして以前のデプロイと設定に戻す方法が作成されます。バックエンドサービスのパフォーマンスと動作に問題がなければ、クライアントまたはクライアント/サーバー Service Connect 設定をフロントエンドサービスに追加します。それらの新しいタスクに追加された Service Connect プロキシを使用するのは、新しいデプロイのタスクのみです。この設定に問題がある場合は、デプロイロールバック検出または AWS Management Console、AWS CLI、AWS SDK などのバックエンドサービスをロールバックして以前のデプロイと設定に戻す方法を使用することで、ロールバックして以前の設定に戻すことができます。Service Connect ではなく DNS に基づく別のサービス検出システムを使用する場合、フロントエンドまたはクライアントアプリケーションは、ローカル DNS キャッシュの有効期限が切れてから新しいエンドポイントと変更されたエンドポイント設定の使用を開始しますが、これには通常数時間かかります。

ネットワーク

デフォルトでは、Service Connect プロキシは、タスク定義ポートマッピングから `containerPort` をリッスンします。セキュリティグループルールでは、クライアントが実行されるサブネットからこのポートへの受信 (イングレス) トラフィックを許可する必要があります。

Service Connect サービス設定でポート番号を設定した場合であっても、Service Connect プロキシがリッスンするクライアント/サーバーサービスのポートは変更されません。このポート番号を設定すると、Amazon ECS はそれらのタスク内の Service Connect プロキシ上で、クライアントサービスが接続するエンドポイントのポートを変更します。クライアントサービスのプロキシは、`containerPort` を使用してクライアント/サーバーサービスのプロキシに接続します。

Service Connect プロキシがリッスンするポートを変更する場合は、クライアント/サーバーサービスの Service Connect 設定で `ingressPortOverride` を変更してください。このポート番号を変更する場合は、このサービスへのトラフィックが使用するこのポートのインバウンドトラフィックを許可する必要があります。

Service Connect 用に設定された Amazon ECS サービスにアプリケーションが送信するトラフィックは、Amazon VPC およびサブネットにおいて、ルートテーブルルールおよびネットワーク ACL ルールにより、使用している `containerPort` と `ingressPortOverride` のポート番号が許可されている必要があります。

Service Connect を使用して VPC 間でトラフィックを送信できます。ルートテーブルルール、ネットワーク ACL、セキュリティグループに対する同じ要件が両方の VPC に適用されます。

例えば、2 つのクラスターは異なる VPC でタスクを作成します。各クラスターのサービスは、同じ名前空間を使用するように設定されています。これら 2 つのサービスのアプリケーションは、VPC DNS 設定なしで名前空間のすべてのエンドポイントを解決できます。ただし、VPC ピアリング、VPC またはサブネットのルートテーブル、そして VPC ネットワーク ACL により、`containerPort` と `ingressPortOverride` のポート番号のトラフィックが許可されない限り、プロキシは接続できません。

`bridge` ネットワークモードを使用するタスクでは、動的ポートの上限範囲でのトラフィックを許可するインバウンドルールを含むセキュリティグループを作成する必要があります。次に、Service Connect クラスター内のすべての EC2 インスタンスにセキュリティグループを割り当てます。

Service Connect プロキシ

Service Connect 設定を使用してサービスを作成または更新した場合、新しいタスクが開始されるたびに、Amazon ECS はタスクに新しいコンテナを追加します。別のコンテナを使用するこのパターンは、`sidecar` と呼ばれます。このコンテナはタスク定義には存在せず、設定できません。Amazon ECS は、サービス内のコンテナ設定を管理します。これにより、Service Connect を使用せずに、複数のサービス、名前空間、タスク間で同じタスク定義を再利用できます。

プロキシリソース

- タスク定義では、CPU パラメータとメモリパラメータを設定する必要があります。

  Service Connect プロキシコンテナの処理能力を向上させるために、お客様のタスク CPU とメモリに、256 CPU ユニットと 64 MiB 以上のメモリを追加することをお勧めします。AWS Fargate では、ユーザーが設定できる最小のメモリ容量は 512 MiB です。Amazon EC2 では、タスク定義メモリが必要です。
- サービスでは、Service Connect 設定でログ設定を設定します。
- このサービスのタスクがピーク負荷時に 1 秒あたり 500 を超えるリクエストを受信すると予想される場合は、Service Connect プロキシコンテナのこのタスク定義で、タスク CPU に 512 CPU ユニットを追加することをお勧めします。
- 名前空間内に 100 個以上の Service Connect サービス、または名前空間内のすべての Amazon ECS サービスに合計で 2000 個以上のタスクを作成する場合、Service Connect プロキシコンテナのタスクに対して 128 MiB のメモリを追加することをお勧めします。これは、名前空間内のすべての Amazon ECS サービスで使用されるすべてのタスク定義で行う必要があります。

プロキシ設定

アプリケーションは、アプリケーションと同じタスクでサイドカーコンテナ内のプロキシに接続します。Amazon ECS は、アプリケーションが同じ名前空間のエンドポイント名に接続されている場合にのみアプリケーションがプロキシに接続するように、タスクとコンテナを設定します。その他のすべてのトラフィックはプロキシを使用しません。他のトラフィックには、同じ VPC 内の IP アドレス、AWS サービス エンドポイント、外部トラフィックが含まれます。

負荷分散

Service Connect は、Service Connect エンドポイントのタスク間の負荷分散にラウンドロビン方式を使用するようにプロキシを設定します。接続元のタスクにあるローカルプロキシは、エンドポイントを提供するクライアントサーバーサービス内のタスクの 1 つを選択します。

例えば、「local」という名前空間のクライアントサービスとして設定されたサービスで WordPress を実行するタスクについて考えてみます。MySQL データベースを実行する 2 つのタスクを持つ、他のサービスがあります。このサービスは、同じ名前空間内の Service Connect を通じて `mysql` と呼ばれるエンドポイントを提供するように構成されています。WordPress タスクでは、WordPress アプリケーションはエンドポイント名を使用してデータベースに接続します。この名前への接続は、同じタスクのサイドカーコンテナで実行されるプロキシに送られます。その後、プロキシはラウンドロビン方式を使用してどちらの MySQL タスクにも接続できます。

負荷分散戦略: ラウンドロビン

外れ値の検知

この機能では、以前に失敗した接続についてプロキシが保持しているデータを使用して、失敗した接続があったホストに新しい接続を送信しないようにします。Service Connect は、プロキシの外れ値検出機能を設定して、パッシブなヘルスチェックを提供します。

前の例を使用すると、プロキシはいすれかの MySQL タスクに接続できます。プロキシが特定の MySQL タスクに複数の接続を行い、直近 30 秒間以内に 5 つ以上の接続が失敗した場合、プロキシはその MySQL タスクを 30 ~ 300 秒間回避します。

再試行

Service Connect は、プロキシを通過して失敗した接続を再試行するようにプロキシを設定し、2 回目の試行では、前の接続のホストを使用しません。これにより、Service Connect を介した各接続が 1 回限りの理由で失敗することがなくなります。

再試行回数: 2

タイムアウト

Service Connect は、クライアント/サーバーアプリケーションが応答するまで最大時間待機するようにプロキシを構成します。デフォルトのタイムアウト値は 15 秒ですが、更新できます。

任意指定のパラメータ:

idleTimeout - アイドル時に接続がアクティブな状態を維持する時間 (秒)。`0` の値は、`idleTimeout` を無効にします。

`HTTP/HTTP2/GRPC` の `idleTimeout` デフォルトは 5 分です。

`TCP` に対する `idleTimeout` デフォルトは 1 時間です。

perRequestTimeout - リクエストごとにアップストリームが完全なレスポンスで応答するまで待機する時間。`0` の値は `perRequestTimeout` をオフにします。これは、アプリケーションコンテナの `appProtocol` が `HTTP/HTTP2/GRPC` の場合にのみ設定できます。デフォルト値は 15 秒です。

> **Note**
>
> `idleTimeout` を `perRequestTimeout` より短い時間に設定すると、`perRequestTimeout` ではなく `idleTimeout` が到達した時点で接続は終了します。

考慮事項

Service Connect を使用する場合は、次の点を考慮してください。

- Fargate で実行されるタスクが Service Connect を使用するには、Fargate Linux プラットフォームバージョン `1.4.0` 以上を使用する必要があります。
- コンテナインスタンスの Amazon ECS エージェントバージョンには `1.67.2` 以降が必要です。
- コンテナインスタンスが Service Connect を使用するには、Amazon ECS 最適化 Amazon Linux 2023 AMI バージョン `20230428` 以降、または Amazon ECS 最適化 Amazon Linux 2 AMI バージョン `2.0.20221115` を実行する必要があります。これらのバージョンには、Amazon ECS コンテナエージェントに加えて Service Connect エージェントがあります。Service Connect エージェントの詳細については、GitHub の「Amazon ECS Service Connect エージェント」を参照してください。

- コンテナインスタンスには、リソース `arn:aws:ecs:region:0123456789012:task-set/cluster/*` に対する `ecs:Poll` のアクセス許可が必要です。`ecsInstanceRole` を使用している場合は、アクセス許可を追加する必要はありません。`AmazonEC2ContainerServiceforEC2Role` 管理ポリシーには、必要なアクセス許可があります。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。
- Service Connect でサポートされるのは、ローリングデプロイを使用するサービスのみです。
- `bridge` ネットワークモードを使用し、Service Connect を使用するタスクは、`hostname` コンテナ定義パラメータをサポートしません。
- Service Connect を使用するには、タスク定義でタスクメモリ制限を設定する必要があります。詳細については、「Service Connect プロキシ」を参照してください。
- コンテナのメモリ制限を設定するタスク定義はサポートされていません。

  コンテナにはコンテナメモリ制限を設定できますが、タスクメモリ制限はコンテナメモリ制限の合計よりも大きい数値に設定する必要があります。タスク制限内の追加の CPU とメモリで、コンテナ制限に割り当てられていないものは、Service Connect プロキシコンテナや、コンテナ制限を設定していない他のコンテナによって使用されます。詳細については、「Service Connect プロキシ」を参照してください。
- Service Connect には、同じ AWS アカウント の同じリージョンにある任意の AWS Cloud Map 名前空間を使用するように設定できます。
- 各サービスは 1 つの名前空間のみに属することができます。
- サービスが作成したタスクのみがサポートされます。
- すべてのエンドポイントは、名前空間内で一意である必要があります。
- すべての検出名は、名前空間内で一意である必要があります。
- アプリケーションが新しいエンドポイントを解決できるようにするには、既存のサービスを再デプロイする必要があります。最新のデプロイ後に名前空間に追加された新しいエンドポイントは、タスク構成には追加されません。詳細については、「the section called “Service Connect コンポーネント”」を参照してください。
- Service Connect は、クラスターが削除されても名前空間を削除しません。AWS Cloud Map で名前空間を削除する必要があります。
- Application Load Balancer のトラフィックは、デフォルトで `awsvpc` ネットワークモードの Service Connect エージェントを経由してルーティングされます。サービス以外のトラフィックを Service Connect エージェントをバイパスさせたい場合は、Service Connect サービス設定の `ingressPortOverride` パラメータを使用してください。

Service Connect では、次に示すの機能はサポートされていません。

- Windows コンテナ
- HTTP 1.0
- スタンドアロンのタスク
- ブルー/グリーンおよび外部デプロイタイプを使用するサービス
- Amazon ECS Anywhere の `External` コンテナインスタンスは、Service Connect ではサポートされていません。
- PPv2

Service Connect を利用するリージョン

Amazon ECS Service Connect は以下の AWS リージョンで利用できます。

リージョン名	リージョン
米国東部 (オハイオ)	us-east-2
米国東部 (バージニア北部)	us-east-1
米国西部 (北カリフォルニア)	us-west-1
米国西部 (オレゴン)	us-west-2
AWS GovCloud (米国東部)	us-gov-east-1
AWS GovCloud (米国西部)	us-gov-west-1
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ジャカルタ)	ap-southeast-3
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (大阪)	ap-northeast-3

リージョン名	リージョン
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (メルボルン)	ap-southeast-4
アジアパシフィック (マレーシア)	ap-southeast-5
アジアパシフィック (東京)	ap-northeast-1
カナダ (中部)	ca-central-1
カナダ西部 (カルガリー)	ca-west-1
中国 (北京)	cn-north-1 (注: Service Connect 用の TLS は、このリージョンでは使用できません。)
中国 (寧夏)	cn-northwest-1 (注: Service Connect 用 TLS はこのリージョンではご利用いただけません。)
欧州 (フランクフルト)	eu-central-1
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
欧州 (パリ)	eu-west-3
欧州 (ミラノ)	eu-south-1
欧州 (スペイン)	eu-south-2
欧州 (ストックホルム)	eu-north-1
欧州 (チューリッヒ)	eu-central-2
イスラエル (テルアビブ)	il-central-1

リージョン名	リージョン
中東 (バーレーン)	me-south-1
中東 (UAE)	me-central-1
南米 (サンパウロ)	sa-east-1

Amazon ECS Service Connect 設定の概要

Service Connect を使用する場合、リソースで設定する必要があるパラメータがあります。

Amazon ECS リソースの設定パラメータを以下の表に示します。

パラメータの場所	アプリケーションタイプ	説明	必須
タスク定義	クライアント	クライアントタスク定義には、Service Connect が利用できる変更はありません。	該当なし
タスク定義	クライアント/サーバー	サーバーは、コンテナの `portMappings` のポートに `name` フィールドを追加する必要があります。詳細については、「`portMappings`」を参照してください。	あり
タスク定義	クライアント/サーバー	サーバーは、オプションでアプリケーションプロトコル (HTTP など) を提供して、サーバーアプリケーションのプロトコル固有のメトリクス (`HTTP 5xx` など) を受け取ることができます。	いいえ
サービスの定義	クライアント	クライアントサービスは、名前空間の結合を設定するには `serviceConnectConfiguration` を追加する必要があります。この名前空間に	あり

パラメータの場所	アプリケーションタイプ	説明	必須
		は、このサービスが検出する必要のあるすべてのサーバーサービスが含まれていなければなりません。詳細については、「serviceConnectConfiguration」を参照してください。	
サービスの定義	クライアント/サーバー	サーバーサービスは、サービスが利用できる DNS 名、ポート番号、名前空間を設定するために serviceConnectConfiguration を追加する必要があります。詳細については、「serviceConnectConfiguration」を参照してください。	あり
クラスター	クライアント	クラスターはデフォルトの Service Connect 名前空間を追加できます。クラスター内の新しいサービスは、サービスで Service Connect が設定されている場合は名前空間を継承します。	いいえ
クラスター	クライアント/サーバー	サーバーサービスに適用されるクラスターには、Service Connect が利用できる変更はありません。サーバーのタスク定義とサービスは、それぞれの設定を行う必要があります。	該当なし

Service Connect の設定手順の概要

次の手順では、Service Connect の設定方法の概要を示します。

> **Important**
>
> - Service Connect がお客様のアカウントに AWS Cloud Map サービスを作成します。手動でのインスタンスの登録/登録解除、インスタンス属性の変更、サービスの削除を行ってこれらの AWS Cloud Map リソースを変更すると、アプリケーショントラフィックまたは以降のデプロイで予期しない動作が発生することがあります。
> - Service Connect は、タスク定義内のリンクをサポートしていません。

1. タスク定義のポートマッピングにポート名を追加します。さらに、アプリケーションのレイヤー 7 プロトコルを識別して、追加のメトリクスを取得できます。
2. AWS Cloud Map 名前空間を使用してクラスターを作成するか、名前空間を個別に作成します。単純に構成できるように、名前空間に必要な名前でクラスターを作成し、名前空間に同名を指定します。この場合、Amazon ECS は必要な設定で新しい HTTP 名前空間を作成します。Service Connect は Amazon Route 53 では DNS ホストゾーンを使用または作成しません。
3. サービスを設定して、名前空間内に Service Connect エンドポイントを作成します。
4. サービスをデプロイしてエンドポイントを作成します。Amazon ECS は各タスクに Service Connect プロキシコンテナを追加し、AWS Cloud Map に Service Connect エンドポイントを作成します。このコンテナはタスク定義では設定されていないため、タスク定義を変更せずに再利用して、同じ名前空間または複数の名前空間に複数のサービスを作成できます。
5. クライアントアプリをサービスとしてデプロイしてエンドポイントに接続します。Amazon ECS は Service Connect エンドポイントへの接続を各タスクの Service Connect プロキシ経由で行います。

   アプリケーションは Service Connect エンドポイントへの接続にのみプロキシを使用します。プロキシを使用するための追加の構成はありません。プロキシは、ラウンドロビン負荷分散、外れ値検出、再試行を実行します。プロキシの詳細については、「Service Connect プロキシ」を参照してください。
6. Amazon CloudWatch の Service Connect プロキシ経由のトラフィックを監視します。

クラスターの設定

クラスターの作成時または更新時に、Service Connect のデフォルトの名前空間を設定できます。同じアカウントの同じ AWS リージョンには存在しない名前空間名を指定すると、新しい HTTP 名前空間が作成されます。

クラスターを作成してデフォルトの Service Connect 名前空間を指定した場合、Amazon ECS が名前空間を作成する間、そのクラスターは PROVISIONING ステータスで待機します。クラスターのステータスには、名前空間のステータスを示す attachment が表示されます。アタッチメントは、デフォルトでは AWS CLI に表示されません。表示するには、--include ATTACHMENTS を追加する必要があります。

サービス設定

Service Connect は、必要最小限の設定で済むように設計されています。タスク定義で、Service Connect で使用する各ポートマッピングの名前を設定する必要があります。サービスでクライアントサービスを作成するには、Service Connect をオンにして名前空間を選択する必要があります。クライアント/サーバーサービスを作成するには、いずれかのポートマッピングの名前と一致する単一の Service Connect サービス設定を追加する必要があります。Amazon ECS はタスク定義からポート番号とポート名を再利用して、Service Connect サービスとエンドポイントを定義します。これらの値を上書きするには、コンソールで [Discovery] (検出)、[DNS]、[Port] (ポート) など他のパラメータを使用するか、discoveryName、clientAliases それぞれを Amazon ECS API で使用します。

Amazon ECS Service Connect トラフィックを暗号化する

Amazon ECS Service Connect は、Amazon ECS サービスの Transport Layer Security (TLS) 証明書による自動トラフィック暗号化をサポートしています。Amazon ECS サービスを AWS Private Certificate Authority(AWS Private CA) に向けると、Amazon ECS Service Connect 間のトラフィックを暗号化するための TLS 証明書が Amazon ECS によって自動的にプロビジョニングされます。Amazon ECS は、トラフィックの暗号化に使用される TLS 証明書を生成、ローテーション、および配布します。

Service Connect による自動トラフィック暗号化は、業界をリードする暗号化機能を使用してサービス間の通信を保護し、セキュリティ要件を満たすのに役立ちます。256-bit ECDSA および 2048-bit RSA 暗号化で AWS Private Certificate Authority TLS 証明書と暗号化をサポートしています。デフォルトでは、TLS 1.3 はサポートされていますが、TLS 1.0 ~ 1.2 はサポートされていません。また、プライベート証明書と署名キーを完全に制御できるため、コンプライアンス要件を満たすのに役立ちます。

> **Note**
>
> TLS 1.3 を使用するには、ターゲットのリスナーでも有効にする必要があります。
> Amazon ECS エージェントを通過するインバウンドトラフィックとアウトバウンドトラフィックのみが暗号化されます。

AWS Private Certificate Authority 証明書および Service Connect

証明書を発行するには、追加の IAM アクセス許可が必要です。Amazon ECS には、一連のアクセス許可の概要を示すマネージドリソース信頼ポリシーが用意されています。このポリシーの詳細については、「AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity」を参照してください。

Service Connect 用の AWS Private Certificate Authority モード

AWS Private Certificate Authority は汎用モードと短時間有効モードの 2 つのモードで実行できます。

- 汎用 — 任意の有効期限を設定できる証明書を発行します。
- 短い有効期間 — 最大有効期間が 7 日間の証明書。

Amazon ECS は両方のモードをサポートしていますが、有効期間の短い証明書を使用することをお勧めします。デフォルトでは、証明書は 5 日ごとにローテーションされ、短期モードで実行すると一般的な用途に比べてコストを大幅に節約できます。

Service Connect は証明書の失効をサポートしておらず、代わりに証明書を頻繁にローテーションする短い有効期間の証明書を利用します。Secrets Manager のマネージドローテーションを使用してローテーション頻度を変更したり、シークレットを無効化または削除したりする権限がありますが、これを行うと次のような結果が生じる可能性があります。

- ローテーション頻度の短縮 - ローテーション頻度を短くすると、AWS Private CA、AWS KMS および Secrets Manager、Auto Scaling のローテーションのワークロードが増加するため、コストが高くなります。
- ローテーション頻度が長い - ローテーション頻度が 7 日を超えると、アプリケーションの通信は失敗します。
- シークレットの削除 - シークレットを削除するとローテーションが失敗し、お客様のアプリケーション通信に影響があります。

シークレットローテーションに失敗すると、AWS CloudTrail で `RotationFailed` イベントがに公開されます。`RotationFailed` 用の CloudWatch アラームを設定することもできます。

Important

シークレットにレプリカリージョンを追加しないでください。これにより、Amazon ECS にはリージョンをレプリケーションから削除するアクセス許可がないため、Amazon ECS はシークレットを削除できなくなります。レプリケーションを既に追加している場合は、次のコマンドを実行します。

```
aws secretsmanager remove-regions-from-replication \
 --secret-id SecretId \
 --remove-replica-regions region-name
```

下位認証機関

AWS Private CA、ルートまたは下位を Service Connect TLS に導入して、サービスのエンドエンティティ証明書を発行できます。提供された発行者は、あらゆる場所で署名者および信頼の根源として扱われます。エンドエンティティ証明書は、アプリケーションのさまざまな部分について、さまざまな下位 CA から発行できます。AWS CLI を使用する際に、信頼チェーンを確立する CA の Amazon リソースネーム (ARN) を指定します。

オンプレミス認証機関

オンプレミス CA を使用するには、AWS Private Certificate Authority で下位 CA を作成して設定します。これにより、Amazon ECS ワークロード用に発行されたすべての TLS 証明書が、オンプレミスで実行するワークロードとトラストチェーンを共有し、安全に接続できるようになります。

Important

AWS Private CA に必要なタグ `AmazonECSManaged : true` を自分に追加してください。

Infrastructure as Code

Infrastructure as Code (IaC) ツールで Service Connect TLS を使用する場合は、サービスがドレイン状態のままになるという問題を避けるため、依存関係を正しく設定することが重要です。AWS KMS キーが提供されている場合は、Amazon ECS サービスを終了した後、IAM ロールと AWS Private CA 依存関係を削除する必要があります。

Service Connect と Secrets Manager

Amazon ECS Service Connect を TLS 暗号化で使用する場合、サービスは次の方法で Secrets Manager とやり取りします。

Service Connect は、提供されたインフラストラクチャロールを使用して Secrets Manager 内にシークレットを作成します。これらのシークレットは、Service Connect サービス間のトラフィックを暗号化するための TLS 証明書の関連するプライベートキーを保存するために使用されます。

> **Warning**
>
> Service Connect によるこれらのシークレットの自動作成と管理により、サービスに TLS 暗号化を実装するプロセスが合理化されます。ただし、潜在的なセキュリティへの影響に注意することが重要です。Secrets Manager への読み取りアクセス権を持つ他の IAM ロールは、自動的に作成されたシークレットにアクセスできる場合があります。これにより、アクセスコントロールが適切に設定されていない場合、機密性の高い暗号化マテリアルが権限のない当事者に公開される可能性があります。
> このリスクを軽減するには、次のベストプラクティスに従ってください。
>
> - 特に Service Connect によって作成されたシークレットについては、Secrets Manager へのアクセスを慎重に管理および制限します。
> - IAM ロールとそのアクセス許可を定期的に監査して、最小特権の原則が維持されていることを確認します。

Secrets Manager に読み取りアクセスを許可する場合は、Service Connect によって作成された TLS プライベートキーを除外することを検討してください。これを行うには、IAM ポリシーの条件を使用して、パターンに一致する ARN を持つシークレットを除外します。

```
"arn:aws:secretsmanager:::secret:ecs-sc!"
```

`ecs-sc!` プレフィックスを持つすべてのシークレットに対する `GetSecretValue` アクションを拒否する IAM ポリシーの例:

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

```
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "arn:aws:secretsmanager:*:*:secret:ecs-sc!*"
        }
    ]
}
```

> **Note**
>
> これは一般的な例であり、特定のユースケースと AWS アカウント設定に基づいて調整する必要がある場合があります。IAM ポリシーは、セキュリティを維持しながら意図したアクセスを提供するように、常に徹底的なテストを行ってください。

Service Connect が Secrets Manager とやり取りする方法を理解することで、自動 TLS 暗号化の利点を活用しながら、Amazon ECS サービスのセキュリティをより適切に管理できます。

Service Connect および AWS Key Management Service

AWS Key Management Service を使用して、Service Connect リソースを暗号化および復号化できます。AWS KMS は、AWS によってデータを保護する暗号キーを作成および管理できるサービスです。

Service Connect で AWS KMS を使用する場合は、AWS が管理する AWS 所有キーを使用するか、既存の AWS KMS キーを選択できます。新しい AWS KMS キーを作成して使用することもできます。

独自の暗号化キーを提供する

独自のキーマテリアルを提供することも、AWS Key Management Service を通じて外部キーストアを使用して独自のキーを AWS KMS へインポートし、Amazon ECS Service Connect でそのキーの Amazon リソースネーム (ARN) を指定することもできます。

AWS KMS ポリシーの例を次に示します。すべての *[######]* を独自の値に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "id",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/role-name"
```

```
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyPair"
      ],
      "Resource": "*"
    }
  ]
}
```

キーポリシーの詳細については、「AWS Key Management Service デベロッパーガイド」の「キーポリシーの作成」を参照してください。

> **Note**
>
> Service Connect は対称暗号化 AWS KMS キーのみをサポートします。他のタイプの AWS KMS キーを使用して Service Connect リソースを暗号化することはできません。AWS KMS キーが対称暗号化キーかどうかを判別するには、「非対称 KMS キーを識別する」を参照してください。

AWS Key Management Service 対称暗号化キーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 AWS KMS キー」を参照してください。

Amazon ECS Service Connect の TLS の有効化

Service Connect サービスを作成または更新するとき、トラフィック暗号化を有効にします。

AWS Management Console を使用して既存のネームスペース内のサービスのトラフィック暗号化を有効にするには

1. 証明書を発行するには、追加の IAM アクセス許可が必要です。Amazon ECS には、一連のアクセス許可の概要を示すマネージドリソース信頼ポリシーが用意されています。このポリシーの詳細については、「AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity」を参照してください。
2. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
3. ナビゲーションペインで [名前空間] を選択します。

4. トラフィックの暗号化を有効にする [サービス] のある [名前空間] を選択します。
5. トラフィック暗号化を有効にする [サービス] を選択します。
6. 右上隅の [サービスの更新] を選択し、[Service Connect] セクションまでスクロールします。
7. サービス情報の下にある [トラフィック暗号化を有効にする] を選択して TLS を有効にします。
8. [Service Connect TLS ロール] では、既存のロールを選択するか、新しいロールを作成します。
9. [署名者認証機関] では、既存の認証機関を選択するか、新しい認証機関を作成します。
10. AWS KMS key を選択 では、AWS を所有済みのマネージドキーを選択するか、別のキーを選択できます。新しいものを作成することもできます。

AWS CLI を使用してサービスの TLS を設定する例については、「AWS CLI を使用した Amazon ECS Service Connect の設定」を参照してください。

Amazon ECS Service Connect で TLS が有効になっていることを確認する

Service Connect は、Service Connect エージェントで TLS を開始し、宛先エージェントで TLS を終了します。その結果、アプリケーションコードが TLS のやりとりを認識することはありません。次の手順を使用して、TLS が有効になっていることを確認します。

1. アプリケーションイメージに `openssl` CLI を含めます。
2. SSM 経由でタスクに接続するには、サービスで ECS Exec を有効にします。代わりに、サービスと同じ Amazon VPC で Amazon EC2 インスタンスを起動することもできます。
3. 検証したいサービスからタスクの IP とポートを取得します。タスクの IP アドレスは AWS Cloud Map コンソールで取得できます。この情報は、名前空間のサービス詳細ページに記載されています。
4. 次の例のように `execute-command` を使用して、タスクのいずれかにログオンします。または、ステップ 2 で作成した Amazon EC2 インスタンスにログオンします。

```
$ aws ecs execute-command --cluster cluster-name \
    --task task-id  \
    --container container-name \
    --interactive \
    --command "/bin/sh"
```

> **Note**
>
> DNS 名を直接呼び出しても証明書は公開されません。

5. 接続したシェルで、openssl CLI を使用してタスクに添付されている証明書を確認および表示します。

   例:

```
openssl s_client -connect 10.0.147.43:6379 < /dev/null 2> /dev/null \
| openssl x509 -noout -text
```

   レスポンスの例:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            <serial-number>
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: <issuer>
        Validity
            Not Before: Jan 23 21:38:12 2024 GMT
            Not After : Jan 30 22:38:12 2024 GMT
        Subject: <subject>
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    <pub>
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:redis.yelb-cftc
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:<key-id>

            X509v3 Subject Key Identifier:
                1D:<id>
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
```

```
    Signature Algorithm: ecdsa-with-SHA256
        <hash>
```

AWS CLI を使用した Amazon ECS Service Connect の設定

AWS CLI で Service Connect を使用する Fargate タスクで Amazon ECS サービスを作成できます。

前提条件

Service Connect の前提条件は次のとおりです。

- リージョンが Service Connect をサポートしていることを確認します。詳細については、「Regions with Service Connect」を参照してください。
- AWS CLI の最新バージョンがインストールされ、設定されていることを確認します。詳細については、「Installing or updating to the latest version of the AWS CLI」を参照してください。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- VPC、サブネット、ルートテーブルおよびセキュリティグループが使用できるように作成されています。詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。
- `ecsTaskExecutionRole` という名前のタスク実行ロールがあり、`AmazonECSTaskExecutionRolePolicy` 管理ポリシーがそのロールにアタッチされています。このロールにより、Fargate は NGINX アプリケーションログと Service Connect プロキシログを Amazon CloudWatch Logs に書き込むことができます。詳細については、「タスク実行 ロールの作成」を参照してください。

ステップ 1: クラスターを作成する

次の手順に従って Amazon ECS クラスターと名前空間を作成します。

Amazon ECS クラスターと AWS Cloud Map 名前空間を作成するには

1. `tutorial` という名前の Amazon ECS クラスターを作成して使用します。パラメータ `--service-connect-defaults` は、クラスターのデフォルト名前空間を設定します。この出力の例では、`service-connect` という名前の AWS Cloud Map 名前空間はこのアカウントおよび AWS リージョンには存在しないため、名前空間は Amazon ECS によって作成されています。名前空間はアカウント内の AWS Cloud Map で作成され、他のすべての名前空間でも表示されるため、目的を示す名前を使用します。

```
aws ecs create-cluster --cluster-name tutorial --service-connect-defaults
 namespace=service-connect
```

出力:

```
{
    "cluster": {
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/tutorial",
        "clusterName": "tutorial",
        "serviceConnectDefaults": {
            "namespace": "arn:aws:servicediscovery:us-
west-2:123456789012:namespace/ns-EXAMPLE"
        },
        "status": "PROVISIONING",
        "registeredContainerInstancesCount": 0,
        "runningTasksCount": 0,
        "pendingTasksCount": 0,
        "activeServicesCount": 0,
        "statistics": [],
        "tags": [],
        "settings": [
            {
                "name": "containerInsights",
                "value": "disabled"
            }
        ],
        "capacityProviders": [],
        "defaultCapacityProviderStrategy": [],
        "attachments": [
            {
                "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
                "type": "sc",
                "status": "ATTACHING",
                "details": []
            }
        ],
        "attachmentsStatus": "UPDATE_IN_PROGRESS"
    }
}
}
```

2. クラスターが作成されていることを確認します。

```
aws ecs describe-clusters --clusters tutorial
```

出力:

```
{
    "clusters": [
        {
            "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/tutorial",
            "clusterName": "tutorial",
            "serviceConnectDefaults": {
                "namespace": "arn:aws:servicediscovery:us-
west-2:123456789012:namespace/ns-EXAMPLE"
            },
            "status": "ACTIVE",
            "registeredContainerInstancesCount": 0,
            "runningTasksCount": 0,
            "pendingTasksCount": 0,
            "activeServicesCount": 0,
            "statistics": [],
            "tags": [],
            "settings": [],
            "capacityProviders": [],
            "defaultCapacityProviderStrategy": []
        }
    ],
    "failures": []
}
```

3. (オプション) 名前空間が AWS Cloud Map で作成されていることを確認します。これは AWS Cloud Map で作成されているため、AWS Management Consoleまたは通常の AWS CLI 構成を使用できます。

   例えば、以下の AWS CLI を使用します。

   ```
   aws servicediscovery get-namespace --id ns-EXAMPLE
   ```

   出力:

   ```
   {
       "Namespace": {
   ```

```
        "Id": "ns-EXAMPLE",
        "Arn": "arn:aws:servicediscovery:us-west-2:123456789012:namespace/ns-
EXAMPLE",
        "Name": "service-connect",
        "Type": "HTTP",
        "Properties": {
            "DnsProperties": {
                "SOA": {}
            },
            "HttpProperties": {
                "HttpName": "service-connect"
            }
        },
        "CreateDate": 1661749852.422,
        "CreatorRequestId": "service-connect"
    }
}
```

ステップ 2: サーバー用のサービスを作成する

Service Connect 機能は、Amazon ECS 上の複数のアプリケーションを相互接続することを目的としています。これらのアプリケーションの少なくとも 1 つは、接続するウェブサービスを提供する必要があります。このステップでは、以下を作成します。

- 未修正の公式 NGINX コンテナイメージを使用し、Service Connect 設定を含むタスク定義。
- このサービスへのトラフィック用にサービス検出とサービスメッシュプロキシを提供するために Service Connect を設定する Amazon ECS サービス定義。この構成では、クラスター構成からデフォルトの名前空間を再利用することで、各サービスに対して行うサービス構成の量を減らします。
- Amazon ECS サービス。タスク定義を使用して 1 つのタスクを実行し、Service Connect プロキシ用の追加コンテナを挿入します。プロキシは、タスク定義のコンテナポートマッピングからポートをリッスンします。Amazon ECS で実行されているクライアントアプリケーションで、クライアントタスクのプロキシは、タスク定義ポート名、サービス検出名またはサービスクライアントエイリアス名、およびクライアントエイリアスからのポート番号へのアウトバウンド接続をリッスンします。

Service Connect を使用してウェブサービスを作成するには

1. Fargate と互換性があり、awsvpc ネットワークモードを使用するタスク定義を登録します。以下の手順に従ってください。

   a. 次のタスク定義の内容で、service-connect-nginx.json というファイルを作成します。

   このタスク定義は、ポートマッピングに name および appProtocol パラメータを追加することによって Service Connect を構成します。複数のポートが使用されている場合、ポート名によりサービス構成でこのポートをより識別しやすくなります。また、ポート名は、名前空間内の他のアプリケーションが使用する検出可能な名前としてもデフォルトで使用されています。

   サービスでは ECS Exec が有効になっているため、タスク定義にはタスク IAM ロールが含まれています。

   > **Important**
   >
   > このタスク定義では、logConfiguration を使用して stdout および stderr から Amazon CloudWatch Logs に nginx 出力を送信します。このタスク実行ロールには、CloudWatch Logs ロググループを作成するために必要な追加の権限はありません。AWS Management Consoleまたは AWS CLI を使用して、CloudWatch Logs にロググループを作成します。nginx ログを CloudWatch Logs に送信したくない場合、logConfiguration を削除できます。
   > タスク実行ロールの AWS アカウント ID を AWS アカウント ID に置き換えます。

```
{
    "family": "service-connect-nginx",
    "executionRoleArn": "arn:aws:iam::123456789012:role/ecsTaskExecutionRole",
    "taskRoleArn": "arn:aws:iam::123456789012:role/ecsTaskRole",
    "networkMode": "awsvpc",
    "containerDefinitions": [
        {
        "name": "webserver",
        "image": "public.ecr.aws/docker/library/nginx:latest",
        "cpu": 100,
        "portMappings": [
```

```
            {
                "name": "nginx",
                "containerPort": 80,
                "protocol": "tcp",
                "appProtocol": "http"
            }
        ],
        "essential": true,
        "logConfiguration": {
            "logDriver": "awslogs",
            "options": {
                "awslogs-group": "/ecs/service-connect-nginx",
                "awslogs-region": "region",
                "awslogs-stream-prefix": "nginx"
            }
        }
        }
    ],
    "cpu": "256",
    "memory": "512"
}
```

b. 次の service-connect-nginx.json ファイルを使用して、タスク定義を登録します。

```
aws ecs register-task-definition --cli-input-json file://service-connect-
nginx.json
```

2. サービスを作成します。

a. 作成する Amazon ECS サービスの内容で、service-connect-nginx-service.json という名前のファイルを作成します。この例では、前のステップで作成したタスク定義を使用します。このタスク定義の例では awsvpc ネットワークモードを使用しているため、awsvpcConfiguration が必要となります。

ECS サービスを作成する際に、Fargate の起動タイプと、Service Connect をサポートする LATEST プラットフォームのバージョンを指定します。securityGroups および subnets は、Amazon ECS を使用するための要件を満たしている VPC に属している必要があります。Amazon VPC コンソールからセキュリティグループとサブネット ID を取得できます。

このサービスは、serviceConnectConfiguration パラメータを追加して Service Connect を設定します。クラスターにはデフォルトの名前空間が設定されているため、名前空間は必要ありません。名前空間内の ECS で実行されているクライアントアプリケーションは、portName および clientAliases のポートを使用してこのサービスに接続します。例えば、nginx はルートロケーション / にウェルカムページを提供しているため、http://nginx:80/ を使用してこのサービスにアクセスできます。Amazon ECS で実行されていない、または同じ名前空間にない外部アプリケーションは、タスクの IP アドレスとタスク定義のポート番号を使用して、Service Connect プロキシ経由でこのアプリケーションにアクセスできます。ご使用の tls 設定に合わせて、awsPcaAuthorityArn、kmsKey および IAM ロールの roleArn に対する証明書 arn を追加します。

このサービスは、logConfiguration を使用して stdout および stderr から Amazon CloudWatch Logs にサービス接続プロキシの出力を送信します。このタスク実行ロールには、CloudWatch Logs ロググループを作成するために必要な追加の権限はありません。AWS Management Consoleまたは AWS CLI を使用して、CloudWatch Logs にロググループを作成します。このロググループを作成し、CloudWatch Logs にプロキシログを保存することをお勧めします。プロキシログを CloudWatch Logs に送信したくない場合、logConfiguration を削除できます。

```
{
    "cluster": "tutorial",
    "deploymentConfiguration": {
        "maximumPercent": 200,
        "minimumHealthyPercent": 0
    },
    "deploymentController": {
        "type": "ECS"
    },
    "desiredCount": 1,
    "enableECSManagedTags": true,
    "enableExecuteCommand": true,
    "launchType": "FARGATE",
    "networkConfiguration": {
        "awsvpcConfiguration": {
            "assignPublicIp": "ENABLED",
            "securityGroups": [
                "sg-EXAMPLE"
```

```
            ],
            "subnets": [
                "subnet-EXAMPLE",
                "subnet-EXAMPLE",
                "subnet-EXAMPLE"
            ]
           }
    },
    "platformVersion": "LATEST",
    "propagateTags": "SERVICE",
    "serviceName": "service-connect-nginx-service",
    "serviceConnectConfiguration": {
        "enabled": true,
        "services": [
            {
                "portName": "nginx",
                "clientAliases": [
                    {
                        "port": 80
                    }
                ],
                "tls": {
                   "issuerCertificateAuthority": {
                      "awsPcaAuthorityArn": "certificateArn"
                   },
                   "kmsKey": "kmsKey",
                   "roleArn": "iamRoleArn"
                }
            }
        ],
        "logConfiguration": {
            "logDriver": "awslogs",
            "options": {
                "awslogs-group": "/ecs/service-connect-proxy",
                "awslogs-region": "region",
                "awslogs-stream-prefix": "service-connect-proxy"
            }
        }
    },
    "taskDefinition": "service-connect-nginx"
}
```

b. 次の service-connect-nginx-service.json のファイルを使用して、サービスを作成します。

```
aws ecs create-service --cluster tutorial --cli-input-json file://service-
connect-nginx-service.json
```

出力:

```
{
    "service": {
        "serviceArn": "arn:aws:ecs:us-west-2:123456789012:service/tutorial/
service-connect-nginx-service",
        "serviceName": "service-connect-nginx-service",
        "clusterArn": "arn:aws:ecs:us-west-2:123456789012:cluster/tutorial",
        "loadBalancers": [],
        "serviceRegistries": [],
        "status": "ACTIVE",
        "desiredCount": 1,
        "runningCount": 0,
        "pendingCount": 0,
        "launchType": "FARGATE",
        "platformVersion": "LATEST",
        "platformFamily": "Linux",
        "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-definition/
service-connect-nginx:1",
        "deploymentConfiguration": {
            "deploymentCircuitBreaker": {
                "enable": false,
                "rollback": false
            },
            "maximumPercent": 200,
            "minimumHealthyPercent": 0
        },
        "deployments": [
            {
                "id": "ecs-svc/3763308422771520962",
                "status": "PRIMARY",
                "taskDefinition": "arn:aws:ecs:us-west-2:123456789012:task-
definition/service-connect-nginx:1",
                "desiredCount": 1,
                "pendingCount": 0,
```

```
                "runningCount": 0,
                "failedTasks": 0,
                "createdAt": 1661210032.602,
                "updatedAt": 1661210032.602,
                "launchType": "FARGATE",
                "platformVersion": "1.4.0",
                "platformFamily": "Linux",
                "networkConfiguration": {
                    "awsvpcConfiguration": {
                        "assignPublicIp": "ENABLED",
                        "securityGroups": [
                            "sg-EXAMPLE"
                        ],
                        "subnets": [
                            "subnet-EXAMPLEf",
                            "subnet-EXAMPLE",
                            "subnet-EXAMPLE"
                        ]
                    }
                },
                "rolloutState": "IN_PROGRESS",
                "rolloutStateReason": "ECS deployment ecs-
svc/3763308422771520962 in progress.",
                "failedLaunchTaskCount": 0,
                "replacedTaskCount": 0,
                "serviceConnectConfiguration": {
                    "enabled": true,
                    "namespace": "service-connect",
                    "services": [
                        {
                            "portName": "nginx",
                            "clientAliases": [
                                {
                                    "port": 80
                                }
                            ]
                        }
                    ],
                    "logConfiguration": {
                        "logDriver": "awslogs",
                        "options": {
                            "awslogs-group": "/ecs/service-connect-proxy",
                            "awslogs-region": "us-west-2",
                            "awslogs-stream-prefix": "service-connect-proxy"
```

```
                        },
                        "secretOptions": []
                    }
                },
                "serviceConnectResources": [
                    {
                        "discoveryName": "nginx",
                        "discoveryArn": "arn:aws:servicediscovery:us-
west-2:123456789012:service/srv-EXAMPLE"
                    }
                ]
            }
        ],
        "roleArn": "arn:aws:iam::123456789012:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
        "version": 0,
        "events": [],
        "createdAt": 1661210032.602,
        "placementConstraints": [],
        "placementStrategy": [],
        "networkConfiguration": {
            "awsvpcConfiguration": {
                "assignPublicIp": "ENABLED",
                "securityGroups": [
                    "sg-EXAMPLE"
                ],
                "subnets": [
                    "subnet-EXAMPLE",
                    "subnet-EXAMPLE",
                    "subnet-EXAMPLE"
                ]
            }
        },
        "schedulingStrategy": "REPLICA",
        "enableECSManagedTags": true,
        "propagateTags": "SERVICE",
        "enableExecuteCommand": true
    }
}
```

指定した `serviceConnectConfiguration` は、出力の最初のデプロイ内に表示されます。タスクに変更を加える必要がある方法で ECS サービスを変更すると、Amazon ECS によって新しいデプロイが作成されます。

ステップ 3: 接続できることを確認する

Service Connect が設定され動作していることを確認するには、次の手順に従って外部アプリケーションからウェブサービスに接続します。次に、Service Connect プロキシが作成した CloudWatch にある追加のメトリクスを確認します。

外部アプリケーションからウェブサービスに接続するには

- タスク IP アドレスを使用して、タスク IP アドレスとコンテナポートに接続する

  AWS CLI を使用して `aws ecs list-tasks --cluster tutorial` を使用したタスク ID を取得します。

  サブネットとセキュリティグループがタスク定義のポート上のパブリックインターネットからのトラフィックを許可している場合、コンピュータからパブリック IP に接続できます。ただし、パブリック IP は「describe-tasks」からは利用できないため、手順として、Amazon EC2 AWS Management Consoleまたは AWS CLI に移動して Elastic Network Interface の詳細を取得する必要があります。

  この例では、同じ VPC 内の Amazon EC2 インスタンスはタスクのプライベート IP を使用します。アプリケーションは nginx ですが、`server: envoy` ヘッダーには Service Connect プロキシが使用されていることが表示されます。Service Connect プロキシはタスク定義のコンテナポートをリッスンしています。

```
$ curl -v 10.0.19.50:80/
*   Trying 10.0.19.50:80...
* Connected to 10.0.19.50 (10.0.19.50) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.0.19.50
> User-Agent: curl/7.79.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< server: envoy
```

```
< date: Tue, 23 Aug 2022 03:53:06 GMT
< content-type: text/html
< content-length: 612
< last-modified: Tue, 16 Apr 2019 13:08:19 GMT
< etag: "5cb5d3c3-264"
< accept-ranges: bytes
< x-envoy-upstream-service-time: 0
<
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

Service Connect メトリクスを表示するには

Service Connect プロキシは、アプリケーション (HTTP、HTTP2、gRPC、または TCP 接続) メトリクスを CloudWatch メトリクス内に作成します。CloudWatch コンソールを使用する場合、Amazon ECS 名前空間にある [DiscoveryName]、([DiscoveryName, ServiceName, ClusterName])、[TargetDiscoveryName]、および ([TargetDiscoveryName, ServiceName, ClusterName]) という追加のメトリクスディメンションを確認します。これらのメトリクスおよび

ディメンションの詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「利用可能なメトリクスを表示する」を参照してください。

サービス検出を使用して Amazon ECS サービスを DNS 名で接続する

Amazon ECS サービスはオプションで Amazon ECS サービス検出を使用するように設定できます。サービス検出では、AWS Cloud MapAmazon ECS サービスの HTTP および DNS 名前空間を管理する API アクション。詳細については、『AWS Cloud Map 開発者ガイド』の「AWS Cloud Map とは」を参照してください。

サービスの検出はリ以下のAWSーションで使用できます。

リージョン名	リージョン
米国東部 (バージニア北部)	us-east-1
米国東部 (オハイオ)	us-east-2
米国西部 (北カリフォルニア)	us-west-1
米国西部 (オレゴン)	us-west-2
アフリカ (ケープタウン)	af-south-1
アジアパシフィック (香港)	ap-east-1
アジアパシフィック (ムンバイ)	ap-south-1
アジアパシフィック (ハイデラバード)	ap-south-2
アジアパシフィック (東京)	ap-northeast-1
アジアパシフィック (ソウル)	ap-northeast-2
アジアパシフィック (大阪)	ap-northeast-3
アジアパシフィック (シンガポール)	ap-southeast-1
アジアパシフィック (シドニー)	ap-southeast-2
アジアパシフィック (ジャカルタ)	ap-southeast-3

リージョン名	リージョン
アジアパシフィック (メルボルン)	ap-southeast-4
カナダ (中部)	ca-central-1
カナダ西部 (カルガリー)	ca-west-1
中国 (北京)	cn-north-1
中国 (寧夏)	cn-northwest-1
欧州 (フランクフルト)	eu-central-1
欧州 (チューリッヒ)	eu-central-2
欧州 (アイルランド)	eu-west-1
欧州 (ロンドン)	eu-west-2
欧州 (パリ)	eu-west-3
欧州 (ミラノ)	eu-south-1
欧州 (ストックホルム)	eu-north-1
イスラエル (テルアビブ)	il-central-1
欧州 (スペイン)	eu-south-2
中東 (UAE)	me-central-1
中東 (バーレーン)	me-south-1
南米 (サンパウロ)	sa-east-1
AWS GovCloud (米国東部)	us-gov-east-1
AWS GovCloud (米国西部)	us-gov-west-1

サービス検出の概念

サービス検出は次のコンポーネントで構成されます。

- サービス検出名前空間: 同じドメイン名 (example.com など) を共有するサービスの論理グループ。これはトラフィックをルーティングするドメイン名です。`aws servicediscovery create-private-dns-namespace` コマンドを呼び出しまたは Amazon ECS のコンソールを使用して名前空間を作成できます。`aws servicediscovery list-namespaces` コマンドを使用して、現在のアカウントで作成された名前空間に関するサマリー情報を確認できます。サービス検出コマンドの詳細については、「AWS Cloud Map (サービス検出) AWS CLI Reference Guide」の「create-private-dns-namespace」および「list-namespaces」を参照してください。
- サービス検出サービス: サービス検出名前空間にあり、名前空間のサービス名および DNS 設定から構成されます。これは、次の主要なコンポーネントを提供します。
  - サービスレジストリ: DNS あるいは AWS Cloud Map API アクションを介してサービスを検索し、サービスに接続するために使用できる 1 つ以上の利用可能なエンドポイントを返すことができます。
- サービスディスカバリインスタンス: サービスディスカバリサービスにあり、サービスディレクトリ内の各 Amazon ECS サービスに関連付けられた属性で構成されます。
  - インスタンスの属性: 次のメタデータは、サービスディスカバリ を使用するように設定された各 Amazon ECS サービスのカスタム属性として追加されます。
    - **AWS_INSTANCE_IPV4** –A レコードの場合、インスタンスの詳細が検出されると、Route 53 など、DNS クエリへの応答として AWS Cloud Map が返す IPv4 アドレスおよび `192.0.2.44` が返されます。
    - **AWS_INSTANCE_PORT** – サービスディスカバリサービスに関連付けられたポート値。
    - **AVAILABILITY_ZONE** – タスクが起動したアベイラビリティーゾーン。EC2 起動タイプを使用するタスクの場合、これはコンテナインスタンスが存在するアベイラビリティーゾーンです。Fargate 起動タイプを使用するタスクの場合、これは Elastic Network Interface が存在するアベイラビリティーゾーンです。
    - **REGION** タスクが存在するリージョン。
    - **ECS_SERVICE_NAME** – タスクが属している Amazon ECS サービスの名前。
    - **ECS_CLUSTER_NAME** – タスクが属している Amazon ECS クラスターの名前。
    - **EC2_INSTANCE_ID** タスクが配置されていたコンテナインスタンスの ID。タスクが Fargate 起動タイプを使用している場合、このカスタム属性は追加されません。
    - **ECS_TASK_DEFINITION_FAMILY** タスクが使用しているタスク定義ファミリー。

  - **ECS_TASK_SET_EXTERNAL_ID** タスクセットが外部デプロイ用に作成され、サービス検出レジストリに関連付けられている場合、ECS_TASK_SET_EXTERNAL_ID 属性にはタスクセットの外部 ID が含まれます。
- Amazon ECS ヘルスチェック: Amazon ECS はコンテナレベルのヘルスチェックを定期的に実行します。エンドポイントがヘルスチェックに失敗した場合、このエンドポイントは DNS ルーチングから削除され、異常とマークされます。

サービスの検出に関する考慮事項

サービス検出を使用する際には、以下の点を考慮する必要があります。

- プラットフォームバージョンが v1.1.0 以降を使用する場合、サービスの検出は Fargate タスクでサポートされます。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。
- サービス検出を使用するように構成されたサービスには、サービスごとに 1,000 タスクに制限があります。これは、Route 53 サービスクォータによるものです。
- Amazon ECS コンソールでのサービスの作成ワークフローでは、プライベート DNS 名前空間へのサービスの登録のみがサポートされます。AWS Cloud Map プライベート DNS 名前空間が作成されると、Route 53 プライベートホストゾーンが自動的に作成されます。
- DNS 解決を成功させるには、VPC DNS 属性を設定する必要があります。属性の設定方法については、を参照してください。VPC の DNS サポートのAmazon VPC User Guide。
- パブリック名前空間が使用されている場合でも、 サービス用に作成された DNS レコードは、パブリック IP アドレスではなく、タスクのプライベート IP アドレスに常に登録されます。
- &service-discovery-first; では、awsvpc、bridge、host のいずれかのネットワークモードをタスクで指定する必要があります (none はサポートされていません)。
- サービスタスク定義が awsvpc ネットワークモードを使用する場合、各サービスタスクに A または SRV レコードを自由に組み合わせて作成できます。SRV レコードを使用する場合、ポートが必要です。
- サービスタスク定義が bridge または host ネットワークモードを使用する場合、SRV レコードのみがサポートされる DNS レコードタイプです。各サービスタスクの SRV レコードを作成します。SRV レコードのコンテナ名とコンテナポートの組み合わせをタスク定義から指定する必要があります。
- サービスの検出サービスの DNS レコードは、VPC 内でクエリを実行できます。これは、次の形式を使用します: `<service discovery service name>.<service discovery namespace>`。

- サービス名で DNS クエリを実行すると、A レコードはタスクに対応する IP アドレスのセットを返します。SRV レコードは、タスクごとに IP アドレスとポートのセットを返します。
- 8 つ以下の正常なレコードがある場合、Route 53 はすべての DNS クエリに正常なすべてのレコードを返します。
- すべてのレコードが異常である場合、Route 53 は DNS クエリに最大 8 つの異常なレコードを返します。
- サービス検出はロードバランサーの背後にあるサービスに設定できますが、サービス検出トラフィックは必ずタスクにルーティングされ、ロードバランサーにはルーティングされません。
- サービス検出は Classic Load Balancer の使用をサポートしていません。
- Amazon ECS サービスのサービス検出により管理されるコンテナレベルのヘルスチェックを使用することをお勧めします。
  - HealthCheckCustomConfig—Amazon ECS; はユーザーに代わってヘルスチェックを管理します。Amazon ECS は、コンテナとヘルスチェックの情報、およびタスクの状態を使用して、ヘルスを AWS Cloud Map で更新します。これは、`--health-check-custom-config`パラメータを使用してサービス検出サービスの作成時に指定します。詳細については、AWS Cloud MapAPI リファレンスの「HealthCheckCustomConfig」を参照してください。
- サービス検出を使用するときに作成される AWS Cloud Map リソースは、手動でクリーンアップする必要があります。
- タスクとインスタンスはコンテナのヘルスチェックが値を返すまで `UNHEALTHY` として登録されます。ヘルスチェックが成功した場合、ステータスは `HEALTHY` に更新されます。コンテナのヘルスチェックに失敗すると、サービス検出インスタンスは登録解除されます。

サービス検出の料金

Amazon ECS サービスディスカバリを使用しているお客様には、Route 53 リソースおよび AWS Cloud Map 検出 API オペレーションの料金が発生します。これには、Route 53 ホストゾーンの作成とサービスレジストリへのクエリのコストが含まれます。詳細については、AWS Cloud Mapデベロッパーガイドのの概念およびAWS Cloud Mapの料金を参照してください。

Amazon ECS は、コンテナレベルのヘルスチェックを実行し、この結果を AWS Cloud Map カスタムヘルスチェック API オペレーションに公開します。現在のところ、これは追加コストなしでお客様に提供されています。パブリックに公開されているタスクにネットワークヘルスチェックを設定する場合、このヘルスチェックに対しては課金されます。

サービス検出を使用する新しい Amazon ECS サービスの作成

AWS CLI でサービス検出を使用する Fargate タスクを含むサービスを作成する方法について説明します。

サービス検出をサポートする AWS リージョン のリストについては、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。

Fargate をサポートするリージョンの情報については、「the section called “AWS Fargate リージョン”」 を参照してください。

前提条件

個のチュートリアルを開始する前に、次の前提条件を満たしていることを確認します。

- AWS CLI の最新バージョンがインストールされ、設定されていること。詳細については、「AWS CLIの最新バージョンをインストールまたは更新」を参照してください。
- 「Amazon ECS を使用するようにセットアップする」で説明されているステップが完了しました。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- 少なくとも 1 つの VPC と 1 つのセキュリティグループを作成している。詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。

ステップ 1: AWS Cloud Map でサービス検出リソースを作成する

サービス検出の名前空間およびサービス検出サービスを作成するには、次のステップに従います。

1. プライベート Cloud Map サービス検出の名前空間を作成します。この例では、`tutorial` と呼ばれる名前空間を作成します。*`vpc-abcd1234`* を、既存のいずれかの VPC の ID に置き換えます。

   ```
   aws servicediscovery create-private-dns-namespace \
         --name tutorial \
         --vpc vpc-abcd1234
   ```

   このコマンドの出力は次のとおりです。

   ```
   {
   ```

```
    "OperationId": "h2qe3s6dxftvvt7riu6lfy2f6c3jlhf4-je6chs2e"
}
```

2. 前のステップの出力の OperationId を使用して、プライベート名前空間が正常に作成されたことを確認します。名前空間 ID は後続のコマンドで使用するため、書き留めておきます。

```
aws servicediscovery get-operation \
      --operation-id h2qe3s6dxftvvt7riu6lfy2f6c3jlhf4-je6chs2e
```

出力は次のとおりです。

```
{
    "Operation": {
        "Id": "h2qe3s6dxftvvt7riu6lfy2f6c3jlhf4-je6chs2e",
        "Type": "CREATE_NAMESPACE",
        "Status": "SUCCESS",
        "CreateDate": 1519777852.502,
        "UpdateDate": 1519777856.086,
        "Targets": {
           "NAMESPACE": "ns-uejictsjen2i4eeg"
        }
    }
}
```

3. 前のステップの出力からの NAMESPACE ID を使用して、サービス検出サービスを作成します。この例では、myapplication という名前のサービスが作成されます。サービス ID と ARN は後続のコマンドで使用するため、書き留めておきます。

```
aws servicediscovery create-service \
      --name myapplication \
      --dns-config "NamespaceId="ns-
uejictsjen2i4eeg",DnsRecords=[{Type="A",TTL="300"}]" \
      --health-check-custom-config FailureThreshold=1
```

出力は次のとおりです。

```
{
    "Service": {
       "Id": "srv-utcrh6wavdkggqtk",
        "Arn": "arn:aws:servicediscovery:region:aws_account_id:service/srv-
utcrh6wavdkggqtk",
```

```
        "Name": "myapplication",
        "DnsConfig": {
            "NamespaceId": "ns-uejictsjen2i4eeg",
            "DnsRecords": [
                {
                    "Type": "A",
                    "TTL": 300
                }
            ]
        },
        "HealthCheckCustomConfig": {
            "FailureThreshold": 1
        },
        "CreatorRequestId": "e49a8797-b735-481b-a657-b74d1d6734eb"
    }
}
```

ステップ 2: Amazon ECS リソースを作成する

Amazon ECS クラスター、タスク定義、サービスを作成するには、次のステップに従います。

1. Amazon ECS クラスターを作成します。この例では、tutorial という名前のクラスターを作成します。

```
aws ecs create-cluster \
      --cluster-name tutorial
```

2. Fargate と互換性があり、awsvpc ネットワークモードを使用するタスク定義を登録します。以下の手順に従ってください。

   a. 次のタスク定義の内容で、fargate-task.json というファイルを作成します。

```
{
    "family": "tutorial-task-def",
        "networkMode": "awsvpc",
        "containerDefinitions": [
            {
                "name": "sample-app",
                "image": "public.ecr.aws/docker/library/httpd:2.4",
                "portMappings": [
                    {
                        "containerPort": 80,
```

```
                        "hostPort": 80,
                        "protocol": "tcp"
                    }
                ],
                "essential": true,
                "entryPoint": [
                    "sh",
                    "-c"
                ],
                "command": [
                    "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample
 App</title> <style>body {margin-top: 40px; background-color: #333;} </style>
 </head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample
 App</h1> <h2>Congratulations!</h2> <p>Your application is now running on a
 container in Amazon ECS.</p> </div></body></html>' >  /usr/local/apache2/
htdocs/index.html && httpd-foreground\""
                ]
            }
        ],
        "requiresCompatibilities": [
            "FARGATE"
        ],
        "cpu": "256",
        "memory": "512"
}
```

b. fargate-task.json を使用してタスク定義を登録します。

```
aws ecs register-task-definition \
      --cli-input-json file://fargate-task.json
```

3. 次のステップに従って、ECS サービスを作成します。

a. 作成する ECS サービスの内容で、ecs-service-discovery.json という名前のファイルを作成します。この例では、前のステップで作成したタスク定義を使用します。このタスク定義の例では awsvpc ネットワークモードを使用しているため、awsvpcConfiguration が必要となります。

ECS サービスを作成する際に、Fargate の起動タイプと、サービス検出をサポートする LATEST プラットフォームのバージョンを指定します。AWS Cloud Map でサービス検出サービスが作成される場合、registryArn は返される ARN です。securityGroups および subnets は、Cloud Map 名前空間の作成に使用される VPC に属している必要があり

ます。Amazon VPC コンソールからセキュリティグループとサブネット ID を取得できます。

```
{
    "cluster": "tutorial",
    "serviceName": "ecs-service-discovery",
    "taskDefinition": "tutorial-task-def",
    "serviceRegistries": [
       {
          "registryArn":
 "arn:aws:servicediscovery:region:aws_account_id:service/srv-utcrh6wavdkggqtk"
       }
    ],
    "launchType": "FARGATE",
    "platformVersion": "LATEST",
    "networkConfiguration": {
       "awsvpcConfiguration": {
          "assignPublicIp": "ENABLED",
          "securityGroups": [ "sg-abcd1234" ],
          "subnets": [ "subnet-abcd1234" ]
       }
    },
    "desiredCount": 1
}
```

b. `ecs-service-discovery.json` を使用して ECS サービスを作成します。

```
aws ecs create-service \
      --cli-input-json file://ecs-service-discovery.json
```

ステップ 3: AWS Cloud Map でサービス検出を検証する

サービス検出情報をクエリして、すべてが正常に作成されたことを確認します。サービス検出を設定した後、AWS Cloud Map API オペレーションを使用するか、VPC 内のインスタンスから `dig` を呼び出すことができます。以下の手順に従ってください。

1. サービス検出サービス ID を使用して、サービス検出インスタンスを一覧表示します。リソースクリーンアップのインスタンス ID (太字でマーク) を書き留めます。

```
aws servicediscovery list-instances \
```

```
        --service-id srv-utcrh6wavdkggqtk
```

出力は次のとおりです。

```
{
    "Instances": [
        {
            "Id": "16becc26-8558-4af1-9fbd-f81be062a266",
            "Attributes": {
                "AWS_INSTANCE_IPV4": "172.31.87.2"
                "AWS_INSTANCE_PORT": "80",
                "AVAILABILITY_ZONE": "us-east-1a",
                "REGION": "us-east-1",
                "ECS_SERVICE_NAME": "ecs-service-discovery",
                "ECS_CLUSTER_NAME": "tutorial",
                "ECS_TASK_DEFINITION_FAMILY": "tutorial-task-def"
            }
        }
    ]
}
```

2. サービス検出の名前空間、サービス、および ECS クラスター名などの追加パラメータを使用して、サービス検出インスタンスに関する詳細をクエリします。

```
aws servicediscovery discover-instances \
      --namespace-name tutorial \
      --service-name myapplication \
      --query-parameters ECS_CLUSTER_NAME=tutorial
```

3. サービス検出サービス用に Route 53 ホストゾーンに作成された DNS レコードは、次の AWS CLI コマンドでクエリを実行できます。

   a. 名前空間 ID を使用して、名前空間に関する情報を取得しますが、これには Route 53 ホストゾーン ID が含まれます。

   ```
   aws servicediscovery \
         get-namespace --id ns-uejictsjen2i4eeg
   ```

   出力は次のとおりです。

   ```
   {
   ```

```
    "Namespace": {
        "Id": "ns-uejictsjen2i4eeg",
        "Arn": "arn:aws:servicediscovery:region:aws_account_id:namespace/ns-
uejictsjen2i4eeg",
        "Name": "tutorial",
        "Type": "DNS_PRIVATE",
        "Properties": {
             "DnsProperties": {
                "HostedZoneId": "Z35JQ4ZFDRYPLV"
            }
        },
        "CreateDate": 1519777852.502,
        "CreatorRequestId": "9049a1d5-25e4-4115-8625-96dbda9a6093"
    }
}
```

b. 前のステップの Route 53 ホストゾーン ID (太字のテキストを参照) を使用して、ホストゾーンのリソースレコードセットを取得します。

```
aws route53 list-resource-record-sets \
      --hosted-zone-id Z35JQ4ZFDRYPLV
```

4. dig を使用して、VPC 内のインスタンスから DNS をクエリすることもできます。

```
dig +short myapplication.tutorial
```

ステップ 4: クリーンアップする

このチュートリアルが終了したら、未使用のリソースに対する料金が発生しないように、それに関連付けられたリソースをクリーンアップします。以下の手順に従ってください。

1. 前に書き留めたサービス ID とインスタンス ID を使用して、サービス検出サービスインスタンスの登録を解除します。

```
aws servicediscovery deregister-instance \
      --service-id srv-utcrh6wavdkggqtk \
      --instance-id 16becc26-8558-4af1-9fbd-f81be062a266
```

出力は次のとおりです。

```
{
```

```
    "OperationId": "xhu73bsertlyffhm3faqi7kumsmx274n-jh0zimzv"
}
```

2. 前のステップの出力の OperationId を使用して、サービス検出インスタンスが正常に登録解除されたことを確認します。

```
aws servicediscovery get-operation \
      --operation-id xhu73bsertlyffhm3faqi7kumsmx274n-jh0zimzv
```

```
{
  "Operation": {
        "Id": "xhu73bsertlyffhm3faqi7kumsmx274n-jh0zimzv",
        "Type": "DEREGISTER_INSTANCE",
        "Status": "SUCCESS",
        "CreateDate": 1525984073.707,
        "UpdateDate": 1525984076.426,
        "Targets": {
            "INSTANCE": "16becc26-8558-4af1-9fbd-f81be062a266",
            "ROUTE_53_CHANGE_ID": "C5NSRG1J4I1FH",
            "SERVICE": "srv-utcrh6wavdkggqtk"
        }
    }
}
```

3. サービス ID を使用してサービス検出のサービスを削除します。

```
aws servicediscovery delete-service \
      --id srv-utcrh6wavdkggqtk
```

4. 名前空間 ID を使用してサービス検出の名前空間を削除します。

```
aws servicediscovery delete-namespace \
      --id ns-uejictsjen2i4eeg
```

出力は次のとおりです。

```
{
    "OperationId": "c3ncqglftesw4ibgj5baz6ktaoh6cg4t-jh0ztysj"
}
```

5. 前のステップの出力の OperationId を使用して、サービス検出名前空間が正常に削除されたことを確認します。

```
aws servicediscovery get-operation \
      --operation-id c3ncqglftesw4ibgj5baz6ktaoh6cg4t-jh0ztysj
```

出力は次のとおりです。

```
{
    "Operation": {
        "Id": "c3ncqglftesw4ibgj5baz6ktaoh6cg4t-jh0ztysj",
        "Type": "DELETE_NAMESPACE",
        "Status": "SUCCESS",
        "CreateDate": 1525984602.211,
        "UpdateDate": 1525984602.558,
        "Targets": {
            "NAMESPACE": "ns-rymlehshst7hhukh",
            "ROUTE_53_CHANGE_ID": "CJP2A2M86XW3O"
        }
    }
}
```

6. Amazon ECS サービスに必要な数を更新して 0 にします。次のステップでサービスを削除するには、これを実行する必要があります。

```
aws ecs update-service \
      --cluster tutorial \
      --service ecs-service-discovery \
      --desired-count 0
```

7. Amazon ECS サービスを削除します。

```
aws ecs delete-service \
      --cluster tutorial \
      --service ecs-service-discovery
```

8. Amazon ECS クラスターを削除します。

```
aws ecs delete-cluster \
      --cluster tutorial
```

Amazon VPC Lattice を使用して Amazon ECS サービスを接続、監視、保護する

Amazon VPC Lattice は、Amazon ECS のお客様がコードを変更することなく、AWS コンピューティングサービス、VPC、アカウント全体で構築されたアプリケーションを観察、保護、モニタリングするために使用するマネージドアプリケーションネットワーキングサービスです。

VPC Lattice は、コンピューティングリソースのコレクションであるターゲットグループを使用します。これらのターゲットは、アプリケーションまたはサービスを実行するものであり、Amazon EC2 インスタンス、IP アドレス、Lambda 関数、Application Load Balancer を含みます。Amazon ECS サービスを VPC Lattice ターゲットグループに関連付けることで、お客様は Amazon ECS タスクを VPC Lattice の IP ターゲットとして有効にできるようになりました。Amazon ECS は、登録されたサービスのタスクが起動されると、VPC Lattice ターゲットグループにタスクを自動的に登録します。

> **Note**
>
> 5 つの VPC Lattice 設定を使用する場合、より少ない設定を使用する場合よりも、デプロイ時間がわずかに長くなることがあります。

リスナールールは、条件が満たされたときに、指定されたターゲットグループにトラフィックを転送するために使用されます。リスナーは、設定したポート上のプロトコルを使用して接続リクエストをチェックします。サービスは、リスナーの設定時に定義したルールに基づいて、登録済みターゲットにリクエストをルーティングします。

また、Amazon ECS は、VPC Lattice ヘルスチェックに基づいてタスクが異常と判断された場合、タスクを自動的に置き換えます。VPC Lattice に関連付けると、Amazon ECS のお客様は、AWS Resource Access Manager を使用したクラスター、VPC、アカウント間のサービスへの接続、認可と認証のための IAM 統合、高度なトラフィック管理機能など、VPC Lattice の他の多くのクロスコンピューティング接続、セキュリティ、オブザーバビリティ機能を利用することもできます。

Amazon ECS のお客様は、以下の方法で VPC Lattice の恩恵を受けることができます。

- デベロッパーの生産性の向上 - VPC Lattice は、ネットワーク、セキュリティ、オブザーバビリティの課題をすべてのコンピューティングプラットフォームにおいて統一された方法で処理することで、機能の構築に集中できるようにし、デベロッパーの生産性を向上させます。
- セキュリティ体制の向上 - VPC Lattice を使用すると、デベロッパーはアプリケーションとコンピューティングプラットフォーム間の通信を簡単に認証および保護し、転送中の暗号化を適用し

て、VPC Lattice Auth ポリシーを用いたきめ細かなアクセス制御を適用できます。これにより、業界をリードする規制およびコンプライアンス要件を満たす、より強力なセキュリティ体制を採用できます。

- アプリケーションのスケーラビリティと耐障害性の向上 - VPC Lattice では、パス、ヘッダー、メソッドベースのルーティング、認証、認可、モニタリングなどの機能を持つデプロイされたアプリケーションのネットワークを作成できます。これらの利点は、ワークロードのリソースオーバーヘッドなしで提供され、大幅なレイテンシーを発生させることなく、1 秒あたり数百万のリクエストを生成するマルチクラスターデプロイをサポートできます。
- 異種インフラストラクチャによるデプロイの柔軟性 - VPC Lattice は、Amazon ECS、Fargate、Amazon EC2、Amazon EKS、Lambda などのすべてのコンピューティングサービスで一貫した機能を提供し、組織が各アプリケーションに適したインフラストラクチャを柔軟に選択できるようにします。

VPC Lattice が他の Amazon ECS サービスと連携する仕組み

Amazon ECS で VPC Lattice を使用すると、他の Amazon ECS サービスの使用方法が変わる可能性がありますが、他は変わりません。

アプリケーション ロード バランサー

VPC Lattice の Application Load Balancer ターゲットグループタイプで使用するための、Amazon ECS サービスにリンクする特定の Application Load Balancer を作成する必要がなくなりました。代わりに VPC Lattice ターゲットグループを使用して Amazon ECS サービスを設定するだけで済みます。同時に、Amazon ECS で Application Load Balancer を引き続き使用することを選択することもできます。

Amazon ECS ローリングデプロイ

VPC Lattice では Amazon ECS ローリングデプロイのみが使用可能であり、Amazon ECS はデプロイ中にタスクをサービスに安全に追加および削除します。コードデプロイとブルー/グリーンデプロイはサポートされていません。

VPC Lattice の詳細については、「Amazon VPC Lattice ユーザーガイド」を参照してください。

VPC Lattice を使用するサービスを作成する

AWS Management Consoleまたは AWS CLI のいずれかを使用して、VPC Lattice でサービスを作成できます。

前提条件

個のチュートリアルを開始する前に、次の前提条件を満たしていることを確認します。

- AWS CLI の最新バージョンがインストールされ、設定されていること。詳細については、「AWS Command Line Interface のインストール」を参照してください。
- 「Amazon ECS を使用するようにセットアップする」で説明されているステップが完了しました。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。

AWS Management Consoleで VPC Lattice を使用するサービスを作成する

AWS Management Consoleを使用して VPC Lattice でサービスを作成するには、次のステップに従います。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションページで、[クラスター] を選択します。
3. [クラスター] ページで、サービスを作成するクラスターを選択します。
4. [Services] (サービス) タブから、[Create] (作成) を選択します。

   以前にサービスを作成したことがない場合は、「コンソールを使用した Amazon ECS サービスの作成」のステップに従い、VPC Lattice セクションまで進んだら、これらのステップを続行します。
5. ボタンをオンにして [VPC Lattice を有効にする] ことを選択します。
6. VPC Lattice ターゲットグループの作成時に使用するために作成済みの [Amazon ECS の ECS インフラストラクチャロール] を選択するか、[ECS インフラストラクチャロールの作成] を選択します。
7. VPC を選択します。

   [VPC] は、タスク定義を登録したときに選択したネットワークモードによって異なります。EC2 起動タイプで `host` または `network` モードを使用する場合は、ここで VPC を選択します。

   `awsvpc` モードでは、VPC は [ネットワーク] で選択した VPC に基づいて自動的に選択され、変更することはできません。
8. [ターゲットグループ] で、1 つまたは複数のターゲットグループを選択します。少なくとも 1 つのターゲットグループを選択する必要があります。最大 5 つのターゲットグループを選択でき

ます。追加のターゲットグループを追加するには、[ターゲットグループの追加] を選択します。選択した各ターゲットグループの [ポート名]、[プロトコル]、および [ポート] を選択します。ターゲットグループを削除するには、[削除] を選択します。

> **Note**
>
> - 既存のターゲットグループを追加する場合は、AWS CLI を使用する必要があります。AWS CLI を使用してターゲットグループを追加する方法については、「AWS Command Line Interface リファレンス」の「register-targets」を参照してください。
> - VPC Lattice サービスは複数のターゲットグループを持つことができますが、各ターゲットグループは 1 つのサービスにのみ追加できます。

9. この時点で、VPC Lattice コンソールに移動してセットアップを続行します。ここでは、リスナーのデフォルトアクションまたは既存の VPC Lattice サービスのルールに新しいターゲットグループを含めます。

   詳細については、「Listener rules for your VPC Lattice service」を参照してください。

> **Important**
>
> セキュリティグループにインバウンドルール `vpc-lattice` プレフィックスを許可しないと、タスクやヘルスチェックが失敗する可能性があります。

AWS CLIで VPC Lattice を使用するサービスを作成する

AWS CLI を使用して、VPC Lattice でサービスを作成します。各##############を独自の情報に置き換えます。

1. ターゲットグループ設定ファイルを作成します。以下の例は `tg-config.json` という名前です

```
{
    "ipAddressType": "IPV4",
    "port": 443,
    "protocol": "HTTPS",
    "protocolVersion": "HTTP1",
    "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
}
```

2. 以下のコマンドを使用して、VPC Lattice ターゲットグループを作成します。

```
aws vpc-lattice create-target-group \
    --name my-lattice-target-group-ip \
    --type IP \
    --config file://tg-config.json
```

出力例:

```
{
    "arn": "arn:aws:vpc-lattice:us-east-2:123456789012:targetgroup/
tg-0eaa4b9ab4EXAMPLE",
    "config": {
        "healthCheck": {
            "enabled": true,
            "healthCheckIntervalSeconds": 30,
            "healthCheckTimeoutSeconds": 5,
            "healthyThresholdCount": 5,
            "matcher": {
                "httpCode": "200"
            },
            "path": "/",
            "protocol": "HTTPS",
            "protocolVersion": "HTTP1",
            "unhealthyThresholdCount": 2
        },
        "ipAddressType": "IPV4",
        "port": 443,
        "protocol": "HTTPS",
        "protocolVersion": "HTTP1",
        "vpcIdentifier": "vpc-f1663d9868EXAMPLE"
    },
    "id": "tg-0eaa4b9ab4EXAMPLE",
    "name": "my-lattice-target-group-ip",
    "status": "CREATE_IN_PROGRESS",
    "type": "IP"
}
```

3. 以下の *ecs-service-vpc-lattice.json* という名前の json ファイルは、VPC Lattice ターゲットグループに Amazon ECS サービスをアタッチするために使用される例です。以下の例の portName は、タスク定義で定義したものと同じです。

```
{
    "serviceName": "ecs-service-vpc-lattice",
    "taskDefinition": "ecs-task-def",
        "vpcLatticeConfigurations": [
        {
            "targetGroupArn": "arn:aws:vpc-lattice:us-
west-2:123456789012:targetgroup/tg-0eaa4b9ab4EXAMPLE",
            "portName": "testvpclattice",
            "roleArn": "arn:aws:iam::123456789012:role/
ecsInfrastructureRoleVpcLattice"
        }
    ],
    "desiredCount": 5,
    "role": "ecsServiceRole"
}
```

以下のコマンドを使用して Amazon ECS サービスを作成し、上記の json 例を使用して VPC Lattice ターゲットグループにアタッチします。

```
aws ecs create-service \
    --cluster clusterName \
    --serviceName ecs-service-vpc-lattice \
    --cli-input-json file://ecs-service-vpc-lattice.json
```

> **Note**
>
> Amazon ECS Anywhere は VPC Lattice ではサポートされていません。

Amazon ECS タスクがスケールインイベントによって終了するのを防ぐ

Amazon ECS タスクスケールイン保護を使用すると、サービスの自動スケーリングまたはデプロイからのスケールインイベントによってタスクが終了されるのを防ぐことができます。

特定のアプリケーションでは、使用率が低いときやサービスのデプロイ中に、ミッションクリティカルなタスクがスケールインイベントによって終了されるのを防ぐメカニズムが必要です。例：

- ビデオトランスコーディングジョブなどのキュー処理型の非同期アプリケーションでは、サービスの累積使用率が低い場合でも、一部のタスクは何時間も実行する必要があります。

- あるゲームアプリケーションでは、ゲームサーバーは Amazon ECS タスクとして実行されますが、サーバー再起動時の起動待ち時間を短縮するため、すべてのユーザーがログアウトした場合でも実行を続ける必要があります。
- 新しいコードバージョンをデプロイする場合、再処理にはコストがかかるため、タスクは実行し続ける必要があります。

サービスに属するタスクがスケールインイベントで終了されることを防ぐには、`protectionEnabled` 属性を `true` に設定します。`protectionEnabled` を true に設定すると、タスクはデフォルトで 2 時間保護されます。その後、保護期間は、`expiresInMinutes` 属性を使用してカスタマイズできます。タスクの保護期間は最短で 1 分間、最長で 2,880 分 (48 時間) です。

タスクが必要な作業を完了した後は、`protectionEnabled` 属性を `false` に設定して、以降のスケールインイベントによってタスクが終了されるようにできます。

タスクスケールイン保護メカニズム

Amazon ECS コンテナエージェントエンドポイントまたは Amazon ECS API を使用して、タスクスケールイン保護を設定および取得できます。

- Amazon ECS コンテナエージェントエンドポイント

  保護の必要性を自己判断できるタスクには、Amazon ECS コンテナエージェントエンドポイントを使用することをお勧めします。このアプローチは、キューベースのワークロードまたはジョブ処理ワークロードに使用します。

  コンテナが、例えば SQS メッセージを使用するなどして処理を開始すると、コンテナ内からタスクスケールイン保護のエンドポイントパス「`$ECS_AGENT_URI/task-protection/v1/state`」を使用して `ProtectionEnabled` 属性を設定できます。スケールインイベントの際、Amazon ECS はこのタスクを終了しません。タスクの処理が完了した後は、同じエンドポイントを使用して `ProtectionEnabled` 属性をクリアし、以降のスケールインイベントでタスクが終了されるようにできます。

  Amazon ECS コンテナエージェントエンドポイントの詳細については、「Amazon ECS タスクスケールイン保護のエンドポイント」を参照してください。
- Amazon ECS API

  アプリケーションにアクティブなタスクの状態を追跡するコンポーネントがある場合は、Amazon ECS API を使用してタスクスケールイン保護を設定および取得できま

す。UpdateTaskProtection を使用して、1 つ以上のタスクを保護対象としてマークします。GetTaskProtection を使用して保護ステータスを取得します。

このアプローチの例としては、アプリケーションがゲームサーバーセッションを Amazon ECS タスクとしてホストしている場合が挙げられます。ユーザーがサーバー上のセッション (タスク) にログインすると、そのタスクを保護対象としてマークできます。ユーザーがログアウトした後は、サーバーのアイドル状態を維持することの要件に応じて、このタスク限定でクリアすることも、アクティブなセッションがなくなった同様のタスクについて定期的に保護をクリアすることもできます。

詳細については、「Amazon Elastic Container Service API リファレンス」の「UpdateTaskProtection」と「GetTaskProtection」を参照してください。

両方のアプローチを組み合わせることができます。例えば、Amazon ECS エージェントエンドポイントを使用してコンテナ内からタスク保護を設定し、Amazon ECS API を使用して外部コントローラーサービスからタスク保護を削除するなどです。

考慮事項

タスクスケールイン保護を使用する前に、次の点を考慮してください。

- Amazon ECS エージェントには再試行メカニズムが組み込まれており、そのインターフェイスはよりシンプルであるため、Amazon ECS コンテナエージェントエンドポイントを使用することをお勧めします。
- 既に保護がオンになっているタスクのために UpdateTaskProtection を呼び出すことで、タスクのスケールイン保護の有効期間をリセットできます。
- タスクが必要な作業を完了するのに必要な時間を判断し、それに応じて expiresInMinutes プロパティを設定してください。保護の有効期限を必要以上に長く設定すると、コストが発生すると共に、新しいタスクのデプロイが遅れることになります。
- Amazon ECS コンテナエージェント 1.65.0 以降ではタスクのスケールイン保護がサポートされています。

  エージェントを最新バージョンに更新することで、古いバージョンのAmazon ECS コンテナエージェントを使用する Amazon EC2 インスタンスでこの機能のサポートを追加できます。詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。
- デプロイに関する考慮事項:

- サービスがローリングアップデートを使用する場合、新しいタスクは作成できますが、古いバージョンを実行しているタスクは、protectionEnabled がクリアされるか、または失効するまで終了しません。デプロイ設定の maximumPercentage パラメータは、古いタスクが保護されている場合でも新しいタスクを作成できるように値を調整できます。
- ブルー/グリーン更新が適用されている場合、タスクに protectionEnabled があれば、保護されたタスクを含むブルーデプロイは削除されません。トラフィックは新しいタスクに振り分けられ、古いタスクは protectionEnabled がクリアされるか期限切れになったときのみ削除されます。CodeDeploy または CloudFormation の更新のタイムアウトによっては、デプロイがタイムアウトして、古いブルータスクが残っている場合があります。
- CloudFormation を使用する場合、更新スタックのタイムアウトは 3 時間です。そのため、タスク保護を 3 時間以上設定すると、CloudFormation のデプロイで障害が発生してロールバックが発生する可能性があります。

  古いタスクが保護されている間、CloudFormation スタックは UPDATE_IN_PROGRESS を表示します。タスクのスケールイン保護が削除されるか、または 3 時間のウィンドウ内に失効する場合、デプロイは成功し、UPDATE_COMPLETE ステータスに移行します。デプロイが UPDATE_IN_PROGRESS のまま 3 時間以上滞っていると、デプロイは失敗して UPDATE_FAILED 状態が表示され、古いタスクセットにロールバックされてしまいます。
- 保護されたタスクが原因でデプロイ (ローリングまたはブルー/グリーン) が定常状態に到達できない場合、Amazon ECS はサービスイベントを送信し、これによりユーザーは是正措置を講じることができます。タスクの保護ステータスを更新しようとする際に DEPLOYMENT_BLOCKED エラーメッセージが表示される場合、サービスの要求されるタスク数よりも多くの保護されたタスクがあることを意味します。この問題を解決するには、次のいずれかの操作を実行します。
  - 現在のタスク保護の有効期限が切れるのを待ちます。次に、タスク保護を設定します。
  - どのタスクを停止できるかを決定します。その後、これらのタスクについて protectionEnabled オプションを false に設定して UpdateTaskProtection を使用します。
  - サービスの必要なタスク数を増やして、保護されているタスクの数よりも多くします。

タスクスケールイン保護に必要な IAM アクセス許可

タスクには、以下のアクセス許可を持つ Amazon ECS タスクロールが必要です。

- ecs:GetTaskProtection: Amazon ECS コンテナエージェントが GetTaskProtection を呼び出すことを許可します。

- ecs:UpdateTaskProtection: Amazon ECS コンテナエージェントが UpdateTaskProtection を呼び出すことを許可します。

Amazon ECS タスクスケールイン保護のエンドポイント

Amazon ECS コンテナエージェントは、ECS_AGENT_URI 環境変数を Amazon ECS タスクのコンテナに自動的に挿入して、コンテナエージェント API エンドポイントとやり取りする方法を提供します。

保護の必要性を自己判断できるタスクには、Amazon ECS コンテナエージェントエンドポイントを使用することをお勧めします。

コンテナが処理を開始すると、コンテナ内からタスクスケールイン保護のエンドポイントパス「$ECS_AGENT_URI/task-protection/v1/state」を使用して protectionEnabled 属性を設定できます。

コンテナ内からこの URI への PUT リクエストを使用すると、タスクのスケールイン保護が設定されます。この URI への GET リクエストは、タスクの現在の保護ステータスを返します。

タスクスケールイン保護のリクエストパラメータ

次のリクエストパラメータで、${ECS_AGENT_URI}/task-protection/v1/state エンドポイントを使用してタスクスケールインプロテクションを設定できます。

ProtectionEnabled

true を指定して、タスクを保護できるようにマークします。false を指定して保護を解除し、タスクを終了できるようにします。

型: ブール値

必須: はい

ExpiresInMinutes

タスクが保護されている時間 (分)。最小 1 分から最大 2,880 分 (48 時間) まで指定できます。この期間中、自動スケーリングサービスまたはデプロイからのスケールインイベントによってタスクが終了することはありません。この時間が経過すると、protectionEnabled パラメータは false に設定されます。

時間を指定しない場合、タスクは自動的に 120 分 (2 時間) 保護されます。

タイプ: 整数

必須: いいえ

次の例は、異なる継続時間を持つタスク保護を設定する方法を示します。

デフォルトの期間を使用してタスクを保護する方法の例

この例は、デフォルトの期間が 2 時間に設定されているタスクを保護する方法を示しています。

```
curl --request PUT --header 'Content-Type: application/json' ${ECS_AGENT_URI}/task-
protection/v1/state --data '{"ProtectionEnabled":true}'
```

タスクを 60 分間保護する方法の例

この例は、expiresInMinutes パラメータを使用してタスクを 60 分間保護する方法を示しています。

```
curl --request PUT --header 'Content-Type: application/json' ${ECS_AGENT_URI}/task-
protection/v1/state --data '{"ProtectionEnabled":true,"ExpiresInMinutes":60}'
```

タスクを 24 時間保護する方法の例

この例は、expiresInMinutes パラメータを使用してタスクを 24 時間保護する方法を示しています。

```
curl --request PUT --header 'Content-Type: application/json' ${ECS_AGENT_URI}/task-
protection/v1/state --data '{"ProtectionEnabled":true,"ExpiresInMinutes":1440}'
```

PUT リクエストは次のレスポンスを返します。

```
{
  "protection": {
    "ExpirationDate": "2023-12-20T21:57:44.837Z",
    "ProtectionEnabled": true,
    "TaskArn": "arn:aws:ecs:us-west-2:111122223333:task/1234567890abcdef0"
  }
}
```

タスクスケールイン保護のレスポンスパラメータ

次の情報が、JSON レスポンスタスクのスケールインプロテクションエンドポイント ${ECS_AGENT_URI}/task-protection/v1/state から返されます。

`ExpirationDate`

タスクの保護が期限切れになるエポックタイム。タスクが保護されていない場合、この値は NULL です。

`ProtectionEnabled`

タスクのプロテクションステータス。タスクのスケールインプロテクションが有効になっている場合、値は `true` です。それ以外の場合は、`false` です。

`TaskArn`

コンテナが属しているタスクの完全な Amazon リソースネーム (ARN)。

次の例は、保護されたタスクについて返される詳細を示しています。

```
curl --request GET ${ECS_AGENT_URI}/task-protection/v1/state
```

```
{
    "protection":{
        "ExpirationDate":"2023-12-20T21:57:44Z",
        "ProtectionEnabled":true,
        "TaskArn":"arn:aws:ecs:us-west-2:111122223333:task/1234567890abcdef0"
    }
}
```

障害が発生すると、次の情報が返されます。

`Arn`

タスクの完全な Amazon リソースネーム (ARN)。

`Detail`

障害に関する詳細。

`Reason`

失敗の理由。

次の例は、保護されていないタスクについて返される詳細を示しています。

```
{
    "failure":{
        "Arn":"arn:aws:ecs:us-west-2:111122223333:task/1234567890abcdef0",
        "Detail":null,
        "Reason":"TASK_NOT_VALID"
    }
}
```

例外が発生すると、次の情報が返されます。

`requestID`

例外が発生する Amazon ECS API 呼び出しの AWS リクエスト ID。

`Arn`

タスクまたはサービスの完全な Amazon リソースネーム (ARN)。

`Code`

エラーコードです。

`Message`

エラーメッセージです。

> **Note**
>
> `RequestError` または `RequestTimeout` エラーが表示される場合は、ネットワークに問題がある可能性があります。Amazon ECS の VPC エンドポイントを使用してみてください。

次の例は、エラーが発生したときに返される詳細を示したものです。

```
{
    "requestID":"12345-abc-6789-0123-abc",
    "error":{
        "Arn":"arn:aws:ecs:us-west-2:555555555555:task/my-cluster-
name/1234567890abcdef0",
        "Code":"AccessDeniedException",
        "Message":"User: arn:aws:sts::444455556666:assumed-role/my-ecs-task-
role/1234567890abcdef0 is not authorized to perform: ecs:GetTaskProtection on resource:
```

```
 arn:aws:ecs:us-west-2:555555555555:task/test/1234567890abcdef0 because no identity-
based policy allows the ecs:GetTaskProtection action"
    }
}
```

ネットワークの問題や Amazon ECS コントロールプレーンがダウンしているなどの理由で Amazon ECS エージェントが Amazon ECS エンドポイントから応答を得られない場合、次のエラーが表示されます。

```
{
  "error": {
    "Arn": "arn:aws:ecs:us-west-2:555555555555:task/my-cluster-name/1234567890abcdef0",
    "Code": "RequestCanceled",
    "Message": "Timed out calling Amazon ECS Task Protection API"
  }
}
```

Amazon ECS エージェントが Amazon ECS からスロットリング例外を受け取ると、次のエラーが表示されます。

```
{
  "requestID": "12345-abc-6789-0123-abc",
  "error": {
    "Arn": "arn:aws:ecs:us-west-2:555555555555:task/my-cluster-name/1234567890abcdef0",
    "Code": "ThrottlingException",
    "Message": "Rate exceeded"
  }
}
```

Amazon ECS および Fargate ワークロードでフォールトインジェクションを使用する

お客様は、Amazon EC2 と Fargate の両方で Amazon ECS によるフォールトインジェクションを利用して、特定の障害シナリオに対するアプリケーションの反応をテストできます。これらのテストは、アプリケーションのパフォーマンスと回復力の最適化に使用できる情報を提供します。

フォールトインジェクションが有効になっている場合、Amazon ECS コンテナエージェントはタスクに新しいフォールトインジェクションエンドポイントへのアクセスを許可します。フォールトインジェクションを使用するには、タスク定義にオプションの `enableFaultInjection` パラメータを追加し、値を `true` に設定してオプトインする必要があります。デフォルト値は `false` です。

```
{
    ...
   "enableFaultInjection": true
}
```

> **Note**
>
> フォールトインジェクションは、awsvpc または host ネットワークモードを使用するタスクでのみ機能します。
> フォールトインジェクションは、Windows では使用できません。

AWS Management Consoleでフォールトインジェクションを有効にする方法については、「コンソールを使用して Amazon ECS タスク定義の作成」を参照してください。

AWS Fault Injection Service でテストするには、この機能を有効にする必要があります。詳細については、「AWS FIS aws:ecs:タスクアクションを使用します」を参照してください。

> **Note**
>
> 新しい Amazon ECS 最適化 AMI を使用していない、またはカスタム AMI を使用しているお客様は、フォールトインジェクション機能を使用するには、次の依存関係をインストールする必要があります。
>
> - `tc`
> - `sch_netem` カーネルモジュール

Amazon ECS フォールトインジェクションエンドポイント

Amazon ECS コンテナエージェントは、`ECS_AGENT_URI` 環境変数を Amazon ECS タスクのコンテナに自動的に挿入して、コンテナエージェント API エンドポイントとやり取りする方法を提供します。各エンドポイントには、`/start`、`/stop`、および `/status` エンドポイントが含まれます。エンドポイントは、フォールトインジェクションを有効にしたタスクからのリクエストのみを受け入れ、各エンドポイントにはコンテナあたり 5 秒間に 1 リクエストというレート制限があります。この制限を超えるとエラーが発生します。

> **Note**
>
> フォールトインジェクションエンドポイントを使用するには、Amazon ECS エージェント `version 1.88.0+` が必要です。

フォールトインジェクションで使用する 3 つのエンドポイントは以下のとおりです。

- ネットワークブラックホールポートエンドポイント
- ネットワークパケット損失エンドポイント
- ネットワークレイテンシーエンドポイント

リクエストが成功すると、`/start` エンドポイントを呼び出す場合 `running` のメッセージが記載された `200` 応答コードとなり、`/stop` エンドポイントの場合は `stopped`、`/status` エンドポイントの場合は `running` または `not-running` となります。

```
{
    "Status": <string>
}
```

リクエストが成功しなかった場合は、以下のいずれかのエラーコードを返します。

- `400` – Bad request·
- `409` – フォールトインジェクションリクエストが別の実行中の障害と競合する
- `429` – リクエストがスロットリングされました
- `500` – サーバーに予期しないエラーが発生しました

```
{
 "Error":  <string message>
}
```

> **Note**
>
> 1 回に挿入できるのは、1 つのネットワークレイテンシー障害、または 1 つのネットワークパケット損失障害のいずれかです。複数の結果を挿入しようとすると、リクエストは拒否されます。

ネットワークブラックホールポートエンドポイント

`{ECS_AGENT_URI}/fault/v1/network-blackhole-port` エンドポイントは、タスクのネットワーク名前空間内の特定のポートとプロトコルの受信トラフィックまたは送信トラフィックをドロップし、次の 2 つのモードと互換性があります。

- awsvpc — 変更がタスクネットワーク名前空間に適用されます
- ホスト — 変更はデフォルトのネットワーク名前空間コンテナインスタンスに適用されます

{ECS_AGENT_URI}/fault/v1/network-blackhole-port/start

このエンドポイントは、ネットワークブラックホールポートのフォールトインジェクションを開始し、次のパラメータがあります。

ポート

ブラックホールポートのフォールトインジェクションに使用する指定されたポート。

タイプ: 整数

必須: はい

プロトコル

ブラックホールポートのフォールトインジェクションに使用するプロトコル。

タイプ: 文字列

有効な値: `tcp | udp`

必須: はい

TrafficType

フォールトインジェクションで使用されるトラフィックタイプ。

タイプ: 文字列

有効な値: `ingress | egress`

必須: はい

SourcesToFilter

障害から保護されている IPv4 アドレスまたは CIDR ブロックの JSON 配列。

タイプ: 文字列の配列

必須: いいえ

以下は start エンドポイントを使用するためのリクエストの例です (## の値を独自の値に置き換えてください)。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-blackhole-port/start

Http method:POST

Request payload:
{
    "Port": 1234,
    "Protocol": "tcp|udp",
    "TrafficType": "ingress|egress"
    "SourcesToFilter": ["${IP1}", "${IP2}", ...],
}
```

{ECS_AGENT_URI}/fault/v1/network-blackhole-port/stop

このエンドポイントは、リクエストで指定された障害を停止します。このエンドポイントには以下のパラメータがあります。

ポート

停止する必要がある障害の影響を受けたポート。

タイプ: 整数

必須: はい

プロトコル

障害を停止するために使用するプロトコル。

タイプ: 文字列

有効な値: `tcp | udp`

必須: はい

TrafficType

フォールトインジェクションで使用されるトラフィックタイプ。

タイプ: 文字列

有効な値: `ingress | egress`

必須: はい

以下は stop エンドポイントを使用するためのリクエストの例です (## の値を独自の値に置き換えてください)。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-blackhole-port/stop

Http method: POST

Request payload:
{
    "Port": 1234,
    "Protocol": "tcp|udp",
    "TrafficType": "ingress|egress",
}
```

{ECS_AGENT_URI}/fault/v1/network-blackhole-port/status

このエンドポイントは、フォールトインジェクションのステータスを確認するために使用されます。このエンドポイントには以下のパラメータがあります。

ポート

障害のステータスを確認するために影響を受けるポート。

タイプ: 整数

必須: はい

プロトコル

障害のステータスを確認する際に使用するプロトコル。

タイプ: 文字列

有効な値: `tcp | udp`

必須: はい

TrafficType

フォールトインジェクションで使用されるトラフィックタイプ。

タイプ: 文字列

有効な値: `ingress | egress`

必須: はい

以下は `status` エンドポイントを使用するためのリクエストの例です (`##` の値を独自の値に置き換えてください)。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-blackhole-port/status

Http method: POST

Request payload:
{
   "Port": 1234,
   "Protocol": "tcp|udp",
   "TrafficType": "ingress|egress",
}
```

ネットワークレイテンシーエンドポイント

`{ECS_AGENT_URI}/fault/v1/network-latency` エンドポイントは、特定のソースへのトラフィックに対してタスクのネットワークインターフェイスに遅延とジッターを追加します。このエンドポイントは 2 つのモードと互換性があります。

- awsvpc — 変更がタスクネットワークインターフェイスに適用されます
- ホスト — 変更はデフォルトのネットワークインターフェイスに適用されます

{ECS_AGENT_URI}/fault/v1/network-latency/start

この`/start` エンドポイントは、ネットワークレイテンシーのフォールトインジェクションを開始し、以下のパラメータがあります。

DelayMilliseconds

フォールトインジェクションに使用するネットワークインターフェイスに追加する遅延のミリ秒数。

タイプ: 整数

必須: はい

JitterMilliseconds

フォールトインジェクションに使用するネットワークインターフェイスに追加するジッターのミリ秒数。

タイプ: 整数

必須: はい

[Sources] (出典)

フォールトインジェクションで使用する宛先である IPv4 アドレスまたは CIDR ブロックの JSON 配列。

タイプ: 文字列の配列

必須: はい

SourcesToFilter

障害から保護されている IPv4 アドレスまたは CIDR ブロックの JSON 配列。SourcesToFilter は Sources よりも優先されます。

タイプ: 文字列の配列

必須: いいえ

以下は /start エンドポイントを使用するためのリクエストの例です (## の値を独自の値に置き換えてください)。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-latency/start

Http method: POST

Request payload:
{
    "DelayMilliseconds": 123,
    "JitterMilliseconds": 123,
    "Sources": ["${IP1}", "${IP2}", ...],
    "SourcesToFilter": ["${IP1}", "${IP2}", ...],
}
```

{ECS_AGENT_URI}/fault/v1/network-latency/stop and /status

{ECS_AGENT_URI}/fault/v1/network-latency/stop エンドポイントは障害を停止し、{ECS_AGENT_URI}/fault/v1/network-latency/status は障害のステータスを確認します。

以下は、 /stop と /status のエンドポイントを使用する際の 2 つのリクエストの例です。どちらも POST HTTP メソッドを使用します。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-latency/stop
```

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-latency/status
```

ネットワークパケット損失エンドポイント

{ECS_AGENT_URI}/fault/v1/network-packet-loss エンドポイントは、指定されたネットワークインターフェイスへのパケット損失を追加します。このエンドポイントは、次の 2 つのモードと互換性があります。

- awsvpc — 変更がタスクネットワークインターフェイスに適用されます
- ホスト — 変更はデフォルトのネットワークインターフェイスに適用されます

{ECS_AGENT_URI}/fault/v1/network-packet-loss/start

この /start エンドポイントは、ネットワークパケット損失フォールトインジェクションを開始し、以下のパラメータがあります。

LossPercent

パケット損失の割合

タイプ: 整数

必須: はい

[Sources] (出典)

フォールトインジェクションテストに使用する IPv4 アドレスまたは CIDR ブロックの JSON 配列。

タイプ: 文字列の配列

必須: はい

SourcesToFilter

障害から保護されている IPv4 アドレスまたは CIDR ブロックの JSON 配列。SourcesToFilter は Sources よりも優先されます。

タイプ: 文字列の配列

必須: いいえ

以下は start エンドポイントを使用するためのリクエストの例です (## の値を独自の値に置き換えてください)。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-packet-loss/start

Http method: POST

{
    "LossPercent": 6,
    "Sources": ["${IP1}", "${IP2}", ...],
    "SourcesToFilter": ["${IP1}", "${IP2}", ...],
}
```

{ECS_AGENT_URI}/fault/v1/network-packet-loss/stop and /status

{ECS_AGENT_URI}/fault/v1/network-packet-loss/stop エンドポイントは障害を停止し、{ECS_AGENT_URI}/fault/v1/network-packet-loss/status は障害のステータスを確認します。1 回でサポートされる障害のタイプは 1 つだけです。

以下は、/stop と /status のエンドポイントを使用する際の 2 つのリクエストの例です。どちらも POST HTTP メソッドを使用します。

```
Endpoint: ${ECS_AGENT_URI}/fault/v1/network-packet-loss/stop
```

```
Endpoint: ${{ECS_AGENT_URI}/fault/v1/network-packet-loss/status
```

Amazon ECS の短いサービス ARN を長い ARN に移行する

Amazon ECS は、各サービスに一意の Amazon リソースネーム (ARN) を割り当てます。2021 年以前に作成されたサービスは、短いARN 形式を使用しています。

`arn:aws:ecs:region:aws_account_id:service/service-name`

Amazon ECS では、クラスター名を含めるように ARN 形式を変更しました。これは長い ARN 形式です。

`arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

サービスにタグを付けるには、長いARN形式を使用する必要があります。

サービスを再作成することなく、短い ARN 形式のサービスを長い ARN 形式に移行できます。API、CLI、またはコンソールを使用できます。移行オペレーションを元に戻すことはできません。

AWS CloudFormation を使用して短い ARN 形式でサービスにタグ付けする場合は、API、CLI、またはコンソールを使用してサービスを移行する必要があります。移行が完了したら、 AWS CloudFormation を使用してサービスにタグを付けることができます。

Terraform を使用して短い ARN 形式でサービスにタグ付けする場合は、API、CLI、またはコンソールを使用してサービスを移行する必要があります。移行が完了したら、Terraform を使用してサービスにタグを付けることができます。

移行が完了すると、サービスには次の変更が行われます。

- 長い ARN 形式

  `arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`
- コンソールを使用して移行する場合、Amazon ECS はキーを「ecs:serviceArnMigratedAt」に設定し、値を移行タイムスタンプ (UTC 形式) に設定して、サービスにタグを追加します。

  このタグは、タグクォータにカウントされます。
- AWS CloudFormation スタック内の `PhysicalResourceId` がサービス ARN を表す場合、値は変更されず、引き続き短いサービス ARN になります。

前提条件

サービス ARN を移行する前に、次のオペレーションを実行します。

1. 短い ARN 形式 があるかどうかを確認するには、Amazon ECS コンソールでサービスの詳細を表示するか (サービスが短い ARN 形式である場合は警告が表示されます)、または `describe-`

services の serviceARN 戻りパラメータを表示します。ARN にクラスター名が含まれていない場合、短い ARN になります。短い ARN の形式は次のとおりです。

```
arn:aws:ecs:region:aws_account_id:service/service-name
```

2. 作成日をメモします。
3. 短い ARN 形式を使用する IAM ポリシーがある場合は、長い ARN 形式に更新します。

   各###############を独自の情報に置き換えます。

   ```
   arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name
   ```

   詳細については、「AWS Identity and Access Management ユーザーガイド」の「Editing IAM policies」(IAM ポリシーの編集) を参照してください。
4. 短い ARN 形式を使用するツールがある場合は、長い ARN 形式に更新してください。

   各###############を独自の情報に置き換えます。

   ```
   arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name
   ```
5. サービスの長い ARN 形式を有効にします。serviceLongArnFormat オプションを enabled に設定して put-account-setting を実行します。詳細については、「Amazon Elastic Container Service API リファレンス」の「put-account-setting」を参照してください。

   サービスの createdAt 日付が不明な場合は、ルートユーザーとしてコマンドを実行します。

   ```
   aws ecs put-account-setting --name serviceLongArnFormat --value enabled
   ```

   出力例

   ```
   {
       "setting": {
           "name": "serviceLongArnFormat",
           "value": "enabled",
           "principalArn": "arn:aws:iam::123456789012:role/your-role",
           "type": user
       }
   }
   ```
6. タスクの長い ARN 形式を有効にします。taskLongArnFormat オプションを enabled に設定して put-account-setting を実行します。詳細については、「Amazon Elastic Container Service API リファレンス」の「put-account-setting」を参照してください。

サービスの createdAt 日付が不明な場合は、ルートユーザーとしてコマンドを実行します。

```
aws ecs put-account-setting --name taskLongArnFormat --value enabled
```

出力例

```
{
    "setting": {
        "name": "taskLongArnFormat",
        "value": "enabled",
        "principalArn": "arn:aws:iam::123456789012:role/your-role",
        "type": user
    }
}
```

手順

サービス ARN を移行するには、以下を使用します。

コンソール

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Clusters] (クラスター) ページで、クラスターを選択します。
3. [サービス] セクションで、ARN 列に警告があるサービスを選択します。

   [サービス詳細] ページが表示されます。
4. [長い ARN に移行する] を選択します。

   サービス移行ダイアログボックスが表示されます。
5. 移行 を選択します。

CLI

前提条件を完了したら、サービスにタグを付けることができます。次のコマンドを実行してください。

Amazon ECS は、短いARNを持つサービスに対する tag-resource APIリクエストで長い ARN 形式を渡すことを、そのサービスを長い ARN 形式を使用するよう移行するシグナルとみなします。

```
aws ecs tag-resource \
    --resource-arn arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name
    --tags key=key1,value=value1
```

次の例では、キーが「TestService」に設定され、値が「WebServers」に設定されたタグで MyService にタグを付けます。

```
aws ecs tag-resource \
    --resource-arn arn:aws:ecs:us-east-1:123456789012:service/MyCluster/MyService
    --tags key=TestService1,value=WebServers
```

Terraform

前提条件を完了したら、サービスにタグを付けることができます。aws_ecs_service リソースを作成し、tags リファレンスを設定します。詳細については、Terraform ドキュメントの「Resource: aws_ecs_service」を参照してください。

```
resource "aws_ecs_service" "MyService" {
  name    = "example"
  cluster = aws_ecs_cluster.MyService.id

 tags = {
 "Name"  =  "MyService"
 "Environment"  =  "Production"
 "Department"  =  "QualityAssurance"
  }
}
```

次のステップ

サービスにタグを追加できます。詳細については、「Amazon ECS リソースにタグを追加する」を参照してください。

Amazon ECS でタスク定義またはサービスからタスクにタグを伝達する場合は、propagateTags パラメータを指定して update-service を実行します。詳細については、「 AWS Command Line Interface リファレンス」の「create-service」を参照してください。

Amazon ECS サービスのスロットルロジック

Amazon ECS サービススケジューラには、サービスタスクが繰り返し起動に失敗した場合にタスクを起動する頻度を調整するロジックがあります。

サービスのタスクが繰り返し RUNNING 状態への遷移に失敗 (PENDING から直接 STOPPED ステータスに進行) する場合、その後の再起動の試行間隔は最大 27 分まで段階的に増加します。この最大期間は将来変更される可能性があります。この動作により、失敗しているタスクが Amazon ECS クラスターのリソースまたは Fargate のインフラストラクチャのコストに与える影響が軽減されます。サービスによって調整ロジックが開始されると、次のサービスイベントメッセージが表示されます。

```
(service service-name) is unable to consistently start tasks successfully.
```

Amazon ECS は、失敗したサービスの再試行を停止することはありません。また、再起動間隔を増やす以外に変更を加えようとすることもありません。サービスの調整ロジックにはユーザーが調整できるパラメータは用意されていません。

新しいタスク定義を使用するようにサービスを更新する場合、サービスは即時通常の調整されていない状態に戻ります。詳細については、「コンソールを使用した Amazon ECS サービスの更新」を参照してください。

このロジックを開始する一般的な原因を以下に示します。この問題に対処するには、手動で次のアクションを実行することをお勧めします。

- クラスターでタスクをホストするためのリソース (ポート、メモリ、CPU ユニットなど) が不足している。この場合、不十分なリソースサービスイベントメッセージも表示されます。
- Amazon ECS; コンテナエージェントがタスクの Docker イメージをプルできない。これは、コンテナイメージ名、イメージ、またはタグが不正であったり、プライベートレジストリの認証またはアクセス権限がないためである可能性があります。この場合、停止されたタスクのエラーに CannotPullContainerError も表示されます。
- コンテナインスタンスでコンテナを作成するために十分なディスク容量が不足している。この場合、停止されたタスクのエラーに CannotCreateContainerError も表示されます。詳細については、「Amazon ECS の Docker API error (500): devmapper のトラブルシューティング」を参照してください。

> **Important**
>
> RUNNING 状態になった後で停止されたタスクは、調整ロジックまたは関連サービスイベントメッセージを開始しません。例えば、サービスの Elastic Load Balancing ヘルスチェックに失敗すると、異常を示すフラグがタスクに設定され、Amazon ECS が登録を解除して、タスクを停止するとします。この時点では、タスクはスロットリングされていません。タスクのコンテナコマンドでゼロ以外の終了コードで即時終了した場合でも、タスクは既に RUNNING

状態に移行しています。コマンドのエラーが原因で即時失敗したタスクは、スロットリングやサービスイベントメッセージを生じさせません。

Amazon ECS サービス定義パラメータ

サービス定義は、Amazon ECS サービスの実行方法を定義します。サービス定義では、次のパラメータを指定できます。

起動タイプ

`launchType`

タイプ: 文字列

有効な値: `EC2` | `FARGATE` | `EXTERNAL`

必須: いいえ

サービスを実行する起動タイプ。起動タイプを指定しない場合は、デフォルトで `capacityProviderStrategy` が使用されます。詳しくは、「Amazon ECS 起動タイプ」を参照してください。

`launchType` を指定した場合、`capacityProviderStrategy` パラメータを省略する必要があります。

キャパシティープロバイダー戦略

`capacityProviderStrategy`

タイプ: オブジェクトの配列

必須: いいえ

サービスに使用するキャパシティープロバイダー戦略。

キャパシティープロバイダー戦略は、1 つ以上のキャパシティープロバイダーと、それらに割り当てる `base` と `weight` で構成されます。キャパシティープロバイダーは、キャパシティープロバイダー戦略で使用するクラスターに関連付ける必要があります。PutClusterCapacityProviders

API は、キャパシティープロバイダーをクラスターに関連付けるために使用されます。ACTIVE または UPDATING ステータスのキャパシティープロバイダーのみを使用できます。

capacityProviderStrategy を指定した場合、launchType パラメータを省略する必要があります。capacityProviderStrategy または launchType を指定しない場合は、クラスターの defaultCapacityProviderStrategy が使用されます。

Auto Scaling グループを使用するキャパシティープロバイダーを指定する場合は、キャパシティープロバイダーが既に作成されている必要があります。新しいキャパシティープロバイダーは、CreateCapacityProvider API オペレーションで作成できます。

AWS Fargate キャパシティープロバイダーを使用するには、FARGATE または FARGATE_SPOT キャパシティープロバイダーを指定します。AWS Fargate キャパシティープロバイダーはすべてのアカウントで使用でき、クラスターに関連付けるだけで使用できるようになります。

PutClusterCapacityProviders API オペレーションは、クラスターの作成後にクラスターで使用可能なキャパシティープロバイダーのリストを更新するために使用されます。

capacityProvider

タイプ: 文字列

必須: はい

キャパシティープロバイダーの短縮名または完全な Amazon リソースネーム (ARN)。

weight

タイプ: 整数

有効な範囲: 0 ~ 1,000 の整数。

必須: いいえ

ウエイト値は、指定したキャパシティープロバイダーを使用する起動済みタスクの総数に対する相対的な割合を示します。

例えば、2 つのキャパシティープロバイダーを含む戦略があり、両方の重みが 1 であるとします。ベースが満たされると、タスクは 2 つのキャパシティープロバイダー間で均等に分割されます。同じロジックを使用して、capacityProviderA に 1 の重みを指定し、capacityProviderB に 4 の重みを指定するとします。その後、capacityProviderA を使用して実行される 1 つのタスクごとに、4 つのタスクが capacityProviderB を使用します。

base

タイプ: 整数

有効な範囲: 0 ~ 100,000 の整数。

必須: いいえ

ベース値は、指定されたキャパシティープロバイダーで実行するタスクの最小限の数を指定します。キャパシティープロバイダー戦略では、ベースを定義できるキャパシティープロバイダーは 1 つだけです。

タスク定義

taskDefinition

タイプ: 文字列

必須: いいえ

family と revision (family:revision)、またはサービスで実行されるタスク定義の完全な Amazon リソースネーム (ARN) 。revision を指定しない場合、指定したファミリーの最新の ACTIVE リビジョンが使用されます。

ローリングアップデート (ECS) デプロイメントコントローラーを使用する場合は、タスク定義を指定する必要があります。

プラットフォームオペレーティングシステム

platformFamily

タイプ: 文字列

必須: 条件による

デフォルト: Linux

このパラメータは Fargate でホストされている Amazon ECS サービスに必要です。

このパラメータは、Amazon EC2 でホストされている Amazon ECS サービスでは無視されます。

サービスを実行するコンテナ上のオペレーティングシステム。有効な値は、LINUX、WINDOWS_SERVER_2019_FULL、WINDOWS_SERVER_2019_CORE、WINDOWS_SERVER_2 および WINDOWS_SERVER_2022_CORE です。

サービスに指定するすべてのタスクの platformFamily 値は、サービス platformFamily 値と一致する必要があります。例えば、platformFamily を WINDOWS_SERVER_2019_FULL に設定すると、すべてのタスクの platformFamily 値は WINDOWS_SERVER_2019_FULL でなければなりません。

プラットフォームバージョン

`platformVersion`

タイプ: 文字列

必須: いいえ

サービス内のタスクが実行されているプラットフォームのバージョン。プラットフォームのバージョンは、Fargate 起動タイプを使用するタスクに対してのみ指定されています。指定されない場合、デフォルトで最新バージョン (LATEST) が使用されます。

AWS Fargate プラットフォームのバージョンを使って、Fargate タスクインフラストラクチャの特定のランタイム環境を参照できます。プラットフォームのバージョンに LATEST を指定してタスクを実行またはサービスを作成すると、プラットフォームの最新バージョンをタスクで利用できるようになります。サービスをスケールアップする場合は、これらのタスクには、サービスの最新のデプロイで指定されたプラットフォームのバージョンが提供されます。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。

> **Note**
>
> プラットフォームのバージョンは、EC2 起動タイプを使用するタスクには指定されません。

クラスター

`cluster`

タイプ: 文字列

必須: いいえ

サービスを実行するクラスターの短い名前または完全な Amazon リソースネーム (ARN)。クラスターを指定しない場合は、default クラスターが使用されます。

サービス名

serviceName

タイプ: 文字列

必須: はい

サービスの名前。最大 255 文字の英字 (大文字と小文字)、数字、ハイフン、アンダースコアを使用できます。サービス名は同じクラスター内で一意になるようにしてください。ただし、リージョン内の複数のクラスター間や複数のリージョンにまたがるクラスター間では、同様の名前のサービスがあっても構いません。

スケジュール戦略

schedulingStrategy

タイプ: 文字列

有効な値: REPLICA | DAEMON

必須: いいえ

使用するスケジュール戦略。スケジュール戦略が指定されていない場合は、REPLICA 戦略が使用されます。詳細については、「Amazon ECS サービス」を参照してください。

利用できる 2 つのサービススケジューラ戦略があります。

- REPLICA - レプリカスケジュール戦略では、クラスター全体で必要数のタスクを配置して維持します。デフォルトでは、サービススケジューラによってタスクはアベイラビリティーゾーン間に分散されます。タスク配置の戦略と制約を使用すると、タスク配置の決定をカスタマイズできます。詳細については、「レプリカ戦略」を参照してください。
- DAEMON - デーモンのスケジュール戦略では、指定したすべてのタスク配置制約を満たすクラスター内のアクティブなコンテナインスタンスごとに、1 つのタスクのみをデプロイします。こ

の戦略を使用する場合、タスクの必要数や配置戦略、サービスの自動スケーリングポリシーを指定する必要はありません。詳細については、「デーモン戦略」を参照してください。

> **Note**
>
> Fargate タスクは DAEMON スケジュール戦略をサポートしていません。

必要数

`desiredCount`

タイプ: 整数

必須: いいえ

指定されたタスク定義のインスタンスをサービス内に配置し、実行し続ける数です。

このパラメータは、REPLICA スケジュール戦略を使用する場合に必要です。サービスが DAEMON スケジュール戦略を使用する場合、このパラメータはオプションです。

サービスの自動スケーリングを使用する場合、現在実行中のサービスを、現在実行中のタスク数よりも少ない `desiredCount` で更新すると、サービスは指定された `desiredCount` までスケールダウンされます

デプロイ設定

`deploymentConfiguration`

タイプ: オブジェクト

必須: いいえ

デプロイ時に実行されるタスクの数と、タスクの停止および開始の順序を制御するオプションのデプロイパラメータ。

`maximumPercent`

タイプ: 整数

必須: いいえ

サービスでローリング更新 (ECS) のデプロイタイプが使用されている場合、maximumPercent パラメータは、デプロイ時に RUNNING、STOPPING、または PENDING 状態で許可されるサービスのタスクの上限数を表します。これは、最も近い整数に切り捨てられた desiredCount のパーセンテージ (%) として表されます。このパラメータを使用して、デプロイのバッチサイズを定義できます。例えば、サービスで REPLICA サービススケジューラを使用して、desiredCount が 4 タスク、maximumPercent の値が 200% とすると、スケジューラは 4 つの古いタスクを停止する前に、4 つの新しいタスクを開始します。そのために必要なクラスターリソースを使用できることが前提です。REPLICA サービススケジューラを使用するサービスのデフォルトの maximumPercent 値は 200% です。

Amazon ECS スケジューラはこのパラメータを使用して、置き換えタスクを開始するためのクラスターリソースが使用可能である限り、最初に置き換えタスクを開始してから、異常なタスクを停止することで、異常なタスクを置き換えます。スケジューラが異常なタスクを置き換える仕組みの詳細については、「Amazon ECS サービス」を参照してください。

サービスで DAEMON サービススケジューラタイプを使用している場合、maximumPercent は 100% のままにする必要があります。これは、デフォルト値です。

デプロイ時のタスクの最大数は、desiredCount に maximumPercent/100 を乗算したもので、最も近い整数値に切り下げられます。

サービスで Blue/Green (CODE_DEPLOY) または EXTERNAL のいずれかのデプロイタイプと EC2 起動タイプを使用するタスクが使用されている場合、最大パーセントの値はデフォルト値に設定されます。この値は、コンテナインスタンスが DRAINING 状態にある間、サービス内で RUNNING 状態を保つタスクの数の上限を定義する目的で使用されます。

> **Note**
>
> Blue/Green (CODE_DEPLOY) または EXTERNAL デプロイタイプのいずれかを使用し、EC2 起動タイプを使用するタスクがあるサービスのカスタム maximumPercent 値を指定することはできません。

サービスが Blue/Green (CODE_DEPLOY) または EXTERNAL デプロイタイプのいずれかを使用し、サービス内のタスクが Fargate 起動タイプを使用する場合、最大パーセント値は使用されません。サービスを説明する際にも、この値は返されます。

`minimumHealthyPercent`

タイプ: 整数

必須: いいえ

サービスでローリング更新 (ECS) のデプロイタイプが使用されている場合、minimumHealthyPercent は、デプロイ時に RUNNING 状態に留まる必要があるサービスのタスクの下限数を表します。これは、最も近い整数に切り上げられた desiredCount のパーセンテージ (%) として表されます。このパラメータを使用して、追加のクラスターキャパシティーを使用せずにデプロイできます。

例えば、サービスで desiredCount が 4 タスク、minimumHealthyPercent が 50%、maximumPercent が 100% とすると、サービススケジューラは 2 つの新しいタスクを開始する前に、2 つの既存のタスクを停止してクラスターのキャパシティを解放できます。

いずれかのタスクに異常があり、maximumPercent が Amazon ECS スケジューラによる置き換えタスクの開始を許可しない場合、スケジューラは minimumHealthyPercent を制約として使用して、置き換えタスクを起動するためのキャパシティを解放するために、異常なタスクを 1 つずつ停止します。スケジューラが異常なタスクを置き換える仕組みの詳細については、「Amazon ECS サービス」を参照してください。

ロードバランサーを使用しないサービスの場合は、次のことを考慮してください。

- サービスのタスク内のすべての必須コンテナがヘルスチェックに合格すると、サービスは正常と見なされます。
- タスクにヘルスチェックが定義された必須コンテナがない場合、サービススケジューラは、タスクが RUNNING 状態に達した後 40 秒間待ってから、正常性の最小割合の合計にカウントします。
- タスクに、ヘルスチェックが定義された必須コンテナが 1 つ以上ある場合、サービススケジューラは、タスクが正常ステータスに達するのを待ってから、正常性の最小割合の合計にカウントします。タスク内のすべての必須コンテナがヘルスチェックに合格すると、タスクは正常と見なされます。サービススケジューラが待つことができる時間は、コンテナのヘルスチェックの設定によって決まります。詳細については、「ヘルスチェック」を参照してください。

ロードバランサーを使用するサービスについては、次のことを考慮してください。

- タスクにヘルスチェックが定義されている必須コンテナがない場合、サービススケジューラは、ロードバランサーターゲットグループのヘルスチェックが正常ステータスを返すのを待ってから、正常性の最小割合の合計にカウントします。
- タスクにヘルスチェックが定義されている必須コンテナがある場合、サービススケジューラは、タスクが正常なステータスになり、ロードバランサーターゲットグループのヘルス

チェックが正常ステータスを返すのを待ってから、タスクを正常性の最小割の合計にカウントします。

レプリカサービスの minimumHealthyPercent のデフォルト値は 100% です。DAEMON サービススケジュールを使用しているデフォルトの minimumHealthyPercent 値は、AWS CLI、AWS SDK、API では 0%、AWS Management Console では 50% です。

デプロイ時の正常なタスクの最小数は、desiredCount に minimumHealthyPercent/100 を乗算したもので、最も近い整数値に切り上げられます。

サービスで Blue/Green (CODE_DEPLOY) または EXTERNAL のデプロイタイプとタスクが使用されていて、EC2 起動タイプを使用するタスクが実行されている場合、最小ヘルス率の値はデフォルト値に設定されます。この値は、コンテナインスタンスが DRAINING 状態にある間、サービス内で RUNNING 状態を保つタスクの数の下限を定義する目的で使用されます。

> **Note**
>
> Blue/Green (CODE_DEPLOY) または EXTERNAL デプロイタイプのいずれかを使用し、EC2 起動タイプを使用するタスクがあるサービスのカスタム maximumPercent 値を指定することはできません。

サービスが Blue/Green (CODE_DEPLOY) または EXTERNAL デプロイタイプのいずれかを使用していて、Fargate 起動タイプを使用するタスクを実行している場合、最小ヘルス率の値は使用されませんが、サービスの説明時に値が返されます。

デプロイメントコントローラー

deploymentController

タイプ: オブジェクト

必須: いいえ

サービスで使用するデプロイコントローラータイプ。デプロイメントコントローラーが指定されていない場合は、ECS コントローラーが使用されます。詳細については、「Amazon ECS サービス」を参照してください。

type

タイプ: 文字列

有効な値: ECS | CODE_DEPLOY | EXTERNAL

必須: はい

使用するデプロイコントローラータイプ。次の 3 つのデプロイコントローラータイプを使用できます。

ECS

ローリング更新 (ECS) デプロイタイプでは、コンテナの現在実行されているバージョンを最新バージョンに置き換えられます。ローリング更新中に Amazon ECS がサービスに追加または削除するコンテナの数は、deploymentConfiguration で指定されるように、サービスのデプロイ中に許可される正常なタスクの最小数と最大数を調整することで制御されます。

CODE_DEPLOY

Blue/Green (CODE_DEPLOY) デプロイタイプは、CodeDeploy による ブルー/グリーンデプロイモデルを使用することにより、本稼働トラフィックを送信する前に、サービスの新しいデプロイを確認できます。

EXTERNAL

サードパーティーのデプロイコントローラーを使用して Amazon ECS サービスのデプロイプロセスを完全に制御することが必要な場合は、外部デプロイタイプを使用します。

タスクの配置

placementConstraints

タイプ: オブジェクトの配列

必須: いいえ

サービスのタスクに使用する、配置制約オブジェクトの配列。タスクごとに最大 10 個の制約を指定できます。この制限数には、タスク定義内の制約と、実行時に指定される制約が含まれます。Fargate 起動タイプを使用している場合、タスク配置の制約事項はサポートされません。

type

タイプ: 文字列

必須: いいえ

制約のタイプ。特定のグループの各タスクが確実に別のコンテナインスタンスで実行されるようにするには、distinctInstance を使用します。選択対象を有効な候補グループに制約するには、memberOf を使用します。値 distinctInstance はタスク定義ではサポートされていません。

expression

タイプ: 文字列

必須: いいえ

制約に適用されるクラスタークエリ言語表現。制約タイプが distinctInstance である場合は、式を指定できません。詳細については、「Amazon ECS タスク用のコンテナインスタンスを定義する式を作成する」を参照してください。

placementStrategy

タイプ: オブジェクトの配列

必須: いいえ

サービスのタスクで使用する配置戦略オブジェクト。サービスごとに最大 4 つの戦略ルールを指定できます。

type

タイプ: 文字列

有効な値: random | spread | binpack

必須: いいえ

配置戦略のタイプ。random 配置戦略は、タスクを利用可能な候補にランダムに配置します。spread 配置戦略は、field パラメータに基づいて、利用可能候補間で均等にタスクを分散して配置します。binpack 戦略は、field パラメータで指定したリソースの利用可能量が最も少ない利用可能候補にタスクを配置します。例えば、メモリの binpack 戦略を使用する場合、タスクは残りのメモリの量は最も少ないがタスクを実行するのに十分なインスタンスに配置されます。

field

タイプ: 文字列

必須: いいえ

配置戦略を適用するフィールド。spread 配置戦略では、有効な値は instanceId (または同じ効果を持つ host)、または attribute:ecs.availability-zone などのコンテナインスタンスに適用される任意のプラットフォームまたはカスタム属性です。binpack 配置戦略では、有効な値は cpu および memory です。random 配置戦略では、このフィールドは使用されません。

[タグ]

tags

タイプ: オブジェクトの配列

必須: いいえ

サービスに適用し、サービスの分類と整理に役立つメタデータ。タグはそれぞれ、1 つのキーとオプションの 1 つの値で設定されており、どちらもお客様側が定義します。サービスが削除されると、タグも削除されます。サービスには最大 50 個のタグを適用できます。詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。

key

タイプ: 文字列

長さの制限: 最小長は 1 です。最大長は 128 です。

必須: いいえ

タグを構成するキーと値のペアの一部。キーは、より具体的なタグ値のカテゴリのように動作する、一般的なラベルです。

value

タイプ: 文字列

長さの制約: 最小長は 0 です。最大長は 256 です。

必須: いいえ

タグを構成するキーと値のペアのオプションの一部。値はタグカテゴリ (キー) の記述子として機能します。

`enableECSManagedTags`

型: ブール値

有効な値: `true` | `false`

必須: いいえ

サービスのタスクに Amazon ECS マネージドタグを使用するか否かを指定します。値を指定しない場合、デフォルトは `false` になります。詳細については、「請求にタグを使用する」を参照してください。

`propagateTags`

タイプ: 文字列

有効な値: `TASK_DEFINITION` | `SERVICE`

必須: いいえ

タグをタスク定義またはサービスからサービスのタスクへコピーするかどうかを指定します。値を指定しない場合、タグはコピーされません。タグは、サービス作成中のサービス内のタスクにのみコピーすることができます。タグをサービス作成後またはタスク作成後のタスクに追加するには、`TagResource` API アクションを使用します。

ネットワーク構成

`networkConfiguration`

タイプ: オブジェクト

必須: いいえ

サービスのネットワーク構成。このパラメータは `awsvpc` ネットワークモードを使用して独自の Elastic Network Interface を受け取るタスク定義の場合に必要です。その他のネットワークモードではサポートされていません。Fargate 起動タイプを使用している場合、`awsvpc` ネットワークモードが必要です。Amazon EC2 起動タイプのネットワークの詳細については、「EC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。Fargate 起動タイプのネットワークの詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。

awsvpcConfiguration

タイプ: オブジェクト

必須: いいえ

タスクまたはサービスのサブネットとセキュリティグループを表すオブジェクト。

subnets

タイプ: 文字列の配列

必須: はい

タスクまたはサービスに関連付けられたサブネット。awsvpcConfiguration に従って指定できるサブネットは 16 個に制限されています。

securityGroups

タイプ: 文字列の配列

必須: いいえ

タスクまたはサービスに関連付けられたセキュリティグループ。セキュリティグループを指定しないと、VPC のデフォルトのセキュリティグループが使用されます。awsvpcConfiguration に基づいて指定できるセキュリティグループは 5 つに制限されています。

assignPublicIP

タイプ: 文字列

有効な値: ENABLED | DISABLED

必須: いいえ

タスクの Elastic Network Interface がパブリック IP アドレスを受け取るかどうかを示します。値を指定しない場合、デフォルト値の DISABLED が使用されます。

healthCheckGracePeriodSeconds

タイプ: 整数

必須: いいえ

タスクが RUNNING 状態になった後、Amazon ECS サービススケジューラが異常な Elastic Load Balancing ターゲットのヘルスチェック、コンテナのヘルスチェック、VPC Lattice のヘルスチェック、Route 53 のヘルスチェックを無視する期間 (秒単位)。これが有効であるのは、ロードバランサーを使用するようにサービスが設定されている場合のみです。サービスにロードバランサーを定義している場合、ヘルスチェックの猶予期間値を指定しないと、デフォルト値の 0 が使用されます。

サービスのタスクで、ヘルスチェックを開始して応答するまでに時間がかかる場合は、ヘルスチェックの猶予期間として最大 2,147,483,647 秒まで指定できます。この間は、ECS サービススケジューラはヘルスチェックのステータスを無視します。この猶予期間により、ECS サービススケジューラがタスクを異常とマークして時間より前に停止することがなくなります。

Elastic Load Balancing を使用しない場合、タスク定義のヘルスチェックパラメータの `startPeriod` を使用することをお勧めします。コンテナのヘルスチェックを使用して Amazon ECS タスク状態を判定する

`loadBalancers`

タイプ: オブジェクトの配列

必須: いいえ

サービスで使用するロードバランサーを表すロードバランサーオブジェクト。Application Load Balancer または Network Load Balancer を使,用するサービスの場合、6 個以上のターゲットグループはアタッチできません。

サービスの作成後にロードバランサーの設定を AWS Management Console から変更することはできません。AWS Copilot、AWS CloudFormation、AWS CLI、SDK のいずれかを使用して、AWS CodeDeploy ブルー/グリーンまたは外部ではなく、ECS ローリングデプロイコントローラのみのロードバランサー設定を変更できます。ロードバランサー設定を追加、更新、削除すると、Amazon ECS は、更新された Elastic Load Balancing 設定で新しいデプロイを開始します。これにより、タスクがロードバランサーに登録およびロードバランサーから登録解除されます。Elastic Load Balancing 設定を更新する前に、テスト環境でこれを検証することをお勧めします。設定の変更方法の詳細については、「Amazon Elastic Containers サービス API リファレンス」の UpdateService を参照してください。

Application Load Balancer および Network Load Balancers では、このオブジェクトには、ロードバランサーターゲットグループ ARN、コンテナ名 (コンテナの定義に表示)、ロードバランサーからアクセスされるコンテナポートが含まれている必要があります。このサービスのタスクがコ

ンテナインスタンスに配置されると、コンテナインスタンスとポートの組み合わせは、指定したターゲットグループのターゲットとして登録されます。

`targetGroupArn`

タイプ: 文字列

必須: いいえ

サービスに関連付ける Elastic Load Balancing ターゲットグループの完全な Amazon リソースネーム (ARN)。

ターゲットグループ ARN は、Application Load Balancer または Network Load Balancer を使用する場合にのみ指定します。

`loadBalancerName`

タイプ: 文字列

必須: いいえ

サービスに関連付けるロードバランサーの名前。

Application Load Balancer または Network Load Balancer を使用している場合は、ロードバランサーの名前パラメータを省略します。

`containerName`

タイプ: 文字列

必須: いいえ

ロードバランサーに関連付けるコンテナの名前 (コンテナ定義に表示)。

`containerPort`

タイプ: 整数

必須: いいえ

ロードバランサーに関連付けるコンテナのポート。このポートは、サービスのタスクが使用しているタスク定義の `containerPort` に対応する必要があります。EC2 起動タイプを使用するタスクの場合、コンテナインスタンスは、ポートマッピングの `hostPort` でインバウンドトラフィックを許可する必要があります。

`role`

タイプ: 文字列

必須: いいえ

Amazon ECS によるロードバランサーの呼び出しを許可する IAM ロールの短縮名または完全な ARN。このパラメーターは、サービスの単一のターゲットグループでロードバランサーを使用していて、タスク定義がawsvpcネットワークモードを使用していない場合にのみ許可されます。`role` パラメータを指定する場合、`loadBalancers` パラメータでロードバランサーのオブジェクトも指定する必要があります。

指定したロールに / 以外のパスがある場合は、完全なロール ARN を指定するか (推奨)、ロール名の前にパスを付ける必要があります。例えば、ロールの名前が `bar` で、パスが `/foo/` の場合、ロール名として `/foo/bar` を指定します。詳細については、IAM ユーザーガイドの「わかりやすい名前とパス」を参照してください。

> **Important**
>
> アカウントが既に Amazon ECS サービスリンクロールを作成している場合は、ここでロールを指定しない限り、そのロールがサービスにデフォルトで使用されます。タスク定義で awsvpc ネットワークモードを使用している場合はサービスにリンクされたロールが必要です。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。

`serviceConnectConfiguration`

タイプ: オブジェクト

必須: いいえ

このサービスがサービスを検出して接続し、名前空間内の他のサービスによって検出され接続されるための設定。

詳細については、「Service Connect を使用して Amazon ECS サービスを短縮名で接続する」を参照してください。

`enabled`

型: ブール値

必須: はい

このサービスで Service Connect を使用するかどうかを指定します。

`namespace`

タイプ: 文字列

必須: いいえ

Service Connect で使用する AWS Cloud Map 名前空間の短縮名または完全な Amazon リソースネーム (ARN)。名前空間は、Amazon ECS サービスおよびクラスターと同じ AWS リージョンにある必要があります。名前空間のタイプは Service Connect に影響しません。AWS Cloud Map の詳細については、「AWS Cloud Map デベロッパーガイド」の「Working with Services」(サービスの使用) を参照してください。

`services`

タイプ: オブジェクトの配列

必須: いいえ

Service Connect サービスオブジェクトの配列。これらは、他の Amazon ECS サービスがこのサービスに接続するために使用する名前とエイリアスです (エンドポイントとも呼ばれます)。

名前空間のメンバーである「クライアント」 Amazon ECS サービスが名前空間内の他のサービスに接続するだけであれば、このフィールドは必要ありません。その一例が、サービスに接続されているロードバランサーまたは他の方法で受信リクエストを受け入れるフロントエンドアプリケーションです。

オブジェクトは、タスク定義からポートを選択し、AWS Cloud Map サービスの名前や、クライアントアプリケーションがこのサービスを参照するためのエイリアス (エンドポイントとも呼ばれます) とポートの配列を割り当てます。

`portName`

タイプ: 文字列

必須: はい

`portName` は、この Amazon ECS サービスのタスク定義内のすべてのコンテナからの、`portMappings` のいずれかの `name` と一致する必要があります。

`discoveryName`

タイプ: 文字列

必須: いいえ

`discoveryName` は、この Amazon ECS サービス用に Amazon ECS が作成する新しい AWS Cloud Map サービスの名前です。これは AWS Cloud Map 名前空間内で一意である必要があります。

このフィールドを指定しない場合、`portName` が使用されます。

`clientAliases`

タイプ: オブジェクトの配列

必須: いいえ

このサービス接続サービスのクライアントエイリアスのリストです。これらを使用して、クライアントアプリケーションで使用できる名前を割り当てます。このリストで使用できるクライアントエイリアスの最大数は 1 です。

各エイリアス (「エンドポイント」) は、他の Amazon ECS サービス (「クライアント」) がこのサービスに接続するために使用できる DNS 名とポート番号です。

名前とポートの組み合わせは、名前空間内で一意である必要があります。

これらの名前は、クライアントサービスの各タスク内で設定され、AWS Cloud Map では設定されません。これらの名前を解決するための DNS リクエストはタスクから離れることはなく、Elastic Network Interface ごとの 1 秒あたりの DNS リクエストの割り当てにもカウントされません。

`port`

タイプ: 整数

必須: はい

サービス接続プロキシのリスニングポート番号です。このポートは、同じ名前空間内のすべてのタスク内で使用できます。

クライアント Amazon ECS サービスのアプリケーションが変更されないようにするには、クライアントアプリケーションがデフォルトで使用するのと同じポートを設定します。

dnsName

タイプ: 文字列

必須: いいえ

dnsName は、このサービスに接続するためにクライアントタスクのアプリケーションで使用する名前です。この名前は有効な DNS ラベルでなければなりません。

このフィールドが指定されない場合、デフォルト値は discoveryName.namespace になります。discoveryName が指定されない場合、タスク定義から portName が使用されます。

クライアント Amazon ECS サービスのアプリケーションが変更されないようにするには、クライアントアプリケーションがデフォルトで使用するのと同じ名前を設定します。例えば、一般的な名前として database や db、または mysql や redis などのデータベース名の小文字表記が挙げられます。

ingressPortOverride

タイプ: 整数

必須: いいえ

(オプション) Service Connect プロキシがリッスンするポート番号です。

このフィールドの値を使用して、このアプリケーションのタスク定義で portMapping という名称で指定されているポート番号のトラフィックに対してプロキシをバイパスしてから、Amazon VPC セキュリティグループでそのポート番号を使用して、この Amazon ECS サービスのプロキシへのトラフィックを許可します。

awsvpc モードでは、このアプリケーションのタスク定義で portMapping という名称で指定されているコンテナポート番号がデフォルト値になります。bridge モードでは、Service Connect プロキシの動的エフェメラルポートがデフォルト値になります。

logConfiguration

タイプ: LogConfiguration オブジェクト

必須: いいえ

これにより、Service Connect プロキシログの公開場所が定義されます。このログは、予期しないイベント発生時のデバッグに使用します。この設定は、この Amazon ECS サー

ビスの各タスクの Service Connect プロキシコンテナに `logConfiguration` パラメータを設定します。タスク定義でプロキシコンテナが指定されていません。

この Amazon ECS サービスのタスク定義のアプリケーションコンテナと同じログ設定を使用することをお勧めします。FireLens では、これはアプリケーションコンテナのログ設定です。`fluent-bit` または `fluentd` コンテナイメージを使用するのは FireLens ログルーターコンテナではありません。

`serviceRegistries`

タイプ: オブジェクトの配列

必須: いいえ

サービスのサービス検出設定の詳細。詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。

`registryArn`

型: 文字列

必須: いいえ

サービスレジストリの Amazon リソースネーム (ARN)。現在サポートされているサービスレジストリは AWS Cloud Map です。詳細については、AWS Cloud Map デベロッパーガイドの「サービスの使用」を参照してください。

`port`

タイプ: 整数

必須: いいえ

サービス検出サービスが SRV レコードを指定した場合に使用されるポート値。このフィールドは、`awsvpc` ネットワークモードと SRV レコードの両方が使用されている場合に必要です。

`containerName`

タイプ: 文字列

必須: いいえ

サービス検出サービスに使用されるコンテナ名の値。この値は、タスク定義で指定されます。サービスタスクが指定するタスク定義に bridge または host ネットワークモードが使用されている場合は、タスク定義からの containerName と containerPort の組み合わせを指定する必要があります。サービスタスクが指定するタスク定義に awsvpcネットワークモードが使用され、SRV DNS タイプのレコードが使用されている場合は、containerName と containerPort の組み合わせを指定するか、port 値を指定する必要があります (両方は指定しないでください)。

containerPort

タイプ: 整数

必須: いいえ

サービス検出サービスに使用されるポートの値。この値は、タスク定義で指定されます。サービスタスクが指定するタスク定義に bridge または host ネットワークモードが使用されている場合は、タスク定義からの containerName と containerPort の組み合わせを指定する必要があります。サービスタスクが指定するタスク定義に awsvpc ネットワークモードが使用され、SRV DNS タイプのレコードが使用されている場合は、containerName と containerPort の組み合わせを指定するか、port 値を指定する必要があります (両方は指定しないでください)。

クライアントトークン

clientToken

タイプ: 文字列

必須: いいえ

リクエストのべき等のために割り当てる一意の識別子 (大文字と小文字を区別)。最大 32 文字の ASCII 文字を使用できます。

アベイラビリティーゾーンの再調整

availabilityZoneRebalancing

タイプ: 文字列

必須: いいえ

サービスがアベイラビリティーゾーンの再調整を使用するかどうかを示します。有効な値は ENABLED および DISABLED です。アベイラビリティーゾーンのリバランスの詳細については、「アベイラビリティーゾーン間での Amazon ECS サービスの調整」を参照してください。

ボリューム設定

`volumeConfigurations`

タイプ: オブジェクト

必須: いいえ

サービスによって管理されるタスク用のボリュームを作成するのに使用される設定。サービス内のタスクごとに 1 つのボリュームが作成されます。このオブジェクトを使用して設定できるのは、タスク定義で「`configuredAtLaunch`」とマークされているボリュームだけです。このオブジェクトは、サービスによって管理されるタスクに Amazon EBS データボリュームをアタッチするのに必要です。詳細については、「Amazon EBS ボリューム」を参照してください。

`name`

タイプ: 文字列

必須: はい

サービスを作成または更新するときに設定されるボリュームの名前。最大 255 文字の英字 (大文字と小文字)、数字、アンダースコア (_)、ハイフン (-) が可能です。この値は、タスク定義で指定されたボリューム名と一致する必要があります。

`managedEBSVolume`

タイプ: オブジェクト

必須: いいえ

サービスの作成または更新時にサービスによって管理されるタスクにアタッチされる Amazon EBS ボリュームのボリューム設定。

`encrypted`

型: ブール値

必須: いいえ

有効な値: `true|false`

サービスによって管理されるタスクにアタッチされる Amazon EBS ボリュームを暗号化するかどうかを指定します。アカウントのデフォルトで Amazon EBS 暗号化を有効にしている場合、この設定は無効になり、ボリュームは暗号化されます。デフォルトでの EBS 暗号化の詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS暗号化をデフォルトで有効にする」を参照してください。

`kmsKeyId`

タイプ: 文字列

必須: いいえ

Amazon EBS 暗号化に使用する AWS Key Management Service (AWS KMS) キーの識別子。このパラメータが指定されなかった場合は、Amazon EBS 用の AWS KMS key が使用されます。`KmsKeyId` を指定する場合、暗号化された状態は `true` である必要があります。

以下のいずれかを使用して KMS キーを指定できます。

- キー ID – `1234abcd-12ab-34cd-56ef-1234567890ab` など。
- キーエイリアス – `alias/ExampleAlias` など。
- キー ARN – `arn:aws:kms:us-east-1:012345678910:key/1234abcd-12ab-34cd-56ef-1234567890ab` など。
- エイリアス ARN – `arn:aws:kms:us-east-1:012345678910:alias/ExampleAlias` など。

> **Important**
>
> AWS では、KMS キーを非同期で認証します。したがって、無効な ID、エイリアス、または ARN を指定すると、アクションは正常に行われているように見える場合がありますが、最終的には失敗します。詳細については、「Troubleshooting Amazon EBS volume attachment issues」を参照してください。

`volumeType`

タイプ: 文字列

必須: いいえ

有効な値: gp2|gp3|io1|io2|sc1|st1|standard

EBS ボリュームタイプ。詳細については、「Amazon EBS ユーザーガイド」の「Amazon EBS ボリュームタイプ」を参照してください。デフォルトのボリュームタイプは gp3 です。

> **Note**
>
> standard ボリュームタイプは、Fargate タスクにアタッチするように設定された Amazon EBS ボリュームではサポートされていません。

`sizeInGiB`

タイプ: 整数

必須: いいえ

有効な範囲: 1 ~ 16,384 の整数。

EBS ボリュームのギビバイト (GiB) でのサイズ。アタッチするボリュームを設定するスナップショット ID を指定しない場合は、サイズ値を指定する必要があります。スナップショットを使用してボリュームをアタッチするように設定した場合、デフォルト値はスナップショットサイズです。スナップショットサイズ以上のサイズを指定できます。

gp2 および gp3 ボリュームタイプでは、有効範囲は 1 ~ 16,384 です。

io1 および io2 ボリュームタイプでは、有効範囲は 4 ~ 16,384 です。

st1 および sc1 ボリュームタイプでは、有効範囲は 125 ~ 16,384 です。

standard ボリュームタイプでは、有効範囲は 1 ~ 1,024 です。

`snapshotId`

タイプ: 文字列

必須: いいえ

ECS タスクにアタッチされた新しいボリュームの作成に使用される既存の EBS ボリュームのスナップショットの ID。

`iops`

タイプ: 整数

必須: いいえ

1 秒あたりの I/O 操作の数 (IOPS)。gp3、io1、io2 ボリュームの場合、これはボリュームでプロビジョニングされている IOPS の数を表します。gp2 ボリュームの場合、この値はボリュームのベースラインパフォーマンスと、バースト用の I/O クレジットがこのボリュームに蓄積されるレートを表します。このパラメータは、io1 と io2 のボリュームに必須です。このパラメータは、gp2、st1、sc1、standard ボリュームではサポートされていません。

gp3 ボリュームでは、値の有効範囲は 3,000 ~ 16,000 です。

io1 ボリュームでは、値の有効範囲は 100 ~ 64,000 です。

io2 ボリュームでは、値の有効範囲は 100 ~ 64,000 です。

`throughput`

タイプ: 整数

必須: いいえ

サービスによって管理されるタスクにアタッチされたボリュームにプロビジョニングするスループット。

> **Important**
> このパラメータは、gp3 ボリュームのみでサポートされています。

`roleArn`

タイプ: 文字列

必須: はい

タスク用の Amazon EBS リソースを管理するための Amazon ECS アクセス許可を提供するインフラストラクチャ AWS Identity and Access Management (IAM) ロールの Amazon リソース ARN (ARN)。詳細については、「Amazon ECS インフラストラクチャ IAM ロール」を参照してください。

`tagSpecifications`

タイプ: オブジェクト

必須: いいえ

サービス管理型の Amazon EBS ボリュームに適用されるタグの指定。

`resourceType`

タイプ: 文字列

必須: はい

有効な値: `volume`

作成時にタグ付けするリソースのタイプ。

`tags`

タイプ: オブジェクトの配列

必須: いいえ

分類と整理に役立つようにボリュームに適用するメタデータ。タグはそれぞれ、1 つのキーとオプションの 1 つの値で構成されており、どちらもユーザーが定義します。`AmazonECSCreated` と `AmazonECSManaged` は Amazon ECS がユーザーに代わって追加する予約済みのタグなので、独自のタグを最大 48 個指定できます。ボリュームが削除されると、タグも削除されます。詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。

`key`

タイプ: 文字列

長さの制限: 最小長は 1 です。最大長は 128 です。

必須: いいえ

タグを構成するキーと値のペアの一部。キーは、より具体的なタグ値のカテゴリのように動作する、一般的なラベルです。

`value`

タイプ: 文字列

長さの制約: 最小長は 0 です。最大長は 256 です。

必須: いいえ

タグを構成するキーと値のペアのオプションの一部。値はタグカテゴリ (キー) の記述子として機能します。

`propagateTags`

タイプ: 文字列

有効な値: `TASK_DEFINITION` | `SERVICE` | `NONE`

必須: いいえ

タグをタスク定義またはサービスからボリュームにコピーするかどうかを指定します。`NONE` を指定した場合、または値を指定しない場合、タグはコピーされません。

`fileSystemType`

タイプ: 文字列

必須: いいえ

有効な値: `xfs|ext3|ext4|NTFS`

ボリューム上のファイルシステムのタイプ。ボリュームのファイルシステムタイプによって、ボリューム内でのデータの格納方法と取得方法が決まります。スナップショットから作成されたボリュームでは、スナップショットの作成時にボリュームが使用していたのと同じファイルシステムタイプを指定する必要があります。ファイルシステムのタイプが一致しない場合、タスクは開始できません。

Linux の有効な値は `xfs`、`ext3`, `and ext4` です。Linux タスクにアタッチされているボリュームのデフォルトは XFS です。

Windows の有効な値は NTFS です。TWindows タスクにアタッチされるボリュームのデフォルトは NTFS です。

サービス定義テンプレート

以下に、Amazon ECS サービス定義の JSON 表現を示します。

Amazon EC2 起動タイプ

```
{
    "cluster": "",
    "serviceName": "",
    "taskDefinition": "",
    "loadBalancers": [
        {
            "targetGroupArn": "",
            "loadBalancerName": "",
            "containerName": "",
            "containerPort": 0
        }
    ],
    "serviceRegistries": [
        {
            "registryArn": "",
            "port": 0,
            "containerName": "",
            "containerPort": 0
        }
    ],
    "desiredCount": 0,
    "clientToken": "",
    "launchType": "EC2",
    "capacityProviderStrategy": [
        {
            "capacityProvider": "",
            "weight": 0,
            "base": 0
        }
    ],
    "platformVersion": "",
    "role": "",
    "deploymentConfiguration": {
        "deploymentCircuitBreaker": {
            "enable": true,
            "rollback": true
        },
        "maximumPercent": 0,
        "minimumHealthyPercent": 0,
        "alarms": {
            "alarmNames": [
                ""
```

```
            ],
            "enable": true,
            "rollback": true
        }
    },
    "placementConstraints": [
        {
            "type": "distinctInstance",
            "expression": ""
        }
    ],
    "placementStrategy": [
        {
            "type": "binpack",
            "field": ""
        }
    ],
    "networkConfiguration": {
        "awsvpcConfiguration": {
            "subnets": [
                ""
            ],
            "securityGroups": [
                ""
            ],
            "assignPublicIp": "DISABLED"
        }
    },
    "healthCheckGracePeriodSeconds": 0,
    "schedulingStrategy": "REPLICA",
    "deploymentController": {
        "type": "EXTERNAL"
    },
    "tags": [
        {
            "key": "",
            "value": ""
        }
    ],
    "enableECSManagedTags": true,
    "propagateTags": "TASK_DEFINITION",
    "enableExecuteCommand": true,
    "availabilityZoneRebalancing": "ENABLED",
    "serviceConnectConfiguration": {
```

```
        "enabled": true,
        "namespace": "",
        "services": [
            {
                "portName": "",
                "discoveryName": "",
                "clientAliases": [
                    {
                        "port": 0,
                        "dnsName": ""
                    }
                ],
                "ingressPortOverride": 0
            }
        ],
        "logConfiguration": {
            "logDriver": "journald",
            "options": {
                "KeyName": ""
            },
            "secretOptions": [
                {
                    "name": "",
                    "valueFrom": ""
                }
            ]
        }
    },
    "volumeConfigurations": [
        {
            "name": "",
            "managedEBSVolume": {
                "encrypted": true,
                "kmsKeyId": "",
                "volumeType": "",
                "sizeInGiB": 0,
                "snapshotId": "",
                "iops": 0,
                "throughput": 0,
                "tagSpecifications": [
                    {
                        "resourceType": "volume",
                        "tags": [
                            {
```

```
                                "key": "",
                                "value": ""
                            }
                        ],
                        "propagateTags": "NONE"
                    }
                ],
                "roleArn": "",
                "filesystemType": ""
            }
        }
    ]
}
```

Fargate 起動タイプ

```
{
    "cluster": "",
    "serviceName": "",
    "taskDefinition": "",
    "loadBalancers": [
        {
            "targetGroupArn": "",
            "loadBalancerName": "",
            "containerName": "",
            "containerPort": 0
        }
    ],
    "serviceRegistries": [
        {
            "registryArn": "",
            "port": 0,
            "containerName": "",
            "containerPort": 0
        }
    ],
    "desiredCount": 0,
    "clientToken": "",
    "launchType": "FARGATE",
    "capacityProviderStrategy": [
        {
            "capacityProvider": "",
            "weight": 0,
```

```
            "base": 0
        }
    ],
    "platformVersion": "",
    "platformFamily": "",
    "role": "",
    "deploymentConfiguration": {
        "deploymentCircuitBreaker": {
            "enable": true,
            "rollback": true
        },
        "maximumPercent": 0,
        "minimumHealthyPercent": 0,
        "alarms": {
            "alarmNames": [
                ""
            ],
            "enable": true,
            "rollback": true
        }
    },
    "placementStrategy": [
        {
            "type": "binpack",
            "field": ""
        }
    ],
    "networkConfiguration": {
        "awsvpcConfiguration": {
            "subnets": [
                ""
            ],
            "securityGroups": [
                ""
            ],
            "assignPublicIp": "DISABLED"
        }
    },
    "healthCheckGracePeriodSeconds": 0,
    "schedulingStrategy": "REPLICA",
    "deploymentController": {
        "type": "EXTERNAL"
    },
    "tags": [
```

```
        {
            "key": "",
            "value": ""
        }
    ],
    "enableECSManagedTags": true,
    "propagateTags": "TASK_DEFINITION",
    "enableExecuteCommand": true,
    "availabilityZoneRebalancing": "ENABLED",
    "serviceConnectConfiguration": {
        "enabled": true,
        "namespace": "",
        "services": [
            {
                "portName": "",
                "discoveryName": "",
                "clientAliases": [
                    {
                        "port": 0,
                        "dnsName": ""
                    }
                ],
                "ingressPortOverride": 0
            }
        ],
        "logConfiguration": {
            "logDriver": "journald",
            "options": {
                "KeyName": ""
            },
            "secretOptions": [
                {
                    "name": "",
                    "valueFrom": ""
                }
            ]
        }
    },
    "volumeConfigurations": [
        {
            "name": "",
            "managedEBSVolume": {
                "encrypted": true,
                "kmsKeyId": "",
```

```
                "volumeType": "",
                "sizeInGiB": 0,
                "snapshotId": "",
                "iops": 0,
                "throughput": 0,
                "tagSpecifications": [
                    {
                        "resourceType": "volume",
                        "tags": [
                            {
                                "key": "",
                                "value": ""
                            }
                        ],
                        "propagateTags": "NONE"
                    }
                ],
                "roleArn": "",
                "filesystemType": ""
            }
        }
    ]
}
```

このサービス定義テンプレートは、次の AWS CLI コマンドを使用して作成できます。

```
aws ecs create-service --generate-cli-skeleton
```

Amazon ECS リソースにタグ付けする

Amazon ECS リソースを管理しやすくするために、タグを使用してオプションで各リソースに独自のメタデータを割り当てることができます。各タグは、キー、および値 (オプション) で構成されます。

タグを使用すると、Amazon ECS リソースを目的、所有者、環境などの、さまざまな方法で分類することができます。これは、同じ種類のリソースが多い場合に役立ちます。リソースに割り当てたタグに基づいて、特定のリソースをすばやく識別できます。例えば、アカウントの Amazon ECS コンテナインスタンスの一連のタグを定義できます。これは、各インスタンスの所有者とスタックレベルを追跡するのに役立ちます。

コストと使用状況レポートでタグを使用できます。これらのレポートを使用して、Amazon ECS リソースのコストと使用状況を分析できます。詳細については、「the section called “使用状況レポート”」を参照してください。

> **Warning**
>
> タグキーとその値を返す API は多数あります。`DescribeTags` へのアクセスを拒否しても、他の API から返されるタグへのアクセスは自動的に拒否されません。ベストプラクティスとして、機密データをタグに含めないようお勧めします。

各リソースタイプのニーズを満たす一連のタグキーを考案することをお勧めします。リソースの管理を容易にするために、タグキーの一貫したセットを使用できます。追加したタグに基づいてリソースを検索およびフィルタリングできます。

タグには、Amazon ECS に関連する意味はなく、完全に文字列として解釈されます。タグのキーと値は編集でき、タグはリソースからいつでも削除できます。タグの値を空の文字列に設定することはできますが、タグの値を 空値 に設定することはできません。そのリソースの既存のタグと同じキーを持つタグを追加した場合、古い値は新しい値によって上書きされます。リソースを削除すると、リソースのタグも削除されます。

AWS Identity and Access Management (IAM) を使用すると、AWS アカウント内のどのユーザーがタグを管理するアクセス許可を持っているかを制御できます。

リソースのタグ付け方法

Amazon ECS タスク、サービス、タスク定義、およびクラスターへのタグ付けには、次のような複数の方法が存在します。

- AWS Management Console、Amazon ECS API、AWS、または AWS CLI SDK を使用して、ユーザーが手動でリソースにタグ付けする。
- ユーザーが Amazon ECS マネージドタグのオプションを選択して、サービスを作成する、あるいはスタンドアロンのタスクを実行する。

  新しく起動されたすべてのタスクに対し、Amazon ECS が自動的なタグ付けを行う。詳細については、「the section called “Amazon ECS マネージドのタグ”」を参照してください。
- ユーザーがコンソールを使用してリソースを作成する。そのリソースに対し、コンソールが自動的にタグ付けを行います。

  これらのタグは、AWS CLI、および AWS SDK のレスポンスとして返され、コンソールに表示されます。これらのタグを、ユーザーが変更または削除することはできません。

  追加されたタグの詳細については、「Amazon ECS リソースのタグ付けのサポート」表内で、「コンソールによって自動的に追加されるタグ」列を参照してください。

リソースの作成時にタグを指定したにも関わらず、そのタグが適用されない場合、Amazon ECS は、対象の作成プロセスをロールバックします。これにより、リソースがタグ付きで作成されるか、まったく作成されないようになるため、タグ付けされていないリソースが存在することがなくなります。作成時にリソースにタグ付けすることで、リソース作成後にカスタムタグ付けスクリプトを実行する必要がなくなります。

以下の表に、タグ付けをサポートしている Amazon ECS リソースを示します。

リソース	タグをサポート	タグの伝播をサポート	コンソールによって自動的に追加されたタグ
Amazon ECS タスク	可能	はい、タスク定義からサポートします。	[Key] (キー): `aws:ecs:clusterName` 値: `cluster-name`

リソース	タグをサポート	タグの伝播をサポート	コンソールによって自動的に追加されたタグ
Amazon ECS サービス	可能	はい、タスク定義またはサービス内のタスクへのサービスのいずれかからサポートします。	[Key] (キー): `ecs:service:stackId` 値 `arn:aws:cloudformation: arn`
Amazon ECSの タスクセット	可能	いいえ	該当なし
Amazon ECS のタスク定義	可能	不可	[Key] (キー): `ecs:taskDefinition:createdFrom` 値: `ecs-console-v2`

リソース	タグをサポート	タグの伝播をサポート	コンソールによって自動的に追加されたタグ
Amazon ECS クラスター	可能	不可	[Key] (キー): `aws:cloudformation:logical-id` 値: `ECSCluster` [Key] (キー): `aws:cloudformation:stack-id` 値: `arn:aws:cloudformation: arn` [Key] (キー): `aws:cloudformation:stack-name` 値: `ECS-Console-V2-Cluster- EXAMPLE`
Amazon ECS コンテナインスタンス	可能	はい、Amazon EC2 インスタンスからサポートします。詳細については、「Amazon ECS コンテナインスタンスにタグを追加する」を参照してください。	該当なし

リソース	タグをサポート	タグの伝播をサポート	コンソールによって自動的に追加されたタグ
Amazon ECS 外部インスタンス	可能	いいえ	該当なし
Amazon ECS キャパシティープロバイダー	はい。 事前定義された FARGATE および FARGATE_SPOT キャパシティープロバイダーに対し、タグ付けすることはできません。	不可	該当なし

作成時のリソースのタグ付け

次のリソースは、Amazon ECS API、AWS CLI、または AWS SDK を使用した作成時のタグ付けをサポートしています。

- Amazon ECS タスク
- Amazon ECS サービス
- Amazon ECS タスク定義
- Amazon ECSの タスクセット
- Amazon ECS クラスター
- Amazon ECS コンテナインスタンス
- Amazon ECS キャパシティープロバイダー

Amazon ECS には、リソースの作成にタグ付け認可を使用するオプションがあります。AWS アカウント がタグの承認用に設定されている場合、ユーザーには、リソースを作成するアクションの許可が必要です (`ecsCreateCluster` など)。リソース作成アクションでタグが指定されている場合、AWS は追加の認可を実行して、ユーザーまたはロールがタグを作成するための許可を持って

いるかどうかを確認します。したがって、ecs:TagResource アクションを使用するための明示的な許可を付与する必要があります。詳細については、「the section called “リソース作成時のタグ付け”」を参照してください。オプションを設定する方法については、「the section called “タグ付け認可”」を参照してください。

制限事項

タグには以下の制限があります。

- 1 つのリソースに対して最大 50 個のタグを関連付けることができます。
- 1 つのリソースに対してタグキーを繰り返すことはできません。各タグキーは一意である必要があり、それぞれに使用できる値は 1 つのみです。
- キーの値には最大 128 UTF-8 文字を使用できます。
- 値の最大長は 256 UTF-8 文字です。
- 複数の AWS のサービスおよびリソースがタグ付けスキーマを使用する場合、使用する文字の種類を制限します。一部のサービスでは、使用できる文字に制限がある場合があります。通常、使用できる文字は、英字、数字、スペース、および特殊文字 **+**、**-**、**=**、**.**、**_**、**:**、**/**、**@** です。
- タグのキーと値では、大文字と小文字が区別されます。
- キーまたは値のプレフィックスとして、aws:、AWS:、またはこれら大文字または小文字の任意の組み合わせを使用することはできません。これらは AWS でのみ使用するように予約されています。このプレフィックスを持つタグのキーや値を編集または削除することはできません。このプレフィックスを持つタグは、リソースあたりのタグ数の制限にはカウントされません。

Amazon ECS マネージドのタグ

Amazon ECS マネージド タグを使用すると、Amazon ECS は、クラスター情報とユーザーが追加したタスク定義タグまたはサービスタグのいずれかを使用して、新しく起動されたすべてのタスクとタスクにアタッチされた Amazon EBS ボリュームに自動的にタグ付けします。以下は、追加されたタグについて説明しています。

- スタンドアロンタスク – キーには aws:ecs:clusterName を、値にはクラスター名を設定したタグ。ユーザーによって追加されたすべてのタスク定義タグです。スタンドアロンタスクにアタッチされた Amazon EBS ボリュームは、キーが aws:ecs:clusterName としてクラスター名に値が設定されたタグを受け取ります。Amazon EBS ボリュームのタグ付けの詳細については、「Amazon EBS ボリュームのタグ付け」を参照してください。

- サービスの一部であるタスク – キーを aws:ecs:clusterName として、値をクラスター名として設定したタグ。キーには aws:ecs:serviceName を、値にはサービス名を設定したタグです。以下のリソースのいずれかからのタグです。
  - タスク定義 – ユーザーによって追加されたすべてのタスク定義タグ。
  - サービス – ユーザーによって追加されたすべてのサービスタグ。

    サービスの一部であるタスクにアタッチされた Amazon EBS ボリュームは、キーが aws:ecs:clusterName として値がクラスター名に設定されたタグと、キーが aws:ecs:serviceName として値がサービス名に設定されたタグを受け取ります。Amazon EBS ボリュームのタグ付けの詳細については、「Amazon EBS ボリュームのタグ付け」を参照してください。

この機能には、以下のオプションが必要です。

- 新しい Amazon リソースネーム (ARN) とリソース識別子 (ID) 形式にオプトインする必要があります。詳細については、「Amazon リソースネーム (ARN) と ID」を参照してください。
- API を使用してサービスを作成したり、タスクを実行したりするときは、run-task と create-service の enableECSManagedTags を true に設定する必要があります。詳細については、「AWS Command Line Interface API リファレンス」の「CreateService」および「RunTask」を参照してください。
- Amazon ECS はマネージドタグを使用して、クラスターの Auto Scaling などの一部の機能をいつ有効にするかを判断します。Amazon ECS が機能を効果的に管理できるように、タグを手動で変更しないことをお勧めします。

請求にタグを使用する

AWS は、Amazon ECS リソースのコストおよび使用量を分析するために使用できる、Cost Explorer と呼ばれるレポートツールを提供します。

Cost Explorer を使用して、使用状況とコストのグラフを表示できます。過去 13 か月からデータを表示でき、また次の 3 か月間にどのくらい使用する可能性があるかを予測します。Cost Explorer を使用すると、時間の経過とともに AWS リソースに費やす金額のパターンを確認できます。例えば、Cost Explorer を使用して、さらに調べる必要がある分野を特定し、コストを把握するために使用できる傾向を確認できます。データの時間範囲を指定したり、時間データを日または月ごとに表示することもできます。

コストと使用状況レポートには、Amazon ECS マネージドのタグ、またはユーザーにより追加されたタグを使用できます。詳細については、「Amazon ECS 使用状況レポート」を参照してください。

リソースを組み合わせたコストを確認するには、同じタグキー値を持つリソースに基づいて、請求情報を整理します。例えば、複数のリソースに特定のアプリケーション名のタグを付け、請求情報を整理することで、複数のサービスを利用しているアプリケーションの合計コストを確認することができます。タグによるコスト配分レポートの設定の詳細については、AWS Billing ユーザーガイドのコスト配分月次レポートを参照してください。

さらに、[コスト配分データの分割] をオンにして、コストと使用状況レポートでタスクレベルの CPU とメモリの使用状況データを取得できます。詳細については、「タスクレベルのコストと使用状況レポート」を参照してください。

> **Note**
>
> レポートをオンにしている場合、当月のデータを表示できるようになるまでに最大 24 時間かかることがあります。

Amazon ECS リソースにタグを追加する

新規または既存のタスク、サービス、タスク定義、またはクラスターにタグ付けできます。コンテナインスタンスのタグ付けについては、「Amazon ECS コンテナインスタンスにタグを追加する」を参照してください。

> **Warning**
>
> 個人情報 (PII) などの機密情報や秘匿性の高い情報はタグに追加しないようにします。タグは、多くの AWS のサービス (請求など) からアクセスできます。タグは、プライベートデータや機密データに使用することを意図していません。

リソースの作成時に、次のリソースを使用してタグを指定できます。

タスク	コンソール	AWS CLI	API アクション
1 つまたは複数のタスクを実行する	Amazon ECS タスクとしてのア	実行タスク	RunTask

タスク	コンソール	AWS CLI	API アクション
	プリケーションの実行		
サービスを作成します。	コンソールを使用した Amazon ECS サービスの作成	サービスの作成	CreateService
タスクセットを作成します。	サードパーティーのコントローラーを使用して Amazon ECS サービスをデプロイする	タスクセットを作成	CreateTaskSet
タスク定義を登録する	the section called “コンソールを使用したタスク定義の作成”	タスク定義を登録	RegisterTaskDefinition
クラスターを作成する。	Fargate 起動タイプ用の Amazon ECS クラスターを作成する	クラスター作成	CreateCluster
1 つまたは複数のコンテナインスタンスを実行する	Amazon ECS Linux コンテナインスタンスの起動	実行インスタンス	RunInstances

既存のリソースにタグを追加する (Amazon ECS コンソール)

Amazon ECS では、クラスター、サービス、タスク定義に関連付けられているタグを、そのリソースのページから直接追加または削除できます。

個々のリソースのタグを変更するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションバーから、使用する AWS リージョン を選択します。
3. ナビゲーションペインでリソースタイプ (例:Clusters (クラスター) を選択します
4. リソースリストからリソースを選択し、[Tags] (タグ) タブを選択してから、[Manage tags] (タグの管理) を選択します。
5. タグを設定します。

   [タグを追加] [Add tag] (タグを追加) を選択し、以下を実行します。

   - [キー] にはキー名を入力します。
   - [値] にキー値を入力します。
6. [Save] を選択します。

既存のリソースにタグを追加する (AWS CLI)

AWS CLI または API を使用して、1 つ以上のタグを追加または上書きできます。

- AWS CLI - tag-resource
- API アクション - TagResource

Amazon ECS コンテナインスタンスにタグを追加する

以下のいずれかの方法で、コンテナインスタンスにタグを関連付けることができます。

- 方法 1 – Amazon EC2、API、CLI、またはコンソールを使用してコンテナインスタンスを作成するときに、コンテナエージェントの設定パラメータ `ECS_CONTAINER_INSTANCE_TAGS` を使用してインスタンスにユーザーデータを渡すことで、タグを指定します。これにより、Amazon ECS のコンテナインスタンスにのみ関連付けられているタグが作成され、Amazon EC2 API では一覧表示できなくなります。詳細については、「Amazon ECS Linux コンテナインスタンスをブートストラップしてデータを渡す」を参照してください。

  > **Important**
  >
  > Amazon EC2 Auto Scaling グループを使用してコンテナインスタンスを起動する場合は、ECS_CONTAINER_INSTANCE_TAGS エージェント設定パラメータを使用してタグを

追加する必要があります。これは、Auto Scaling グループを使用して起動される Amazon EC2 インスタンスにタグを追加する方法によるものです。

コンテナインスタンスにタグを関連付けるユーザーデータスクリプトの例を次に示します。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
ECS_CONTAINER_INSTANCE_TAGS={"tag_key": "tag_value"}
EOF
```

- 方法 2 – Amazon EC2 API、CLI、またはコンソールを使用してコンテナインスタンスを作成する場合、最初に TagSpecification.N パラメータを使用してタグを指定します。その後、コンテナエージェント設定パラメータ ECS_CONTAINER_INSTANCE_PROPAGATE_TAGS_FROM を使用して、ユーザーデータをインスタンスに渡します。これにより、Amazon EC2 から Amazon ECS に伝播されます。

  以下に、Amazon EC2 インスタンスに関連付けられたタグを伝播し、さらに MyCluster という名前のクラスターでインスタンスを登録するユーザーデータスクリプトの例を示します。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
ECS_CONTAINER_INSTANCE_PROPAGATE_TAGS_FROM=ec2_instance
EOF
```

  コンテナインスタンスのタグが Amazon EC2 から Amazon ECS に伝達されることを許可するには、以下のアクセス許可を コンテナインスタンスの IAM ロールにインラインポリシーとして手動で追加します。詳細については、「IAM ポリシーの追加と削除」を参照してください。

  - ec2:DescribeTags

  これらのアクセス許可を追加するために使用される、ポリシーの例を次に示します。

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

```
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        }
    ]
}
```

外部コンテナインスタンス

次のいずれかの方法を使用して、外部コンテナインスタンスにタグを関連付けることができます。

- 方法 1 — インストールスクリプトを実行して外部インスタンスをクラスターに登録する前に、Amazon ECS コンテナエージェント設定ファイル (/etc/ecs/ecs.configを追加しECS_CONTAINER_INSTANCE_TAGSコンテナエージェント設定パラメーター。これにより、外部インスタンスに関連付けられているタグが作成されます。

  構文の例を次に示します。

  ```
  ECS_CONTAINER_INSTANCE_TAGS={"tag_key": "tag_value"}
  ```

- 方法 2 — 外部インスタンスがクラスターに登録された後、AWS Management Console を使用して、タグを追加できます。詳細については、「既存のリソースにタグを追加する (Amazon ECS コンソール)」を参照してください。

Amazon ECS 使用状況レポート

AWS は、Amazon ECS リソースのコストおよび使用量を分析するために使用できる、Cost Explorer と呼ばれるレポートツールを提供します。

Cost Explorer を使用して、使用状況とコストのグラフを表示できます。過去 13 か月からデータを表示でき、また次の 3 か月間にどのくらい使用する可能性があるかを予測します。Cost Explorer を使用すると、時間の経過とともに AWS リソースに費やす金額のパターンを確認できます。例えば、Cost Explorer を使用して、さらに調べる必要がある分野を特定し、コストを把握するために使用できる傾向を確認できます。データの時間範囲を指定したり、時間データを日または月ごとに表示することもできます。

コストと使用状況レポートの計測データには、すべての Amazon ECS タスクの使用状況が示されます。計測データには、実行された各タスクの CPU 使用量が vCPU-Hours として、メモリ使用量が

GB-Hours として含まれます。データがどのように示されるかは、タスクの起動タイプによって異なります。

Fargate 起動タイプを使用するタスクの場合、lineItem/Operation 列には FargateTask が表示され、各タスクに関連するコストが見られます。

EC2 起動タイプを使用するタスクの場合、lineItem/Operation 列には ECSTask-EC2 が表示され、それらのタスクに直接関連するコストはありません。メモリの使用状況など、レポートに表示される計測データは、指定された請求期間にタスクが予約したリソースの合計を表します。このデータを使用して、Amazon EC2 インスタンスの基盤となるクラスターのコストを決定できます。Amazon EC2 インスタンスのコストと使用状況データは、Amazon EC2 サービスの下に個別に示されます。

Amazon ECS マネージドタグを使用して各タスクが属するサービスやクラスターを識別することもできます。詳細については、「請求にタグを使用する」を参照してください。

> **Important**
>
> 計測データは、2018 年 11 月 16 日以降に起動したタスクでのみ表示されます。この日付より前に起動したタスクには、計測データが表示されません。

Cost Explorer でコスト配分データを並べ替えるために使用できるフィールドの例を次に示します。

- クラスター名
- サービス名
- リソースタグ
- 起動タイプ
- AWS リージョン
- 使用タイプ

AWSのコストと使用状況レポートの作成の詳細については、AWS Billingユーザーガイドの AWSのコストと使用状況レポート を参照してください。

タスクレベルのコストと使用状況レポート

AWS Cost Management は、Fargate のタスクや EC2 のタスクを含む、Amazon ECS の各タスクの AWS Cost and Usage Report における CPU とメモリの使用状況データを提供できます。このデータはコスト配分データの分割と呼ばれます。このデータを使用して、アプリケーションのコストと使用

状況を分析できます。さらに、コスト配分タグとコストカテゴリを使用して、個々のビジネスユニットやチームにコストを分割して割り当てることができます。コスト配分データの分割の詳細については、「AWS Cost and Usage Report ユーザーガイド」の「コスト配分データの分割について」を参照してください。

AWS Cost Management Console で、アカウントのためにタスクレベルのコスト配分データの分割をオプトインできます。管理 (支払者) アカウントをお持ちの場合は、支払者アカウントからオプトインして、すべてのリンクされたアカウントにこの設定を適用できます。

[コスト配分データの分割] を設定すると、レポートの splitLineItem ヘッダーの下に追加の列が表示されます。詳細については、「AWS Cost and Usage Report ユーザーガイド」の「明細の分割の詳細」を参照してください。

EC2 のタスクの場合、このデータは、リソースの使用状況または予約、およびインスタンスの残りのリソースに基づいて、EC2 インスタンスのコストを分割します。

前提条件は次のとおりです。

- `ECS_DISABLE_METRICS` Amazon ECS エージェント設定パラメータを `false` に設定します。

  この設定が `false` である場合、Amazon ECS エージェントはメトリクスを Amazon CloudWatch に送信します。Linux では、この設定はデフォルトで `false` であり、メトリクスは CloudWatch に送信されます。Windows では、この設定はデフォルトで `true` であるため、メトリクスを CloudWatch に送信して AWS Cost Management が使用できるようにするためには、設定を `false` に変更する必要があります。ECS エージェント設定の詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。
- 信頼できるメトリクスの最小 Docker バージョンは、Amazon ECS 最適化 AMI 20220607 以降に含まれる Docker バージョン v20.10.13 以降です。

コスト配分データの分割を使用するには、レポートを作成し、[コスト配分データの分割] を選択する必要があります。詳細については、「AWS Cost and Usage Report ユーザーガイド」の「コストと使用状況レポートを作成する」を参照してください。

AWS Cost Management は、タスクの CPU とメモリの使用状況を使用してコスト配分データの分割を計算します。使用状況が利用できない場合、AWS Cost Management は、使用状況の代わりにタスクの CPU とメモリの予約を使用できます。CUR が予約を使用していることがわかった場合は、コンテナインスタンスが前提条件を満たしていること、およびタスクリソースの使用状況メトリクスが CloudWatch に表示されることを確認します。

Amazon ECS のモニタリング

モニタリングは、Amazon ECS および AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、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必要があります。Amazon ECS のモニタリングを開始する前に、以下の質問に対する回答を盛り込んだモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのリソースをモニタリングしますか?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- どのモニタリングツールを利用しますか?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

使用可能になるメトリクスは、クラスター内のタスクとサービスの起動タイプに応じて異なります。サービスに Fargate 起動タイプを使用している場合、サービスの監視を支援するための CPU とメモリの使用状況メトリクスが提供されます。Amazon EC2起動タイプの場合、基盤となるインフラストラクチャを構成する EC2 インスタンスを所有し、それらのインスタンスをモニタリングする必要があります。CPU とメモリの予約率と使用率の追加のメトリクスは、クラスター、サービス、およびタスクで使用できます。

次のステップでは、さまざまなタイミングと負荷条件でパフォーマンスを測定することにより、お客様の環境で通常の Amazon ECS のパフォーマンスのベースラインを確定します。Amazon ECS のモニタリングでは、過去のモニタリングデータを保存し、現在のパフォーマンスデータと比較することで、パフォーマンスの通常パターンと異常パターンを特定し、問題に対処する方法を考案できます。

ベースラインを確立するには、少なくとも、次の項目をモニタリングする必要があります。

- Amazon ECS クラスターの CPU とメモリの予約率および使用率に関するメトリクス
- Amazon ECS サービスの CPU とメモリの使用率メトリクス

  詳細については、「Amazon ECS メトリクスの表示」を参照してください。

Amazon ECS モニタリングのベストプラクティス

Amazon ECS をモニタリングするには、次のベストプラクティスを使用します。

- モニタリングに優先順位を設定し、小さな問題が大きな問題に発展する前に阻止する
- 以下の質問に対する回答を盛り込んだモニタリング計画を作成する
  - どのような目的でモニタリングしますか?
  - どのリソースをモニタリングしますか?
  - どのくらいの頻度でこれらのリソースをモニタリングしますか?
  - どのモニタリングツールを利用しますか?
  - 誰がモニタリングタスクを実行しますか?
  - 問題が発生したときに誰が通知を受け取りますか?
- モニタリングは可能な限り自動化します。
- Amazon ECS ログファイルを確認します。詳細については、「Amazon ECS コンテナエージェントログの表示」を参照してください。
- Runtime Monitoring を使用すると、 AWS 環境内のアカウント、コンテナ、ワークロード、およびデータを保護することができます。詳細については、「ランタイムモニタリングを使用して不正な動作を特定する」を参照してください。

Amazon ECS のモニタリングツール

AWS は、Amazon ECS のモニタリングに使用できるさまざまなツールを提供します。これらのツールの一部はモニタリングを行うように設定できますが、一部のツールは手動による介入が必要です。モニタリングタスクをできるだけ自動化することをお勧めします。

自動モニタリングツール

以下の自動化されたモニタリングツールを使用して、Amazon ECS を監視し、問題が発生したときにレポートできます。

- Amazon CloudWatch のアラーム – 単一のメトリクスを指定した期間モニタリングし、特定のしきい値に対する複数の期間にわたるメトリクスの値に基づいて、1 つ以上のアクションを実行します。アクションは、Amazon Simple Notification Service (Amazon SNS) のトピックまたは Amazon EC2 Auto Scaling のポリシーに送信される通知です。CloudWatch アラームは、特定の状態にあるという理由だけでアクションを呼び出すことはありません。状態が変更され、指定された期間維持

されている必要があります。詳細については、「CloudWatch を使用して Amazon ECS をモニタリングする」を参照してください。

Fargate 起動タイプを使用するタスクがあるサービスでは、CloudWatch アラームを使用して、CPU やメモリの使用率などの CloudWatch メトリクスに基づいてサービス内のタスクをスケールインおよびスケールアウトできます。詳細については、「Amazon ECS サービスを自動的にスケールする」を参照してください。

EC2 起動タイプを使用するタスクまたはサービスがあるクラスターでは、CloudWatch アラームを使用して、クラスターのメモリ使用率などの CloudWatch メトリクスに基づいてコンテナインスタンスをスケールインおよびスケールアウトできます。

Amazon ECS に最適化された Amazon Linux AMI で起動されたコンテナインスタンスの場合は、CloudWatch Logs を使用してコンテナインスタンスのさまざまなログを 1 つの便利な場所で表示できます。CloudWatch エージェントをコンテナインスタンスにインストールする必要があります。詳細については、Amazon CloudWatch ユーザーガイドの「コマンドラインを使用して CloudWatch エージェントをダウンロードおよび設定する」を参照してください。また、`ecsInstanceRole` ロールに `ECS-CloudWatchLogs` ポリシーを追加する必要があります。詳細については、「コンテナインスタンスのモニタリングに必要なアクセス許可」を参照してください。

- Amazon CloudWatch Logs – タスク定義で`awslogs` ログドライバーを指定することで、Amazon ECS タスクのコンテナからの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 ECS ログを CloudWatch に送信する 」を参照してください。

  Amazon ECS コンテナインスタンスからのオペレーティングシステムおよび Amazon ECS コンテナエージェントのログファイルをモニタリング、保存、アクセスすることもできます。この方法を使用したログへのアクセスは、EC2 起動タイプを使用するコンテナの場合で使うことができます。

- Amazon CloudWatch Events - イベントに一致したものを 1 つ以上のターゲットの関数またはストリームに渡して、変更、状態の情報の収集、是正措置を行います。詳細については、このガイドの「EventBridge を使用して Amazon ECS エラーへの対応を自動化する」および「Amazon EventBridge ユーザーガイド」の「EventBridge is the evolution of Amazon CloudWatch Events」を参照してください。

- Container Insights – コンテナ化されたアプリケーションとマイクロサービスからメトリクスとログを収集、集計、要約します。Container Insights は、埋め込みメトリクス形式を使用して、パフォーマンスログイベントとしてデータを収集します。このパフォーマンスログイベントは、高濃度データを取り込み、大規模に格納することが可能な構造化された JSON スキーマを使用す

るエントリです。CloudWatch は、このデータから、クラスター、タスク、サービスのレベルで CloudWatch メトリクスとして集計されたメトリクスを作成します。Container Insights が収集するメトリクスは、CloudWatch 自動ダッシュボードで使用でき、CloudWatch コンソールの [メトリクス] セクションでも表示できます。

- AWS CloudTrail のログのモニタリング – アカウント間でログファイルを共有し、CloudTrail のログファイルを CloudWatch Logs に送信してリアルタイムでモニタリングします。また、ログを処理するアプリケーションを Java で作成し、CloudTrail からの提供後にログファイルが変更されていないことを確認します。詳細については、「AWS CloudTrail を使用して Amazon ECS API コールをログに記録する」と、AWS CloudTrail ユーザーガイドの「CloudTrail ログファイルの操作」を参照してください。
- ランタイムモニタリング – AWS 環境内のクラスターとコンテナの脅威を検出します。Runtime Monitoring では、ファイルアクセス、プロセス実行、ネットワーク接続などの個々の Amazon ECS ワークロードを実行時に可視化する、GuardDuty セキュリティエージェントを使用します。

手動モニタリングツール

Amazon ECS のモニタリングでもう 1 つ重要な点は、CloudWatch のアラームの対象外の項目を手動でモニタリングすることです。Trusted Advisor、CloudWatch、その他の AWS コンソールのダッシュボードには、AWS 環境の状態が一目でわかるように表示されます。コンテナインスタンスおよびタスクのコンテナのログファイルも確認することをお勧めします。

- Amazon ECS コンソール:
  - EC2 起動タイプのクラスターメトリクス
  - サービスメトリクス
  - サービスのヘルスステータス
  - サービスデプロイイベント
- CloudWatch のホームページ:
  - 現在のアラームとステータス
  - アラームとリソースのグラフ
  - サービスのヘルスステータス

  また、CloudWatch を使用して以下のことを行えます。
  - 重要なサービスをモニタリングするためにカスタマイズされたダッシュボードを作成する。
  - メトリクスデータをグラフ化して、問題のトラブルシューティングを行い、傾向を確認する。

  - AWS リソースのすべてのメトリクスを検索およびブラウズする。
  - 問題があることを通知するアラームを作成/編集する。
- コンテナのヘルスチェック - コンテナ上でローカルに実行され、アプリケーションのヘルスと可用性を検証するコマンドです。これは、タスク定義でコンテナごとに構成します。
- AWS Trusted Advisor は、AWS リソースのパフォーマンス、信頼性、セキュリティ、費用効率を向上するためのモニタリングに役立ちます。すべてのユーザーは、4 つの Trusted Advisor; チェックを利用できます。ビジネスまたはエンタープライズサポートプランのユーザーは、50 以上のチェックを利用できます。詳細については、「AWS Trusted Advisor」を参照してください。

  Trusted Advisor には Amazon ECS に関連する以下のチェックがあります。

  - 1 つのアベイラビリティーゾーンでサービスが実行されていることを示す耐障害性。
  - 複数のアベイラビリティーゾーンでスプレッド配置戦略を使用していないことを示す耐障害性。
- AWS Compute Optimizer は、AWS リソースの設定と使用率のメトリクスを分析するサービスです。Compute Optimizer は、リソースが最適かどうかを報告し、最適化に関するレコメンデーションを生成してコストを削減およびワークロードのパフォーマンスを改善します。

  詳細については、「Amazon ECS に関する AWS Compute Optimizer 推奨事項」を参照してください。

CloudWatch を使用して Amazon ECS をモニタリングする

Amazon CloudWatch を使用して Amazon ECS リソースモニタリングすることで、Amazon ECSからraw データを収集して、リアルタイムに近い読み取り可能なメトリクスに加工することができます。これらの統計情報は 2 週間単位で記録されるため、履歴情報にアクセスしてクラスターやサービスの動作をより的確に把握できます。Amazon ECS のメトリクスデータは 1 分間隔で自動的に CloudWatch に送信されます。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

Amazon ECS には、クラスターとサービスの無料メトリクスがあります。追加料金で、CPU、メモリ、EBS ファイルシステムの使用率など、タスクごとのメトリクスについて、クラスターに対して Amazon ECS CloudWatch Container Insights を有効にすることができます。コンテナインサイトの詳細については、オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視するを参照してください。

考慮事項

Amazon ECS CloudWatch メトリクスを使用する際には、以下の点を考慮する必要があります。

- Fargate でホストされるどの Amazon ECS サービスでも、CloudWatch の CPU とメモリの使用率メトリクスが自動的に備わっているため、手動の手順を踏む必要はありません。

- Amazon EC2 インスタンスでホストされているどの Amazon ECS タスクまたはサービスでも、CloudWatch メトリクスを生成するために、Amazon EC2 インスタンスにコンテナエージェントのバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) が必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。
- 信頼性の高い CloudWatch メトリクスの最低 Docker バージョンは Docker `20.10.13` バージョン以降です。
- Amazon EC2 インスタンスには、IAM ロールに Amazon EC2 インスタンスを起動するのに使用する `ecs:StartTelemetrySession` アクセス許可も必要です。CloudWatch メトリクスが Amazon ECS で使用可能になる前に Amazon ECS コンテナインスタンス IAM ロールを作成した場合は、このアクセス許可の追加が必要になる場合があります。コンテナインスタンス IAM ロールとコンテナインスタンスのマネージド IAM ポリシーのアタッチについては、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。
- Amazon ECS コンテナエージェント設定で `ECS_DISABLE_METRICS=true` を設定することで、Amazon EC2 インスタンスでの CloudWatch メトリクス収集を無効にできます。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

推奨メトリクス

Amazon ECS には、リソースをモニタリングするのに使用できる無料 CloudWatch メトリクスが用意されています。このメトリクスを使用して、クラスター全体の CPU とメモリの予約率と CPU、メモリ、EBS ファイルシステムの使用率、およびクラスター内のサービスの CPU、メモリ、EBS ファイルシステムの使用率を測定できます。GPU のワークロードについては、クラスター全体の GPU 予約率を測定できます。

Amazon ECS タスクがクラスターでホストされているインフラストラクチャによって、利用可能なメトリクスが決まります。Fargate インフラストラクチャでホストされているタスクでは、サービスのモニタリングを支援するために、CPU、メモリ、EBS ファイルシステムの使用率メトリクスが Amazon ECS により提供されます。EC2 インスタンスでホストされるタスクでは、CPU、メ

モリ、GPU の予約率メトリクス、および CPU とメモリの使用率メトリクスが、クラスターおよびサービスレベルで Amazon ECS により提供されます。基盤となるインフラストラクチャを構成する Amazon EC2 インスタンスを個別にモニタリングする必要があります。Amazon EC2 インスタンスのモニタリングの詳細については、「Amazon EC2 ユーザーガイド」の「Amazon EC2 のモニタリング」を参照してください。

Amazon ECS で使用する推奨アラームについては、「Amazon CloudWatch Logs ユーザーガイド」にある以下のいずれかを参照してください。

- Amazon ECS
- Container Insights を使用する Amazon ECS

Amazon ECS メトリクスの表示

クラスターでリソースを実行したら、Amazon ECS と CloudWatch のコンソールでメトリクスを表示できます。Amazon ECS コンソールでは、クラスターとサービスのメトリクスの 24 時間の最大、最小、平均が表示されます。CloudWatch コンソールでは、リソースを詳細でカスタマイズ可能な表示で示します。また、サービスの実行中タスク数も表示します。

Amazon ECS コンソール

Amazon ECS サービスの CPU とメモリの使用率メトリクスを Amazon ECS サービス コンソールで使用できます。サービスメトリクスについてのビューには、過去 24 時間の平均値、最小値、最大値が、5 分ごとのデータポイントとともに表示されます。詳細については、「Amazon ECS サービスの使用率メトリクス」を参照してください。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. メトリクスを表示するクラスターを選択します。
3. 表示するメトリクスを決定します。

メトリクスの表示元	ステップ
クラスター	クラスターの詳細のページで、[メトリクス] タブを選択します。CloudWatch コンソールには、有効になっている場合に CloudWatch コンテ

メトリクスの表示元	ステップ
	ナインサイトのメトリクスを表示できるリンクも用意されています。
サービス	クラスターの詳細のページの [サービス] タブで、目的のサービスを選択します。このメトリクスは、[正常性とメトリクス] タブで利用可能になります。

CloudWatch コンソール

Fargate 起動タイプでは、Amazon ECS サービスのメトリクスも CloudWatch コンソールに表示できます。コンソールで Amazon ECS メトリクスの最も詳細なビューを表示できます。必要に応じてこのビューをカスタマイズできます。サービス使用率とサービス実行中のタスク数を表示できます。

EC2 起動タイプでは、Amazon ECS クラスターおよびサービスのメトリクスも CloudWatch コンソールに表示できます。コンソールで Amazon ECS メトリクスの最も詳細なビューを表示できます。必要に応じてこのビューをカスタマイズできます。

メトリクスの表示方法の詳細については、「Amazon CloudWatch ユーザーガイド」の「使用可能なメトリクスの表示」を参照してください。

Amazon ECS CloudWatch メトリクス

CloudWatch 使用状況メトリクスを使用して、アカウントのリソースの使用状況を把握できます。これらのメトリクスを使用して、CloudWatch グラフやダッシュボードで現在のサービスの使用状況を可視化できます。

`CPUReservation`

クラスターまたはサービスで予約されている CPU ユニットの割合。

CPU の予約率 (`ClusterName` でフィルタリング) は、クラスター上の Amazon ECS タスクによって予約されている CPU ユニットの総数を、クラスターに登録されているすべての Amazon EC2 インスタンスの CPU ユニットの総数で割った数で測定されます。`ACTIVE` または

DRAINING ステータスの Amazon EC2 インスタンスのみが、CPU 予約率メトリクスに影響します。このメトリクスは、Amazon EC2 インスタンスでホストされるタスクでのみサポートされています。

有効なディメンション: ClusterName。

便利な統計: Average、Minimum、Maximum

単位: パーセント。

CPUUtilization

クラスターまたはサービスで使用されている CPU ユニットの割合。

クラスターレベルの CPU 使用率 (ClusterName でフィルタリング) は、クラスター上の Amazon ECS タスクによって使用されている CPU ユニットの総数を、クラスターに登録されているすべての Amazon EC2 インスタンスの CPU ユニットの総数で割った値で測定されます。ACTIVE または DRAINING ステータスの Amazon EC2 インスタンスのみが、CPU 予約率メトリクスに影響します。クラスターレベルのメトリクスは、Amazon EC2 インスタンスでホストされるタスクでのみサポートされています。

サービスレベルの CPU 使用率 (ClusterName、ServiceName でフィルタリング) は、サービスに属するタスクによって使用されている CPU ユニットの総数を、サービスに属するタスク用に予約されている CPU ユニットの総数で割った値で測定されます。サービスレベルのメトリクスは、Amazon EC2 インスタンスと Fargate でホストされているタスクでサポートされています。

有効なディメンション: ClusterName、ServiceName。

便利な統計: Average、Minimum、Maximum

単位: パーセント。

MemoryReservation

クラスターでタスクを実行することで予約されているメモリの割合。

クラスターのメモリ予約率は、クラスター上の Amazon ECS タスクによって予約されているメモリの合計を、クラスターに登録されているすべての Amazon EC2 インスタンスのメモリの合計で割った値で測定されます。このメトリクスは ClusterName でのみフィルタリング可能です。ACTIVE または DRAINING ステータスの Amazon EC2 インスタンスのみが、メモリ予約率メトリクスに影響します。クラスターレベルのメモリ予約率メトリクスは、Amazon EC2 インスタンスでホストされるタスクでのみサポートされています。

> **Note**
>
> メモリ使用量率を計算する際、MemoryReservation が指定されると、合計メモリの代わりにその値が計算に使用されます。

有効なディメンション: ClusterName。

便利な統計: Average、Minimum、Maximum

単位: パーセント。

MemoryUtilization

クラスターまたはサービスで使用されているメモリの割合。

クラスターレベルのメモリ使用率 (ClusterName でフィルタリング) は、クラスター上の Amazon ECS タスクによって使用されているメモリの合計を、クラスターに登録されているすべての Amazon EC2 インスタンスメモリの合計で割った値で測定されます。ACTIVE または DRAINING ステータスの Amazon EC2 インスタンスのみが、メモリ使用率メトリクスに影響します。クラスターレベルのメトリクスは、Amazon EC2 インスタンスでホストされるタスクでのみサポートされています。

サービスレベルのメモリ使用率は (ClusterName、ServiceName でフィルタリング)、サービスに属するタスクによって使用されているメモリの合計を、サービスに属するタスク用に予約されているメモリの合計で割った値で測定されます。サービスレベルのメトリクスは、Amazon EC2 インスタンスと Fargate でホストされているタスクでサポートされています。

有効なディメンション: ClusterName、ServiceName。

便利な統計: Average、Minimum、Maximum

単位: パーセント。

EBSFilesystemUtilization

サービス内のタスクによって使用されている Amazon EBS ファイルシステムの割合。

サービスレベルの EBS ファイルシステム使用率メトリクス (ClusterName、ServiceName でフィルタリング) は、サービスに属するタスクによって使用されている EBS ファイルシステムの合計を、サービスに属するすべてのタスクに割り当てられている EBS ファイルシステムスト

レージの合計で割った値で測定されます。サービスレベルの EBS ファイルシステム使用率メトリクスは、EBS ボリュームがアタッチされている Amazon EC2 インスタンス (コンテナエージェントバージョン `1.79.0`) と Fargate (プラットフォームバージョン `1.4.0`) でホストされているタスクでのみ使用できます。

> **Note**
>
> Fargate でホストされているタスクでは、Fargate によってのみ使用されるディスク上のスペースがあります。Fargate が使用するスペースにコストは発生しませんが、`df` のようなツールで使用されるこの追加ストレージが表示されます。

有効なディメンション: `ClusterName, ServiceName`。

便利な統計: Average、Minimum、Maximum

単位: パーセント。

`GPUReservation`

使用可能な GPUs の合計に対する、クラスター内の実行中のタスクによって予約されている GPU の割合。

クラスターレベルの GPU 予約率メトリクスは、クラスター上の Amazon ECS タスクによって予約されている GPU の数を、クラスターに登録された GPU を備えたすべての Amazon EC2 インスタンスで使用可能な GPU の総数で割った値で測定されます。`ACTIVE` または `DRAINING` ステータスの Amazon EC2 インスタンスのみが、GPU 予約率メトリクスに影響します。

有効なディメンション: `ClusterName`。

便利な統計: Average、Minimum、Maximum

すべての統計: Average、Minimum、Maximum、Sum、Sample Count。

単位: パーセント。

`ActiveConnectionCount`

選択した `DiscoveryName` を共有するタスクで実行される、クライアントから Amazon ECS Service Connect プロキシへの、アクティブな同時接続の総数。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `DiscoveryName` および `DiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

`NewConnectionCount`

選択した `DiscoveryName` を共有するタスクで実行される、クライアントから Amazon ECS Service Connect プロキシに確立された新しい接続の総数。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `DiscoveryName` および `DiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

`ProcessedBytes`

Service Connect プロキシによって処理されたインバウンドトラフィックの総バイト数。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `DiscoveryName` および `DiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: バイト

`RequestCount`

Service Connect プロキシによって処理されたインバウンドトラフィックリクエストの数。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

また、タスク定義のポートマッピングで `appProtocol` を設定する必要があります。

有効なディメンション: `DiscoveryName` および `DiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

`GrpcRequestCount`

Service Connect プロキシによって処理された gRPC インバウンドトラフィックリクエストの数。

このメトリクスは、Amazon ECS Service Connect を設定していて、タスク定義のポートマッピングで `appProtocol` が `GRPC` である場合にのみ使用できます。

有効なディメンション: `DiscoveryName` および `DiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

`HTTPCode_Target_2XX_Count`

これらのタスクによってアプリケーションによって生成された 200 から 299 の数字の HTTP レスポンスコードの数。これらのタスクがターゲットです。このメトリクスは、これらのタスクでアプリケーションによって Service Connect プロキシに送信された応答のみをカウントし、直接送信された応答はカウントしません。

このメトリクスは、Amazon ECS Service Connect を設定していて、タスク定義のポートマッピングで `appProtocol` が `HTTP` または `HTTP2` である場合にのみ使用できます。

有効なディメンション: `TargetDiscoveryName` および `TargetDiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

`HTTPCode_Target_3XX_Count`

これらのタスクによってアプリケーションによって生成された 300 から 399 の数字の HTTP レスポンスコードの数。これらのタスクがターゲットです。このメトリクスは、これらのタスクでアプリケーションによって Service Connect プロキシに送信された応答のみをカウントし、直接送信された応答はカウントしません。

このメトリクスは、Amazon ECS Service Connect を設定していて、タスク定義のポートマッピングで `appProtocol` が `HTTP` または `HTTP2` である場合にのみ使用できます。

有効なディメンション: TargetDiscoveryName および TargetDiscoveryName, ServiceName, ClusterName。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

HTTPCode_Target_4XX_Count

これらのタスクによってアプリケーションによって生成された 400 から 499 の数字の HTTP レスポンスコードの数。これらのタスクがターゲットです。このメトリクスは、これらのタスクでアプリケーションによって Service Connect プロキシに送信された応答のみをカウントし、直接送信された応答はカウントしません。

このメトリクスは、Amazon ECS Service Connect を設定していて、タスク定義のポートマッピングで appProtocol が HTTP または HTTP2 である場合にのみ使用できます。

有効なディメンション: TargetDiscoveryName および TargetDiscoveryName, ServiceName, ClusterName。

便利な統計: Average、Minimum、Maximum、Sum

単位: カウント.

HTTPCode_Target_5XX_Count

これらのタスクによってアプリケーションによって生成された 500 から 599 の数字の HTTP レスポンスコードの数。これらのタスクがターゲットです。このメトリクスは、これらのタスクでアプリケーションによって Service Connect プロキシに送信された応答のみをカウントし、直接送信された応答はカウントしません。

このメトリクスは、Amazon ECS Service Connect を設定していて、タスク定義のポートマッピングで appProtocol が HTTP または HTTP2 である場合にのみ使用できます。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

RequestCountPerTarget

選択した DiscoveryName を共有する各ターゲットによって受信されたリクエストの平均数。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `TargetDiscoveryName` および `TargetDiscoveryName, ServiceName, ClusterName`。

便利な統計: Average。

単位: カウント.

`TargetProcessedBytes`

Service Connect プロキシによって処理された総バイト数。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `TargetDiscoveryName` および `TargetDiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: バイト

`TargetResponseTime`

アプリケーションリクエスト処理のレイテンシー。リクエストがターゲットタスクの Service Connect プロキシに到達してから、ターゲットアプリケーションからの応答がプロキシに受信されるまでの経過時間 (ミリ秒)。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `TargetDiscoveryName` および `TargetDiscoveryName, ServiceName, ClusterName`。

便利な統計: Average、Minimum、Maximum。

すべての統計: Average、Minimum、Maximum、Sum、Sample Count。

単位: ミリ秒

`ClientTLSNegotiationErrorCount`

TLS 接続に失敗した合計回数。このメトリクスは TLS が有効になっている場合にのみ使用されます。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション: `DiscoveryName`、`DiscoveryName`、`ServiceName`、`ClusterName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

`TargetTLSNegotiationErrorCount`

クライアント証明書の欠落、AWS Private CA 検証の失敗、または SAN 検証の失敗により TLS 接続が失敗した合計回数。このメトリクスは TLS が有効になっている場合にのみ使用されます。

このメトリクスは、Amazon ECS Service Connect を設定した場合にのみ使用できます。

有効なディメンション:
`ServiceName`、`ClusterName`、`TargetDiscoveryName`、`TargetDiscoveryName`。

便利な統計: Average、Minimum、Maximum、Sum。

単位: カウント.

Amazon ECS メトリクスのディメンション

Amazon ECS メトリックスは `AWS/ECS` 名前空間を使用し、以下のディメンションのメトリックスを提供しています。Amazon ECS は、タスクが `RUNNING` 状態にあるリソースのメトリクスのみを送信します。例えば、クラスターに 1 つのサービスがあるが、このサービスに `RUNNING` 状態のタスクがない場合、CloudWatch に送信されるメトリクスはありません。2 つのサービスがあり、1 つに実行中のタスクがあるが、別の 1 つに実行中のタスクがない場合、実行中のタスクがあるサービスのメトリクスのみが送信されます。

`ClusterName`

このディメンションにより、指定したクラスター内のすべてのリソースから、リクエストしたデータがフィルタ処理されます。すべての Amazon ECS メトリクスは `ClusterName` でフィルタ処理されます。

`ServiceName`

このディメンションにより、指定したクラスター内の特定サービスのすべてのリソースから、リクエストしたデータがフィルタ処理されます。

`DiscoveryName`

このディメンションは、トラフィックメトリクスをリクエストするデータを、すべての Amazon ECS クラスター全体の指定された Service Connect 検出名にフィルタリングします。

実行中のコンテナ内の特定のポートには、複数の検出名を指定できることに注意してください。

`DiscoveryName, ServiceName, ClusterName`

このディメンションは、トラフィックメトリクスをリクエストするデータを、このクラスター内のこのサービスによって作成された、この検出名を持つタスク全体の指定された Service Connect 検出名にフィルタリングします。

異なる名前空間の複数のサービスで同じ検出名を再利用した場合、このディメンションを使用して特定のサービスのインバウンドトラフィックメトリクスを確認できます。

実行中のコンテナ内の特定のポートには、複数の検出名を指定できることに注意してください。

`TargetDiscoveryName`

このディメンションは、トラフィックメトリクスをリクエストするデータを、すべての Amazon ECS クラスター全体の指定された Service Connect 検出名にフィルタリングします。

`DiscoveryName` とは異なり、このトラフィックメトリクスは、この名前空間に Service Connect 設定がある他の Amazon ECS タスクから送信される、この `DiscoveryName` へのインバウンドトラフィックのみを測定します。これには、クライアントのみ、またはクライアントとサーバーの Service Connect 設定を使用したサービスによって実行されるタスクが含まれます。

実行中のコンテナ内の特定のポートには、複数の検出名を指定できることに注意してください。

`TargetDiscoveryName, ServiceName, ClusterName`

このディメンションは、トラフィックメトリクスにリクエストしたデータを指定された Service Connect 検出名にフィルタリングしますが、このクラスター内のこのサービスによって作成されたタスクからのトラフィックのみをカウントします。

このディメンションを使用して、別のサービスの特定のクライアントからのインバウンドトラフィックメトリクスを確認できます。

`DiscoveryName, ServiceName, ClusterName` とは異なり、このトラフィックメトリクスは、この名前空間に Service Connect 設定がある他の Amazon ECS タスクから送信される、この `DiscoveryName` へのインバウンドトラフィックのみを測定します。これには、クライアントのみ、またはクライアントとサーバーの Service Connect 設定を使用したサービスによって実行されるタスクが含まれます。

実行中のコンテナ内の特定のポートには、複数の検出名を指定できることに注意してください。

AWS Fargate 使用状況メトリクス

CloudWatch 使用状況メトリクスを使用して、アカウントのリソースの使用状況を把握できます。これらのメトリクスを使用して、CloudWatch グラフやダッシュボードで現在のサービスの使用状況を可視化できます。

AWS Fargate 使用状況メトリクスは、AWS のサービスクォータに対応しています。使用量がサービスクォータに近づいたときに警告するアラームを設定することもできます。Fargate のサービスのクォータの詳細については、「AWS Fargate Service Quotas」を参照してください。

AWS Fargate は、AWS/Usage 名前空間に以下のメトリクスを公開します。

メトリクス	説明
ResourceCount	アカウントで実行されている指定されたリソースの合計数。リソースは、メトリクスに関連付けられたディメンションによって定義されます。

以下のディメンションは、AWS Fargate によって発行される使用状況メトリクスを絞り込むために使用されます。

ディメンション	説明
Service	リソースを含む AWS のサービスの名前。AWS Fargate 使用状況メトリクスの場合、このディメンションの値は Fargate です。
Type	レポートされるエンティティのタイプ。現在、AWS Fargate 使用状況メトリクスの有効な値は Resource のみです。
Resource	実行中のリソースタイプ。実行中のリソースタイプ。現在、AWS Fargate 使用状況メトリクスの有効な値は vCPU のみです。これは、実行中のインスタンスに関する情報を返します。
Class	追跡されているリソースのクラス。追跡されているリソースのクラス。Resource ディメンションの値として vCPU を使用する AWS Fargate 使用状況メトリクスの場合、有効な値は Standard/OnDemand と Standard/Spot です。

Service Quotas コンソールを使用することで、使用状況をグラフで可視化したり、AWS Fargate 使用量がサービスクォータに近づくと警告するアラームを設定したりできます。クォータ値のしきい値に近づいたときに通知する CloudWatch アラームを作成する方法については、「Service Quotas ユーザーガイド」の「Service Quotas と Amazon CloudWatch アラーム」を参照してください。

.

Amazon ECS クラスターの予約率メトリクス

クラスターの予約メトリクスは、クラスター内のアクティブな各コンテナインスタンスに登録された CPU、メモリ、GPUs に対する、クラスター内のすべての Amazon ECS タスクによって予約されている CPU、メモリ、GPUs の割合として測定されます。ステータスが ACTIVE または DRAINING であるコンテナインスタンスのみが、クラスター予約メトリクスに影響します。このメトリクスは、EC2 インスタンスでホストされるタスクまたはサービスを含むクラスターでのみサポートされています。AWS Fargate でタスクがホストされているクラスターではサポートされていません。

```
                              (Total CPU units reserved by tasks in cluster) x 100
Cluster CPU reservation =
 ---------------------------------------------------------------
                           (Total CPU units registered by container instances in
 cluster)
```

```
                                 (Total MiB of memory reserved by tasks in cluster x
 100)
Cluster memory reservation =
 ---------------------------------------------------------------------
                              (Total MiB of memory registered by container instances in
 cluster)
```

```
                                (Total GPUs reserved by tasks in cluster x 100)
Cluster GPU reservation =
 ---------------------------------------------------------------------
                              (Total GPUs registered by container instances in cluster)
```

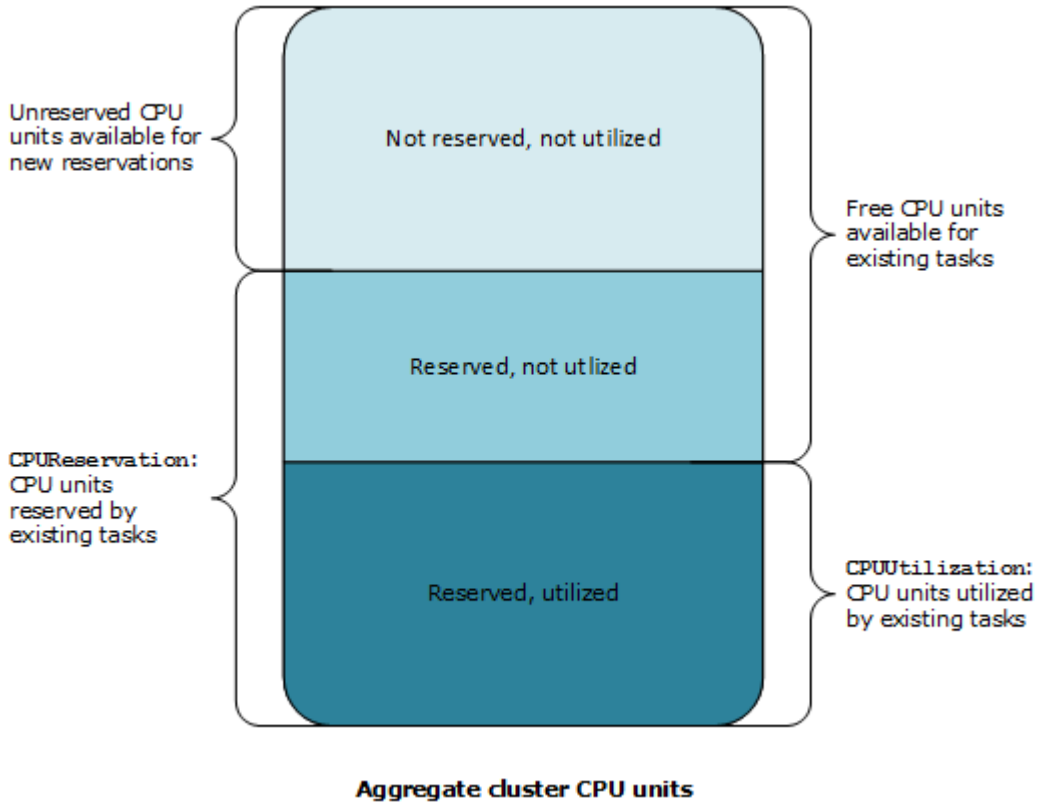
クラスターでタスクを実行すると、Amazon ECS はタスク定義を解析し、そのコンテナの定義で指定されている CPU ユニット、メモリ (MiB)、GPUs の合計を予約します。Amazon ECS は毎分、クラスター内で実行中の各タスクによって現在予約されている CPU ユニットの数、メモリ (MiB)、GPU の数を計算します。クラスター内で実行中のすべてのタスクによって予約されている CPU、メモリ、GPUs の合計が計算され、その数字がクラスターに登録されているリ

ソースの合計に対する割合として CloudWatch にレポートされます。タスク定義でソフト制限 (memoryReservation) を指定する場合、予約メモリの容量を計算するためにその制限が使用されます。それ以外の場合は、ハード制限 (memory) が使用されます。クラスター内のタスクによって予約されるメモリの合計 MiB には、一時ファイルシステム (tmpfs) のボリュームサイズが含まれます。タスク定義で定義されている場合、sharedMemorySize も含まれます。ハード制限とソフト制限、共有メモリサイズ、tmpfs ボリュームサイズの詳細については、「タスク定義パラメータ」を参照してください。

例えば、クラスターに 2 つのアクティブなコンテナインスタンス、c4.4xlarge インスタンスおよび c4.large インスタンスが登録されているとします。c4.4xlarge インスタンスは、CPU ユニット 16,384、メモリ 30,158 MiB でクラスターに登録されています。c4.large インスタンスは、CPU ユニット 2,048、メモリ 3,768 MiB で登録されています。このクラスターの合計リソースは、CPU ユニット 18,432、メモリ 33,926 MiB です。

このタスク定義により、1,024 CPU ユニットと 2,048 MiB のメモリが予約され、このクラスター内で 10 個のタスクが開始されている (その他のタスクが現在実行されていない) 場合、合計 10,240 CPU ユニットと 20,480 MiB のメモリが予約されています。この場合、クラスターについて CPU 予約率 55%、メモリ予約率 60% として CloudWatch にレポートされます。

以下の図では、クラスターに登録されている CPU ユニットの合計と、それらの予約率および使用率が既存のタスクおよび新規タスク配置にどのように影響するかを示しています。下段 (予約済み、使用中) および中段 (予約済み、未使用) ブロックは、クラスターで実行中の既存タスクで予約されている CPU ユニットの合計、または CPUReservation CloudWatch メトリクスを表しています。下段ブロックは、実行中のタスクがクラスターで実際に使用している予約 CPU ユニット、または CPUUtilization CloudWatch メトリクスを表しています。上段ブロックは既存のタスクによって予約されていない CPU ユニットを表します。これらの CPU ユニットを新しいタスクの配置に利用できます。既存タスクの CPU リソースを増やす必要がある場合に、これらの予約されていない CPU ユニットを使用することもできます。詳細については、「cpu」タスク定義パラメータのドキュメントを参照してください。



Amazon ECS クラスターの使用率メトリクス

クラスター使用率メトリクスは CPU、メモリのほか、タスクに EBS ボリュームがアタッチされている場合は EBS ファイルシステムの使用率にも使用できます。このメトリクスは、Amazon EC2 インスタンスでホストされるタスクまたはサービスを含むクラスターでのみサポートされています。AWS Fargate でタスクがホストされているクラスターではサポートされていません。

Amazon ECS クラスターレベルの CPU とメモリの使用率メトリクス

CPU とクラスターの使用率は、クラスターに登録されたアクティブな Amazon EC2 インスタンスのそれぞれに登録された CPU とメモリの合計に対する、クラスター上のすべてのタスクによって使用されている CPU とメモリの割合で測定されます。`ACTIVE` または `DRAINING` ステータスの Amazon EC2 インスタンスのみが、クラスター使用率メトリクスに影響します。

```
                                (Total CPU units used by tasks in cluster) x 100
Cluster CPU utilization =
 ------------------------------------------------------------------
                           (Total CPU units registered by container instances in
 cluster)
```

```
                                    (Total MiB of memory used by tasks in cluster x
 100)
Cluster memory utilization =
 ------------------------------------------------------------------
                              (Total MiB of memory registered by container instances in
 cluster)
```

各 Amazon EC2 コンテナインスタンスの Amazon ECS エージェントは毎分、Amazon EC2 インスタンスで実行中の各タスクで現在使用されている CPU ユニット数とメモリの MiB を計算し、この情報は Amazon ECS にレポートされます。クラスターで実行中のすべてのタスクで使用されている CPU とメモリの合計が計算され、その数字がクラスターの予約リソースの合計に対する比率として CloudWatch にレポートされます。

例えば、クラスターに 2 つのアクティブな Amazon EC2 インスタンス、`c4.4xlarge` インスタンスと `c4.large` インスタンスが登録されているとします。`c4.4xlarge` インスタンスは、CPU ユニット数 `16,384`、メモリ `30,158` MiB でクラスターに登録されています。`c4.large` インスタンスは、CPU ユニット数 `2,048`、メモリ `3,768` MiB で登録されています。このクラスターの合計リソースは、CPU ユニット数 `18,432`、メモリ `33,926` MiB です。

このクラスターで 10 個のタスクが実行中で、各タスクが `1,024` CPU ユニットとメモリ `2,048` MiB を消費する場合、クラスターでは合計で `10,240` CPU ユニットとメモリ `20,480` MiB が使用されます。この場合、クラスターについて CPU 使用率 55%、メモリ使用率 60% として CloudWatch にレポートされます。

Amazon ECS クラスターレベルの Amazon EBS ファイルシステムの使用率

クラスターレベルの EBS ファイルシステム使用率メトリクスは、クラスターで実行されているタスクによって使用されている EBS ファイルシステムの合計を、クラスター内のすべてのタスクに割り当てられた EBS ファイルシステムストレージの合計で割った値で測定されます。

```
                                       (Total GB of EBS filesystem used by tasks in
 cluster x 100)
Cluster EBS filesystem utilization =
 ---------------------------------------------------------------
                                       (Total GB of EBS filesystem allocated to tasks
 in cluster)
```

Amazon ECS サービスの使用率メトリクス

サービス使用率メトリクスは CPU、メモリのほか、タスクに EBS ボリュームがアタッチされている場合は EBS ファイルシステムの使用率にも使用できます。サービスレベルのメトリクスは、Amazon EC2 インスタンスと Fargate の両方でタスクをホストするサービスでサポートされています。

サービスレベルの CPU とメモリの使用率

CPU とメモリの使用率は、サービスのタスク定義で指定された CPU とメモリに対する、クラスターのサービスに属する Amazon ECS タスクによって使用されている CPU とメモリの割合で測定されます。

```
                                    (Total CPU units used by tasks in service) x 100
Service CPU utilization =
 ------------------------------------------------------------------------------
                          (Total CPU units specified in task definition) x (number of
 tasks in service)
```

```
                                     (Total MiB of memory used by tasks in service) x
 100
Service memory utilization =
 ---------------------------------------------------------------------------------
                               (Total MiB of memory specified in task definition) x
 (number of tasks in service)
```

Amazon ECS コンテナエージェントは毎分、サービスが所有するタスクのそれぞれで現在使用されている CPU ユニット数とメモリの MiB を計算し、この情報は Amazon ECS にレポートされます。クラスターで実行中のサービスが所有するすべてのタスクで使用されている CPU とメモリの合計が計算され、その数字がサービスのタスク定義でサービス用に指定されたリソースの合計に対する比率として CloudWatch にレポートされます。ソフト制限 (`memoryReservation`) を指定した場合、予約メモリの容量を計算するためにその制限が使用されます。それ以外の場合は、ハード制限 (`memory`) が使用されます。ハードリミットとソフトリミットの詳細については、「タスクサイズ」を参照してください。

例えば、サービスのタスク定義で 512 CPU ユニットおよび 1,024 MiB のメモリを (ハードリミットの `memory` パラメータとともに) コンテナ全体で指定しているとします。サービスの実行タスクの必要数は 1 であり、1 つの `c4.large` コンテナインスタンス (2,048 CPU ユニット、3,768 MiB の合計メモリ) を使用してクラスターで実行されます。また、クラスターで実行されている他のタスクはあ

りません。タスクは 512 CPU ユニットを指定していますが、2,048 CPU ユニットを搭載したコンテナインスタンスで唯一実行されているタスクであるため、指定した量の 4 倍 (2,048/512) まで使用できます。ただし、指定した 1,024 MiB のメモリはハード制限であり、それを超えることはできません。したがってこの場合、サービスのメモリ使用率は 100% を超えることはできません。

前の例で、ハードリミットの `memory` パラメータの代わりにソフト制限の `memoryReservation` を使用した場合、サービスのタスクでは、必要に応じて指定された 1,024 MiB を超えるメモリを使用できます。この場合、サービスのメモリ使用率が 100% を超える可能性があります。

アプリケーションのメモリ使用率が短時間で突然急上昇した場合、Amazon ECS は毎分複数のデータポイントを収集し、CloudWatch に送信される 1 つのデータポイントに集約するため、サービスメモリ使用率の増加を見ることがありません。

このタスクが一定期間中に CPU 負荷の高い作業を実行し、使用可能な 2,048 CPU ユニットすべてと 512 MiB のメモリを使用している場合、サービスからは CPU 使用率 400%、メモリ使用率 50% としてレポートされます。タスクがアイドル状態で 128 CPU ユニットおよび 128 MiB のメモリを使用している場合、サービスからは CPU 使用率 25%、メモリ使用率 12.5% としてレポートされます。

> **Note**
>
> この例では、CPU 単位がコンテナレベルで定義されている場合に、CPU 使用率が 100% を超えるだけです。タスク・レベルで CPU ユニットを定義した場合、使用率は定義されたタスク・レベルの制限を超えません。

サービスレベルの EBS ファイルシステム使用率

サービスレベルの EBS ファイルシステムの使用率は、サービスに属するタスクによって使用されている EBS ファイルシステムの合計を、サービスに属するすべてのタスクに割り当てられている EBS ファイルシステムストレージの合計で割った値で測定されます。

```
                                    (Total GB of EBS filesystem used by tasks in the
 service x 100)
Service EBS filesystem utilization =
 ------------------------------------------------------------------
                                    (Total GB of EBS filesystem allocated to tasks
 in the service)
```

サービスの **RUNNING** タスク数

CloudWatch メトリクスを使用して、RUNNING 状態のサービス内のタスク数を表示できます。例えば、このメトリクスに CloudWatch アラームを設定して、サービスで実行中のタスクの数が指定された値を下回った場合にアラートを送信できます。

Amazon ECS CloudWatch Container Insights のサービス **RUNNING** タスク数

Amazon ECS CloudWatch Container Insights を使用すると、[Number of Running Tasks] (実行中のタスクの数) (`RunningTaskCount`) メトリクスがクラスターごとおよびサービスごとに利用できます。Container Insights は、`containerInsights` アカウント設定にオプトインして作成された新しいすべてのクラスターで、またはクラスター作成時にクラスター設定を有効にすることで個々のクラスターで、または UpdateClusterSettings API を使用して既存のクラスターで、使用できます。CloudWatch Container インサイトによって収集されたメトリクスは、カスタムメトリクスとして課金されます。CloudWatch の料金の詳細については、 CloudWatch の料金をご覧ください。

このメトリクスを表示するには、「Amazon CloudWatch ユーザーガイド」の「Amazon ECS Container Insights のメトリクス」を参照してください。

EventBridge を使用して Amazon ECS エラーへの対応を自動化する

Amazon EventBridge を使用すると、AWS のサービスを自動化して、アプリケーションの可用性の問題やリソース変更といったシステムイベントに自動的に対応できます。AWS のサービスからのイベントは、ほぼリアルタイムに EventBridge に提供されます。どのイベントに興味があるのか、イベントがルールに一致した場合にどのように自動的に実行するアクションをとるのか簡単なルールを指定して書き込みすることができます。自動的に設定できるオペレーションには、以下が含まれます。

- CloudWatch Logs のロググループへのイベントの追加
- AWS Lambda 関数の呼び出し
- Amazon EC2 Run Command の呼び出し
- Amazon Kinesis Data Streams へのイベントの中継
- AWS Step Functions ステートマシンのアクティブ化
- Amazon SNS トピックまたは Amazon Simple Queue Service (Amazon SQS) キューに通知する

詳細については、「Amazon EventBridge ユーザーガイド」の「Getting started with Amazon EventBridge」を参照してください。

Amazon ECS の Eventbridge イベントを使用して、Amazon ECS クラスターの現在の状態に関するほぼリアルタイムの通知を受け取ることができます。タスクで EC2 起動タイプを使用している場合は、コンテナインスタンスと、それらのコンテナインスタンスで実行中のすべてのタスクの現在の状態の両方の状態を確認できます。タスクで Fargate 起動タイプを使用している場合、コンテナインスタンスの状態を確認できます。

Eventbridge を使用して Amazon ECS 上にカスタムスケジューラを構築し、クラスター間のタスクを調整するとともに、クラスターの状態をほぼリアルタイムにモニタリングできます。Amazon ECS サービス に対して Amazon ECS 状態の変更を絶え間なくポーリングするスケジューリングおよびモニタリングのコードをなくし、代わりに、Eventbridge ターゲットを使用して非同期的に状態の変更に対応できます。ターゲットには、AWS Lambda、Amazon Simple Queue Service、Amazon Simple Notification Service、Amazon Kinesis Data Streams

Amazon ECS イベントストリームは、イベントごとに少なくとも 1 回必ず送信されます。重複したイベントが送信された場合、イベントには重複を識別できるだけの十分な情報が備わっています。詳細については、「Amazon ECS イベントの処理」を参照してください。

イベントは相対的な順番になっているため、特定のイベントがいつ発生したかは、他のイベントとの前後関係から簡単に判断できます。

トピック

Amazon ECS イベント

Amazon ECS は、各タスクとサービスの状態を追跡します。タスクやサービスの状態が変わると、イベントが生成され、Amazon EventBridge に送信されます。これらのイベントは、タスク状態変更イベントおよびサービスアクションイベントとして分類されます。各イベントとその考えられる原因については、以下のセクションで詳しく説明します。

Amazon ECS は、コンテナインスタンスの状態変更イベント、タスク状態変更イベント、サービスアクション、サービスデプロイ状態変更イベントというイベントタイプを生成し、EventBridge に送信します。

- コンテナインスタンス状態変更
- タスク状態変更

- デプロイの状態変更
- サービスアクション

> **Note**
>
> 今後、Amazon ECS には他の種類のイベント、ソース、詳細が追加される場合があります。コードのイベント JSON データを逆シリアル化する場合は、不明なプロパティが追加されたときに問題が発生しないように、アプリケーションが不明なプロパティに対応できるようにしてください。

同じアクティビティに対して複数のイベントが生成される場合もあります。例えば、コンテナインスタンスでタスクが開始されると、この新しいタスクに対してタスク状態変更イベントが生成されます。コンテナインスタンスの使用可能なリソース (CPU、メモリ、使用可能なポートなど) の変更に対応するため、コンテナインスタンス状態変更イベントがアカウントに生成されます。同様に、コンテナインスタンスが終了すると、コンテナインスタンス、コンテナエージェント接続ステータス、およびコンテナインスタンスで実行されている各タスクに対してイベントが生成されます。

コンテナ状態変更イベントとタスク状態変更イベントには 2 つの `version` フィールドがあります。1 つはイベントの本体で、もう 1 つはイベントの `detail` オブジェクトです。次に、これら 2 つのフィールドの違いについて説明します。

- イベントの本文の `version` フィールドは、すべてのイベントで `0` に設定されています。EventBridge パラメータの詳細については、「Amazon EventBridge ユーザーガイド」の「AWSサービスイベントメタデータ」を参照してください。
- イベントの `detail` オブジェクトの `version` フィールドは、関連付けられているリソースのバージョンについて説明します。リソースの状態が変わるたびに、このバージョンはインクリメントされます。イベントは複数回送信できるため、このフィールドで重複するイベントを識別できます。重複するイベントには、`detail` オブジェクト内で同じバージョンがあります。EventBridge で Amazon ECS コンテナインスタンスおよびタスク状態をレプリケートする場合は、Amazon ECS API によって報告されるリソースのバージョンとそのリソースについて EventBridge で報告されるバージョン (`detail` オブジェクト内) を比較して、イベントストリームでのバージョンが最新であることを確認できます。

サービスアクションイベントには、本体の `version` フィールドのみが含まれます。

サービスアクションイベントは、次の 2 つの異なるフィールドでサービスを指定します。

- `create-service` が生成したイベントの場合、サービスは `serviceName` フィールドに設定されます。
- `update-service` が生成したイベントの場合、サービスは `service` フィールドに設定されます。

サービスイベントを自動化ツールで処理する場合、両方のフィールドをコーディングする必要があります。

サービスアクションイベントのルールを作成する方法については、「Amazon ECS サービスアクションイベント」を参照してください。

Amazon ECS と EventBridge を統合する方法に関する追加情報については、「Amazon EventBridge と Amazon ECS の統合」を参照してください。

Amazon ECS コンテナインスタンス状態変更イベント

以下の場合は、コンテナインスタンス状態変更イベントが発生します。

ユーザーが `StartTask`、`RunTask`、`StopTask` API オペレーションを直接または AWS Management Console や SDKs 経由で呼び出します。

コンテナインスタンスでタスクを配置または停止すると、コンテナインスタンスの使用可能なリソース (CPU、メモリ、使用可能なポートなど) が変更されます。

Amazon ECS サービススケジューラがタスクを開始または停止する。

コンテナインスタンスでタスクを配置または停止すると、コンテナインスタンスの使用可能なリソース (CPU、メモリ、使用可能なポートなど) が変更されます。

`SubmitTaskStateChange`Amazon ECSコンテナエージェントは、目的の`RUNNING`ステータスがタスクの`STOPPED`ステータスでAPIオペレーションを呼び出します。

Amazon ECS コンテナエージェントは、コンテナインスタンスでタスクの状態をモニタリングし、状態に変更があるとレポートします。`RUNNING` であるべきタスクが `STOPPED` に変わると、エージェントは停止したタスクに割り当てられているリソース (CPU、メモリ、使用可能なポートなど) を解放します。

ユーザーが `DeregisterContainerInstance` API オペレーションを使用してコンテナインスタンスを直接または AWS Management Console や SDKs 経由で登録解除します。

コンテナインスタンスを登録解除すると、コンテナインスタンスのステータスと Amazon ECS コンテナエージェントの接続ステータスが変更されます。

EC2 インスタンスの停止に伴ってタスクが停止されました。

コンテナインスタンスを停止すると、このコンテナインスタンスで実行されているタスクのステータスは `STOPPED` に変わります。

Amazon ECS コンテナエージェントがコンテナインスタンスを初めて登録します。

Amazon ECS コンテナエージェントで初めてコンテナインスタンスを (起動時または手動による初回起動時に) 登録するときに、インスタンスの状態変更イベントが作成されます。

Amazon ECS コンテナエージェントが、Amazon ECS と接続または接続解除する。

Amazon ECS コンテナエージェントが Amazon ECS バックエンドと接続または接続解除すると、コンテナインスタンスの `agentConnected` ステータスが変わります。

> **Note**
>
> Amazon ECS コンテナエージェントは、通常の操作の一環として、1 時間に数回切断して再接続するため、エージェントの接続イベントが予期されます。これらのイベントは、コンテナエージェントまたはコンテナインスタンスに問題があることを示すものではありません。

インスタンスの Amazon ECS コンテナエージェントをアップグレードします。

コンテナインスタンスの詳細には、コンテナエージェントバージョンのオブジェクトが含まれています。エージェントをアップグレードすると、このバージョン情報が変わり、イベントが発生します。

Example コンテナインスタンス状態変更イベント

コンテナインスタンスの状態変更イベントは、次の形式で配信されます。以下の `detail` セクションは、「Amazon Elastic Container Service API リファレンス」の DescribeContainerInstances API オペレーションから返される ContainerInstance オブジェクトに似ています。EventBridge パラメータの詳細については、「Amazon EventBridge ユーザーガイド」の「AWSサービスイベントメタデータ」を参照してください。

```
{
  "version": "0",
  "id": "8952ba83-7be2-4ab5-9c32-6687532d15a2",
  "detail-type": "ECS Container Instance State Change",
  "source": "aws.ecs",
```

```
  "account": "111122223333",
  "time": "2016-12-06T16:41:06Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ecs:us-east-1:111122223333:container-instance/
b54a2a04-046f-4331-9d74-3f6d7f6ca315"
  ],
  "detail": {
    "agentConnected": true,
    "attributes": [
      {
        "name": "com.amazonaws.ecs.capability.logging-driver.syslog"
      },
      {
        "name": "com.amazonaws.ecs.capability.task-iam-role-network-host"
      },
      {
        "name": "com.amazonaws.ecs.capability.logging-driver.awslogs"
      },
      {
        "name": "com.amazonaws.ecs.capability.logging-driver.json-file"
      },
      {
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.17"
      },
      {
        "name": "com.amazonaws.ecs.capability.privileged-container"
      },
      {
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.18"
      },
      {
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.19"
      },
      {
        "name": "com.amazonaws.ecs.capability.ecr-auth"
      },
      {
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.20"
      },
      {
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.21"
      },
      {
```

```
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.22"
      },
      {
        "name": "com.amazonaws.ecs.capability.docker-remote-api.1.23"
      },
      {
        "name": "com.amazonaws.ecs.capability.task-iam-role"
      }
    ],
    "clusterArn": "arn:aws:ecs:us-east-1:111122223333:cluster/default",
    "containerInstanceArn": "arn:aws:ecs:us-east-1:111122223333:container-instance/
b54a2a04-046f-4331-9d74-3f6d7f6ca315",
    "ec2InstanceId": "i-f3a8506b",
    "registeredResources": [
      {
        "name": "CPU",
        "type": "INTEGER",
        "integerValue": 2048
      },
      {
        "name": "MEMORY",
        "type": "INTEGER",
        "integerValue": 3767
      },
      {
        "name": "PORTS",
        "type": "STRINGSET",
        "stringSetValue": [
          "22",
          "2376",
          "2375",
          "51678",
          "51679"
        ]
      },
      {
        "name": "PORTS_UDP",
        "type": "STRINGSET",
        "stringSetValue": []
      }
    ],
    "remainingResources": [
      {
        "name": "CPU",
```

```
        "type": "INTEGER",
        "integerValue": 1988
      },
      {
        "name": "MEMORY",
        "type": "INTEGER",
        "integerValue": 767
      },
      {
        "name": "PORTS",
        "type": "STRINGSET",
        "stringSetValue": [
          "22",
          "2376",
          "2375",
          "51678",
          "51679"
        ]
      },
      {
        "name": "PORTS_UDP",
        "type": "STRINGSET",
        "stringSetValue": []
      }
    ],
    "status": "ACTIVE",
    "version": 14801,
    "versionInfo": {
      "agentHash": "aebcbca",
      "agentVersion": "1.13.0",
      "dockerVersion": "DockerVersion: 1.11.2"
    },
    "updatedAt": "2016-12-06T16:41:06.991Z"
  }
}
```

Amazon ECS タスク状態変更イベント

以下の場合は、タスク状態変更イベントが発生します。

ユーザーが StartTask、RunTask、StopTask API オペレーションを直接または AWS Management Console、AWS CLI、SDKs 経由で呼び出します。

タスクを開始または停止すると、新しいタスクリソースが作成されるか、既存のタスクリソースの状態が変更されます。

Amazon ECS サービススケジューラがタスクを開始または停止する。

タスクを開始または停止すると、新しいタスクリソースが作成されるか、既存のタスクリソースの状態が変更されます。

Amazon ECS コンテナエージェントが SubmitTaskStateChange API オペレーションを呼び出す。

Amazon EC2 起動タイプでは、Amazon ECS コンテナエージェントは、コンテナインスタンス上のタスクの状態をモニタリングします。Amazon ECS コンテナエージェントは、状態に変更があるとレポートします。状態の変更には、PENDING から RUNNING または RUNNING から STOPPED への変更が含まれます。

ユーザーが、DeregisterContainerInstance API オペレーションと force フラグを直接または AWS Management Console や SDKs. 経由で使用して、基盤となるコンテナインスタンスの登録解除を強制します。

コンテナインスタンスを登録解除すると、コンテナインスタンスのステータスと Amazon ECS コンテナエージェントの接続ステータスが変更されます。コンテナインスタンスでタスクが実行されている場合、登録解除を許可するには force フラグを設定する必要があります。これにより、インスタンスのすべてのタスクが停止します。

基盤となるコンテナインスタンスが停止または終了する。

コンテナインスタンスを停止または終了すると、このコンテナインスタンスで実行されているタスクのステータスは STOPPED に変わります。

タスクのコンテナの状態が変わる。

Amazon ECS コンテナエージェントは、タスク内のコンテナの状態をモニタリングします。例えば、タスク内で実行されているコンテナが停止すると、このコンテナの状態変更に伴ってイベントが生成されます。

Fargate Spot キャパシティープロバイダーを使用するタスクは、終了通知を受け取ります。

タスクが FARGATE_SPOT キャパシティープロバイダーを使用していて、スポットの中断により停止すると、タスク状態変更イベントが生成されます。

Example タスク状態変更イベント

タスク状態変更イベントは、次の形式で配信されます。以下の `detail` セクションは、「Amazon Elastic Container Service API リファレンス」の DescribeTasks API オペレーションから返される Task オブジェクトに似ています。コンテナが Amazon ECR でホストされているイメージを使用している場合は、`imageDigest` フィールドが返されます。

> **Note**
>
> `createdAt`、`connectivityAt`、`pullStartedAt`、`startedAt`、`pullStoppedAt`、`updatedAt` の各フィールド値は、`DescribeTasks` アクションのレスポンスでは UNIX タイムスタンプであり、タスク状態変更イベントでは ISO 文字列タイムスタンプです。

EventBridge パラメータの詳細については、「Amazon EventBridge ユーザーガイド」の「AWSサービスイベントメタデータ」を参照してください。

必須コンテナのいずれかが終了したためにタスクの実行が停止した場合に限りタスクイベントをキャプチャする、Amazon EventBridge イベントルールを設定する方法の詳細については、「Amazon ECS タスク停止イベントに関する Amazon Simple Notification Service アラートの送信」を参照してください。

```
{
    "version": "0",
    "id": "3317b2af-7005-947d-b652-f55e762e571a",
    "detail-type": "ECS Task State Change",
    "source": "aws.ecs",
    "account": "111122223333",
    "time": "2020-01-23T17:57:58Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecs:us-west-2:111122223333:task/FargateCluster/
c13b4cb40f1f4fe4a2971f76ae5a47ad"
    ],
    "detail": {
        "attachments": [
            {
                "id": "1789bcae-ddfb-4d10-8ebe-8ac87ddba5b8",
                "type": "eni",
                "status": "ATTACHED",
                "details": [
```

```
                    {
                        "name": "subnetId",
                        "value": "subnet-abcd1234"
                    },
                    {
                        "name": "networkInterfaceId",
                        "value": "eni-abcd1234"
                    },
                    {
                        "name": "macAddress",
                        "value": "0a:98:eb:a7:29:ba"
                    },
                    {
                        "name": "privateIPv4Address",
                        "value": "10.0.0.139"
                    }
                ]
            }
        ],
        "availabilityZone": "us-west-2c",
        "clusterArn": "arn:aws:ecs:us-west-2:111122223333:cluster/FargateCluster",
        "containers": [
            {
                "containerArn": "arn:aws:ecs:us-west-2:111122223333:container/
cf159fd6-3e3f-4a9e-84f9-66cbe726af01",
                "lastStatus": "RUNNING",
                "name": "FargateApp",
                "image": "111122223333.dkr.ecr.us-west-2.amazonaws.com/hello-
repository:latest",
                "imageDigest":
 "sha256:74b2c688c700ec95a93e478cdb959737c148df3fbf5ea706abe0318726e885e6",
                "runtimeId":
 "ad64cbc71c7fb31c55507ec24c9f77947132b03d48d9961115cf24f3b7307e1e",
                "taskArn": "arn:aws:ecs:us-west-2:111122223333:task/FargateCluster/
c13b4cb40f1f4fe4a2971f76ae5a47ad",
                "networkInterfaces": [
                    {
                        "attachmentId": "1789bcae-ddfb-4d10-8ebe-8ac87ddba5b8",
                        "privateIpv4Address": "10.0.0.139"
                    }
                ],
                "cpu": "0"
            }
        ],
```

```
        "createdAt": "2020-01-23T17:57:34.402Z",
        "launchType": "FARGATE",
        "cpu": "256",
        "memory": "512",
        "desiredStatus": "RUNNING",
        "group": "family:sample-fargate",
        "lastStatus": "RUNNING",
        "overrides": {
            "containerOverrides": [
                {
                    "name": "FargateApp"
                }
            ]
        },
        "connectivity": "CONNECTED",
        "connectivityAt": "2020-01-23T17:57:38.453Z",
        "pullStartedAt": "2020-01-23T17:57:52.103Z",
        "startedAt": "2020-01-23T17:57:58.103Z",
        "pullStoppedAt": "2020-01-23T17:57:55.103Z",
        "updatedAt": "2020-01-23T17:57:58.103Z",
        "taskArn": "arn:aws:ecs:us-west-2:111122223333:task/FargateCluster/
c13b4cb40f1f4fe4a2971f76ae5a47ad",
        "taskDefinitionArn": "arn:aws:ecs:us-west-2:111122223333:task-definition/
sample-fargate:1",
        "version": 4,
        "platformVersion": "1.3.0"
    }
}
```

Amazon ECS サービスアクションイベント

Amazon ECS は、詳細タイプ ECS サービスアクションのサービスアクションイベントを送信します。コンテナインスタンスおよびタスク状態変更イベントとは異なり、サービスアクションイベントの `details` レスポンスフィールドにバージョン番号は含まれません。次に、Amazon ECS サービス アクションイベントの EventBridge ルールを作成するために使用されるイベントパターンを示します。詳細については、「Amazon EventBridge ユーザーガイド」の「Getting started with EventBridge」を参照してください。

```
{
    "source": [
        "aws.ecs"
    ],
```

```
    "detail-type": [
        "ECS Service Action"
    ]
}
```

Amazon ECS は、INFO、WARN、ERROR イベントタイプのイベントを送信します。以下はサービスアクションイベントです。

INFO イベントタイプのサービスアクションイベント

SERVICE_STEADY_STATE

サービスは正常であり、目的のタスクの数であるため、安定した状態に達します。サービススケジューラは定期的にステータスを報告するため、このメッセージを複数回受信する場合があります。

TASKSET_STEADY_STATE

タスクセットは正常で、目的のタスクの数であるため、定常状態に達します。

CAPACITY_PROVIDER_STEADY_STATE

サービスに関連付けられたキャパシティープロバイダーが定常状態に達します。

SERVICE_DESIRED_COUNT_UPDATED

サービススケジューラが、サービスまたはタスクセットに対して計算された目的のカウントを更新するとき。このイベントは、目的のカウントがユーザーによって手動で更新されるときには送信されません。

TASKS_STOPPED

サービスが実行中のタスクを停止しました。

SERVICE_DEPLOYMENT_IN_PROGRESS

サービスデプロイが進行中です。サービスデプロイは、ロールバックまたは新しいサービスリビジョンのいずれかです。

SERVICE_DEPLOYMENT_COMPLETED

サービスデプロイが定常状態であり、完了しています。サービスデプロイは、ロールバック、または更新されたサービスリビジョンのデプロイのいずれかです。

WARN イベントタイプのサービスアクションイベント

SERVICE_TASK_START_IMPAIRED

サービスは一貫してタスクを正常に起動することができません。

SERVICE_DISCOVERY_INSTANCE_UNHEALTHY

サービス検出を使用するサービスに、異常なタスクが含まれています。サービススケジューラは、サービスレジストリ内のタスクが正常でないことを検出します。

VPC_LATTICE_TARGET_UNHEALTHY

VPC Lattice を使用するサービスが、VPC Lattice のターゲットの 1 つに異常を検出しました。

ERROR イベントタイプのサービスアクションイベント

SERVICE_DAEMON_PLACEMENT_CONSTRAINT_VIOLATED

DAEMON サービススケジューラ戦略を使用するサービス内のタスクは、サービスの配置制約戦略を満たさなくなりました。

ECS_OPERATION_THROTTLED

Amazon ECS API スロットルの制限により、サービススケジューラが調整されました。

SERVICE_DISCOVERY_OPERATION_THROTTLED

AWS Cloud Map API スロットルの制限により、サービススケジューラが調整されました。これは、サービス検出を使用するように設定されたサービスで発生する可能性があります。

SERVICE_TASK_PLACEMENT_FAILURE

サービススケジューラがタスクを配置できません。原因は、reason フィールドに説明されます。

このサービスイベントが生成される一般的な原因は、タスクを配置するためのクラスターでリソースが不足しているためです。例えば、使用可能なコンテナインスタンスに CPU またはメモリ容量が不足しているか、使用可能なコンテナインスタンスがない場合などです。もう 1 つの一般的な原因は、Amazon ECS コンテナエージェントがコンテナインスタンスで切断され、スケジューラがタスクを配置できない場合です。

SERVICE_TASK_CONFIGURATION_FAILURE

設定エラーのため、サービススケジューラがタスクを配置できません。原因は、reason フィールドに説明されます。

このサービスイベントが生成される一般的な原因は、タグがサービスに適用されてはいるが、ユーザーまたはロールがリージョンで新しい Amazon リソースネーム (ARN) 形式にオプトインしていないためです。詳細については、「Amazon リソースネーム (ARN) と ID」を参照してください。もう 1 つの一般的な原因は、Amazon ECS が提供されたタスク IAM ロールを継承できなかったことです。

`SERVICE_HEALTH_UNKNOWN`

サービスがタスクのヘルスデータを記述できませんでした。

`SERVICE_DEPLOYMENT_FAILED`

サービスデプロイが定常状態に達しませんでした。これは、CloudWatch がトリガーされたとき、またはサーキットブレーカーがサービスデプロイの失敗を検出したときに発生します。

Example サービス定常状態イベント

サービス定常状態イベントは、次の形式で配信されます。EventBridge パラメータの詳細については、「Amazon EventBridge ユーザーガイド」の「EventBridge イベント」を参照してください。

```
{
    "version": "0",
    "id": "af3c496d-f4a8-65d1-70f4-a69d52e9b584",
    "detail-type": "ECS Service Action",
    "source": "aws.ecs",
    "account": "111122223333",
    "time": "2019-11-19T19:27:22Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
    ],
    "detail": {
        "eventType": "INFO",
        "eventName": "SERVICE_STEADY_STATE",
        "clusterArn": "arn:aws:ecs:us-west-2:111122223333:cluster/default",
        "createdAt": "2019-11-19T19:27:22.695Z"
    }
}
```

Example キャパシティープロバイダー定常状態イベント

キャパシティプロバイダーの定常状態イベントは、次の形式で配信されます。

```
{
    "version": "0",
    "id": "b9baa007-2f33-0eb1-5760-0d02a572d81f",
    "detail-type": "ECS Service Action",
    "source": "aws.ecs",
    "account": "111122223333",
    "time": "2019-11-19T19:37:00Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
    ],
    "detail": {
        "eventType": "INFO",
        "eventName": "CAPACITY_PROVIDER_STEADY_STATE",
        "clusterArn": "arn:aws:ecs:us-west-2:111122223333:cluster/default",
        "capacityProviderArns": [
            "arn:aws:ecs:us-west-2:111122223333:capacity-provider/ASG-tutorial-
capacity-provider"
        ],
        "createdAt": "2019-11-19T19:37:00.807Z"
    }
}
```

Example サービスタスク開始障害イベント

サービスタスク開始障害イベントは、次の形式で配信されます。

```
{
    "version": "0",
    "id": "57c9506e-9d21-294c-d2fe-e8738da7e67d",
    "detail-type": "ECS Service Action",
    "source": "aws.ecs",
    "account": "111122223333",
    "time": "2019-11-19T19:55:38Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
    ],
    "detail": {
        "eventType": "WARN",
        "eventName": "SERVICE_TASK_START_IMPAIRED",
        "clusterArn": "arn:aws:ecs:us-west-2:111122223333:cluster/default",
        "createdAt": "2019-11-19T19:55:38.725Z"
```

```
    }
}
```

Example サービスタスク配置失敗イベント

サービスタスク配置失敗イベントは、次の形式で配信されます。詳細については、「Amazon EventBridge ユーザーガイド」の「EventBridge イベント」を参照してください。

次の例では、タスクは FARGATE_SPOT キャパシティープロバイダーを使用しようとしましたが、サービススケジューラは Fargate Spot キャパシティーを取得できませんでした。

```
{
    "version": "0",
    "id": "ddca6449-b258-46c0-8653-e0e3a6d0468b",
    "detail-type": "ECS Service Action",
    "source": "aws.ecs",
    "account": "111122223333",
    "time": "2019-11-19T19:55:38Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
    ],
    "detail": {
        "eventType": "ERROR",
        "eventName": "SERVICE_TASK_PLACEMENT_FAILURE",
        "clusterArn": "arn:aws:ecs:us-west-2:111122223333:cluster/default",
        "capacityProviderArns": [
            "arn:aws:ecs:us-west-2:111122223333:capacity-provider/FARGATE_SPOT"
        ],
        "reason": "RESOURCE:FARGATE",
        "createdAt": "2019-11-06T19:09:33.087Z"
    }
}
```

次の EC2 起動タイプの例では、コンテナインスタンス 2dd1b186f39845a584488d2ef155c131 でタスクを起動しようとしたが、CPU が不十分なため、サービススケジューラがタスクを実行できませんでした。

```
{
  "version": "0",
  "id": "ddca6449-b258-46c0-8653-e0e3a6d0468b",
  "detail-type": "ECS Service Action",
```

```
  "source": "aws.ecs",
  "account": "111122223333",
  "time": "2019-11-19T19:55:38Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
  ],
  "detail": {
    "eventType": "ERROR",
    "eventName": "SERVICE_TASK_PLACEMENT_FAILURE",
    "clusterArn": "arn:aws:ecs:us-west-2:111122223333:cluster/default",
    "containerInstanceArns": [
    "arn:aws:ecs:us-west-2:111122223333:container-instance/
default/2dd1b186f39845a584488d2ef155c131"
    ],
    "reason": "RESOURCE:CPU",
    "createdAt": "2019-11-06T19:09:33.087Z"
  }
}
```

Amazon ECS サービスデプロイ状態変更イベント

Amazon ECS は、詳細タイプの [ECS Deployment State Change] を使用してサービスデプロイ状態変更イベントを送信します。以下は、Amazon ECS サービスデプロイ状態変更イベントの Eventbridgeルールを作成するために使用されるイベントパターンです。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「Amazon EventBridge の開始方法」を参照してください。

```
{
    "source": [
        "aws.ecs"
    ],
    "detail-type": [
        "ECS Deployment State Change"
    ]
}
```

Amazon ECS は、INFO、と ERROR イベントタイプのイベントを送信します。次に、サービスデプロイ状態の変更イベントを示します。

`SERVICE_DEPLOYMENT_IN_PROGRESS`

サービスデプロイは進行中です。このイベントは、初期デプロイとロールバックデプロイの両方で送信されます。

`SERVICE_DEPLOYMENT_COMPLETED`

サービスのデプロイが完了しました。このイベントは、デプロイ後にサービスが定常状態になると、送信されます。

`SERVICE_DEPLOYMENT_FAILED`

サービスのデプロイに失敗しました。このイベントは、デプロイサーキットブレーカーロジックが有効になっているサービスに対して送信されます。

Example サービスデプロイ進行中イベント

サービスデプロイ進行中イベントは、初期デプロイとロールバックデプロイの両方の開始時に配信されます。両者の違いは `reason` フィールドにあります。EventBridge パラメータの詳細については、「Amazon EventBridge ユーザーガイド」の「AWS サービスイベントメタデータ」を参照してください。

次に、初期デプロイが開始された場合の出力例を示します。

```
{
   "version": "0",
   "id": "ddca6449-b258-46c0-8653-e0e3a6EXAMPLE",
   "detail-type": "ECS Deployment State Change",
   "source": "aws.ecs",
   "account": "111122223333",
   "time": "2020-05-23T12:31:14Z",
   "region": "us-west-2",
   "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
   ],
   "detail": {
        "eventType": "INFO",
        "eventName": "SERVICE_DEPLOYMENT_IN_PROGRESS",
        "deploymentId": "ecs-svc/123",
        "updatedAt": "2020-05-23T11:11:11Z",
        "reason": "ECS deployment deploymentId in progress."
   }
}
```

次に、ロールバックデプロイが開始された場合の出力例を示します。reason フィールドには、サービスがロールバックされるデプロイの ID を指定します。

```
{
   "version": "0",
   "id": "ddca6449-b258-46c0-8653-e0e3aEXAMPLE",
   "detail-type": "ECS Deployment State Change",
   "source": "aws.ecs",
   "account": "111122223333",
   "time": "2020-05-23T12:31:14Z",
   "region": "us-west-2",
   "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
   ],
   "detail": {
        "eventType": "INFO",
        "eventName": "SERVICE_DEPLOYMENT_IN_PROGRESS",
        "deploymentId": "ecs-svc/123",
        "updatedAt": "2020-05-23T11:11:11Z",
        "reason": "ECS deployment circuit breaker: rolling back to
 deploymentId deploymentID."
   }
}
```

Example サービスデプロイ完了イベント

サービスデプロイ完了状態イベントは、次の形式で配信されます。詳細については、「タスクを置き換えて Amazon ECS サービスをデプロイする」を参照してください。

```
{
   "version": "0",
   "id": "ddca6449-b258-46c0-8653-e0e3aEXAMPLE",
   "detail-type": "ECS Deployment State Change",
   "source": "aws.ecs",
   "account": "111122223333",
   "time": "2020-05-23T12:31:14Z",
   "region": "us-west-2",
   "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
   ],
   "detail": {
        "eventType": "INFO",
        "eventName": "SERVICE_DEPLOYMENT_COMPLETED",
```

```
        "deploymentId": "ecs-svc/123",
        "updatedAt": "2020-05-23T11:11:11Z",
        "reason": "ECS deployment deploymentID completed."
    }
}
```

Example サービスデプロイ失敗イベント

サービスデプロイ失敗イベントは、次の形式で配信されます。サービスデプロイ失敗状態イベントは、デプロイサーキットブレーカーロジックが有効になっているサービスに対してのみ送信されます。詳細については、「タスクを置き換えて Amazon ECS サービスをデプロイする」を参照してください。

```
{
    "version": "0",
    "id": "ddca6449-b258-46c0-8653-e0e3aEXAMPLE",
    "detail-type": "ECS Deployment State Change",
    "source": "aws.ecs",
    "account": "111122223333",
    "time": "2020-05-23T12:31:14Z",
    "region": "us-west-2",
    "resources": [
        "arn:aws:ecs:us-west-2:111122223333:service/default/servicetest"
    ],
    "detail": {
        "eventType": "ERROR",
        "eventName": "SERVICE_DEPLOYMENT_FAILED",
        "deploymentId": "ecs-svc/123",
        "updatedAt": "2020-05-23T11:11:11Z",
        "reason": "ECS deployment circuit breaker: task failed to start."
    }
}
```

Amazon ECS イベントの処理

Amazon ECS は、少なくとも 1 回 の割合でイベントを送信します。つまり、あるイベントの複数のコピーを受け取る場合があるということです。さらに、イベントは発生順にイベントリスナーに送信されない場合があります。

イベントを適切に順序付けられるように、各イベントの `detail` セクションには `version` プロパティが含まれています。リソースの状態が変わるたびに、この `version` はインクリメントされます。重複するイベントには、`detail` オブジェクト内で同じ `version` バージョンがありま

す。EventBridge で Amazon ECS コンテナインスタンスおよびタスク状態をレプリケートする場合は、Amazon ECS API によって報告されるリソースのバージョンと、そのリソースについて EventBridge で報告される `version` を比較して、イベントストリームでのバージョンが最新であることを確認できます。バージョンプロパティ番号が高いイベントは、バージョン番号が低いイベントより後で発生したものとして処理されます。

例: AWS Lambda 関数でのイベントの処理

次の Python 3.9 で記述された Lambda 関数の例では、タスク状態変更イベントとコンテナインスタンス状態変更イベントの両方をキャプチャし、2 つの Amazon DynamoDB テーブルのいずれかに保存します。

- ECSCtrInstanceState – コンテナインスタンスの最新状態を保存します。テーブル ID は、コンテナインスタンスの `containerInstanceArn` 値です。
- ECSTaskState – タスクの最新状態を保存します。テーブル ID は、タスクの `taskArn` 値です。

```
import json
import boto3

def lambda_handler(event, context):
    id_name = ""
    new_record = {}

    # For debugging so you can see raw event format.
    print('Here is the event:')
    print((json.dumps(event)))

    if event["source"] != "aws.ecs":
       raise ValueError("Function only supports input from events with a source type
 of: aws.ecs")

    # Switch on task/container events.
    table_name = ""
    if event["detail-type"] == "ECS Task State Change":
        table_name = "ECSTaskState"
        id_name = "taskArn"
        event_id = event["detail"]["taskArn"]
    elif event["detail-type"] == "ECS Container Instance State Change":
        table_name = "ECSCtrInstanceState"
        id_name =  "containerInstanceArn"
        event_id = event["detail"]["containerInstanceArn"]
```

```
    else:
        raise ValueError("detail-type for event is not a supported type. Exiting
without saving event.")

    new_record["cw_version"] = event["version"]
    new_record.update(event["detail"])

    # "status" is a reserved word in DDB, but it appears in containerPort
    # state change messages.
    if "status" in event:
        new_record["current_status"] = event["status"]
        new_record.pop("status")


    # Look first to see if you have received a newer version of an event ID.
    # If the version is OLDER than what you have on file, do not process it.
    # Otherwise, update the associated record with this latest information.
    print("Looking for recent event with same ID...")
    dynamodb = boto3.resource("dynamodb", region_name="us-east-1")
    table = dynamodb.Table(table_name)
    saved_event = table.get_item(
        Key={
            id_name : event_id
        }
    )
    if "Item" in saved_event:
        # Compare events and reconcile.
        print(("EXISTING EVENT DETECTED: Id " + event_id + " - reconciling"))
        if saved_event["Item"]["version"] < event["detail"]["version"]:
            print("Received event is a more recent version than the stored event -
updating")
            table.put_item(
                Item=new_record
            )
        else:
            print("Received event is an older version than the stored event -
ignoring")
    else:
        print(("Saving new event - ID " + event_id))

        table.put_item(
            Item=new_record
        )
```

以下の Fargate の例では、Python 3.9 で書かれた Lambda 関数で、タスク状態変更イベントを取得し、以下の Amazon DynamoDB テーブルに保存しています。

```
import json
import boto3

def lambda_handler(event, context):
    id_name = ""
    new_record = {}

    # For debugging so you can see raw event format.
    print('Here is the event:')
    print((json.dumps(event)))

    if event["source"] != "aws.ecs":
       raise ValueError("Function only supports input from events with a source type
 of: aws.ecs")

    # Switch on task/container events.
    table_name = ""
    if event["detail-type"] == "ECS Task State Change":
        table_name = "ECSTaskState"
        id_name = "taskArn"
        event_id = event["detail"]["taskArn"]
    else:
        raise ValueError("detail-type for event is not a supported type. Exiting
 without saving event.")

    new_record["cw_version"] = event["version"]
    new_record.update(event["detail"])

    # "status" is a reserved word in DDB, but it appears in containerPort
    # state change messages.
    if "status" in event:
        new_record["current_status"] = event["status"]
        new_record.pop("status")


    # Look first to see if you have received a newer version of an event ID.
    # If the version is OLDER than what you have on file, do not process it.
    # Otherwise, update the associated record with this latest information.
    print("Looking for recent event with same ID...")
    dynamodb = boto3.resource("dynamodb", region_name="us-east-1")
```

```
    table = dynamodb.Table(table_name)
    saved_event = table.get_item(
        Key={
            id_name : event_id
        }
    )
    if "Item" in saved_event:
        # Compare events and reconcile.
        print(("EXISTING EVENT DETECTED: Id " + event_id + " - reconciling"))
        if saved_event["Item"]["version"] < event["detail"]["version"]:
            print("Received event is a more recent version than the stored event -
updating")
            table.put_item(
                Item=new_record
            )
        else:
            print("Received event is an older version than the stored event -
ignoring")
    else:
        print(("Saving new event - ID " + event_id))

        table.put_item(
            Item=new_record
        )
```

オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する

Container Insights は、コンテナ化されたアプリケーションとマイクロサービスからメトリクスと口グを収集、集計、要約します。すべての Container Insights メトリクスに加えて、追加のタスクとコンテナメトリクスを提供します。

Container Insights は、クラスターで実行中のすべてのコンテナを検出し、パフォーマンススタックの各レイヤーでパフォーマンスデータを収集します。運用データは、パフォーマンスログイベントとして収集されます。これらは、高濃度データを大規模に取り込み、保存できる、構造化された JSON スキーマを使用するエントリです。CloudWatch はこのデータから、クラスター、サービスおよびサービスレベルで、高レベルの集約されたメトリクスを CloudWatch メトリクスとして作成します。このメトリクスには、CPU、メモリ、ディスク、ネットワークなどのリソース使用率が含まれます。メトリクスは、CloudWatch 自動ダッシュボードで使用できます。

このメトリクスは、指定した期間中にタスクが実行されているリソースのみを反映します。例えば、クラスターに 1 つのサービスがあるが、このサービスに RUNNING 状態のタスクがない場合、CloudWatch に送信されるメトリクスはありません。2 つのサービスがあり、1 つに実行中のタスクがあるが、別の 1 つに実行中のタスクがない場合、実行中のタスクがあるサービスのメトリクスのみが送信されます。

2024 年 12 月 2 日、AWS で Amazon ECS 用にオブザーバビリティが強化された Container Insights がリリースされました。このバージョンでは、Amazon EC2 および Fargate の起動タイプを使用して、Amazon ECS クラスターの強化されたオブザーバビリティをサポートしています。Amazon ECS でオブザーバビリティが強化された Container Insights を設定したら、Container Insights はクラスターレベルから環境内のコンテナレベルまで詳細なインフラストラクチャテレメトリを自動的に収集し、これらの重要なパフォーマンスデータを厳選されたダッシュボードに表示し、オブザーバビリティ設定に伴う負担を軽減します。オブザーバビリティが強化された Container Insights を設定する方法の詳細については、「オブザーバビリティが強化された Container Insights」を参照してください。

コンテナ環境で詳細な可視性を提供し、解決までの平均時間を短縮するため、Container Insights ではなく、オブザーバビリティが強化された Container Insights を使用することをお勧めします。詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon ECS 用にオブザーバビリティメトリクスが強化された Container Insights」を参照してください。

表示できるイベントは、Amazon ECS が Amazon EventBridge に送信するイベントです。詳細については、「Amazon ECS イベント」を参照してください。

> **Important**
>
> CloudWatch Container インサイトによって収集されたメトリクスは、カスタムメトリクスとして課金されます。CloudWatch の料金の詳細については、 CloudWatch の料金をご覧ください。

コンテナのヘルスチェックを使用して Amazon ECS タスク状態を判定する

タスク定義を作成するときに、コンテナのヘルスチェックを設定できます。ヘルスチェックは、コンテナ上でローカルに実行され、アプリケーションのヘルスと可用性を検証するコマンドです。

Amazon ECS コンテナエージェントは、タスク定義で指定されたヘルスチェックについてのみ、モニタリングとレポートを行います。Amazon ECS は、コンテナイメージに組み込みた Docker ヘルスチェックについても、コンテナ定義で指定されていない場合はモニタリングしません。コンテナ定義で指定されているヘルスチェックのパラメータは、コンテナイメージ内に存在する Docker ヘルスチェックを上書きします。

タスク定義でヘルスチェックが定義されると、コンテナはコンテナ内でヘルスチェックプロセスを実行し、終了コードを評価してアプリケーションのヘルスを判定します。

ヘルスチェックは以下のパラメータで構成されています。

- コマンド – 正常かどうかを判定するためにコンテナが実行するコマンド。この文字列配列の先頭には、コマンド引数を直接実行するための CMD、またはコンテナのデフォルトシェルでコマンドを実行するための CMD-SHELL を付加できます。
- 間隔 – 各ヘルスチェック間の時間間隔 (秒)。
- タイムアウト – 失敗したと見なされるまでの、ヘルスチェックが正常に終了するのを待つ時間 (秒)。
- 再試行回数 – コンテナが異常と見なされるまでに、失敗したヘルスチェックを再試行する回数。
- 開始期間 – 失敗したヘルスチェックの再試行が最大回数に達する前に、コンテナにブートストラップするまでの時間を与えるオプションの猶予期間です。

  ヘルスチェックが startPeriod 内で成功した場合、コンテナは正常であるとみなされ、その後の失敗は最大再試行回数にカウントされます。

タスク定義でヘルスチェックを指定する方法については、「ヘルスチェック」を参照してください。

以下はコンテナのヘルスステータスの取り得る値です。

- HEALTHY — コンテナのヘルスチェックが正常に完了しました。
- UNHEALTHY — コンテナのヘルスチェックが失敗しました。
- UNKNOWN — コンテナのヘルスチェックが評価中か、定義されていない、または Amazon ECS にコンテナのヘルスチェックのステータスがありません。

ヘルスチェックコマンドはコンテナ上で実行されます。そのため、コンテナイメージにそのコマンドを入れる必要があります。

ヘルスチェックは、localhost または 127.0.0.1 にあるコンテナのループバックインターフェイスを介してアプリケーションに接続します。0 である終了コードは成功を示し、ゼロ以外の終了コードは失敗を示します。

コンテナのヘルスチェックを使用する際は、以下の点を考慮してください。

- コンテナのヘルスチェックには、Amazon ECS コンテナエージェントのバージョン 1.17.0 以降が必要です。
- コンテナのヘルスチェックは、Linux プラットフォームバージョン 1.1.0 以降、または Windows プラットフォームバージョン 1.1.0 以降を使用している場合、Fargate タスクでサポートされます。

Amazon ECS がタスクの正常性を判定する方法

タスクの正常性を判定するのに考慮されるのは、必須で、タスク定義にヘルスチェックコマンドが含まれているコンテナだけです。

次のルールが順番に評価されます。

1. ある必須コンテナのステータスが UNHEALTHY の場合、そのタスクステータスが UNHEALTHY である。
2. ある必須コンテナのステータスが UNKNOWN の場合、そのタスクステータスが UNKNOWN である。
3. すべての必須コンテナのステータスが HEALTHY の場合、タスクステータスが HEALTHY である。

必須コンテナ 2 つでの次のタスクの正常性の例を挙げます。

コンテナ 1 の正常性	コンテナ 2 の正常性	タスクの正常性
UNHEALTHY	UNKNOWN	UNHEALTHY
UNHEALTHY	HEALTHY	UNHEALTHY
HEALTHY	UNKNOWN	UNKNOWN
HEALTHY	HEALTHY	HEALTHY

コンテナ 3 つでの次のタスクの正常性の例を挙げます。

コンテナ 1 の正常性	コンテナ 2 の正常性	コンテナ 3 の正常性	タスクの正常性
UNHEALTHY	UNKNOWN	UNKNOWN	UNHEALTHY
UNHEALTHY	UNKNOWN	HEALTHY	UNHEALTHY
UNHEALTHY	HEALTHY	HEALTHY	UNHEALTHY
HEALTHY	UNKNOWN	HEALTHY	UNKNOWN
HEALTHY	UNKNOWN	UNKNOWN	UNKNOWN
HEALTHY	HEALTHY	HEALTHY	HEALTHY

エージェントの切断がヘルスチェックに及ぼす影響

Amazon ECS コンテナエージェントが Amazon ECS サービスから切断されても、コンテナが UNHEALTHY ステータスに移行することはありません。これは、エージェントの再起動中や一時的に使用不可になっている間もコンテナが実行され続けるように設計されているためです。ヘルスチェックのステータスは、Amazon ECS エージェントからの「最後に受信した」レスポンスであるため、コンテナが切断前に HEALTHY であると見なされていた場合、エージェントが再接続されて新たにヘルスチェックが行われるまではそのステータスが残ります。コンテナのヘルスチェックのステータスについては、いかなる仮定もありません。

Amazon ECS コンテナの正常性を表示する

コンテナの正常性は、コンソールで確認することも、API を使用して `DescribeTasks` レスポンスで確認することもできます。詳細については、「Amazon Elastic Container Service API リファレンス」の「DescribeTasks」を参照してください。

Amazon CloudWatch Logs などのコンテナにログ記録を使用する場合は、コンテナの正常性の出力をログに転送するようにヘルスチェックコマンドを設定できます。必ず `2&1` を使用して `stdout` と `stderr` の両方の情報を取得するようにしてください。

```
"command": [
     "CMD-SHELL",
     "curl -f http://localhost/ >> /proc/1/fd/1 2>&1  || exit 1"
   ],
```

Amazon ECS コンテナインスタンスの正常性をモニタリングする

Amazon ECS は、コンテナインスタンスのヘルスモニタリングを提供します。Amazon ECS が、コンテナインスタンスがコンテナの実行を妨げる可能性のある問題を検出したか否かについて、すばやく判断できます。Amazon ECS は、エージェントバージョン 1.57.0 以降を使用して実行中のすべてのコンテナインスタンスに対して自動チェックを実行し、問題を特定します。コンテナインスタンスのエージェントバージョンの検証に関する詳細については、Amazon ECS コンテナエージェントをアップデートする を参照してください。

AWS CLI バージョン 1.22.3 以降、または AWS CLI バージョン 2.3.6 以降を使用する必要があります。AWS CLI をアップデートする情報については、AWS Command Line Interface ユーザーガイドバージョン 2 の「AWS CLI の最新バージョンのインストールまたはアップデート」を参照してください。

コンテナインスタンスの正常性を表示するには、CONTAINER_INSTANCE_HEALTH オプションを使用して describe-container-instances を実行します。

次に示すのは、overallStatus の有効な値です。

- OK
- IMPAIRED
- INSUFFICIENT_DATA
- INITIALIZING

describe-container-instances の実行方法の例を次に示します。

```
aws ecs describe-container-instances \
     --cluster cluster_name \
     --container-instances 47279cd2cadb41cbaef2dcEXAMPLE \
     --include CONTAINER_INSTANCE_HEALTH
```

以下は、出力されたヘルスステータスオブジェクトの例です。

```
"healthStatus": {
 "overallStatus": "OK",
 "details": [{
  "type": "CONTAINER_RUNTIME",
  "status": "OK",
```

```
   "lastUpdated": "2021-11-10T03:30:26+00:00",
   "lastStatusChange": "2021-11-10T03:26:41+00:00"
  }]
}
```

コンテナインスタンスの異常

`overallStatus` が OK 以外のステータスの場合、以下を試してください。

- 待機してから `describe-container-instances` を実行します。
- EC2 コンソールまたは CLI を使用して、コンテナインスタンスの状態を表示します。
- CloudWatch メトリクスを確認します。詳細については、「CloudWatch を使用して Amazon ECS をモニタリングする」を参照してください。
- AWS Health Dashboard をチェックして、サービスに問題があるかどうかを確認してください。

アプリケーショントレースデータを使用して Amazon ECS 最適化の機会を特定する

Amazon ECS は OpenTelemetry 用 AWS Distro と統合して、アプリケーションからトレースデータを収集します。Amazon ECS は OpenTelemetry サイドカーコンテナ用の AWS Distroを使用して、トレースデータを収集し、AWS X-Ray にルーティングします。詳細については、「Amazon ECS の OpenTelemetry Collector 用 AWS Distro の設定」を参照してください。そして、AWS X-Ray を使用してエラーや例外の特定、パフォーマンスのボトルネックや応答時間の分析を行うことができます。

OpenTelemetry Collector 用 AWS Distro がトレースデータを AWS X-Ray に送信するため、アプリケーションがトレースデータを作成できるように設定する必要があります。詳細については、「AWS X-Rayデベロッパーガイド」の「AWS X-Ray用にアプリケーションを計測する」を参照してください。

AWS X-Ray を使用した AWS Distro for OpenTelemetry の統合に必要な IAM 権限

Amazon ECS と AWS Distro for OpenTelemetry の統合には、タスク用のロールを作成し、タスク定義でそのロールを指定する必要があります。コンテナログが CloudWatch Logs にルーティングされるように AWS Distro for OpenTelemetry サイドカーを設定することをお勧めします。

> **Important**
>
> AWS Distro for OpenTelemetry 統合を使用してアプリケーションメトリクスの収集も行う場合は、タスク用の IAM ロールに、その統合に必要な権限も含まれている必要があります。詳細については、「アプリケーションメトリクスを使用して Amazon ECS アプリケーションのパフォーマンスを相関させる」を参照してください。

次のポリシーを作成し、タスク実行ロールにアタッチします。

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:DescribeLogGroups",
                "logs:PutRetentionPolicy",
                "xray:PutTraceSegments",
                "xray:PutTelemetryRecords",
                "xray:GetSamplingRules",
                "xray:GetSamplingTargets",
                "xray:GetSamplingStatisticSummaries",
                "ssm:GetParameters"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

6. [次へ] をクリックします。

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

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

タスク定義で AWS X-Ray 統合向け OpenTelemetry サイドカー用 AWS Distro の指定

Amazon ECS コンソールでは、[トレース収集の使用] オプションを使用することにより、OpenTelemetry サイドカーコンテナ用の AWS Distro の作成が簡素化されます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

Amazon ECS コンソールを使用していない場合、OpenTelemetry サイドカーコンテナ用 AWS Distro をタスク定義に追加できます。次のタスク定義のスニペットは、AWS X-Ray 統合向けの OpenTelemetry サイドカー用 AWS Distro を追加するためのコンテナの定義を示します。

```
{
 "family": "otel-using-xray",
 "taskRoleArn": "arn:aws:iam::111122223333:role/AmazonECS_OpenTelemetryXrayRole",
 "executionRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
 "containerDefinitions": [{
   "name": "aws-otel-emitter",
   "image": "application-image",
   "logConfiguration": {
```

```
    "logDriver": "awslogs",
    "options": {
     "awslogs-create-group": "true",
     "awslogs-group": "/ecs/aws-otel-emitter",
     "awslogs-region": "us-east-1",
     "awslogs-stream-prefix": "ecs"
    }
   },
   "dependsOn": [{
    "containerName": "aws-otel-collector",
    "condition": "START"
   }]
  },
  {
   "name": "aws-otel-collector",
   "image": "public.ecr.aws/aws-observability/aws-otel-collector:v0.30.0",
   "essential": true,
   "command": [
    "--config=/etc/ecs/otel-instance-metrics-config.yaml"
   ],
   "logConfiguration": {
    "logDriver": "awslogs",
    "options": {
     "awslogs-create-group": "True",
     "awslogs-group": "/ecs/ecs-aws-otel-sidecar-collector",
     "awslogs-region": "us-east-1",
     "awslogs-stream-prefix": "ecs"
    }
   }
  }
 ],
 "networkMode": "awsvpc",
 "requiresCompatibilities": [
  "FARGATE"
 ],
 "cpu": "1024",
 "memory": "3072"
}
```

アプリケーションメトリクスを使用して Amazon ECS アプリケーションのパフォーマンスを相関させる

Fargate の Amazon ECS は、Fargate で実行されているアプリケーションからメトリクスを収集してそれを Amazon CloudWatch または Amazon Managed Service for Prometheus のいずれかにエクスポートすることをサポートしています。

収集したメタデータを使用すると、アプリケーションパフォーマンスデータを基礎となるインフラストラクチャデータと相関させることができるため、問題解決までの平均時間を短縮できます。

Amazon ECS は、OpenTelemetry サイドカーコンテナ用 AWS Distro を使用して、アプリケーションメトリクスを収集して宛先にルーティングします。Amazon ECS コンソールエクスペリエンスでは、タスク定義の作成時にこの統合を追加するプロセスが簡素化されます。

トピック

アプリケーションメトリクスを Amazon CloudWatch にエクスポートする

Fargate の Amazon ECS は、カスタムメトリクスとして、Amazon CloudWatch にカスタムアプリケーションメトリクスをエクスポートすることをサポートしています。これは、OpenTelemetry サイドカーコンテナ用 AWS Distro をタスク定義に追加することによって実行します。Amazon ECS コンソールでは、新しいタスク定義の作成時に [メトリクス収集の使用] オプションを追加することでこのプロセスが簡素化されます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

アプリケーションメトリクスは、ロググループ名 `/aws/ecs/application/metrics` を使用して CloudWatch Logs にエクスポートされ、メトリクスは `ECS/AWSOTel/Application` ネームスペースで表示できます。アプリケーションは、OpenTelemetry SDK を使用して計測する必要があります。詳細については、「AWS Distro for OpenTelemetry ドキュメント」の「AWS Distro for OpenTelemetry の概要」を参照してください。

考慮事項

OpenTelemetry 用 AWS Distro と Fargate 統合に Amazon ECS を使用して Amazon CloudWatch にアプリケーションメトリクスを送信する場合、次のことを考慮する必要があります。

- この統合では、カスタムアプリケーションメトリクスのみを CloudWatch に送信します。タスクレベルのメトリクスが必要な場合は、Amazon ECS クラスター設定で Container Insights を有効にします。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。
- AWS Distro for OpenTelemetry の統合は、Fargate でホストされている Amazon ECS ワークロード、および、Amazon EC2 インスタンスでホストされている Amazon ECS ワークロード用としてサポートされています。現在、外部インスタンスはサポートされていません。
- CloudWatch は、メトリクスごとに最大 30 個のディメンションをサポートします。デフォルトの Amazon ECS は `TaskARN`、`ClusterARN`、`LaunchType`、`TaskDefinitionFamily`、`TaskDefinitionRevision` ディメンションをメトリクスに含めることが既定となります。残りの 25 個のディメンションは、アプリケーションで定義できます。30 個以上のディメンションが設定されている場合、CloudWatch はそれらを表示できません。この場合、アプリケーションメトリクスは `ECS/AWSOTel/Application` CloudWatch のメトリクス名前空間に表示されますが、ディメンションは表示されません。アプリケーションを計測して、さらにディメンションを追加できます。詳細については、「AWS Distro for OpenTelemetry ドキュメント」の「AWS Distro for OpenTelemetry で CloudWatch のメトリクスを使用する」を参照してください。

OpenTelemetry 用 AWS Distro と Amazon CloudWatch の統合に必要な IAM 許可

Amazon ECS と OpenTelemetry 用 AWS Distro の統合には、タスク用 IAM ロールを作成し、タスク定義でロールを指定する必要があります。OpenTelemetry サイドカー用 AWS Distro サイドカーを、CloudWatch ログに対するルートコンテナログにも構成することをお勧めします。これには、タスク実行 IAM ロールを作成して、タスク定義でも指定する必要があります。Amazon ECS コンソールは、ユーザーに代わってタスク実行 IAM ロールを処理しますが、タスク IAM ロールは手動で作成してタスク定義に追加する必要があります。タスクの実行 IAM ロールの詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

> **Important**
>
> OpenTelemetry 用 AWS Distro 統合を使用してアプリケーションのトレースデータも収集する場合、タスク IAM ロールもその統合に必要な許可が含まれていることを確認します。詳細については、「アプリケーショントレースデータを使用して Amazon ECS 最適化の機会を特定する」を参照してください。
> アプリケーションに権限が追加で必要な場合は、それらの権限をこのポリシーに追加する必要があります。各タスク定義では、タスク用の IAM ロールを 1 個のみ指定できます。例え

ば、Systems Manager に保存されているカスタム設定ファイルを使用する場合、この IAM ポリシーに `ssm:GetParameters` 権限を追加する必要があります。

Elastic Container Service のサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] で [エラスティックコンテナサービス] を選択し、次に [エラスティックコンテナのサービスタスク] を選択します。
5. [Next] を選択します。
6. [アクセス許可を追加] セクションで [AWSDistroOpenTelemetryPolicyForXray] を検索し、そのポリシーを選択します。
7. (オプション) アクセス許可の境界を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。

   a. [アクセス許可の境界の設定] セクションを開き、[アクセス許可の境界を使用してロールのアクセス許可の上限を設定する] を選択します。

      IAM には、アカウント内の AWS 管理ポリシーとカスタマー管理ポリシーのリストがあります。

   b. アクセス許可の境界として使用するポリシーを選択します。
8. [Next] を選択します。
9. このロールの目的を識別しやすいロール名またはロール名サフィックスを入力します。

> **Important**
>
> ロールに名前を付けるときは、次のことに注意してください。
>
> - ロール名は AWS アカウント内で一意である必要があります。ただし、大文字と小文字は区別されません。
>
>   例えば、**`PRODROLE`** と **`prodrole`** の両方の名前でロールを作成することはできません。ロール名がポリシーまたは ARN の一部として使用される場合、ロール名は大文

字と小文字が区別されます。ただし、サインインプロセスなど、コンソールにロール名がユーザーに表示される場合、ロール名は大文字と小文字が区別されません。

- 他のエンティティがロールを参照する可能性があるため、ロールを作成した後にロール名を編集することはできません。

10. (オプション) [説明] にロールの説明を入力します。
11. (オプション) ロールのユースケースとアクセス許可を編集するには、[ステップ 1: 信頼されたエンティティを選択] または [ステップ 2: アクセス権限を追加] のセクションで [編集] を選択します。
12. (オプション) ロールの識別、整理、検索を簡単にするには、キーと値のペアとしてタグを追加します。IAM でのタグの使用の詳細については、「IAM ユーザーガイド」の「AWS Identity and Access Management リソースのタグ」を参照してください。
13. ロールを確認したら、[ロールを作成] を選択します。

タスク定義の OpenTelemetry サイドカー用 AWS Distro を指定

Amazon ECS コンソールでは、[メトリクス収集の使用] オプションを使用することで、OpenTelemetry サイドカーコンテナ用の AWS Distro を作成するエクスペリエンスが簡素化されます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

Amazon ECS コンソールを使用していない場合、OpenTelemetry サイドカーコンテナ用 AWS Distro を手動でタスク定義に追加できます。次のタスク定義の例は、Amazon CloudWatch 統合に OpenTelemetry サイドカー用 AWS Distro を追加するためのコンテナの定義を示しています。

```
{
 "family": "otel-using-cloudwatch",
 "taskRoleArn": "arn:aws:iam::111122223333:role/AmazonECS_OpenTelemetryCloudWatchRole",
 "executionRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
 "containerDefinitions": [
    {
   "name": "aws-otel-emitter",
   "image": "application-image",
   "logConfiguration": {
    "logDriver": "awslogs",
    "options": {
     "awslogs-create-group": "true",
     "awslogs-group": "/ecs/aws-otel-emitter",
```

```
      "awslogs-region": "us-east-1",
      "awslogs-stream-prefix": "ecs"
     }
    },
    "dependsOn": [{
     "containerName": "aws-otel-collector",
     "condition": "START"
    }]
   },
   {
    "name": "aws-otel-collector",
    "image": "public.ecr.aws/aws-observability/aws-otel-collector:v0.30.0",
    "essential": true,
    "command": [
     "--config=/etc/ecs/ecs-cloudwatch.yaml"
    ],
    "logConfiguration": {
     "logDriver": "awslogs",
     "options": {
      "awslogs-create-group": "True",
      "awslogs-group": "/ecs/ecs-aws-otel-sidecar-collector",
      "awslogs-region": "us-east-1",
      "awslogs-stream-prefix": "ecs"
     }
    }
   }
  ],
  "networkMode": "awsvpc",
  "requiresCompatibilities": [
   "FARGATE"
  ],
  "cpu": "1024",
  "memory": "3072"
}
```

アプリケーションメトリクスを Amazon Managed Service for Prometheus にエクスポートする

Amazon ECS は、タスクレベル CPU、メモリ、ネットワーク、ストレージメトリクス、カスタムアプリケーションメトリクスを Amazon Managed Service for Prometheus へエクスポートすることをサポートしています。これは、OpenTelemetry サイドカーコンテナ用 AWS Distro をタスク定義に追加することによって実行します。Amazon ECS コンソールでは、新しいタスク定義の作成時に [メト

リクス収集の使用] オプションを追加することでこのプロセスが簡素化されます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

メトリクスは Amazon Managed Service for Prometheus にエクスポートされ、Amazon Managed Grafana ダッシュボードを使用して閲覧できます。アプリケーションは、Prometheus ライブラリまたは OpenTelemetry SDK のいずれかとインストルメント化する必要があります。OpenTelemetry SDK を使用したアプリケーションの計測の詳細については、AWS Distro for OpenTelemetry ドキュメントの「AWS Distro for OpenTelemetry の概要」を参照してください。

Prometheus ライブラリを使用する場合は、アプリケーションがメトリクスデータのスクレイプに使用する `/metrics` のエンドポイントを公開する必要があります。Prometheus ライブラリを使用してアプリケーションを計測する詳細については、「Prometheus ドキュメント」の「Prometheus クライアントライブラリ」を参照してください。

考慮事項

AWS Distro for OpenTelemetry での Fargate 統合で Amazon ECS を使用し、 Amazon Managed Service for Prometheus にアプリケーションメトリクスを送信する場合には、次のことを考慮する必要があります。

- AWS Distro for OpenTelemetry の統合は、Fargate でホストされている Amazon ECS ワークロード、および、Amazon EC2 インスタンスでホストされている Amazon ECS ワークロード用としてサポートされています。現在、外部インスタンスはサポートされていません。
- デフォルトの OpenElementry 用 AWS Distro には、Amazon Managed Service for Prometheus へエクスポートするとき、アプリケーションメトリクス用にタスクレベルのディメンションがすべて含まれています。アプリケーションをインストルメント化して、ディメンションを追加することもできます。詳細については、「AWS Distro for OpenTelemetry ドキュメント」の「Amazon Managed Service for Prometheus のリモート書き込みの使用開始」を参照してください。

OpenTelemetry 用 AWS Distro と Amazon Managed Service for Prometheus の統合に必要な IAM 許可

OpenTelemetry サイドカー用 AWS Distro を使用して Amazon ECS と Amazon Managed Service for Prometheus の統合には、タスク IAM ロールを作成してタスク定義でロールを指定する必要があります。このタスク用の IAM ロールは、タスク定義を登録する前に、次の手順を使用して手動で作成する必要があります。

OpenTelemetry サイドカー用 AWS Distro サイドカーを、CloudWatch ログに対するルートコンテナログにも構成することをお勧めします。これには、タスク実行 IAM ロールを作成して、タスク定

義でも指定する必要があります。Amazon ECS コンソールは、ユーザーに代わってタスク実行 IAM ロールを処理しますが、タスク IAM ロールは手動で作成する必要があります。タスク実行用の IAM ロールを作成する方法の詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

> **Important**
>
> OpenTelemetry 用 AWS Distro 統合を使用してアプリケーションのトレースデータも収集する場合、タスク IAM ロールもその統合に必要な許可が含まれていることを確認します。詳細については、「アプリケーショントレースデータを使用して Amazon ECS 最適化の機会を特定する」を参照してください。

Elastic Container Service のサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] で [エラスティックコンテナサービス] を選択し、次に [エラスティックコンテナのサービスタスク] を選択します。
5. [Next] を選択します。
6. [アクセス許可の追加] セクションで [AmazonPrometheusRemoteWriteAccess] を検索し、そのポリシーを選択します。
7. (オプション) アクセス許可の境界を設定します。このアドバンスド機能は、サービスロールで使用できますが、サービスにリンクされたロールではありません。

   a. [アクセス許可の境界の設定] セクションを開き、[アクセス許可の境界を使用してロールのアクセス許可の上限を設定する] を選択します。

      IAM には、アカウント内の AWS 管理ポリシーとカスタマー管理ポリシーのリストがあります。

   b. アクセス許可の境界として使用するポリシーを選択します。
8. [Next] を選択します。
9. このロールの目的を識別しやすいロール名またはロール名サフィックスを入力します。

> **Important**
>
> ロールに名前を付けるときは、次のことに注意してください。
>
> - ロール名は AWS アカウント内で一意である必要があります。ただし、大文字と小文字は区別されません。
>
> 例えば、**PRODROLE** と **prodrole** の両方の名前でロールを作成することはできません。ロール名がポリシーまたは ARN の一部として使用される場合、ロール名は大文字と小文字が区別されます。ただし、サインインプロセスなど、コンソールにロール名がユーザーに表示される場合、ロール名は大文字と小文字が区別されません。
> - 他のエンティティがロールを参照する可能性があるため、ロールを作成した後にロール名を編集することはできません。

10. (オプション) [説明] にロールの説明を入力します。
11. (オプション) ロールのユースケースとアクセス許可を編集するには、[ステップ 1: 信頼されたエンティティを選択] または [ステップ 2: アクセス権限を追加] のセクションで [編集] を選択します。
12. (オプション) ロールの識別、整理、検索を簡単にするには、キーと値のペアとしてタグを追加します。IAM でのタグの使用の詳細については、「IAM ユーザーガイド」の「AWS Identity and Access Management リソースのタグ」を参照してください。
13. ロールを確認したら、[ロールを作成] を選択します。

タスク定義の OpenTelemetry サイドカー用 AWS Distro を指定

Amazon ECS コンソールでは、[メトリクス収集の使用] オプションを使用することで、OpenTelemetry サイドカーコンテナ用の AWS Distro を作成するエクスペリエンスが簡素化されます。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。

Amazon ECS コンソールを使用していない場合、OpenTelemetry サイドカーコンテナ用 AWS Distro を手動でタスク定義に追加できます。次のタスク定義の例は、Amazon Managed Service for Prometheus 統合向けに OpenTelemetry サイドカー用 AWS Distro を追加するためのコンテナの定義を示しています。

```
{
 "family": "otel-using-cloudwatch",
```

```
 "taskRoleArn": "arn:aws:iam::111122223333:role/AmazonECS_OpenTelemetryCloudWatchRole",
 "executionRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
 "containerDefinitions": [{
   "name": "aws-otel-emitter",
   "image": "application-image",
   "logConfiguration": {
    "logDriver": "awslogs",
    "options": {
     "awslogs-create-group": "true",
     "awslogs-group": "/ecs/aws-otel-emitter",
     "awslogs-region": "aws-region",
     "awslogs-stream-prefix": "ecs"
    }
   },
   "dependsOn": [{
    "containerName": "aws-otel-collector",
    "condition": "START"
   }]
  },
  {
   "name": "aws-otel-collector",
   "image": "public.ecr.aws/aws-observability/aws-otel-collector:v0.30.0",
   "essential": true,
   "command": [
    "--config=/etc/ecs/ecs-amp.yaml"
   ],
   "environment": [{
    "name": "AWS_PROMETHEUS_ENDPOINT",
    "value": "https://aps-workspaces.aws-region.amazonaws.com/workspaces/
ws-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/api/v1/remote_write"
   }],
   "logConfiguration": {
    "logDriver": "awslogs",
    "options": {
     "awslogs-create-group": "True",
     "awslogs-group": "/ecs/ecs-aws-otel-sidecar-collector",
     "awslogs-region": "aws-region",
     "awslogs-stream-prefix": "ecs"
    }
   }
  }
 ],
 "networkMode": "awsvpc",
 "requiresCompatibilities": [
```

```
  "FARGATE"
 ],
 "cpu": "1024",
 "memory": "3072"
}
```

AWS CloudTrail を使用して Amazon ECS API コールをログに記録する

Amazon Elastic Container Service は、ユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、Amazon ECS へのすべての API コールをイベントとしてキャプチャします。キャプチャされる呼び出しには、Amazon ECS コンソールからの呼び出しと、Amazon ECS API オペレーションへのコード呼び出しが含まれます。CloudTrail で収集された情報を使用して、Amazon ECS に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その他の詳細を確認できます。

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。アイデンティティ情報は、以下を判別するのに役立ちます。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービス によって送信されたかどうか。

アカウントを作成すると、AWS アカウント で CloudTrail がアクティブになり、自動的に CloudTrail の[イベント履歴] にアクセスできるようになります。CloudTrail の [イベント履歴] では、AWS リージョン で過去 90 日間に記録された 管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント で過去 90 日間のイベントを継続的に記録するには、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。AWS Management Console を使用して作成した証跡はマルチリージョンです。AWS CLI を使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント内のすべて AWS リージョン でアクティビティを把握するため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョン に記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウント の証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail の Amazon ECS 管理イベント

管理イベントでは、AWS アカウント のリソースに対して実行される管理オペレーションについての情報が得られます。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

Amazon Elastic Container Service は、すべての Amazon ECS コントロールプレーンオペレーションを管理イベントとしてログに記録します。例えば、CreateService、RunTask、および DeleteCluster セ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。Amazon ECS が CloudTrail に記録する Amazon Elastic Container Service コントロールプレーンオペレーションのリストについては、「Amazon Elastic Container Service API リファレンス」を参照してください。

Amazon ECS イベントの例

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。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、イベントは特定の順序で表示されません。

以下の例は、CreateService アクションを示す CloudTrail イベントエントリです。

> **Note**
>
> この例は、読みやすくするために書式設定しています。CloudTrail ログファイルでは、すべてのエントリとイベントが単一の行に連結されています。さらに、この例は 1 つの Amazon ECS エントリに限定しています。実際の CloudTrail ログファイルには、複数の AWS のサービスからのエントリとイベントが表示されます。

```
{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:account_name",
        "arn": "arn:aws:sts::123456789012:user/Mary_Major",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-06-20T18:32:25Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
```

```
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Mary_Major"
            }
        }
    },
    "eventTime": "2018-06-20T19:04:36Z",
    "eventSource": "ecs.amazonaws.com",
    "eventName": "CreateCluster",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.12",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "clusterName": "default"
    },
    "responseElements": {
        "cluster": {
            "clusterArn": "arn:aws:ecs:us-east-1:123456789012:cluster/default",
            "pendingTasksCount": 0,
            "registeredContainerInstancesCount": 0,
            "status": "ACTIVE",
            "runningTasksCount": 0,
            "statistics": [],
            "clusterName": "default",
            "activeServicesCount": 0
        }
    },
    "requestID": "cb8c167e-EXAMPLE",
    "eventID": "e3c6f4ce-EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


CloudTrail レコードの内容については、「AWS CloudTrail ユーザーガイド」の「CloudTrail record contents」を参照してください。

Amazon ECS メタデータを使用したワークロードのモニタリング

タスクとコンテナのメタデータを使用して、ワークロードをトラブルシューティングしたり、ランタイム環境に基づいて設定を変更したりすることができます。

メタデータには以下のカテゴリが含まれます。

- タスクが実行されている場所に関する情報を提供するタスクレベルの属性。
- Docker ID、名前、およびイメージの詳細を提供するコンテナレベルの属性。

  これにより、コンテナを可視化できます。
- IP アドレス、サブネットおよびネットワークモードなどのネットワーク設定。

  これはネットワークの設定やトラブルシューティングに役立ちます。
- タスクのステータスと正常性

  これにより、タスクが実行されているかどうかを確認できます。

次のいずれかの方法で、メタデータを表示できます。

- コンテナメタデータファイル

  Amazon ECS コンテナエージェントのバージョン 1.15.0 以降では、コンテナまたはホストコンテナインスタンス内でさまざまなコンテナメタデータを使用できます。この機能を有効にすると、タスク、コンテナ、およびコンテナ内部のコンテナインスタンスまたはホストコンテナインスタンスに関する情報をクエリできます。メタデータファイルはホストインスタンスで作成され、Docker ボリュームとしてコンテナにマウントされるため、タスクが AWS Fargate でホストされているときは使用できません。
- タスクメタデータエンドポイント

  Amazon ECS コンテナエージェントは、各コンテナに環境変数を注入します。これは、タスクメタデータエンドポイントと呼ばれ、コンテナにさまざまなタスクメタデータと Docker 統計を提供します。
- コンテナの詳細分析

  Amazon ECS コンテナエージェントは、エージェントが実行しているコンテナインスタンスおよびインスタンスで実行されている関連タスクに関する詳細を収集する API オペレーションを提供します。

Amazon ECS 環境変数

環境変数は、タスクの実行に使用される容量など、タスク動作を制御します。Amazon ECS は、次の環境変数をタスクに設定します。

- AWS_CONTAINER_CREDENTIALS_RELATIVE_URI - SDK が認証情報をリクエストするときに使用する完全な HTTP URL エンドポイントが含まれます。これにはスキームとホストの両方が含まれます。詳細については、「AWS SDK リファレンスガイド」の「コンテナ認証情報プロバイダー」を参照してください。
- ECS_CONTAINER_METADATA_URI_V4 - タスクメタデータバージョン 4 のアドレス。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。
- ECS_CONTAINER_METADATA_URI - タスクメタデータバージョン 3 のアドレス。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 3」を参照してください。
- ECS_AGENT_URI - Fargate でサポートされているさまざまなエンドポイントの基本アドレス。詳細については、以下を参照してください。
  - Amazon ECS タスクスケールイン保護のエンドポイント
  - Amazon ECS フォールトインジェクションエンドポイント
- AWS_EXECUTION_ENV - タスクが実行される起動タイプに関する情報。
  - Fargate の場合、Amazon ECS はこれを AWS_ECS_FARGATE に設定します。
  - EC2 の場合、Amazon ECS はこれを AWS_ECS_EC2 に設定します。
- AWS_DEFAULT_REGION – AWS リージョン のデフォルト AWS アカウント。これは、タスクが実行されるデフォルトのリージョンです。
- AWS_REGION - タスクが実行されるリージョン。定義されている場合、この値は AWS_DEFAULT_REGION を上書きします。

タスクメタデータで環境変数を表示できます。詳細については、次のトピックのいずれかを参照してください。

- Fargate - Fargate のタスクで使用できる Amazon ECS タスクメタデータ
- EC2 - EC2 のタスクで使用できる Amazon ECS タスクメタデータ

Amazon ECS コンテナメタデータファイル

Amazon ECS コンテナエージェントのバージョン 1.15.0 以降では、コンテナまたはホストコンテナインスタンス内でさまざまなコンテナメタデータを使用できます。この機能を有効にすると、タスク、コンテナ、およびコンテナ内部のコンテナインスタンスまたはホストコンテナインスタンスに関する情報をクエリできます。メタデータファイルはホストインスタンスで作成され、Docker ボリュームとしてコンテナにマウントされるため、タスクが AWS Fargate でホストされているときは使用できません。

コンテナメタデータファイルは、コンテナがクリーンアップされるときにホストインスタンスでクリーンアップされます。ECS_ENGINE_TASK_CLEANUP_WAIT_DURATION コンテナエージェント変数により、クリーンアップを実行するタイミングを調整できます。詳細については、「Amazon ECS タスクとイメージの自動クリーンアップ」を参照してください。

トピック

- コンテナメタデータファイルの場所
- Amazon ECS コンテナメタデータをオンにする
- Amazon ECS コンテナメタデータファイル形式

コンテナメタデータファイルの場所

デフォルトでは、コンテナメタデータファイルは、次のホストパスとコンテナパスに書き込まれます。

- Linux インスタンスの場合:
  - ホストポート: `/var/lib/ecs/data/metadata/cluster_name/task_id/container_name/ecs-container-metadata.json`

    > **Note**
    >
    > Linux ホストパスでは、エージェントの起動時にデフォルトのデータディレクトリマウントパス (`/var/lib/ecs/data`) が使用されます。Amazon ECS に最適化された AMI を使用しない場合 (または、`ecs-init` パッケージを使用してコンテナエージェントを開始および維持しない場合) は、ECS_HOST_DATA_DIR エージェント設定変数を、コンテナエージェントの状態ファイルがあるホストパスに設定します。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

  - コンテナパス: `/opt/ecs/metadata/random_ID/ecs-container-metadata.json`
- Windows インスタンスの場合:
  - ホストポート: `C:\ProgramData\Amazon\ECS\data\metadata\task_id\container_name\ecs-container-metadata.json`
  - コンテナパス: `C:\ProgramData\Amazon\ECS\metadata\random_ID\ecs-container-metadata.json`

ただし、簡単にアクセスできるようにするため、コンテナメタデータファイルの場所は、コンテナ内の ECS_CONTAINER_METADATA_FILE 環境変数に設定されます。コンテナ内から、以下のコマンドを使用してファイルの内容を読み取ることができます。

- Linux インスタンスの場合:

```
cat $ECS_CONTAINER_METADATA_FILE
```

- Windows インスタンス (PowerShell) の場合:

```
Get-Content -path $env:ECS_CONTAINER_METADATA_FILE
```

Amazon ECS コンテナメタデータをオンにする

コンテナメタデータは、ECS_ENABLE_CONTAINER_METADATA コンテナエージェント変数を true に設定して、コンテナインスタンスレベルでオンにできます。/etc/ecs/ecs.config 設定ファイルでこの変数を設定し、エージェントを再起動できます。実行時 (エージェントコンテナが起動するとき) に、Docker 環境変数として設定することもできます。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

エージェントの起動時に ECS_ENABLE_CONTAINER_METADATA が true に設定されている場合、それ以降に作成されたのコンテナに対してメタデータファイルが作成されます。Amazon ECS コンテナエージェントは、ECS_ENABLE_CONTAINER_METADATA コンテナエージェント変数が true に設定される前に作成されたコンテナに対してメタデータファイルを作成することはできません。すべてのコンテナがメタデータファイルを受け取るようにするには、コンテナインスタンスの起動時に、このエージェント変数を設定します。以下は、この変数を設定し、コンテナインスタンスをクラスターに登録するユーザーデータスクリプトの例です。

```
#!/bin/bash
cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=your_cluster_name
ECS_ENABLE_CONTAINER_METADATA=true
EOF
```

Amazon ECS コンテナメタデータファイル形式

次の情報は、コンテナのメタデータ JSON ファイルに保存されます。

`Cluster`

コンテナのタスクが実行されているクラスターの名前。

`ContainerInstanceARN`

ホストコンテナインスタンスの完全な Amazon リソースネーム (ARN)。

`TaskARN`

コンテナが属しているタスクの完全な Amazon リソースネーム (ARN)。

`TaskDefinitionFamily`

コンテナで使用しているタスク定義ファミリーの名前。

`TaskDefinitionRevision`

コンテナが使用しているタスク定義リビジョン。

`ContainerID`

コンテナの Docker コンテナ ID (Amazon ECS コンテナの ID ではありません)。

`ContainerName`

コンテナ用の Amazon ECS タスク定義からのコンテナ名。

`DockerContainerName`

Docker デーモンがコンテナに使用するコンテナ名 (例えば、docker ps コマンドの出力に表示される名前)。

`ImageID`

コンテナの起動に使用される Docker イメージの SHA ダイジェスト。

`ImageName`

コンテナの起動に使用される Docker イメージのイメージ名とタグ。

`PortMappings`

コンテナに関連付けられているすべてのポートマッピング。

`ContainerPort`

公開されるコンテナのポート。

`HostPort`

公開されるホストコンテナインスタンスのポート。

`BindIp`

Docker によってコンテナに割り当てられたバインド IP アドレス。この IP アドレスは、bridge ネットワークモードでのみ適用され、コンテナインスタンスからのみアクセス可能です。

`Protocol`

ポートマッピングに使用されるネットワークプロトコル。

`Networks`

コンテナのネットワークモードと IP アドレス。

`NetworkMode`

コンテナが属するタスクのネットワークモード。

`IPv4Addresses`

コンテナに関連付けられた IP アドレス。

> **Important**
>
> タスクで awsvpc ネットワークモードを使用している場合、コンテナの IP アドレスは返されません。この場合は、次のコマンドを使用して /etc/hosts ファイルを読み取ることにより IP アドレスを取得できます。
>
> ```
> tail -1 /etc/hosts | awk '{print $1}'
> ```

`MetadataFileStatus`

メタデータファイルのステータス。ステータスが READY である場合、メタデータファイルは最新で完了済みです。ファイルがまだ準備できていない場合 (例えば、タスクが開始された時点)、切り捨てられたバージョンのファイル形式を使用できます。コンテナが開始されたが、メタデータがまだ書き込まれていないという競合状態が発生する可能性を回避するため、メタデータファイルを解析し、メタデータに基づいてこのパラメータが READY に設定されるのを待つことができます。これは通常、コンテナの開始から 1 秒未満で使用できます。

`AvailabilityZone`

ホストコンテナインスタンスが存在するアベイラビリティーゾーン。

`HostPrivateIPv4Address`

コンテナが属するタスクのプライベート IP アドレス。

`HostPublicIPv4Address`

コンテナが属するタスクのパブリック IP アドレス。

Example Amazon ECS コンテナメタデータファイル(**READY**)

次の例では、READY ステータスのコンテナメタデータファイルを示します。

```
{
    "Cluster":"arn:aws:ecs:us-east-1:123456789012:cluster/MyCluster",
    "TaskARN":"arn:aws:ecs:us-east-1:123456789012:task/MyCluster/
b593651c4d6b44a6b2b583f45c957e15",
    "Family":"curltest-container",
    "Revision":"2",
    "DesiredStatus":"RUNNING",
    "KnownStatus":"RUNNING",
    "Limits":
        {
            "CPU":0.25,
            "Memory":512
        },
    "PullStartedAt":"2025-01-17T20:56:17.394610044Z",
    "PullStoppedAt":"2025-01-17T20:56:25.282708213Z",
    "AvailabilityZone":"us-east-1b",
    "LaunchType":"FARGATE",
    "Containers":[
        {
            "DockerId":"b593651c4d6b44a6b2b583f45c957e15-3356213583",
            "Name":"curltest","DockerName":"curltest",
            "Image":"public.ecr.aws/amazonlinux/amazonlinux:latest",

 "ImageID":"sha256:7f371357694782356b65c7fd60dd1ca124c47bd5ed1b1ffe7c0e17f562898367",
            "Labels":
                {
                    "com.amazonaws.ecs.cluster":"arn:aws:ecs:us-
east-1:123456789012:cluster/MyCluster",
                    "com.amazonaws.ecs.container-name":"curltest",
                    "com.amazonaws.ecs.task-arn":"arn:aws:ecs:us-
east-1:123456789012:task/MyCluster/b593651c4d6b44a6b2b583f45c957e15",
```

```
                    "com.amazonaws.ecs.task-definition-family":"curltest-
container","com.amazonaws.ecs.task-definition-version":"2"
                },
            "DesiredStatus":"RUNNING",
            "KnownStatus":"RUNNING",
            "Limits":
                {
                    "CPU":2
                },
            "CreatedAt":"2025-01-17T20:56:26.180347056Z",
            "StartedAt":"2025-01-17T20:56:26.180347056Z",
            "Type":"NORMAL",
            "LogDriver":"awslogs",
            "LogOptions":
                {
                    "awslogs-create-group":"true",
                    "awslogs-group":"/ecs/curltest-container",
                    "awslogs-region":"us-east-1",
                    "awslogs-stream":"ecs/curltest/b593651c4d6b44a6b2b583f45c957e15"
                       },
            "ContainerARN":"arn:aws:ecs:us-east-1:123456789012:container/MyCluster/
b593651c4d6b44a6b2b583f45c957e15/934575e8-5bdb-478f-b763-2341a85b690e",
            "Networks":[
                {
                    "NetworkMode":"awsvpc",
                    "IPv4Addresses":["10.0.1.58"]
                }
            ],
            "Snapshotter":"overlayfs"
        }
    ],
    "ClockDrift":
        {
            "ClockErrorBound":0.487801,"ReferenceTimestamp":"2025-01-17T20:56:02Z",
            "ClockSynchronizationStatus":"SYNCHRONIZED"
        },
    "FaultInjectionEnabled":false
}
```

Example 不完全な Amazon ECS コンテナメタデータファイル (まだ **READY** でない)

次の例では、まだ READY ステータスに達していないコンテナメタデータファイルを示します。ファイルの情報は、タスクの定義から既知であるいくつかのパラメータに限定されます。コンテナメタデータファイルは、コンテナの開始後 1 秒以内に準備できます。

```
{
    "Cluster": "default",
    "ContainerInstanceARN": "arn:aws:ecs:us-west-2:012345678910:container-instance/
default/1f73d099-b914-411c-a9ff-81633b7741dd",
    "TaskARN": "arn:aws:ecs:us-west-2:012345678910:task/default/
d90675f8-1a98-444b-805b-3d9cabb6fcd4",
    "ContainerName": "metadata"
}
```

EC2 のタスクで使用できる Amazon ECS タスクメタデータ

Amazon ECS コンテナエージェントでは、さまざまなタスクメタデータおよび [Docker]統計を取得するメソッドを提供します。これは、タスクメタデータエンドポイントと呼ばれます。以下のバージョンが利用できます。

- タスクメタデータエンドポイントバージョン 4 コンテナにさまざまなメタデータと Docker 統計を提供します。ネットワークレートデータも提供できます。少なくともバージョン1.39.0のAmazon ECS コンテナエージェントを実行しているAmazon EC2 Linuxインスタンスで起動されたAmazon ECSタスクで利用できます。awsvpc ネットワークモードを使用するAmazon EC2 Windows インスタンスの場合、Amazon ECS コンテナエージェントは少なくともバージョン 1.54.0 でなければなりません。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。
- タスクメタデータエンドポイントバージョン 3 コンテナにさまざまなメタデータと Docker 統計を提供します。少なくともバージョン1.21.0のAmazon ECS コンテナエージェントを実行しているAmazon EC2 Linuxインスタンスで起動されたAmazon ECSタスクで利用できます。awsvpc ネットワークモードを使用するAmazon EC2 Windows インスタンスの場合、Amazon ECS コンテナエージェントは少なくともバージョン 1.54.0 でなければなりません。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 3」を参照してください。
- タスクメタデータエンドポイントバージョン2–少なくともバージョン 1.17.0のAmazonECS コンテナエージェントを実行しているAmazon EC2 Linuxインスタンスで起動されたAmazon ECS タスクで利用できます。awsvpc ネットワークモードを使用するAmazon EC2 Windows インスタンスの場合、Amazon ECS コンテナエージェントは少なくともバージョン 1.54.0 でなければなりま

せん。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 2」を参照してください。

また、Amazon ECS タスクが Amazon EC2 でホストされている場合は、インスタンスメタデータサービス (IMDS) エンドポイントを使用してタスクホストのメタデータにアクセスできます。次のコマンドは、タスクをホストするインスタンス内から実行すると、ホストインスタンスの ID を一覧表示します。

```
curl http://169.254.169.254/latest/meta-data/instance-id
```

エンドポイントから取得できる情報は、*instance-id* などのようなカテゴリに分類されます。エンドポイントを使用して取得できるホストインスタンスのメタデータのさまざまなカテゴリの詳細については、「インスタンスメタデータのカテゴリ」を参照してください。

Amazon ECS タスクメタデータエンドポイントバージョン 4

Amazon ECS コンテナエージェントは、各コンテナに環境変数を注入します。これは、タスクメタデータエンドポイントと呼ばれ、コンテナにさまざまなタスクメタデータと Docker 統計を提供します。

タスクメタデータとネットワークレートの統計は CloudWatch に送信され、 AWS Management Console で表示できます。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。

> **Note**
>
> Amazon ECS は、以前のバージョンのタスクメタデータエンドポイントを提供しています。新しいタスクメタデータエンドポイントバージョンを今後作成する必要がないように、追加のメタデータをバージョン 4 の出力に追加できます。既存のメタデータが削除されたり、メタデータのフィールド名が変更されたりすることはありません。

環境変数は、デフォルトでは、少なくともバージョン `1.39.0` の Amazon ECS コンテナエージェントを実行している Amazon ECS Linux インスタンスで起動された Amazon EC2 タスクのコンテナに挿入されます。`awsvpc` ネットワークモードを使用するAmazon EC2 Windows インスタンスの場合、Amazon ECS コンテナエージェントは少なくともバージョン `1.54.0` でなければなりません。詳細については、「Amazon ECS Linux コンテナインスタンスの管理」を参照してください。

> **Note**
>
> エージェントを最新バージョンに更新することで、古いバージョンのAmazon ECS コンテナエージェントを使用する Amazon EC2 インスタンスでこの機能のサポートを追加できます。詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

タスクメタデータエンドポイントバージョン 4 のパス

次のタスクメタデータエンドポイントパスをコンテナで使用できます。

`${ECS_CONTAINER_METADATA_URI_V4}`

このパスはコンテナのメタデータを返します。

`${ECS_CONTAINER_METADATA_URI_V4}/task`

このパスはタスクのメタデータを返します。これには、タスクに関連付けられたすべてのコンテナのコンテナ ID および名前のリストが含まれています。このエンドポイントのレスポンスの詳細については、「Amazon ECS タスクメタデータ V4 JSON レスポンス」を参照してください。

`${ECS_CONTAINER_METADATA_URI_V4}/taskWithTags`

このパスは、`ListTagsForResource` API を使用して取得できるタスクとコンテナインスタンスタグに加えて、`/task` エンドポイントに含まれるタスクのメタデータを返します。タグメタデータの取得時に受信したエラーは、レスポンスの `Errors` フィールドに含まれます。

> **Note**
>
> この`Errors`フィールドは、少なくとも`1.50.0`バージョンのコンテナエージェントを実行しているAmazon EC2 Linux インスタンスでホストされているタスクの応答にのみ表示されます。`awsvpc` ネットワークモードを使用するAmazon EC2 Windows インスタンスの場合、Amazon ECS コンテナエージェントは少なくともバージョン `1.54.0` でなければなりません。
> このエンドポイントには、`ecs.ListTagsForResource` アクセス許可が必要です。

`${ECS_CONTAINER_METADATA_URI_V4}/stats`

このパスは特定のコンテナの Docker 統計を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

少なくともバージョン `1.43.0` のコンテナエージェントを実行しているAmazon EC2 Linuxインスタンスでホストされている `awsvpc` または `bridge` ネットワークモードを使用するAmazon ECS タスクの場合、応答に追加のネットワークレート統計が含まれます。他のすべてのタスクでは、レスポンスには累積ネットワーク統計のみが含まれます。

`${ECS_CONTAINER_METADATA_URI_V4}/task/stats`

このパスはタスクに関連付けられたすべてのコンテナの Docker 統計を返します。これをサイドカーコンテナで使用し、ネットワークメトリクスを抽出できます。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

少なくともバージョン `1.43.0` のコンテナエージェントを実行しているAmazon EC2 Linuxインスタンスでホストされている `awsvpc` または `bridge` ネットワークモードを使用するAmazon ECS タスクの場合、応答に追加のネットワークレート統計が含まれます。他のすべてのタスクでは、レスポンスには累積ネットワーク統計のみが含まれます。

Amazon ECS タスクメタデータ V4 JSON レスポンス

次の情報が、タスクメタデータエンドポイント (`${ECS_CONTAINER_METADATA_URI_V4}/task`) JSON レスポンスから返されます。これには、タスク内の各コンテナのメタデータに加えて、タスクに関連付けられたメタデータも含まれます。

`Cluster`

タスクが属する Amazon ECS クラスターの Amazon リソースネーム (ARN)または短縮名。

`ServiceName`

タスクが属しているサービスの名前。ServiceName は、タスクがサービスに関連付けられている場合、Amazon EC2 と Amazon ECS Anywhere コンテナインスタンスに表示されます。

> **Note**
>
> この `ServiceName` メタデータは、Amazon ECS コンテナエージェントのバージョン `1.63.1`、もしくはそれ以降を使用している場合にのみ含まれます。

`VPCID`

Amazon EC2 コンテナインスタンスの VPC ID。このフィールドは、Amazon EC2 インスタンスでのみ表示されます。

> **Note**
>
> この `VPCID` メタデータは、Amazon ECS コンテナエージェントのバージョン `1.63.1`、もしくはそれ以降を使用している場合にのみ含まれます。

`TaskARN`

コンテナが属しているタスクの Amazon リソースネーム (ARN)。

`Family`

タスクの Amazon ECS タスク定義のファミリー。

`Revision`

タスクの Amazon ECS タスク定義のリビジョン。

`DesiredStatus`

Amazon ECSからのタスクの望ましいステータス。

`KnownStatus`

Amazon ECS からのタスクの既知のステータス。

`Limits`

CPU (vCPU で表される) やメモリなど、タスク レベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`PullStartedAt`

最初のコンテナイメージのプル開始時のタイムスタンプ。

`PullStoppedAt`

最後のコンテナイメージのプル終了時のタイムスタンプ。

`AvailabilityZone`

タスクがあるアベイラビリティーゾーン。

> **Note**
>
> アベイラビリティーゾーンのメタデータは、プラットフォームバージョン 1.4 以降 (Linux) または 1.0.0 (Windows) を使用する Fargate タスクでのみ使用できます。

`LaunchType`

タスクが使用している起動タイプ。クラスター容量プロバイダーを使用する場合、タスクが Fargate インフラストラクチャと EC2 インフラストラクチャのいずれを使用しているかを示します。

> **Note**
>
> この`LaunchType`メタデータは、Amazon ECS Linux コンテナエージェントのバージョン`1.45.0` 以降 (Linux) または 1.0.0 以降 (Windows) を使用している場合にのみ含まれます。

`Containers`

タスクに関連付けられている各コンテナのコンテナメタデータのリスト。

`DockerId`

コンテナの Docker ID。

Fargate を使用する場合、IDは32桁の16進数に10桁の数字が続きます。

`Name`

タスク定義で指定されたコンテナの名前。

`DockerName`

Docker に提供されたコンテナの名前。Amazon ECSコンテナエージェントはコンテナに一意の名前を生成し、同じタスク定義の複数のコピーが単一のインスタンスで実行される場合に名前の競合を回避します。

`Image`

コンテナのイメージ。

`ImageID`

イメージの SHA-256 ダイジェスト。

`Ports`

コンテナに対して公開されている任意のポート。公開ポートがない場合はこのパラメータは省略されます。

`Labels`

コンテナに適用された任意のラベル。ラベルが適用されていない場合はこのパラメータは省略されます。

`DesiredStatus`

Amazon ECSからのコンテナの望ましいステータス。

`KnownStatus`

Amazon ECS からのコンテナの既知のステータス。

`ExitCode`

コンテナの終了コード。このパラメータは、コンテナが終了していない場合は省略されます。

`Limits`

CPU (CPU 単位で表される) やメモリなど、コンテナレベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`CreatedAt`

コンテナ作成時のタイムスタンプ。このパラメータは、コンテナがまだ作成されていない場合は省略されます。

`StartedAt`

コンテナ起動時のタイムスタンプ。このパラメータは、コンテナがまだ起動していない場合は省略されます。

`FinishedAt`

コンテナ停止時のタイムスタンプ。このパラメータは、コンテナがまだ停止していない場合は省略されます。

`Type`

コンテナのタイプ。タスク定義で指定されているコンテナのタイプは `NORMAL` です。他のコンテナタイプは無視してかまいません。これらはAmazon ECS コンテナエージェントによってプロビジョニングされる内部タスクリソースで使用されます。

`LogDriver`

コンテナに使用されるログドライバー。

> **Note**
>
> このLogDriverメタデータは、Amazon ECS Linux コンテナエージェントのバージョン1.45.0、もしくはそれ以降を使用している場合にのみ含まれます。

`LogOptions`

コンテナに定義されたログドライバオプション。

> **Note**
>
> このLogOptionsメタデータは、Amazon ECS Linux コンテナエージェントのバージョン1.45.0、もしくはそれ以降を使用している場合にのみ含まれます。

`ContainerARN`

コンテナの Amazon リソースネーム (ARN)。

> **Note**
>
> このContainerARNメタデータは、Amazon ECS Linux コンテナエージェントのバージョン1.45.0、もしくはそれ以降を使用している場合にのみ含まれます。

`Networks`

ネットワークモードや IP アドレスなど、コンテナのネットワーク情報。ネットワーク情報が定義されていない場合はこのパラメータは省略されます。

`RestartCount`

コンテナが再起動された回数。

> **Note**
>
> `RestartCount` メタデータが含まれるのは、コンテナの再起動ポリシーが有効になっている場合のみです。詳細については、「コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する」を参照してください。

`ExecutionStoppedAt`

タスクの `DesiredStatus` が `STOPPED` に移行した時のタイムスタンプ。これは、必須コンテナが `STOPPED` に移行したときに発生します。

Amazon ECS タスクメタデータ v4 の例

以下の例は、タスクメタデータエンドポイントそれぞれからの出力例を示しています。

コンテナメタデータレスポンスの例

`${ECS_CONTAINER_METADATA_URI_V4}` エンドポイントにクエリを実行すると、コンテナ自体に関するメタデータのみが返されます。以下に出力例を示します。

```
{
    "DockerId": "ea32192c8553fbff06c9340478a2ff089b2bb5646fb718b4ee206641c9086d66",
    "Name": "curl",
    "DockerName": "ecs-curltest-24-curl-cca48e8dcadd97805600",
    "Image": "111122223333.dkr.ecr.us-west-2.amazonaws.com/curltest:latest",
    "ImageID":
 "sha256:d691691e9652791a60114e67b365688d20d19940dde7c4736ea30e660d8d3553",
    "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "curl",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/8f03e41243824aea923aca126495f665",
        "com.amazonaws.ecs.task-definition-family": "curltest",
        "com.amazonaws.ecs.task-definition-version": "24"
    },
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
```

```
    "Limits": {
        "CPU": 10,
        "Memory": 128
    },
    "CreatedAt": "2020-10-02T00:15:07.620912337Z",
    "StartedAt": "2020-10-02T00:15:08.062559351Z",
    "Type": "NORMAL",
    "LogDriver": "awslogs",
    "LogOptions": {
        "awslogs-create-group": "true",
        "awslogs-group": "/ecs/metadata",
        "awslogs-region": "us-west-2",
        "awslogs-stream": "ecs/curl/8f03e41243824aea923aca126495f665"
    },
    "ContainerARN": "arn:aws:ecs:us-west-2:111122223333:container/0206b271-
b33f-47ab-86c6-a0ba208a70a9",
    "Networks": [
        {
            "NetworkMode": "awsvpc",
            "IPv4Addresses": [
                "10.0.2.100"
            ],
            "AttachmentIndex": 0,
            "MACAddress": "0e:9e:32:c7:48:85",
            "IPv4SubnetCIDRBlock": "10.0.2.0/24",
            "PrivateDNSName": "ip-10-0-2-100.us-west-2.compute.internal",
            "SubnetGatewayIpv4Address": "10.0.2.1/24"
        }
    ]
}
```

タスクメタデータレスポンスの例

${ECS_CONTAINER_METADATA_URI_V4}/task エンドポイントをクエリすると、タスク内の各コンテナのメタデータに加えて、コンテナが一部であるタスクに関するメタデータが返されます。以下に出力例を示します。

```
{
    "Cluster": "default",
    "TaskARN": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
    "Family": "curltest",
    "ServiceName": "MyService",
```

```
    "Revision": "26",
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
    "PullStartedAt": "2020-10-02T00:43:06.202617438Z",
    "PullStoppedAt": "2020-10-02T00:43:06.31288465Z",
    "AvailabilityZone": "us-west-2d",
    "VPCID": "vpc-1234567890abcdef0",
    "LaunchType": "EC2",
    "Containers": [
        {
            "DockerId":
 "598cba581fe3f939459eaba1e071d5c93bb2c49b7d1ba7db6bb19deeb70d8e38",
            "Name": "~internal~ecs~pause",
            "DockerName": "ecs-curltest-26-internalecspause-e292d586b6f9dade4a00",
            "Image": "amazon/amazon-ecs-pause:0.1.0",
            "ImageID": "",
            "Labels": {
                "com.amazonaws.ecs.cluster": "default",
                "com.amazonaws.ecs.container-name": "~internal~ecs~pause",
                "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
                "com.amazonaws.ecs.task-definition-family": "curltest",
                "com.amazonaws.ecs.task-definition-version": "26"
            },
            "DesiredStatus": "RESOURCES_PROVISIONED",
            "KnownStatus": "RESOURCES_PROVISIONED",
            "Limits": {
                "CPU": 0,
                "Memory": 0
            },
            "CreatedAt": "2020-10-02T00:43:05.602352471Z",
            "StartedAt": "2020-10-02T00:43:06.076707576Z",
            "Type": "CNI_PAUSE",
            "Networks": [
                {
                    "NetworkMode": "awsvpc",
                    "IPv4Addresses": [
                        "10.0.2.61"
                    ],
                    "AttachmentIndex": 0,
                    "MACAddress": "0e:10:e2:01:bd:91",
                    "IPv4SubnetCIDRBlock": "10.0.2.0/24",
                    "PrivateDNSName": "ip-10-0-2-61.us-west-2.compute.internal",
                    "SubnetGatewayIpv4Address": "10.0.2.1/24"
```

```
                }
            ]
        },
        {
            "DockerId":
 "ee08638adaaf009d78c248913f629e38299471d45fe7dc944d1039077e3424ca",
            "Name": "curl",
            "DockerName": "ecs-curltest-26-curl-a0e7dba5aca6d8cb2e00",
            "Image": "111122223333.dkr.ecr.us-west-2.amazonaws.com/curltest:latest",
            "ImageID":
 "sha256:d691691e9652791a60114e67b365688d20d19940dde7c4736ea30e660d8d3553",
            "Labels": {
                "com.amazonaws.ecs.cluster": "default",
                "com.amazonaws.ecs.container-name": "curl",
                "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
                "com.amazonaws.ecs.task-definition-family": "curltest",
                "com.amazonaws.ecs.task-definition-version": "26"
            },
            "DesiredStatus": "RUNNING",
            "KnownStatus": "RUNNING",
            "Limits": {
                "CPU": 10,
                "Memory": 128
            },
            "CreatedAt": "2020-10-02T00:43:06.326590752Z",
            "StartedAt": "2020-10-02T00:43:06.767535449Z",
            "Type": "NORMAL",
            "LogDriver": "awslogs",
            "LogOptions": {
                "awslogs-create-group": "true",
                "awslogs-group": "/ecs/metadata",
                "awslogs-region": "us-west-2",
                "awslogs-stream": "ecs/curl/158d1c8083dd49d6b527399fd6414f5c"
            },
            "ContainerARN": "arn:aws:ecs:us-west-2:111122223333:container/
abb51bdd-11b4-467f-8f6c-adcfe1fe059d",
            "Networks": [
                {
                    "NetworkMode": "awsvpc",
                    "IPv4Addresses": [
                        "10.0.2.61"
                    ],
                    "AttachmentIndex": 0,
```

```
                    "MACAddress": "0e:10:e2:01:bd:91",
                    "IPv4SubnetCIDRBlock": "10.0.2.0/24",
                    "PrivateDNSName": "ip-10-0-2-61.us-west-2.compute.internal",
                    "SubnetGatewayIpv4Address": "10.0.2.1/24"
                }
            ]
        }
    ]
}
```

タグメタデータの応答を持つタスクの例

${ECS_CONTAINER_METADATA_URI_V4}/taskWithTags エンドポイントをクエリすると、タスクおよびコンテナインスタンスタグを含むタスクに関するメタデータが返されます。以下に出力例を示します。

```
{
    "Cluster": "default",
    "TaskARN": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
    "Family": "curltest",
    "ServiceName": "MyService",
    "Revision": "26",
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
    "PullStartedAt": "2020-10-02T00:43:06.202617438Z",
    "PullStoppedAt": "2020-10-02T00:43:06.31288465Z",
    "AvailabilityZone": "us-west-2d",
    "VPCID": "vpc-1234567890abcdef0",
    "TaskTags": {
        "tag-use": "task-metadata-endpoint-test"
    },
    "ContainerInstanceTags":{
        "tag_key":"tag_value"
    },
    "LaunchType": "EC2",
    "Containers": [
        {
            "DockerId":
 "598cba581fe3f939459eaba1e071d5c93bb2c49b7d1ba7db6bb19deeb70d8e38",
            "Name": "~internal~ecs~pause",
            "DockerName": "ecs-curltest-26-internalecspause-e292d586b6f9dade4a00",
            "Image": "amazon/amazon-ecs-pause:0.1.0",
```

```
            "ImageID": "",
            "Labels": {
                "com.amazonaws.ecs.cluster": "default",
                "com.amazonaws.ecs.container-name": "~internal~ecs~pause",
                "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
                "com.amazonaws.ecs.task-definition-family": "curltest",
                "com.amazonaws.ecs.task-definition-version": "26"
            },
            "DesiredStatus": "RESOURCES_PROVISIONED",
            "KnownStatus": "RESOURCES_PROVISIONED",
            "Limits": {
                "CPU": 0,
                "Memory": 0
            },
            "CreatedAt": "2020-10-02T00:43:05.602352471Z",
            "StartedAt": "2020-10-02T00:43:06.076707576Z",
            "Type": "CNI_PAUSE",
            "Networks": [
                {
                    "NetworkMode": "awsvpc",
                    "IPv4Addresses": [
                        "10.0.2.61"
                    ],
                    "AttachmentIndex": 0,
                    "MACAddress": "0e:10:e2:01:bd:91",
                    "IPv4SubnetCIDRBlock": "10.0.2.0/24",
                    "PrivateDNSName": "ip-10-0-2-61.us-west-2.compute.internal",
                    "SubnetGatewayIpv4Address": "10.0.2.1/24"
                }
            ]
        },
        {
            "DockerId":
 "ee08638adaaf009d78c248913f629e38299471d45fe7dc944d1039077e3424ca",
            "Name": "curl",
            "DockerName": "ecs-curltest-26-curl-a0e7dba5aca6d8cb2e00",
            "Image": "111122223333.dkr.ecr.us-west-2.amazonaws.com/curltest:latest",
            "ImageID":
 "sha256:d691691e9652791a60114e67b365688d20d19940dde7c4736ea30e660d8d3553",
            "Labels": {
                "com.amazonaws.ecs.cluster": "default",
                "com.amazonaws.ecs.container-name": "curl",
```

```
                "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
                "com.amazonaws.ecs.task-definition-family": "curltest",
                "com.amazonaws.ecs.task-definition-version": "26"
            },
            "DesiredStatus": "RUNNING",
            "KnownStatus": "RUNNING",
            "Limits": {
                "CPU": 10,
                "Memory": 128
            },
            "CreatedAt": "2020-10-02T00:43:06.326590752Z",
            "StartedAt": "2020-10-02T00:43:06.767535449Z",
            "Type": "NORMAL",
            "LogDriver": "awslogs",
            "LogOptions": {
                "awslogs-create-group": "true",
                "awslogs-group": "/ecs/metadata",
                "awslogs-region": "us-west-2",
                "awslogs-stream": "ecs/curl/158d1c8083dd49d6b527399fd6414f5c"
            },
            "ContainerARN": "arn:aws:ecs:us-west-2:111122223333:container/
abb51bdd-11b4-467f-8f6c-adcfe1fe059d",
            "Networks": [
                {
                    "NetworkMode": "awsvpc",
                    "IPv4Addresses": [
                        "10.0.2.61"
                    ],
                    "AttachmentIndex": 0,
                    "MACAddress": "0e:10:e2:01:bd:91",
                    "IPv4SubnetCIDRBlock": "10.0.2.0/24",
                    "PrivateDNSName": "ip-10-0-2-61.us-west-2.compute.internal",
                    "SubnetGatewayIpv4Address": "10.0.2.1/24"
                }
            ]
        }
    ]
}
```

エラーメタデータレスポンスのタグを含むタスクの例

${ECS_CONTAINER_METADATA_URI_V4}/taskWithTags エンドポイントをクエリすると、タスクおよびコンテナインスタンスタグを含むタスクに関するメタデータが返されます。タグ付けデータの取得中にエラーが発生した場合は、そのエラーがレスポンスで返されます。コンテナインスタンスに関連付けられた IAM ロール に ecs:ListTagsForResource の権限が付与されていない場合の出力例を次に示します。

```
{
    "Cluster": "default",
    "TaskARN": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
    "Family": "curltest",
    "ServiceName": "MyService",
    "Revision": "26",
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
    "PullStartedAt": "2020-10-02T00:43:06.202617438Z",
    "PullStoppedAt": "2020-10-02T00:43:06.31288465Z",
    "AvailabilityZone": "us-west-2d",
    "VPCID": "vpc-1234567890abcdef0",
    "Errors": [
        {
            "ErrorField": "ContainerInstanceTags",
            "ErrorCode": "AccessDeniedException",
            "ErrorMessage": "User: arn:aws:sts::111122223333:assumed-
role/ecsInstanceRole/i-0744a608689EXAMPLE is not authorized to perform:
 ecs:ListTagsForResource on resource: arn:aws:ecs:us-west-2:111122223333:container-
instance/default/2dd1b186f39845a584488d2ef155c131",
            "StatusCode": 400,
            "RequestId": "cd597ef0-272b-4643-9bd2-1de469870fa6",
            "ResourceARN": "arn:aws:ecs:us-west-2:111122223333:container-instance/
default/2dd1b186f39845a584488d2ef155c131"
        },
        {
            "ErrorField": "TaskTags",
            "ErrorCode": "AccessDeniedException",
            "ErrorMessage": "User: arn:aws:sts::111122223333:assumed-
role/ecsInstanceRole/i-0744a608689EXAMPLE is not authorized to perform:
 ecs:ListTagsForResource on resource: arn:aws:ecs:us-west-2:111122223333:task/
default/9ef30e4b7aa44d0db562749cff4983f3",
            "StatusCode": 400,
            "RequestId": "862c5986-6cd2-4aa6-87cc-70be395531e1",
```

```
            "ResourceARN": "arn:aws:ecs:us-west-2:111122223333:task/
default/9ef30e4b7aa44d0db562749cff4983f3"
        }
    ],
    "LaunchType": "EC2",
    "Containers": [
        {
            "DockerId":
 "598cba581fe3f939459eaba1e071d5c93bb2c49b7d1ba7db6bb19deeb70d8e38",
            "Name": "~internal~ecs~pause",
            "DockerName": "ecs-curltest-26-internalecspause-e292d586b6f9dade4a00",
            "Image": "amazon/amazon-ecs-pause:0.1.0",
            "ImageID": "",
            "Labels": {
                "com.amazonaws.ecs.cluster": "default",
                "com.amazonaws.ecs.container-name": "~internal~ecs~pause",
                "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
                "com.amazonaws.ecs.task-definition-family": "curltest",
                "com.amazonaws.ecs.task-definition-version": "26"
            },
            "DesiredStatus": "RESOURCES_PROVISIONED",
            "KnownStatus": "RESOURCES_PROVISIONED",
            "Limits": {
                "CPU": 0,
                "Memory": 0
            },
            "CreatedAt": "2020-10-02T00:43:05.602352471Z",
            "StartedAt": "2020-10-02T00:43:06.076707576Z",
            "Type": "CNI_PAUSE",
            "Networks": [
                {
                    "NetworkMode": "awsvpc",
                    "IPv4Addresses": [
                        "10.0.2.61"
                    ],
                    "AttachmentIndex": 0,
                    "MACAddress": "0e:10:e2:01:bd:91",
                    "IPv4SubnetCIDRBlock": "10.0.2.0/24",
                    "PrivateDNSName": "ip-10-0-2-61.us-west-2.compute.internal",
                    "SubnetGatewayIpv4Address": "10.0.2.1/24"
                }
            ]
        },
```

```
        {
            "DockerId":
 "ee08638adaaf009d78c248913f629e38299471d45fe7dc944d1039077e3424ca",
            "Name": "curl",
            "DockerName": "ecs-curltest-26-curl-a0e7dba5aca6d8cb2e00",
            "Image": "111122223333.dkr.ecr.us-west-2.amazonaws.com/curltest:latest",
            "ImageID":
 "sha256:d691691e9652791a60114e67b365688d20d19940dde7c4736ea30e660d8d3553",
            "Labels": {
                "com.amazonaws.ecs.cluster": "default",
                "com.amazonaws.ecs.container-name": "curl",
                "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/
default/158d1c8083dd49d6b527399fd6414f5c",
                "com.amazonaws.ecs.task-definition-family": "curltest",
                "com.amazonaws.ecs.task-definition-version": "26"
            },
            "DesiredStatus": "RUNNING",
            "KnownStatus": "RUNNING",
            "Limits": {
                "CPU": 10,
                "Memory": 128
            },
            "CreatedAt": "2020-10-02T00:43:06.326590752Z",
            "StartedAt": "2020-10-02T00:43:06.767535449Z",
            "Type": "NORMAL",
            "LogDriver": "awslogs",
            "LogOptions": {
                "awslogs-create-group": "true",
                "awslogs-group": "/ecs/metadata",
                "awslogs-region": "us-west-2",
                "awslogs-stream": "ecs/curl/158d1c8083dd49d6b527399fd6414f5c"
            },
            "ContainerARN": "arn:aws:ecs:us-west-2:111122223333:container/
abb51bdd-11b4-467f-8f6c-adcfe1fe059d",
            "Networks": [
                {
                    "NetworkMode": "awsvpc",
                    "IPv4Addresses": [
                        "10.0.2.61"
                    ],
                    "AttachmentIndex": 0,
                    "MACAddress": "0e:10:e2:01:bd:91",
                    "IPv4SubnetCIDRBlock": "10.0.2.0/24",
                    "PrivateDNSName": "ip-10-0-2-61.us-west-2.compute.internal",
```

```
                    "SubnetGatewayIpv4Address": "10.0.2.1/24"
                }
            ]
        }
    ]
}
```

コンテナ統計レスポンスの例

${ECS_CONTAINER_METADATA_URI_V4}/stats エンドポイントにクエリを実行すると、コンテナのネットワークメトリクスが返されます。少なくともバージョン 1.43.0 のコンテナエージェントを実行しているAmazon EC2 インスタンスでホストされている awsvpc または bridge ネットワークモードを使用するAmazon ECS タスクの場合、応答に追加のネットワークレート統計が含まれます。他のすべてのタスクでは、レスポンスには累積ネットワーク統計のみが含まれます。

次に、bridge ネットワークモードを使用する Amazon ECS の Amazon EC2 タスクからの出力例を示します。

```
{
    "read": "2020-10-02T00:51:13.410254284Z",
    "preread": "2020-10-02T00:51:12.406202398Z",
    "pids_stats": {
        "current": 3
    },
    "blkio_stats": {
        "io_service_bytes_recursive": [

        ],
        "io_serviced_recursive": [

        ],
        "io_queue_recursive": [

        ],
        "io_service_time_recursive": [

        ],
        "io_wait_time_recursive": [

        ],
        "io_merged_recursive": [

        ],
```

```
        "io_time_recursive": [

        ],
        "sectors_recursive": [

        ]
    },
    "num_procs": 0,
    "storage_stats": {

    },
    "cpu_stats": {
        "cpu_usage": {
            "total_usage": 360968065,
            "percpu_usage": [
                182359190,
                178608875
            ],
            "usage_in_kernelmode": 40000000,
            "usage_in_usermode": 290000000
        },
        "system_cpu_usage": 13939680000000,
        "online_cpus": 2,
        "throttling_data": {
            "periods": 0,
            "throttled_periods": 0,
            "throttled_time": 0
        }
    },
    "precpu_stats": {
        "cpu_usage": {
            "total_usage": 360968065,
            "percpu_usage": [
                182359190,
                178608875
            ],
            "usage_in_kernelmode": 40000000,
            "usage_in_usermode": 290000000
        },
        "system_cpu_usage": 13937670000000,
        "online_cpus": 2,
        "throttling_data": {
            "periods": 0,
            "throttled_periods": 0,
```

```
            "throttled_time": 0
        }
    },
    "memory_stats": {
        "usage": 1806336,
        "max_usage": 6299648,
        "stats": {
            "active_anon": 606208,
            "active_file": 0,
            "cache": 0,
            "dirty": 0,
            "hierarchical_memory_limit": 134217728,
            "hierarchical_memsw_limit": 268435456,
            "inactive_anon": 0,
            "inactive_file": 0,
            "mapped_file": 0,
            "pgfault": 4185,
            "pgmajfault": 0,
            "pgpgin": 2926,
            "pgpgout": 2778,
            "rss": 606208,
            "rss_huge": 0,
            "total_active_anon": 606208,
            "total_active_file": 0,
            "total_cache": 0,
            "total_dirty": 0,
            "total_inactive_anon": 0,
            "total_inactive_file": 0,
            "total_mapped_file": 0,
            "total_pgfault": 4185,
            "total_pgmajfault": 0,
            "total_pgpgin": 2926,
            "total_pgpgout": 2778,
            "total_rss": 606208,
            "total_rss_huge": 0,
            "total_unevictable": 0,
            "total_writeback": 0,
            "unevictable": 0,
            "writeback": 0
        },
        "limit": 134217728
    },
    "name": "/ecs-curltest-26-curl-c2e5f6e0cf91b0bead01",
    "id": "5fc21e5b015f899d22618f8aede80b6d70d71b2a75465ea49d9462c8f3d2d3af",
```

```
    "networks": {
        "eth0": {
            "rx_bytes": 84,
            "rx_packets": 2,
            "rx_errors": 0,
            "rx_dropped": 0,
            "tx_bytes": 84,
            "tx_packets": 2,
            "tx_errors": 0,
            "tx_dropped": 0
        }
    },
    "network_rate_stats": {
        "rx_bytes_per_sec": 0,
        "tx_bytes_per_sec": 0
    }
}
```

タスク統計情報のレスポンス例

${ECS_CONTAINER_METADATA_URI_V4}/task/stats エンドポイントにクエリを実行すると、コンテナが属しているタスクに関するネットワークメトリクスが返されます。以下に出力例を示します。

```
{
    "01999f2e5c6cf4df3873f28950e6278813408f281c54778efec860d0caad4854": {
        "read": "2020-10-02T00:51:32.51467703Z",
        "preread": "2020-10-02T00:51:31.50860463Z",
        "pids_stats": {
            "current": 1
        },
        "blkio_stats": {
            "io_service_bytes_recursive": [

            ],
            "io_serviced_recursive": [

            ],
            "io_queue_recursive": [

            ],
            "io_service_time_recursive": [
```

```
            ],
            "io_wait_time_recursive": [

            ],
            "io_merged_recursive": [

            ],
            "io_time_recursive": [

            ],
            "sectors_recursive": [

            ]
        },
        "num_procs": 0,
        "storage_stats": {

        },
        "cpu_stats": {
            "cpu_usage": {
                "total_usage": 177232665,
                "percpu_usage": [
                    13376224,
                    163856441
                ],
                "usage_in_kernelmode": 0,
                "usage_in_usermode": 160000000
            },
            "system_cpu_usage": 13977820000000,
            "online_cpus": 2,
            "throttling_data": {
                "periods": 0,
                "throttled_periods": 0,
                "throttled_time": 0
            }
        },
        "precpu_stats": {
            "cpu_usage": {
                "total_usage": 177232665,
                "percpu_usage": [
                    13376224,
                    163856441
                ],
                "usage_in_kernelmode": 0,
```

```
                "usage_in_usermode": 160000000
            },
            "system_cpu_usage": 13975800000000,
            "online_cpus": 2,
            "throttling_data": {
                "periods": 0,
                "throttled_periods": 0,
                "throttled_time": 0
            }
        },
        "memory_stats": {
            "usage": 532480,
            "max_usage": 6279168,
            "stats": {
                "active_anon": 40960,
                "active_file": 0,
                "cache": 0,
                "dirty": 0,
                "hierarchical_memory_limit": 9223372036854771712,
                "hierarchical_memsw_limit": 9223372036854771712,
                "inactive_anon": 0,
                "inactive_file": 0,
                "mapped_file": 0,
                "pgfault": 2033,
                "pgmajfault": 0,
                "pgpgin": 1734,
                "pgpgout": 1724,
                "rss": 40960,
                "rss_huge": 0,
                "total_active_anon": 40960,
                "total_active_file": 0,
                "total_cache": 0,
                "total_dirty": 0,
                "total_inactive_anon": 0,
                "total_inactive_file": 0,
                "total_mapped_file": 0,
                "total_pgfault": 2033,
                "total_pgmajfault": 0,
                "total_pgpgin": 1734,
                "total_pgpgout": 1724,
                "total_rss": 40960,
                "total_rss_huge": 0,
                "total_unevictable": 0,
                "total_writeback": 0,
```

```
                "unevictable": 0,
                "writeback": 0
            },
            "limit": 4073377792
        },
        "name": "/ecs-curltest-26-internalecspause-a6bcc3dbadfacfe85300",
        "id": "01999f2e5c6cf4df3873f28950e6278813408f281c54778efec860d0caad4854",
        "networks": {
            "eth0": {
                "rx_bytes": 84,
                "rx_packets": 2,
                "rx_errors": 0,
                "rx_dropped": 0,
                "tx_bytes": 84,
                "tx_packets": 2,
                "tx_errors": 0,
                "tx_dropped": 0
            }
        },
        "network_rate_stats": {
            "rx_bytes_per_sec": 0,
            "tx_bytes_per_sec": 0
        }
    },
    "5fc21e5b015f899d22618f8aede80b6d70d71b2a75465ea49d9462c8f3d2d3af": {
        "read": "2020-10-02T00:51:32.512771349Z",
        "preread": "2020-10-02T00:51:31.510597736Z",
        "pids_stats": {
            "current": 3
        },
        "blkio_stats": {
            "io_service_bytes_recursive": [

            ],
            "io_serviced_recursive": [

            ],
            "io_queue_recursive": [

            ],
            "io_service_time_recursive": [

            ],
            "io_wait_time_recursive": [
```

```
            ],
            "io_merged_recursive": [

            ],
            "io_time_recursive": [

            ],
            "sectors_recursive": [

            ]
        },
        "num_procs": 0,
        "storage_stats": {

        },
        "cpu_stats": {
            "cpu_usage": {
                "total_usage": 379075681,
                "percpu_usage": [
                    191355275,
                    187720406
                ],
                "usage_in_kernelmode": 60000000,
                "usage_in_usermode": 310000000
            },
            "system_cpu_usage": 13977800000000,
            "online_cpus": 2,
            "throttling_data": {
                "periods": 0,
                "throttled_periods": 0,
                "throttled_time": 0
            }
        },
        "precpu_stats": {
            "cpu_usage": {
                "total_usage": 378825197,
                "percpu_usage": [
                    191104791,
                    187720406
                ],
                "usage_in_kernelmode": 60000000,
                "usage_in_usermode": 310000000
            },
```

```
            "system_cpu_usage": 13975800000000,
            "online_cpus": 2,
            "throttling_data": {
                "periods": 0,
                "throttled_periods": 0,
                "throttled_time": 0
            }
        },
        "memory_stats": {
            "usage": 1814528,
            "max_usage": 6299648,
            "stats": {
                "active_anon": 606208,
                "active_file": 0,
                "cache": 0,
                "dirty": 0,
                "hierarchical_memory_limit": 134217728,
                "hierarchical_memsw_limit": 268435456,
                "inactive_anon": 0,
                "inactive_file": 0,
                "mapped_file": 0,
                "pgfault": 5377,
                "pgmajfault": 0,
                "pgpgin": 3613,
                "pgpgout": 3465,
                "rss": 606208,
                "rss_huge": 0,
                "total_active_anon": 606208,
                "total_active_file": 0,
                "total_cache": 0,
                "total_dirty": 0,
                "total_inactive_anon": 0,
                "total_inactive_file": 0,
                "total_mapped_file": 0,
                "total_pgfault": 5377,
                "total_pgmajfault": 0,
                "total_pgpgin": 3613,
                "total_pgpgout": 3465,
                "total_rss": 606208,
                "total_rss_huge": 0,
                "total_unevictable": 0,
                "total_writeback": 0,
                "unevictable": 0,
                "writeback": 0
```

```
            },
            "limit": 134217728
        },
        "name": "/ecs-curltest-26-curl-c2e5f6e0cf91b0bead01",
        "id": "5fc21e5b015f899d22618f8aede80b6d70d71b2a75465ea49d9462c8f3d2d3af",
        "networks": {
            "eth0": {
                "rx_bytes": 84,
                "rx_packets": 2,
                "rx_errors": 0,
                "rx_dropped": 0,
                "tx_bytes": 84,
                "tx_packets": 2,
                "tx_errors": 0,
                "tx_dropped": 0
            }
        },
        "network_rate_stats": {
            "rx_bytes_per_sec": 0,
            "tx_bytes_per_sec": 0
        }
    }
}
```

Amazon ECS タスクメタデータエンドポイントバージョン 3

> **Important**
>
> タスクメタデータのバージョン 3 エンドポイントは、現在アクティブにメンテナンスされていません。タスクメタデータバージョン 4 エンドポイントを更新して、最新のメタデータエンドポイント情報を取得することをお勧めします。詳細については、「the section called “タスクメタデータエンドポイントバージョン 4”」を参照してください。
>
> AWS Fargate でホストされている Amazon ECS タスクを使用している場合は、「Fargate 上のタスク用の Amazon ECS タスクのメタデータエンドポイントバージョン 3」を参照してください。

Amazon ECS コンテナエージェントの 1.21.0 バージョン以降では、エージェントはタスクの各コンテナに、環境変数 ECS_CONTAINER_METADATA_URI を挿入します。タスクメタデータバージョン 3 エンドポイントに対してクエリを実行すると、さまざまなタスクメタデータおよび Docker 統計 をタ

スクで利用できます。bridge ネットワークモードを使用するタスクの場合、/stats エンドポイントにクエリを実行する際にネットワークメトリクスを使用できます。

タスクメタデータエンドポイントバージョン 3 の機能は、プラットフォームのバージョン v1.3.0 以降で 1.54.0 Fargate 起動タイプを使用するタスクと、EC2 起動タイプを使用し、Amazon EC2 コンテナエージェントのバージョン 1.21.0 以降を実行する Amazon EC2 Linux インフラストラクチャで起動されるタスク、または、Amazon EC2コンテナエージェントの最新のバージョン awsvpc を実行するAmazon ECS Windows インフラストラクチャで起動され、ネットワークモードで使用するタスクは、デフォルトで有効になります。詳細については、「Amazon ECS Linux コンテナインスタンスの管理」を参照してください。

エージェントを最新バージョンに更新することで、古いコンテナインスタンスにこの機能のサポートを追加できます。詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

> **Important**
>
> Fargate 起動タイプおよびプラットフォーム v1.3.0 以前を使用するタスクでは、タスクメタデータバージョン 2 エンドポイントはサポートされています。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 2」を参照してください。

タスクメタデータエンドポイントバージョン 3 パス

次のタスクメタデータエンドポイントをコンテナで使用できます。

`${ECS_CONTAINER_METADATA_URI}`

このパスはコンテナのメタデータ JSON を返します。

`${ECS_CONTAINER_METADATA_URI}/task`

このパスはタスクのメタデータ JSON を返します。これには、タスクに関連付けられたすべてのコンテナのコンテナ ID および名前のリストが含まれています。このエンドポイントのレスポンスの詳細については、「Amazon ECS タスクメタデータ v3 JSON レスポンス」を参照してください。

`${ECS_CONTAINER_METADATA_URI}/taskWithTags`

このパスは、ListTagsForResource API を使用して取得できるタスクとコンテナインスタンスタグに加えて、/task エンドポイントに含まれるタスクのメタデータを返します。

`${ECS_CONTAINER_METADATA_URI}/stats`

このパスは特定の Docker コンテナの Docker 統計 JSON を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

`${ECS_CONTAINER_METADATA_URI}/task/stats`

このパスはタスクに関連付けられたすべてのコンテナの Docker 統計 JSON を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

Amazon ECS タスクメタデータ v3 JSON レスポンス

次の情報が、タスクメタデータエンドポイント (`${ECS_CONTAINER_METADATA_URI}/task`) JSON レスポンスから返されます。

`Cluster`

タスクが属する Amazon ECS クラスターの Amazon リソースネーム (ARN)または短縮名。

`TaskARN`

コンテナが属しているタスクの Amazon リソースネーム (ARN)。

`Family`

タスクの Amazon ECS タスク定義のファミリー。

`Revision`

タスクの Amazon ECS タスク定義のリビジョン。

`DesiredStatus`

Amazon ECSからのタスクの望ましいステータス。

`KnownStatus`

Amazon ECS からのタスクの既知のステータス。

`Limits`

CPU (vCPU で表される) やメモリなど、タスク レベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`PullStartedAt`

最初のコンテナイメージのプル開始時のタイムスタンプ。

`PullStoppedAt`

最後のコンテナイメージのプル終了時のタイムスタンプ。

`AvailabilityZone`

タスクがあるアベイラビリティーゾーン。

> **Note**
>
> アベイラビリティーゾーンのメタデータは、プラットフォームバージョン 1.4 以降 (Linux) または 1.0.0 以降 (Windows) を使用する Fargate タスクでのみ使用できます。

`Containers`

タスクに関連付けられている各コンテナのコンテナメタデータのリスト。

`DockerId`

コンテナの Docker ID。

`Name`

タスク定義で指定されたコンテナの名前。

`DockerName`

Docker に提供されたコンテナの名前。Amazon ECSコンテナエージェントはコンテナに一意の名前を生成し、同じタスク定義の複数のコピーが単一のインスタンスで実行される場合に名前の競合を回避します。

`Image`

コンテナのイメージ。

`ImageID`

イメージの SHA-256 ダイジェスト。

`Ports`

コンテナに対して公開されている任意のポート。公開ポートがない場合はこのパラメータは省略されます。

`Labels`

コンテナに適用された任意のラベル。ラベルが適用されていない場合はこのパラメータは省略されます。

`DesiredStatus`

Amazon ECSからのコンテナの望ましいステータス。

`KnownStatus`

Amazon ECS からのコンテナの既知のステータス。

`ExitCode`

コンテナの終了コード。このパラメータは、コンテナが終了していない場合は省略されます。

`Limits`

CPU (CPU 単位で表される) やメモリなど、コンテナレベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`CreatedAt`

コンテナ作成時のタイムスタンプ。このパラメータは、コンテナがまだ作成されていない場合は省略されます。

`StartedAt`

コンテナ起動時のタイムスタンプ。このパラメータは、コンテナがまだ起動していない場合は省略されます。

`FinishedAt`

コンテナ停止時のタイムスタンプ。このパラメータは、コンテナがまだ停止していない場合は省略されます。

`Type`

コンテナのタイプ。タスク定義で指定されているコンテナのタイプは `NORMAL` です。他のコンテナタイプは無視してかまいません。これらはAmazon ECS コンテナエージェントによってプロビジョニングされる内部タスクリソースで使用されます。

`Networks`

ネットワークモードや IP アドレスなど、コンテナのネットワーク情報。ネットワーク情報が定義されていない場合はこのパラメータは省略されます。

`ClockDrift`

基準時刻とシステム時刻の違いに関する情報。これは、Linux オペレーティングシステムに適用されます。この機能では、Amazon Time Sync Service を使用してクロックの精度を測定し、コンテナのクロックエラー範囲を特定します。詳細については、「Linux インスタンス用 Amazon EC2 ユーザーガイド」の「Linux インスタンスの時刻の設定」を参照してください。

`ReferenceTime`

クロック精度の基礎。Amazon ECS は、`2021-09-07T16:57:44Z` などの NTP を通じて協定世界時 (UTC) の世界標準を使用しています。

`ClockErrorBound`

UTC へのオフセットとして定義されるクロックエラーの対策。この誤差は、基準時刻とシステム時刻の差 (ミリ秒単位) です。

`ClockSynchronizationStatus`

最新のシステム時刻と基準時刻間の同期試行における成功状況を示します。

有効な値は `SYNCHRONIZED` および `NOT_SYNCHRONIZED` です。

`ExecutionStoppedAt`

タスクの `DesiredStatus` が `STOPPED` に移行した時のタイムスタンプ。これは、必須コンテナが `STOPPED` に移行したときに発生します。

Amazon ECS タスクメタデータ v3 の例

以下の例は、タスクメタデータエンドポイントからの出力を示しています。

コンテナメタデータレスポンスの例

`${ECS_CONTAINER_METADATA_URI}` エンドポイントにクエリを実行すると、コンテナ自体に関するメタデータのみが返されます。以下に出力例を示します。

```
{
    "DockerId": "43481a6ce4842eec8fe72fc28500c6b52edcc0917f105b83379f88cac1ff3946",
    "Name": "nginx-curl",
    "DockerName": "ecs-nginx-5-nginx-curl-ccccb9f49db0dfe0d901",
    "Image": "nrdlngr/nginx-curl",
    "ImageID":
 "sha256:2e00ae64383cfc865ba0a2ba37f61b50a120d2d9378559dcd458dc0de47bc165",
    "Labels": {
```

```
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "nginx-curl",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
        "com.amazonaws.ecs.task-definition-version": "5"
    },
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
    "Limits": {
        "CPU": 512,
        "Memory": 512
    },
    "CreatedAt": "2018-02-01T20:55:10.554941919Z",
    "StartedAt": "2018-02-01T20:55:11.064236631Z",
    "Type": "NORMAL",
    "Networks": [
        {
            "NetworkMode": "awsvpc",
            "IPv4Addresses": [
                "10.0.2.106"
            ]
        }
    ]
}
```

タスクメタデータレスポンスの例

${ECS_CONTAINER_METADATA_URI}/task エンドポイントにクエリを実行すると、コンテナが属しているタスクに関するメタデータが返されます。以下に出力例を示します。

1 つのコンテナタスクの JSON レスポンスを次に示します。

```
{
  "Cluster": "default",
  "TaskARN": "arn:aws:ecs:us-east-2:012345678910:task/9781c248-0edd-4cdb-9a93-
f63cb662a5d3",
  "Family": "nginx",
  "Revision": "5",
  "DesiredStatus": "RUNNING",
  "KnownStatus": "RUNNING",
  "Containers": [
    {
```

```
      "DockerId": "731a0d6a3b4210e2448339bc7015aaa79bfe4fa256384f4102db86ef94cbbc4c",
      "Name": "~internal~ecs~pause",
      "DockerName": "ecs-nginx-5-internalecspause-acc699c0cbf2d6d11700",
      "Image": "amazon/amazon-ecs-pause:0.1.0",
      "ImageID": "",
      "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "~internal~ecs~pause",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RESOURCES_PROVISIONED",
      "KnownStatus": "RESOURCES_PROVISIONED",
      "Limits": {
        "CPU": 0,
        "Memory": 0
      },
      "CreatedAt": "2018-02-01T20:55:08.366329616Z",
      "StartedAt": "2018-02-01T20:55:09.058354915Z",
      "Type": "CNI_PAUSE",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "10.0.2.106"
          ]
        }
      ]
    },
    {
      "DockerId": "43481a6ce4842eec8fe72fc28500c6b52edcc0917f105b83379f88cac1ff3946",
      "Name": "nginx-curl",
      "DockerName": "ecs-nginx-5-nginx-curl-ccccb9f49db0dfe0d901",
      "Image": "nrdlngr/nginx-curl",
      "ImageID":
 "sha256:2e00ae64383cfc865ba0a2ba37f61b50a120d2d9378559dcd458dc0de47bc165",
      "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "nginx-curl",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
```

```
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RUNNING",
      "KnownStatus": "RUNNING",
      "Limits": {
        "CPU": 512,
        "Memory": 512
      },
      "CreatedAt": "2018-02-01T20:55:10.554941919Z",
      "StartedAt": "2018-02-01T20:55:11.064236631Z",
      "Type": "NORMAL",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "10.0.2.106"
          ]
        }
      ]
    }
  ],
  "PullStartedAt": "2018-02-01T20:55:09.372495529Z",
  "PullStoppedAt": "2018-02-01T20:55:10.552018345Z",
  "AvailabilityZone": "us-east-2b"
}
```


Amazon ECS タスクメタデータエンドポイントバージョン 2

> **Important**
>
> タスクメタデータのバージョン 2 エンドポイントは、現在アクティブにメンテナンスされていません。タスクメタデータバージョン 4 エンドポイントを更新して、最新のメタデータエンドポイント情報を取得することをお勧めします。詳細については、「the section called “タスクメタデータエンドポイントバージョン 4”」を参照してください。

Amazon ECS コンテナエージェントのバージョン 1.17.0 から、さまざまなタスクメタデータおよび [Docker 統計]を、Amazon ECS コンテナエージェントによって指定される HTTP エンドポイントで awsvpc ネットワークモードを使用するタスクで利用できます。

awsvpc ネットワークモードで起動されたタスクに属するすべてのコンテナには、事前定義されたリンクローカルアドレス範囲内のローカル IPv4 アドレスが割り当てられます。コンテナがメタデータ

エンドポイントにクエリを実行する場合、Amazon ECS コンテナエージェントは、一意の IP アドレスに基づいてコンテナが属するタスクを判断し、そのタスクのメタデータと統計情報を返します。

タスクメタデータの有効化

タスクメタデータバージョン 2 機能は、デフォルトで次のタスクに対して有効に設定されています。

- プラットフォームバージョンが v1.1.0 以降の Fargate 起動タイプを使用するタスク。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。
- awsvpc ネットワークモードも使用し、Amazon ECSコンテナエージェントのバージョン1.17.0以上を実行しているAmazon EC2 Linuxインフラストラクチャまたは Amazon ECS コンテナエージェントの1.54.0バージョン以上を実行しているAmazon EC2 Windows インフラストラクチャで起動されるEC2 起動タイプを使用するタスク。詳細については、「Amazon ECS Linux コンテナインスタンスの管理」を参照してください。

エージェントを最新バージョンに更新することで、古いコンテナインスタンスにこの機能のサポートを追加できます。詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

タスクメタデータエンドポイントのパス

次の API エンドポイントをコンテナで使用できます。

`169.254.170.2/v2/metadata`

このエンドポイントはタスクのメタデータ JSON を返します。これには、タスクに関連付けられたすべてのコンテナのコンテナ ID および名前のリストが含まれています。このエンドポイントのレスポンスの詳細については、「タスクメタデータ JSON レスポンス」を参照してください。

`169.254.170.2/v2/metadata/<container-id>`

このエンドポイントは指定された Docker コンテナ ID のメタデータ JSON を返します。

`169.254.170.2/v2/metadata/taskWithTags`

このパスは、ListTagsForResource API を使用して取得できるタスクとコンテナインスタンスタグに加えて、/task エンドポイントに含まれるタスクのメタデータを返します。

`169.254.170.2/v2/stats`

このエンドポイントはタスクに関連付けられたすべてのコンテナの Docker 統計 JSON を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

`169.254.170.2/v2/stats/<container-id>`

このエンドポイントは指定された Docker コンテナ ID の Docker 統計 JSON を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

タスクメタデータ JSON レスポンス

次の情報が、タスクメタデータエンドポイント (`169.254.170.2/v2/metadata`) JSON レスポンスから返されます。

`Cluster`

タスクが属する Amazon ECS クラスターの Amazon リソースネーム (ARN)または短縮名。

`TaskARN`

コンテナが属しているタスクの Amazon リソースネーム (ARN)。

`Family`

タスクの Amazon ECS タスク定義のファミリー。

`Revision`

タスクの Amazon ECS タスク定義のリビジョン。

`DesiredStatus`

Amazon ECSからのタスクの望ましいステータス。

`KnownStatus`

Amazon ECS からのタスクの既知のステータス。

`Limits`

CPU (vCPU で表される) やメモリなど、タスク レベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`PullStartedAt`

最初のコンテナイメージのプル開始時のタイムスタンプ。

`PullStoppedAt`

最後のコンテナイメージのプル終了時のタイムスタンプ。

`AvailabilityZone`

タスクがあるアベイラビリティーゾーン。

> **Note**
>
> アベイラビリティーゾーンのメタデータは、プラットフォームバージョン 1.4 以降 (Linux) または 1.0.0 以降 (Windows) を使用する Fargate タスクでのみ使用できます。

`Containers`

タスクに関連付けられている各コンテナのコンテナメタデータのリスト。

`DockerId`

コンテナの Docker ID。

`Name`

タスク定義で指定されたコンテナの名前。

`DockerName`

Docker に提供されたコンテナの名前。Amazon ECSコンテナエージェントはコンテナに一意の名前を生成し、同じタスク定義の複数のコピーが単一のインスタンスで実行される場合に名前の競合を回避します。

`Image`

コンテナのイメージ。

`ImageID`

イメージの SHA-256 ダイジェスト。

`Ports`

コンテナに対して公開されている任意のポート。公開ポートがない場合はこのパラメータは省略されます。

`Labels`

コンテナに適用された任意のラベル。ラベルが適用されていない場合はこのパラメータは省略されます。

`DesiredStatus`

Amazon ECSからのコンテナの望ましいステータス。

`KnownStatus`

Amazon ECS からのコンテナの既知のステータス。

`ExitCode`

コンテナの終了コード。このパラメータは、コンテナが終了していない場合は省略されます。

`Limits`

CPU (CPU 単位で表される) やメモリなど、コンテナレベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`CreatedAt`

コンテナ作成時のタイムスタンプ。このパラメータは、コンテナがまだ作成されていない場合は省略されます。

`StartedAt`

コンテナ起動時のタイムスタンプ。このパラメータは、コンテナがまだ起動していない場合は省略されます。

`FinishedAt`

コンテナ停止時のタイムスタンプ。このパラメータは、コンテナがまだ停止していない場合は省略されます。

`Type`

コンテナのタイプ。タスク定義で指定されているコンテナのタイプは `NORMAL` です。他のコンテナタイプは無視してかまいません。これらはAmazon ECS コンテナエージェントによってプロビジョニングされる内部タスクリソースで使用されます。

`Networks`

ネットワークモードや IP アドレスなど、コンテナのネットワーク情報。ネットワーク情報が定義されていない場合はこのパラメータは省略されます。

`ClockDrift`

基準時刻とシステム時刻の違いに関する情報。これは、Linux オペレーティングシステムに適用されます。この機能では、Amazon Time Sync Service を使用してクロックの精度を測定し、コンテナのクロックエラー範囲を特定します。詳細については、「Linux インスタンス用 Amazon EC2 ユーザーガイド」の「Linux インスタンスの時刻の設定」を参照してください。

`ReferenceTime`

クロック精度の基礎。Amazon ECS は、`2021-09-07T16:57:44Z` などの NTP を通じて協定世界時 (UTC) の世界標準を使用しています。

`ClockErrorBound`

UTC へのオフセットとして定義されるクロックエラーの対策。この誤差は、基準時刻とシステム時刻の差 (ミリ秒単位) です。

`ClockSynchronizationStatus`

最新のシステム時刻と基準時刻間の同期試行における成功状況を示します。

有効な値は `SYNCHRONIZED` および `NOT_SYNCHRONIZED` です。

`ExecutionStoppedAt`

タスクの `DesiredStatus` が `STOPPED` に移行した時のタイムスタンプ。これは、必須コンテナが `STOPPED` に移行したときに発生します。

タスクメタデータレスポンスの例

1 つのコンテナタスクの JSON レスポンスを次に示します。

```
{
  "Cluster": "default",
  "TaskARN": "arn:aws:ecs:us-east-2:012345678910:task/9781c248-0edd-4cdb-9a93-
f63cb662a5d3",
  "Family": "nginx",
  "Revision": "5",
  "DesiredStatus": "RUNNING",
  "KnownStatus": "RUNNING",
  "Containers": [
    {
      "DockerId": "731a0d6a3b4210e2448339bc7015aaa79bfe4fa256384f4102db86ef94cbbc4c",
      "Name": "~internal~ecs~pause",
      "DockerName": "ecs-nginx-5-internalecspause-acc699c0cbf2d6d11700",
```

```
      "Image": "amazon/amazon-ecs-pause:0.1.0",
      "ImageID": "",
      "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "~internal~ecs~pause",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RESOURCES_PROVISIONED",
      "KnownStatus": "RESOURCES_PROVISIONED",
      "Limits": {
        "CPU": 0,
        "Memory": 0
      },
      "CreatedAt": "2018-02-01T20:55:08.366329616Z",
      "StartedAt": "2018-02-01T20:55:09.058354915Z",
      "Type": "CNI_PAUSE",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "10.0.2.106"
          ]
        }
      ]
    },
    {
      "DockerId": "43481a6ce4842eec8fe72fc28500c6b52edcc0917f105b83379f88cac1ff3946",
      "Name": "nginx-curl",
      "DockerName": "ecs-nginx-5-nginx-curl-ccccb9f49db0dfe0d901",
      "Image": "nrdlngr/nginx-curl",
      "ImageID":
 "sha256:2e00ae64383cfc865ba0a2ba37f61b50a120d2d9378559dcd458dc0de47bc165",
      "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "nginx-curl",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RUNNING",
```

```
      "KnownStatus": "RUNNING",
      "Limits": {
        "CPU": 512,
        "Memory": 512
      },
      "CreatedAt": "2018-02-01T20:55:10.554941919Z",
      "StartedAt": "2018-02-01T20:55:11.064236631Z",
      "Type": "NORMAL",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "10.0.2.106"
          ]
        }
      ]
    }
  ],
  "PullStartedAt": "2018-02-01T20:55:09.372495529Z",
  "PullStoppedAt": "2018-02-01T20:55:10.552018345Z",
  "AvailabilityZone": "us-east-2b"
}
```


Fargate のタスクで使用できる Amazon ECS タスクメタデータ

FargateのAmazon ECS は、コンテナとその一部であるタスクに関するさまざまなメタデータ、ネットワークメトリクス、および Docker 統計情報を取得する方法を提供します。これは、タスクメタデータエンドポイントと呼ばれます。Fargate タスクのAmazon ECSでは、次のタスクメタデータエンドポイントバージョンを使用できます:

- タスクメタデータエンドポイントバージョン 4 – プラットフォームバージョン 1.4.0 以降を使用するタスクで利用可能です。
- タスクメタデータエンドポイントバージョン 3 – プラットフォームバージョン 1.1.0 以降を使用するタスクで利用可能です。

awsvpc ネットワークモードで起動されたタスクに属するすべてのコンテナには、事前定義されたリンクローカルアドレス範囲内のローカル IPv4 アドレスが割り当てられます。コンテナがメタデータエンドポイントにクエリを実行する場合、コンテナエージェントは、一意の IP アドレスに基づいてコンテナが属するタスクを判断し、そのタスクのメタデータと統計情報を返します。

トピック

Fargate のタスク用の Amazon ECS タスクメタデータエンドポイントバージョン 4

> **Important**
>
> Amazon EC2 インスタンスでホストされている Amazon ECS タスクを使用している場合は、「Amazon ECS タスクのメタデータエンドポイント」を参照してください。

Fargateのプラットフォームバージョン1.4.0以降、ECS_CONTAINER_METADATA_URI_V4 という名前の環境変数がタスク内の各コンテナに挿入されます。タスクメタデータエンドポイントバージョン 4 に対してクエリを実行すると、さまざまなタスクメタデータおよび Docker 統計をタスクで利用できます。

タスクメタデータエンドポイントバージョン 4 は、バージョン 3 と同じように動作しますが、コンテナとタスクに関する追加のネットワークメタデータを提供します。/stats エンドポイントにクエリを実行するときにも追加のネットワークメトリクスを使用できます。

タスクメタデータエンドポイントは、プラットフォームバージョン 1.4.0 以降を使用する AWS Fargate 上で実行される、すべての Amazon ECS タスクに対してデフォルトでオンになっています。

> **Note**
>
> 新しいタスクメタデータエンドポイントバージョンを今後作成する必要がないように、追加のメタデータをバージョン 4 の出力に追加できます。既存のメタデータが削除されたり、メタデータのフィールド名が変更されたりすることはありません。

Fargate タスクメタデータエンドポイントバージョン 4 のパス

次のタスクメタデータエンドポイントをコンテナで使用できます。

`${ECS_CONTAINER_METADATA_URI_V4}`

このパスはコンテナのメタデータを返します。

`${ECS_CONTAINER_METADATA_URI_V4}/task`

このパスはタスクのメタデータを返します。これには、タスクに関連付けられたすべてのコンテナのコンテナ ID および名前のリストが含まれています。このエンドポイントのレスポンスの詳細については、「Fargate のタスク用の Amazon ECS タスクメタデータ v4 JSON レスポンス」を参照してください。

`${ECS_CONTAINER_METADATA_URI_V4}/stats`

このパスは Docker コンテナの Docker 統計を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

> **Note**
>
> AWS FargateでのAmazon ECS タスクは、コンテナの統計を返す前にコンテナを約 1 秒間実行する必要があります。

`${ECS_CONTAINER_METADATA_URI_V4}/task/stats`

このパスはタスクに関連付けられたすべてのコンテナの Docker 統計を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

> **Note**
>
> AWS FargateでのAmazon ECS タスクは、コンテナの統計を返す前にコンテナを約 1 秒間実行する必要があります。

Fargate のタスク用の Amazon ECS タスクメタデータ v4 JSON レスポンス

次のメタデータは、タスクメタデータエンドポイント (`${ECS_CONTAINER_METADATA_URI_V4}/task`) JSON レスポンスで返されます。

`Cluster`

タスクが属する Amazon ECS クラスターの Amazon リソースネーム (ARN)または短縮名。

`VPCID`

Amazon EC2 コンテナインスタンスの VPC ID。このフィールドは、Amazon EC2 インスタンスでのみ表示されます。

> **Note**
>
> この VPCID メタデータは、Amazon ECS コンテナエージェントのバージョン 1.63.1、もしくはそれ以降を使用している場合にのみ含まれます。

`TaskARN`

コンテナが属しているタスクの Amazon リソースネーム (ARN)。

`Family`

タスクの Amazon ECS タスク定義のファミリー。

`Revision`

タスクの Amazon ECS タスク定義のリビジョン。

`DesiredStatus`

Amazon ECSからのタスクの望ましいステータス。

`KnownStatus`

Amazon ECS からのタスクの既知のステータス。

`Limits`

CPU (vCPU で表される) やメモリなど、タスクレベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`PullStartedAt`

最初のコンテナイメージのプル開始時のタイムスタンプ。

`PullStoppedAt`

最後のコンテナイメージのプル終了時のタイムスタンプ。

`AvailabilityZone`

タスクがあるアベイラビリティーゾーン。

> **Note**
>
> アベイラビリティーゾーンのメタデータは、プラットフォームバージョン 1.4 以降 (Linux) または 1.0.0 (Windows) を使用する Fargate タスクでのみ使用できます。

`LaunchType`

タスクが使用している起動タイプ。クラスター容量プロバイダーを使用する場合、タスクが Fargate インフラストラクチャと EC2 インフラストラクチャのいずれを使用しているかを示します。

> **Note**
>
> このLaunchTypeメタデータは、Amazon ECS Linux コンテナエージェントのバージョン1.45.0 以降 (Linux) または 1.0.0 以降 (Windows) を使用している場合にのみ含まれます。

`EphemeralStorageMetrics`

このタスクのエフェメラルストレージの予約サイズと現在の使用量。

> **Note**
>
> Fargate はディスク上のスペースを予約します。スペースは Fargate によってのみ使用されます。これには課金されることはありません。これらのメトリクスには表示されません。ただし、この追加ストレージは、df などの他のツールでも確認できます。

`Utilized`

このタスクの現在のエフェメラルストレージ使用量 (MiB 単位)。

`Reserved`

このタスクの予約済みエフェメラルストレージ (MiB 単位)。エフェメラルストレージのサイズは、実行中のタスクでは変更できません。タスク定義で ephermalStorage オブジェクトを指定して、エフェメラルストレージの量を変更できます。ephermalStorage は MiB ではなく GiB 単位で指定されます。ephermalStorage および EphemeralStorageMetrics は、Fargate Linux プラットフォームのバージョン 1.4.0 以降でのみ使用できます。

`Containers`

タスクに関連付けられている各コンテナのコンテナメタデータのリスト。

`DockerId`

コンテナの Docker ID。

Fargate を使用する場合、IDは32桁の16進数に10桁の数字が続きます。

`Name`

タスク定義で指定されたコンテナの名前。

`DockerName`

Docker に提供されたコンテナの名前。Amazon ECSコンテナエージェントはコンテナに一意の名前を生成し、同じタスク定義の複数のコピーが単一のインスタンスで実行される場合に名前の競合を回避します。

`Image`

コンテナのイメージ。

`ImageID`

イメージの SHA-256 ダイジェスト。

`Ports`

コンテナに対して公開されている任意のポート。公開ポートがない場合はこのパラメータは省略されます。

`Labels`

コンテナに適用された任意のラベル。ラベルが適用されていない場合はこのパラメータは省略されます。

`DesiredStatus`

Amazon ECSからのコンテナの望ましいステータス。

`KnownStatus`

Amazon ECS からのコンテナの既知のステータス。

`ExitCode`

コンテナの終了コード。このパラメータは、コンテナが終了していない場合は省略されます。

`Limits`

CPU (CPU 単位で表される) やメモリなど、コンテナレベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`CreatedAt`

コンテナ作成時のタイムスタンプ。このパラメータは、コンテナがまだ作成されていない場合は省略されます。

`StartedAt`

コンテナ起動時のタイムスタンプ。このパラメータは、コンテナがまだ起動していない場合は省略されます。

`FinishedAt`

コンテナ停止時のタイムスタンプ。このパラメータは、コンテナがまだ停止していない場合は省略されます。

`Type`

コンテナのタイプ。タスク定義で指定されているコンテナのタイプは `NORMAL` です。他のコンテナタイプは無視してかまいません。これらはAmazon ECS コンテナエージェントによってプロビジョニングされる内部タスクリソースで使用されます。

`LogDriver`

コンテナに使用されるログドライバー。

> **Note**
>
> この`LogDriver`メタデータは、Amazon ECS Linux コンテナエージェントのバージョン`1.45.0`、もしくはそれ以降を使用している場合にのみ含まれます。

`LogOptions`

コンテナに定義されたログドライバオプション。

> **Note**
>
> この`LogOptions`メタデータは、Amazon ECS Linux コンテナエージェントのバージョン`1.45.0`、もしくはそれ以降を使用している場合にのみ含まれます。

`ContainerARN`

コンテナの Amazon リソースネーム (ARN)。

> **Note**
>
> このContainerARNメタデータは、Amazon ECS Linux コンテナエージェントのバージョン1.45.0、もしくはそれ以降を使用している場合にのみ含まれます。

`Networks`

ネットワークモードや IP アドレスなど、コンテナのネットワーク情報。ネットワーク情報が定義されていない場合はこのパラメータは省略されます。

`Snapshotter`

このコンテナイメージをダウンロードするために containerd によって使用された snapshotter。有効な値はデフォルトの `overlayfs` です。`soci` は SOCI インデックスによる遅延読み込み時に使用されます。このパラメータは、Linux プラットフォームバージョン `1.4.0` で実行されるタスクにのみ使用できます。

`RestartCount`

コンテナが再起動された回数。

> **Note**
>
> `RestartCount` メタデータが含まれるのは、コンテナの再起動ポリシーが有効になっている場合のみです。詳細については、「コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する」を参照してください。

`ClockDrift`

基準時刻とシステム時刻の違いに関する情報。この機能では、Amazon Time Sync Service を使用してクロックの精度を測定し、コンテナのクロックエラー範囲を特定します。詳細については、「Linux インスタンス用 Amazon EC2 ユーザーガイド」の「Linux インスタンスの時刻の設定」を参照してください。

`ReferenceTime`

クロック精度の基礎。Amazon ECS は、`2021-09-07T16:57:44Z` などの NTP を通じて協定世界時 (UTC) の世界標準を使用しています。

ClockErrorBound

UTC へのオフセットとして定義されるクロックエラーの対策。この誤差は、基準時刻とシステム時刻の差 (ミリ秒単位) です。

ClockSynchronizationStatus

最新のシステム時刻と基準時刻間の同期試行における成功状況を示します。

有効な値は SYNCHRONIZED および NOT_SYNCHRONIZED です。

ExecutionStoppedAt

タスクの DesiredStatus が STOPPED に移行した時のタイムスタンプ。これは、必須コンテナが STOPPED に移行したときに発生します。

Fargate でのタスクの Amazon ECS タスクメタデータ v4 の例

以下の例は、AWS Fargateで実行されるAmazon ECS タスクのタスクメタデータエンドポイントからの出力例を示しています。

コンテナから、タスクメタデータのエンドポイントに続けて curl を使用すると、curl ${ECS_CONTAINER_METADATA_URI_V4}/task などのエンドポイントをクエリできます。

コンテナメタデータレスポンスの例

${ECS_CONTAINER_METADATA_URI_V4} エンドポイントにクエリを実行すると、コンテナ自体に関するメタデータのみが返されます。以下に出力例を示します。

```
{
    "DockerId": "cd189a933e5849daa93386466019ab50-2495160603",
    "Name": "curl",
    "DockerName": "curl",
    "Image": "111122223333.dkr.ecr.us-west-2.amazonaws.com/curltest:latest",
    "ImageID":
 "sha256:25f3695bedfb454a50f12d127839a68ad3caf91e451c1da073db34c542c4d2cb",
    "Labels": {
        "com.amazonaws.ecs.cluster": "arn:aws:ecs:us-west-2:111122223333:cluster/
default",
        "com.amazonaws.ecs.container-name": "curl",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-west-2:111122223333:task/default/
cd189a933e5849daa93386466019ab50",
        "com.amazonaws.ecs.task-definition-family": "curltest",
        "com.amazonaws.ecs.task-definition-version": "2"
```

```
    },
    "DesiredStatus": "RUNNING",
    "KnownStatus": "RUNNING",
    "Limits": {
        "CPU": 10,
        "Memory": 128
    },
    "CreatedAt": "2020-10-08T20:09:11.44527186Z",
    "StartedAt": "2020-10-08T20:09:11.44527186Z",
    "Type": "NORMAL",
    "Networks": [
        {
            "NetworkMode": "awsvpc",
            "IPv4Addresses": [
                "192.0.2.3"
            ],
            "AttachmentIndex": 0,
            "MACAddress": "0a:de:f6:10:51:e5",
            "IPv4SubnetCIDRBlock": "192.0.2.0/24",
            "DomainNameServers": [
                "192.0.2.2"
            ],
            "DomainNameSearchList": [
                "us-west-2.compute.internal"
            ],
            "PrivateDNSName": "ip-10-0-0-222.us-west-2.compute.internal",
            "SubnetGatewayIpv4Address": "192.0.2.0/24"
        }
    ],
    "ContainerARN": "arn:aws:ecs:us-west-2:111122223333:container/05966557-
f16c-49cb-9352-24b3a0dcd0e1",
    "LogOptions": {
        "awslogs-create-group": "true",
        "awslogs-group": "/ecs/containerlogs",
        "awslogs-region": "us-west-2",
        "awslogs-stream": "ecs/curl/cd189a933e5849daa93386466019ab50"
    },
    "LogDriver": "awslogs",
    "Snapshotter": "overlayfs"
}
```

Fargate でのタスクの Amazon ECS タスクメタデータ v4 の例

${ECS_CONTAINER_METADATA_URI_V4}/task エンドポイントにクエリを実行すると、コンテナが属しているタスクに関するメタデータが返されます。以下に出力例を示します。

```
{
  "Cluster": "arn:aws:ecs:us-east-1:123456789012:cluster/MyEmptyCluster",
  "TaskARN": "arn:aws:ecs:us-east-1:123456789012:task/MyEmptyCluster/
bfa2636268144d039771334145e490c5",
  "Family": "sample-fargate",
  "Revision": "5",
  "DesiredStatus": "RUNNING",
  "KnownStatus": "RUNNING",
  "Limits": {
    "CPU": 0.25,
    "Memory": 512
  },
  "PullStartedAt": "2023-07-21T15:45:33.532811081Z",
  "PullStoppedAt": "2023-07-21T15:45:38.541068435Z",
  "AvailabilityZone": "us-east-1d",
  "Containers": [
    {
      "DockerId": "bfa2636268144d039771334145e490c5-1117626119",
      "Name": "curl-image",
      "DockerName": "curl-image",
      "Image": "curlimages/curl",
      "ImageID":
 "sha256:daf3f46a2639c1613b25e85c9ee4193af8a1d538f92483d67f9a3d7f21721827",
      "Labels": {
        "com.amazonaws.ecs.cluster": "arn:aws:ecs:us-east-1:123456789012:cluster/
MyEmptyCluster",
        "com.amazonaws.ecs.container-name": "curl-image",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-east-1:123456789012:task/
MyEmptyCluster/bfa2636268144d039771334145e490c5",
        "com.amazonaws.ecs.task-definition-family": "sample-fargate",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RUNNING",
      "KnownStatus": "RUNNING",
      "Limits": { "CPU": 128 },
      "CreatedAt": "2023-07-21T15:45:44.91368314Z",
      "StartedAt": "2023-07-21T15:45:44.91368314Z",
      "Type": "NORMAL",
      "Networks": [
```

```
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": ["172.31.42.189"],
          "AttachmentIndex": 0,
          "MACAddress": "0e:98:9f:33:76:d3",
          "IPv4SubnetCIDRBlock": "172.31.32.0/20",
          "DomainNameServers": ["172.31.0.2"],
          "DomainNameSearchList": ["ec2.internal"],
          "PrivateDNSName": "ip-172-31-42-189.ec2.internal",
          "SubnetGatewayIpv4Address": "172.31.32.1/20"
        }
      ],
      "ContainerARN": "arn:aws:ecs:us-east-1:123456789012:container/MyEmptyCluster/
bfa2636268144d039771334145e490c5/da6cccf7-1178-400c-afdf-7536173ee209",
      "Snapshotter": "overlayfs"
    },
    {
      "DockerId": "bfa2636268144d039771334145e490c5-3681984407",
      "Name": "fargate-app",
      "DockerName": "fargate-app",
      "Image": "public.ecr.aws/docker/library/httpd:latest",
      "ImageID":
 "sha256:8059bdd0058510c03ae4c808de8c4fd2c1f3c1b6d9ea75487f1e5caa5ececa02",
      "Labels": {
        "com.amazonaws.ecs.cluster": "arn:aws:ecs:us-east-1:123456789012:cluster/
MyEmptyCluster",
        "com.amazonaws.ecs.container-name": "fargate-app",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-east-1:123456789012:task/
MyEmptyCluster/bfa2636268144d039771334145e490c5",
        "com.amazonaws.ecs.task-definition-family": "sample-fargate",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RUNNING",
      "KnownStatus": "RUNNING",
      "Limits": { "CPU": 2 },
      "CreatedAt": "2023-07-21T15:45:44.954460255Z",
      "StartedAt": "2023-07-21T15:45:44.954460255Z",
      "Type": "NORMAL",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": ["172.31.42.189"],
          "AttachmentIndex": 0,
          "MACAddress": "0e:98:9f:33:76:d3",
```

```
          "IPv4SubnetCIDRBlock": "172.31.32.0/20",
          "DomainNameServers": ["172.31.0.2"],
          "DomainNameSearchList": ["ec2.internal"],
          "PrivateDNSName": "ip-172-31-42-189.ec2.internal",
          "SubnetGatewayIpv4Address": "172.31.32.1/20"
        }
      ],
      "ContainerARN": "arn:aws:ecs:us-east-1:123456789012:container/MyEmptyCluster/
bfa2636268144d039771334145e490c5/f65b461d-aa09-4acb-a579-9785c0530cbc",
      "Snapshotter": "overlayfs"
    }
  ],
  "LaunchType": "FARGATE",
  "ClockDrift": {
    "ClockErrorBound": 0.446931,
    "ReferenceTimestamp": "2023-07-21T16:09:17Z",
    "ClockSynchronizationStatus": "SYNCHRONIZED"
  },
  "EphemeralStorageMetrics": {
    "Utilized": 261,
    "Reserved": 20496
  }
}
```

タスク統計情報のレスポンス例

${ECS_CONTAINER_METADATA_URI_V4}/task/stats エンドポイントにクエリを実行すると、コンテナが属しているタスクに関するネットワークメトリクスが返されます。以下に出力例を示します。

```
{
  "3d1f891cded94dc795608466cce8ddcf-464223573": {
    "read": "2020-10-08T21:24:44.938937019Z",
    "preread": "2020-10-08T21:24:34.938633969Z",
    "pids_stats": {},
    "blkio_stats": {
      "io_service_bytes_recursive": [
        {
          "major": 202,
          "minor": 26368,
          "op": "Read",
          "value": 638976
        },
```

```
        {
          "major": 202,
          "minor": 26368,
          "op": "Write",
          "value": 0
        },
        {
          "major": 202,
          "minor": 26368,
          "op": "Sync",
          "value": 638976
        },
        {
          "major": 202,
          "minor": 26368,
          "op": "Async",
          "value": 0
        },
        {
          "major": 202,
          "minor": 26368,
          "op": "Total",
          "value": 638976
        }
      ],
      "io_serviced_recursive": [
        {
          "major": 202,
          "minor": 26368,
          "op": "Read",
          "value": 12
        },
        {
          "major": 202,
          "minor": 26368,
          "op": "Write",
          "value": 0
        },
        {
          "major": 202,
          "minor": 26368,
          "op": "Sync",
          "value": 12
        },
```

```
        {
          "major": 202,
          "minor": 26368,
          "op": "Async",
          "value": 0
        },
        {
          "major": 202,
          "minor": 26368,
          "op": "Total",
          "value": 12
        }
      ],
      "io_queue_recursive": [],
      "io_service_time_recursive": [],
      "io_wait_time_recursive": [],
      "io_merged_recursive": [],
      "io_time_recursive": [],
      "sectors_recursive": []
    },
    "num_procs": 0,
    "storage_stats": {},
    "cpu_stats": {
      "cpu_usage": {
        "total_usage": 1137691504,
        "percpu_usage": [
          696479228,
          441212276,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0
        ],
        "usage_in_kernelmode": 80000000,
        "usage_in_usermode": 810000000
```

```
      },
      "system_cpu_usage": 9393210000000,
      "online_cpus": 2,
      "throttling_data": {
        "periods": 0,
        "throttled_periods": 0,
        "throttled_time": 0
      }
    },
    "precpu_stats": {
      "cpu_usage": {
        "total_usage": 1136624601,
        "percpu_usage": [
          695639662,
          440984939,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0,
          0
        ],
        "usage_in_kernelmode": 80000000,
        "usage_in_usermode": 810000000
      },
      "system_cpu_usage": 9373330000000,
      "online_cpus": 2,
      "throttling_data": {
        "periods": 0,
        "throttled_periods": 0,
        "throttled_time": 0
      }
    },
    "memory_stats": {
      "usage": 6504448,
      "max_usage": 8458240,
      "stats": {
```

```
        "active_anon": 1675264,
        "active_file": 557056,
        "cache": 651264,
        "dirty": 0,
        "hierarchical_memory_limit": 536870912,
        "hierarchical_memsw_limit": 9223372036854772000,
        "inactive_anon": 0,
        "inactive_file": 3088384,
        "mapped_file": 430080,
        "pgfault": 11034,
        "pgmajfault": 5,
        "pgpgin": 8436,
        "pgpgout": 7137,
        "rss": 4669440,
        "rss_huge": 0,
        "total_active_anon": 1675264,
        "total_active_file": 557056,
        "total_cache": 651264,
        "total_dirty": 0,
        "total_inactive_anon": 0,
        "total_inactive_file": 3088384,
        "total_mapped_file": 430080,
        "total_pgfault": 11034,
        "total_pgmajfault": 5,
        "total_pgpgin": 8436,
        "total_pgpgout": 7137,
        "total_rss": 4669440,
        "total_rss_huge": 0,
        "total_unevictable": 0,
        "total_writeback": 0,
        "unevictable": 0,
        "writeback": 0
      },
      "limit": 9223372036854772000
    },
    "name": "curltest",
    "id": "3d1f891cded94dc795608466cce8ddcf-464223573",
    "networks": {
      "eth1": {
        "rx_bytes": 2398415937,
        "rx_packets": 1898631,
        "rx_errors": 0,
        "rx_dropped": 0,
        "tx_bytes": 1259037719,
```

```
        "tx_packets": 428002,
        "tx_errors": 0,
        "tx_dropped": 0
      }
    },
    "network_rate_stats": {
      "rx_bytes_per_sec": 43.298687872232854,
      "tx_bytes_per_sec": 215.39347269466413
    }
  }
}
```

Fargate のタスク用の Amazon ECS タスクメタデータエンドポイントバージョン 3

> **Important**
>
> タスクメタデータのバージョン 3 エンドポイントは、現在アクティブにメンテナンスされていません。タスクメタデータバージョン 4 エンドポイントを更新して、最新のメタデータエンドポイント情報を取得することをお勧めします。詳細については、「the section called "Fargate のタスク用のタスクメタデータエンドポイントバージョン 4"」を参照してください。

Fargateのプラットフォームバージョン1.1.0以降、ECS_CONTAINER_METADATA_URI という名前の環境変数がタスク内の各コンテナに挿入されます。タスクメタデータバージョン 3 エンドポイントに対してクエリを実行すると、さまざまなタスクメタデータおよび Docker 統計 をタスクで利用できます。

タスクメタデータエンドポイント機能は、プラットフォームバージョン1.1.0以降を使用するFargate上でホストされるAmazon ECS タスクに対してデフォルトで有効になります。詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。

Fargate のタスク用のタスクメタデータエンドポイントのパス

次の API エンドポイントをコンテナで使用できます。

`${ECS_CONTAINER_METADATA_URI}`

このパスはコンテナのメタデータ JSON を返します。

`${ECS_CONTAINER_METADATA_URI}/task`

このパスはタスクのメタデータ JSON を返します。これには、タスクに関連付けられたすべてのコンテナのコンテナ ID および名前のリストが含まれています。このエンドポイントのレスポンスの詳細については、「Fargate のタスク用の Amazon ECS タスクメタデータ v3 JSON レスポンス」を参照してください。

`${ECS_CONTAINER_METADATA_URI}/stats`

このパスは特定の Docker コンテナの Docker 統計 JSON を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

`${ECS_CONTAINER_METADATA_URI}/task/stats`

このパスはタスクに関連付けられたすべてのコンテナの Docker 統計 JSON を返します。返される各統計の詳細については、Docker API ドキュメントの「ContainerStats」を参照してください。

Fargate のタスク用の Amazon ECS タスクメタデータ v3 JSON レスポンス

次の情報が、タスクメタデータエンドポイント (`${ECS_CONTAINER_METADATA_URI}/task`) JSON レスポンスから返されます。

`Cluster`

タスクが属する Amazon ECS クラスターの Amazon リソースネーム (ARN)または短縮名。

`TaskARN`

コンテナが属しているタスクの Amazon リソースネーム (ARN)。

`Family`

タスクの Amazon ECS タスク定義のファミリー。

`Revision`

タスクの Amazon ECS タスク定義のリビジョン。

`DesiredStatus`

Amazon ECSからのタスクの望ましいステータス。

`KnownStatus`

Amazon ECS からのタスクの既知のステータス。

`Limits`

CPU (vCPU で表される) やメモリなど、タスク レベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`PullStartedAt`

最初のコンテナイメージのプル開始時のタイムスタンプ。

`PullStoppedAt`

最後のコンテナイメージのプル終了時のタイムスタンプ。

`AvailabilityZone`

タスクがあるアベイラビリティーゾーン。

> **Note**
>
> アベイラビリティーゾーンのメタデータは、プラットフォームバージョン 1.4 以降 (Linux) または 1.0.0 以降 (Windows) を使用する Fargate タスクでのみ使用できます。

`Containers`

タスクに関連付けられている各コンテナのコンテナメタデータのリスト。

`DockerId`

コンテナの Docker ID。

`Name`

タスク定義で指定されたコンテナの名前。

`DockerName`

Docker に提供されたコンテナの名前。Amazon ECSコンテナエージェントはコンテナに一意の名前を生成し、同じタスク定義の複数のコピーが単一のインスタンスで実行される場合に名前の競合を回避します。

`Image`

コンテナのイメージ。

`ImageID`

イメージの SHA-256 ダイジェスト。

`Ports`

コンテナに対して公開されている任意のポート。公開ポートがない場合はこのパラメータは省略されます。

`Labels`

コンテナに適用された任意のラベル。ラベルが適用されていない場合はこのパラメータは省略されます。

`DesiredStatus`

Amazon ECSからのコンテナの望ましいステータス。

`KnownStatus`

Amazon ECS からのコンテナの既知のステータス。

`ExitCode`

コンテナの終了コード。このパラメータは、コンテナが終了していない場合は省略されます。

`Limits`

CPU (CPU 単位で表される) やメモリなど、コンテナレベルで指定されたリソースの制限。リソースの制限が定義されていない場合はこのパラメータは省略されます。

`CreatedAt`

コンテナ作成時のタイムスタンプ。このパラメータは、コンテナがまだ作成されていない場合は省略されます。

`StartedAt`

コンテナ起動時のタイムスタンプ。このパラメータは、コンテナがまだ起動していない場合は省略されます。

`FinishedAt`

コンテナ停止時のタイムスタンプ。このパラメータは、コンテナがまだ停止していない場合は省略されます。

`Type`

コンテナのタイプ。タスク定義で指定されているコンテナのタイプは `NORMAL` です。他のコンテナタイプは無視してかまいません。これらはAmazon ECS コンテナエージェントによってプロビジョニングされる内部タスクリソースで使用されます。

`Networks`

ネットワークモードや IP アドレスなど、コンテナのネットワーク情報。ネットワーク情報が定義されていない場合はこのパラメータは省略されます。

`ClockDrift`

基準時刻とシステム時刻の違いに関する情報。これは、Linux オペレーティングシステムに適用されます。この機能では、Amazon Time Sync Service を使用してクロックの精度を測定し、コンテナのクロックエラー範囲を特定します。詳細については、「Linux インスタンス用 Amazon EC2 ユーザーガイド」の「Linux インスタンスの時刻の設定」を参照してください。

`ReferenceTime`

クロック精度の基礎。Amazon ECS は、`2021-09-07T16:57:44Z` などの NTP を通じて協定世界時 (UTC) の世界標準を使用しています。

`ClockErrorBound`

UTC へのオフセットとして定義されるクロックエラーの対策。この誤差は、基準時刻とシステム時刻の差 (ミリ秒単位) です。

`ClockSynchronizationStatus`

最新のシステム時刻と基準時刻間の同期試行における成功状況を示します。

有効な値は `SYNCHRONIZED` および `NOT_SYNCHRONIZED` です。

`ExecutionStoppedAt`

タスクの `DesiredStatus` が `STOPPED` に移行した時のタイムスタンプ。これは、必須コンテナが `STOPPED` に移行したときに発生します。

Fargate でのタスクの Amazon ECS タスクメタデータ v3 の例

1 つのコンテナタスクの JSON レスポンスを次に示します。

```
{
  "Cluster": "default",
  "TaskARN": "arn:aws:ecs:us-east-2:012345678910:task/9781c248-0edd-4cdb-9a93-
f63cb662a5d3",
  "Family": "nginx",
  "Revision": "5",
  "DesiredStatus": "RUNNING",
  "KnownStatus": "RUNNING",
```

```
  "Containers": [
    {
      "DockerId": "731a0d6a3b4210e2448339bc7015aaa79bfe4fa256384f4102db86ef94cbbc4c",
      "Name": "~internal~ecs~pause",
      "DockerName": "ecs-nginx-5-internalecspause-acc699c0cbf2d6d11700",
      "Image": "amazon/amazon-ecs-pause:0.1.0",
      "ImageID": "",
      "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "~internal~ecs~pause",
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RESOURCES_PROVISIONED",
      "KnownStatus": "RESOURCES_PROVISIONED",
      "Limits": {
        "CPU": 0,
        "Memory": 0
      },
      "CreatedAt": "2018-02-01T20:55:08.366329616Z",
      "StartedAt": "2018-02-01T20:55:09.058354915Z",
      "Type": "CNI_PAUSE",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "10.0.2.106"
          ]
        }
      ]
    },
    {
      "DockerId": "43481a6ce4842eec8fe72fc28500c6b52edcc0917f105b83379f88cac1ff3946",
      "Name": "nginx-curl",
      "DockerName": "ecs-nginx-5-nginx-curl-ccccb9f49db0dfe0d901",
      "Image": "nrdlngr/nginx-curl",
      "ImageID":
 "sha256:2e00ae64383cfc865ba0a2ba37f61b50a120d2d9378559dcd458dc0de47bc165",
      "Labels": {
        "com.amazonaws.ecs.cluster": "default",
        "com.amazonaws.ecs.container-name": "nginx-curl",
```

```
        "com.amazonaws.ecs.task-arn": "arn:aws:ecs:us-
east-2:012345678910:task/9781c248-0edd-4cdb-9a93-f63cb662a5d3",
        "com.amazonaws.ecs.task-definition-family": "nginx",
        "com.amazonaws.ecs.task-definition-version": "5"
      },
      "DesiredStatus": "RUNNING",
      "KnownStatus": "RUNNING",
      "Limits": {
        "CPU": 512,
        "Memory": 512
      },
      "CreatedAt": "2018-02-01T20:55:10.554941919Z",
      "StartedAt": "2018-02-01T20:55:11.064236631Z",
      "Type": "NORMAL",
      "Networks": [
        {
          "NetworkMode": "awsvpc",
          "IPv4Addresses": [
            "10.0.2.106"
          ]
        }
      ]
    }
  ],
  "PullStartedAt": "2018-02-01T20:55:09.372495529Z",
  "PullStoppedAt": "2018-02-01T20:55:10.552018345Z",
  "AvailabilityZone": "us-east-2b"
}
```

Amazon ECS コンテナの詳細分析

Amazon ECS コンテナエージェントは、エージェントが実行しているコンテナインスタンスおよびインスタンスで実行されている関連タスクに関する詳細を収集する API オペレーションを提供します。コンテナインスタンス内から curl コマンドを使用して Amazon ECS コンテナエージェント (ポート 51678) をクエリし、コンテナインスタンスのメタデータまたはタスク情報を受け取ることができます。

> **Important**
>
> メタデータを取得するには、Amazon ECS にアクセスするための IAM; ロールがコンテナインスタンスに必要です。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

コンテナインスタンスのメタデータを表示するには、SSH 経由でコンテナインスタンスにログインし、以下のコマンドを実行します。メタデータには、Amazon ECS コンテナインスタンス ID、コンテナインスタンスが登録されているクラスター、 Amazon ECS コンテナエージェントのバージョン情報が含まれます。

```
curl -s http://localhost:51678/v1/metadata | python3 -mjson.tool
```

出力:

```
{
    "Cluster": "cluster_name",
    "ContainerInstanceArn": "arn:aws:ecs:region:aws_account_id:container-
instance/cluster_name/container_instance_id",
    "Version": "Amazon ECS Agent - v1.30.0 (02ff320c)"
}
```

コンテナインスタンスで実行されているすべてのタスクの情報を表示するには、SSH 経由でコンテナインスタンスにログインし、以下のコマンドを実行します。

```
curl http://localhost:51678/v1/tasks
```

出力:

```
{
    "Tasks": [
        {
            "Arn": "arn:aws:ecs:us-west-2:012345678910:task/default/example5-58ff-46c9-
ae05-543f8example",
            "DesiredStatus": "RUNNING",
            "KnownStatus": "RUNNING",
            "Family": "hello_world",
            "Version": "8",
```

```
            "Containers": [
                {
          "DockerId":
 "9581a69a761a557fbfce1d0f6745e4af5b9dbfb86b6b2c5c4df156f1a5932ff1",
          "DockerName": "ecs-hello_world-8-mysql-fcae8ac8f9f1d89d8301",
          "Name": "mysql",
          "CreatedAt": "2023-10-08T20:09:11.44527186Z",
          "StartedAt": "2023-10-08T20:09:11.44527186Z",
          "ImageID":
 "sha256:2ae34abc2ed0a22e280d17e13f9c01aaf725688b09b7a1525d1a2750e2c0d1de"
        },
        {
          "DockerId":
 "bf25c5c5b2d4dba68846c7236e75b6915e1e778d31611e3c6a06831e39814a15",
          "DockerName": "ecs-hello_world-8-wordpress-e8bfddf9b488dff36c00",
          "Name": "wordpress"
        }
    ]
}
    ]
}
```

コンテナインスタンスで実行されている特定のタスクの情報を表示できます。特定のタスクまたはコンテナを指定するには、以下のいずれかをリクエストに追加します。

- タスク ARN (?taskarn=*task_arn*)
- コンテナの Docker ID (?dockerid=*docker_id*)

コンテナの Docker ID を使用してタスクの情報を取得するには、SSH 経由でコンテナインスタンスにログインし、以下のコマンドを実行します。

> **Note**
>
> バージョン 1.14.2 より前の Amazon ECS コンテナエージェントでは、 docker ps で表示される短縮バージョンではなく、イントロスペクション API 用の完全な Docker コンテナ ID が必要です。コンテナの完全な Docker ID は、コンテナインスタンスで docker ps --no-trunc コマンドを実行して取得できます。

```
curl http://localhost:51678/v1/tasks?dockerid=79c796ed2a7f
```

出力:

```
{
    "Arn": "arn:aws:ecs:us-west-2:012345678910:task/default/e01d58a8-151b-40e8-
bc01-22647b9ecfec",
    "Containers": [
        {
            "DockerId":
 "79c796ed2a7f864f485c76f83f3165488097279d296a7c05bd5201a1c69b2920",
            "DockerName": "ecs-nginx-efs-2-nginx-9ac0808dd0afa495f001",
            "Name": "nginx",
            "CreatedAt": "2023-10-08T20:09:11.44527186Z",
            "StartedAt": "2023-10-08T20:09:11.44527186Z",
            "ImageID":
 "sha256:2ae34abc2ed0a22e280d17e13f9c01aaf725688b09b7a1525d1a2750e2c0d1de"
        }
    ],
    "DesiredStatus": "RUNNING",
    "Family": "nginx-efs",
    "KnownStatus": "RUNNING",
    "Version": "2"
}
```

ランタイムモニタリングを使用して不正な動作を特定する

Amazon GuardDuty は、AWS 環境内のアカウント、コンテナ、ワークロード、データを保護する脅威検知サービスです。GuardDuty は、機械学習（ML）モデル、異常および脅威検出機能を使用して、さまざまなログソースとランタイムアクティビティを継続的に監視し、環境内の潜在的なセキュリティリスクと悪意のあるアクティビティを特定して優先順位を付けます。

GuardDuty のランタイムモニタリングは、AWS ログとネットワークアクティビティを継続的にモニタリングして悪意のある、または不正な動作を特定することで、Fargate および EC2 コンテナインスタンスで実行されているワークロードを保護します。ランタイムモニタリングは、軽量でフルマネージド型の GuardDuty セキュリティエージェントを使用して、ファイルアクセス、プロセス実行、ネットワーク接続などのホスト上動作を分析します。これは、Amazon EC2 インスタンスおよびコンテナワークロードでの権限の昇格、流出した認証情報の使用、悪意のある IP アドレスやドメインとの通信、マルウェアの存在などの問題に対応しています。詳細については、「GuardDuty ユーザーガイド」の「GuardDuty ランタイムモニタリング」を参照してください。

セキュリティ管理者が GuardDuty 用 AWS Organizations での 1 つまたは複数のアカウントでランタイムモニタリングを有効にします。また、Fargate を使用するときに GuardDuty が GuardDuty セキュリティエージェントを自動的にデプロイするかどうかも選択します。クラスターはすべて自動的に保護され、GuardDuty がユーザーに代わってセキュリティエージェントを管理します。

次の場合は、GuardDuty セキュリティエージェントを手動で設定することもできます。

- EC2 コンテナインスタンスを使用する
- ランタイムモニタリングをクラスターレベルで有効にするのにきめ細かな制御が必要

ランタイムモニタリングを使用するには、保護対象のクラスターを設定し、EC2 コンテナインスタンスに GuardDuty セキュリティエージェントをインストールして管理する必要があります。

Amazon ECS でのランタイムモニタリングの仕組み

ランタイムモニタリングは、軽量な GuardDuty セキュリティエージェントを使用して、アプリケーションが基盤となるシステムリソースに対してどのようにリクエストし、アクセスし、消費しているかについて、Amazon ECS ワークロードのアクティビティをモニタリングします。

Fargate タスクでは、GuardDuty セキュリティエージェントは各タスクのサイドカーコンテナとして実行されます。

EC2 コンテナインスタンスでは、GuardDuty セキュリティエージェントはインスタンス上のプロセスとして実行されます。

GuardDuty セキュリティエージェントは、以下のリソースからデータを収集し、そのデータを GuardDuty に送信して処理します。検出結果は GuardDuty コンソールに表示できます。また、AWS Security Hub などのほかの AWS のサービス やサードパーティのセキュリティベンダーに送信して、集計や修復を行うこともできます。検出結果を表示および管理する方法については、Amazon GuardDuty ユーザーガイドの「Amazon GuardDuty 検出結果の管理」を参照してください。

- 次の Amazon ECS API コールからのレスポンス:
  - DescribeClusters

    `--include TAGS` オプションを使用すると、レスポンスパラメータにランタイムモニタリングタグ (タグが設定されている場合) が含まれます。
  - DescribeTasks

Fargate 起動タイプでは、レスポンスパラメータに GuardDuty サイドカーコンテナが含まれます。

- ListAccountSettings

  レスポンスパラメータには、セキュリティ管理者が設定するランタイムモニタリングアカウント設定が含まれます。

- コンテナエージェントのイントロスペクションデータ。詳細については、「Amazon ECS コンテナの詳細分析」を参照してください。
- 起動タイプのタスクメタデータエンドポイント:
  - Amazon ECS タスクメタデータエンドポイントバージョン 4
  - Fargate のタスク用の Amazon ECS タスクメタデータエンドポイントバージョン 4

考慮事項

ランタイムモニタリングを使用する際は、次の点を考慮してください。

- ランタイムモニタリングにはコストが関連付けられています。詳細については、「Amazon GuardDuty の料金」を参照してください。
- ランタイムモニタリングは Amazon ECS Anywhere ではサポートされていません。
- ランタイムモニタリングは Windows オペレーティングシステムではサポートされていません。
- Fargate で Amazon ECS Exec を使用する場合、GuardDuty セキュリティエージェントはサイドカーコンテナとして実行されるため、コンテナ名を指定する必要があります。
- GuardDuty セキュリティエージェントのサイドカーコンテナでは Amazon ECS Exec を使用することはできません。
- クラスターレベルでランタイムモニタリングを制御する IAM ユーザーには、タグ付け用の適切な IAM アクセス許可が必要です。詳細については、「IAM ユーザーガイド」の「IAM チュートリアル: タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する」を参照してください。
- Fargate タスクはタスク実行ロールを使用する必要があります。このロールは、ユーザーに代わって Amazon ECR プライベートリポジトリに保存されている GuardDuty セキュリティエージェントを取得、更新、管理するアクセス許可をタスクに付与します。

リソース使用率

クラスターに追加したタグは、クラスタータグクォータに加算されます。

GuardDuty エージェントサイドカーコンテナは、タスク定義クォータあたりのコンテナ数には可算されません。

ほとんどのセキュリティソフトウェアと同様に、GuardDuty には若干のオーバーヘッドがあります。Fargate のメモリ制限については、「GuardDuty ユーザーガイド」の「CPU とメモリの制限」を参照してください。Amazon EC2 のメモリ制限については、「GuardDuty エージェントの CPU とメモリの制限」を参照してください。

Amazon ECS Fargate ワークロードのランタイムモニタリング

EC2 コンテナインスタンスを使用する場合は、ランタイムモニタリングを手動で設定する必要があります。詳細については、「Amazon ECS での EC2 ワークロードのランタイムモニタリング」を参照してください。

GuardDuty にコンテナインスタンスのセキュリティエージェントを管理させることができます。このオプションは Fargate でのみ使用できます。このオプション (GuardDuty エージェント管理) は GuardDuty で使用できます。

GuardDuty エージェント管理を使用すると、GuardDuty は次の操作を実行します。

- クラスターをホストする VPC ごとに GuardDuty の VPC エンドポイントを作成します。
- 最新の GuardDuty セキュリティエージェントを取得し、すべての新しいスタンドアロン Fargate タスクと新しいサービスデプロイのサイドカーコンテナとしてインストールします。

  新しいサービスデプロイは、サービスを初めて起動したとき、または既存のサービスを [新しいデプロイの強制] オプションで更新したときに実行されます。

Amazon ECS のランタイムモニタリングを有効にする

GuardDuty を設定して、すべての Fargate クラスターのセキュリティエージェントが自動的に管理されるようにすることができます。

前提条件

ランタイムモニタリングを使用するための前提条件は次のとおりです。

- Fargate プラットフォームバージョンは Linux では `1.4.0` 以降である必要があります。
- Amazon ECS の IAM ロールとアクセス許可:
  - Fargate タスクはタスク実行ロールを使用する必要があります。このロールは、ユーザーに代わって GuardDuty セキュリティエージェントを取得、更新、管理するアクセス許可をタスクに付与します。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。
  - 事前定義されたタグを使用してクラスターのランタイムモニタリングを制御します。アクセスポリシーによりタグに基づいてアクセスが制限されている場合は、クラスターにタグを付けるための明示的なアクセス許可を IAM ユーザーに付与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「IAM チュートリアル: タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する」を参照してください。
- Amazon ECR リポジトリへの接続:

  GuardDuty セキュリティエージェントは Amazon ECR リポジトリに保存されます。スタンドアロンタスクとサービスタスクにはそれぞれリポジトリへのアクセスが必要です。次のオプションの 1 つを使用できます。
  - パブリックサブネット内のタスクでは、タスクにパブリック IP アドレスを使用するか、タスクが実行されるサブネットに Amazon ECR の VPC エンドポイントを作成することができます。詳細については、Amazon Elastic コンテナレジストリ ユーザーガイドの Amazon ECR Interface VPC エンドポイント(AWS PrivateLink)を参照してください。
  - プライベートサブネットのタスクでは、ネットワークアドレス変換 (NAT) ゲートウェイを使用するか、タスクが実行されるサブネットに Amazon ECR の VPC エンドポイントを作成することができます。

    詳細については、「プライベートサブネットと NAT ゲートウェイ」を参照してください。
- GuardDuty の `AWSServiceRoleForAmazonGuardDuty` ロールが必要です。詳細については、「Amazon GuardDuty ユーザーガイド」の 「GuardDuty でのサービスにリンクされたロールのアクセス許可」を参照してください。
- ランタイムモニタリングで保護するファイルは、すべてルートユーザーによってアクセスできる必要があります。ファイルのアクセス許可を手動で変更した場合は、`755` に設定する必要があります。

EC2 コンテナインスタンスでランタイムモニタリングを使用するための前提条件は次のとおりです。

- Amazon ECS-AMI のバージョン `20230929` 以降を使用する必要があります。

- コンテナインスタンスで Amazon ECS エージェントをバージョン 1.77 以降で実行する必要があります。
- カーネルのバージョン 5.10 以降を使用する必要があります。
- サポートされている Linux オペレーティングシステムとアーキテクチャについては、「GuardDuty ランタイムモニタリングがサポートしているオペレーティングシステムとワークロードはどれですか」を参照してください。
- Systems Manager を使用してコンテナインスタンスを管理できます。詳細については、「AWS Systems Manager Session Manager ユーザーガイド」の「Systems Manager の EC2 インスタンスのセットアップ」を参照してください。

手順

GuardDuty でランタイムモニタリングを有効にします。この機能を有効にする方法については、「Amazon GuardDuty ユーザーガイド」の「ランタイムモニタリングを有効にする」を参照してください。

既存の Amazon ECS Fargate タスクにランタイムモニタリングを追加する

ランタイムモニタリングを有効にすると、クラスター内のすべての新しいスタンドアロンタスクと新しいサービスデプロイが自動的に保護されます。イミュータビリティの制約を維持するために、既存のタスクは影響を受けません。

前提条件

1. ランタイムモニタリングを有効にします。詳細については、「Amazon ECS のランタイムモニタリングを有効にする」を参照してください。
2. Fargate タスクはタスク実行ロールを使用する必要があります。このロールは、ユーザーに代わって GuardDuty セキュリティエージェントを取得、更新、管理するアクセス許可をタスクに付与します。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

手順

- タスクをすぐに保護するには、次のいずれかのアクションを実行する必要があります。
  - スタンドアロンタスクの場合は、タスクを停止してその後開始します。詳細については、「Amazon ECS タスクの停止」および「Amazon ECS タスクとしてのアプリケーションの実行」を参照してください。

- サービスの一部であるタスクの場合は、「新しいデプロイの強制」オプションを使用してサービスを更新します。詳細については、「コンソールを使用した Amazon ECS サービスの更新」を参照してください。

Amazon ECS クラスターからランタイムモニタリングを削除する

テストに使用するクラスターなど、特定のクラスターを保護対象から除外したい場合があります。そうすると、GuardDuty はクラスター内のリソース上で次のオペレーションを実行します。

- GuardDuty セキュリティエージェントを新しいスタンドアロンの Fargate タスクや新しいサービスデプロイにデプロイしなくなります。

  イミュータビリティの制約を維持するために、ランタイムモニタリングが有効になっている既存のタスクやデプロイは影響を受けません。
- 課金を停止し、タスクの実行時イベントを受け付けなくなります。

手順

以下の手順を実行して、ランタイムモニタリングをクラスターから削除します。

1. Amazon ECS コンソール または AWS CLI を使用して、クラスターの `GuardDutyManaged` タグキーを `false` に設定します。詳細については、「クラスターの更新」または「CLI または API を使用したタグの操作」を参照してください。タグに以下の値を使用します。

   > **Note**
   >
   > Key と Value は大文字と小文字が区別され、この文字列と完全に一致する必要があります。

   Key = `GuardDutyManaged`、Value = `false`
2. クラスターの GuardDuty VPC エンドポイントを削除します。VPC エンドポイントの削除方法の詳細については、「AWS PrivateLink ユーザーガイド」の「インターフェイスエンドポイントの削除」を参照してください。

アカウントから Amazon ECS のランタイムモニタリングを削除する

以降ランタイムモニタリングを使用しない場合は、GuardDuty の機能を無効にします。この機能を無効にする方法については、「Amazon GuardDuty ユーザーガイド」の「ランタイムモニタリングを有効にする」を参照してください。

GuardDuty では以下のオペレーションを実行します。

- クラスターをホストする各 VPC の GuardDuty の VPC エンドポイントを削除します。
- GuardDuty セキュリティエージェントを新しいスタンドアロンの Fargate タスクや新しいサービスのデプロイにデプロイしなくなります。

  イミュータビリティの制約を維持するために、既存のタスクやデプロイは、停止、複製、またはスケーリングされるまで影響を受けません。
- 課金を停止し、タスクの実行時イベントを受け付けなくなります。

Amazon ECS での EC2 ワークロードのランタイムモニタリング

このオプションは、キャパシティーとして EC2 インスタンスを使用する場合や、Fargate でランタイムモニタリングをクラスターレベルできめ細かく制御する必要がある場合に使用します。

事前定義されたタグを追加することで、クラスターをランタイムモニタリング用にプロビジョニングします。

EC2 コンテナインスタンスでは、ユーザーが GuardDuty セキュリティエージェントをダウンロード、インストール、管理します。

Fargate では、GuardDuty がユーザーに代わってセキュリティエージェントを管理します。

Amazon ECS のランタイムモニタリングを有効にする

EC2 インスタンスを使用するクラスターや、Fargate でランタイムモニタリングをクラスターレベルできめ細かく制御する必要がある場合に有効にできます。

ランタイムモニタリングを使用するための前提条件は次のとおりです。

- Fargate プラットフォームバージョンは Linux では `1.4.0` 以降である必要があります。
- Amazon ECS の IAM ロールとアクセス許可:

  - Fargate タスクはタスク実行ロールを使用する必要があります。このロールは、ユーザーに代わって GuardDuty セキュリティエージェントを取得、更新、管理するアクセス許可をタスクに付与します。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。
  - 事前定義されたタグを使用してクラスターのランタイムモニタリングを制御します。アクセスポリシーによりタグに基づいてアクセスが制限されている場合は、クラスターにタグを付けるための明示的なアクセス許可を IAM ユーザーに付与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「IAM チュートリアル: タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する」を参照してください。
- Amazon ECR リポジトリへの接続:

  GuardDuty セキュリティエージェントは Amazon ECR リポジトリに保存されます。スタンドアロンタスクとサービスタスクにはそれぞれリポジトリへのアクセスが必要です。次のオプションの 1 つを使用できます。

  - パブリックサブネット内のタスクでは、タスクにパブリック IP アドレスを使用するか、タスクが実行されるサブネットに Amazon ECR の VPC エンドポイントを作成することができます。詳細については、Amazon Elastic コンテナレジストリ ユーザーガイドの Amazon ECR Interface VPC エンドポイント(AWS PrivateLink)を参照してください。
  - プライベートサブネットのタスクでは、ネットワークアドレス変換 (NAT) ゲートウェイを使用するか、タスクが実行されるサブネットに Amazon ECR の VPC エンドポイントを作成することができます。

    詳細については、「プライベートサブネットと NAT ゲートウェイ」を参照してください。
- GuardDuty の `AWSServiceRoleForAmazonGuardDuty` ロールが必要です。詳細については、「Amazon GuardDuty ユーザーガイド」の 「GuardDuty でのサービスにリンクされたロールのアクセス許可」を参照してください。
- ランタイムモニタリングで保護するファイルは、すべてルートユーザーによってアクセスできる必要があります。ファイルのアクセス許可を手動で変更した場合は、755 に設定する必要があります。

EC2 コンテナインスタンスでランタイムモニタリングを使用するための前提条件は次のとおりです。

- Amazon ECS-AMI のバージョン `20230929` 以降を使用する必要があります。
- コンテナインスタンスで Amazon ECS エージェントをバージョン `1.77` 以降で実行する必要があります。

- カーネルのバージョン 5.10 以降を使用する必要があります。
- サポートされている Linux オペレーティングシステムとアーキテクチャについては、「GuardDuty ランタイムモニタリングがサポートしているオペレーティングシステムとワークロードはどれですか」を参照してください。
- Systems Manager を使用してコンテナインスタンスを管理できます。詳細については、「AWS Systems Manager Session Manager ユーザーガイド」の「Systems Manager の EC2 インスタンスのセットアップ」を参照してください。

GuardDuty でランタイムモニタリングを有効にします。この機能を有効にする方法については、「Amazon GuardDuty ユーザーガイド」の「ランタイムモニタリングを有効にする」を参照してください。

Amazon ECS クラスターのランタイムモニタリングを追加する

クラスターのランタイムモニタリングを設定し、EC2 コンテナインスタンスに GuardDuty セキュリティエージェントをインストールします。

前提条件

1. ランタイムモニタリングを有効にします。詳細については、「Amazon ECS のランタイムモニタリングを有効にする」を参照してください。
2. 事前定義されたタグを使用してクラスターのランタイムモニタリングを制御します。アクセスポリシーによりタグに基づいてアクセスが制限されている場合は、クラスターにタグを付けるための明示的なアクセス許可を IAM ユーザーに付与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「IAM チュートリアル: タグに基づいて AWS リソースにアクセスするためのアクセス許可を定義する」を参照してください。

手順

以下の操作を実行して、ランタイムモニタリングをクラスターに追加します。

1. クラスター VPC ごとに GuardDuty 用の VPC エンドポイントを作成します。詳細については、「GuardDuty ユーザーガイド」の「Amazon VPC エンドポイントの手動作成」を参照してください。
2. EC2 コンテナインスタンスを設定します。

a. クラスター内の EC2 コンテナインスタンスの Amazon ECS エージェントをバージョン 1.77 以降に更新します。詳細については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。

b. クラスターの EC2 コンテナインスタンスに GuardDuty セキュリティエージェントをインストールします。詳細については、「GuardDuty ユーザーガイド」の「Amazon EC2 インスタンスのセキュリティエージェントの手動管理」を参照してください。

   GuardDuty セキュリティエージェントは EC2 コンテナインスタンス上のプロセスとして実行されるため、新規および既存のタスク、デプロイはすべて即座に保護されます。

3. Amazon ECS コンソール または AWS CLI を使用して、クラスターの `GuardDutyManaged` タグキーを `true` に設定します。詳細については、「クラスターの更新」または「CLI または API を使用したタグの操作」を参照してください。タグに以下の値を使用します。

> **Note**
>
> Key と Value は大文字と小文字が区別され、この文字列と完全に一致する必要があります。

Key = `GuardDutyManaged`、Value = `true`

既存の Amazon ECS タスクにランタイムモニタリングを追加する

ランタイムモニタリングを有効にすると、クラスター内のすべての新しいスタンドアロンタスクと新しいサービスデプロイが自動的に保護されます。イミュータビリティの制約を維持するために、既存のタスクは影響を受けません。

前提条件

- ランタイムモニタリングを有効にします。詳細については、「Amazon ECS のランタイムモニタリングを有効にする」を参照してください。

手順

- タスクをすぐに保護するには、次のいずれかのアクションを実行する必要があります。

- スタンドアロンタスクの場合は、タスクを停止してその後開始します。詳細については、Amazon ECS タスクの停止およびAmazon ECS タスクとしてのアプリケーションの実行を参照してください。
- サービスの一部であるタスクの場合は、「新しいデプロイの強制」オプションを使用してサービスを更新します。詳細については、「コンソールを使用した Amazon ECS サービスの更新」を参照してください。

Amazon ECS クラスターからランタイムモニタリングを削除する

ランタイムモニタリングはクラスターから削除できます。そうすると、GuardDuty はクラスター内のすべてのリソースのモニタリングを停止します。

ランタイムモニタリングをクラスターから削除するには

1. Amazon ECS コンソール または AWS CLI を使用して、クラスターの `GuardDutyManaged` タグキーを `false` に設定します。詳細については、「クラスターの更新」または「CLI または API を使用したタグの操作」を参照してください。

   > **Note**
   >
   > Key と Value は大文字と小文字が区別され、この文字列と完全に一致する必要があります。

   Key = `GuardDutyManaged`、Value = `false`
2. クラスター内の EC2 コンテナインスタンスの GuardDuty セキュリティエージェントをアンインストールします。

   詳細については、「GuardDuty ユーザーガイド」の「セキュリティエージェントの手動アンインストール」を参照してください。
3. 各クラスター VPC の GuardDuty VPC エンドポイントを削除します。VPC エンドポイントの削除方法の詳細については、「AWS PrivateLink ユーザーガイド」の「インターフェイスエンドポイントの削除」を参照してください。

Amazon ECS コンテナインスタンスの GuardDuty セキュリティエージェントを更新する

EC2 コンテナインスタンスの GuardDuty セキュリティエージェントを更新する方法については、「Amazon GuardDuty ユーザーガイド」の「GuardDuty セキュリティエージェントの更新」を参照してください。

アカウントから Amazon ECS のランタイムモニタリングを削除する

以降ランタイムモニタリングを使用しない場合は、GuardDuty の機能を無効にします。この機能を無効にする方法については、「Amazon GuardDuty ユーザーガイド」の「ランタイムモニタリングを有効にする」を参照してください。

すべてのクラスターからランタイムモニタリングを削除します。詳細については、「Amazon ECS クラスターからランタイムモニタリングを削除する」を参照してください。

ランタイムモニタリングのトラブルシューティングに関するよくある質問

トラブルシューティングをして、タスクやコンテナでランタイムモニタリングが有効になっていて実行されていることを確認する必要がある場合があります。

トピック

- 自分のアカウントでランタイムモニタリングがアクティブかどうかはどうすればわかりますか?
- クラスターでランタイムモニタリングがアクティブかどうかはどうすればわかりますか?
- GuardDuty セキュリティエージェントが Fargate タスクで実行されているかどうかはどうすればわかりますか?
- GuardDuty セキュリティエージェントが EC2 コンテナインスタンスで実行されているかどうかはどうすればわかりますか?
- クラスターで実行されているタスクにタスク実行ロールがない場合はどうなりますか?
- ランタイムモニタリング対応のクラスターにタグを付けるための正しいアクセス許可を持っているかどうかはどうすればわかりますか?
- Amazon ECR に接続されていない場合はどうなりますか?
- ランタイムモニタリングを有効にした後、Fargate タスクのメモリ不足エラーに対処するにはどうすればよいですか?

自分のアカウントでランタイムモニタリングがアクティブかどうかはどうすればわかりますか?

その情報は、Amazon ECS コンソールの [アカウント設定] ページにあります。

effective-settings オプションを使用して list-account-settings を実行することもできます。

```
aws ecs list-account-settings --effective-settings
```

Output

[name] が guardDutyActivate に設定され、[value] が on に設定された設定は、アカウントが設定済みであることを示します。GuardDuty 管理者に問い合わせて、管理が自動か手動かを確認する必要があります。

```
{
    "setting": {
        "name": "guardDutyActivate",
        "value": "enabled",
        "principalArn": "arn:aws:iam::123456789012:root",
        "type": "aws-managed"
    }
}
```

クラスターでランタイムモニタリングがアクティブかどうかはどうすればわかりますか?

その情報は、Amazon ECS コンソールの [クラスターの詳細] ページの [タグ] タブにあります。

TAGS オプションを使用して describe-clusters を実行することもできます。

次の例は、デフォルトクラスターの出力の例を示しています。

```
aws ecs describe-clusters --cluster default --include TAGS
```

Output

[Key] が GuardDutyManaged に設定され、[Value] が true に設定されたタグは、クラスターがランタイムモニタリング対応の設定になっていることを示します。

```
{
    "clusters": [
        {
            "clusterArn": "arn:aws:ecs:us-east-1:1234567890:cluster/default",
            "clusterName": "default",
            "status": "ACTIVE",
            "registeredContainerInstancesCount": 0,
            "runningTasksCount": 1,
            "pendingTasksCount": 0,
            "activeServicesCount": 0,
            "statistics": [],
            "tags": [
                {
                    "key": "GuardDutyManaged",
                    "value": "true"
                }
            ],
            "settings": [],
            "capacityProviders": [],
            "defaultCapacityProviderStrategy": []
        }
    ],
    "failures": []
}
```

GuardDuty セキュリティエージェントが Fargate タスクで実行されているかどうかはどうすればわかりますか?

Fargate タスクでは、GuardDuty セキュリティエージェントはサイドカーコンテナとして実行されます。

サイドカーは、Amazon ECS コンソールの [タスクの詳細] ページの [コンテナ] に表示されます。

`describe-tasks` を実行することで、[name] が `aws-gd-agent` に設定され、[lastStatus] が `RUNNING` に設定されているコンテナを探すことができます。

次の例は、タスク `aws:ecs:us-east-1:123456789012:task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE` のデフォルトのクラスターの出力を示しています。

```
aws ecs describe-tasks --cluster default --tasks aws:ecs:us-
east-1:123456789012:task/0b69d5c0-d655-4695-98cd-5d2d5EXAMPLE
```

Output

gd-agent という名前のコンテナは RUNNING 状態にあります。

```
"containers": [
      {
        "containerArn": "arn:aws:ecs:us-east-1:123456789012:container/4df26bb4-
f057-467b-a079-96167EXAMPLE",
        "taskArn": "arn:aws:ecs:us-east-1:123456789012:task/0b69d5c0-
d655-4695-98cd-5d2d5EXAMPLE",
        "lastStatus": "RUNNING",
        "healthStatus": "UNKNOWN",
        "memory": "string",
        "name": "aws-gd-agent"
      }
    ]
```

GuardDuty セキュリティエージェントが EC2 コンテナインスタンスで実行されているかどうかはどうすればわかりますか?

以下のコマンドを実行して、ステータスを表示します。

```
sudo systemctl status amazon-guardduty-agent
```

ログファイルは次の場所にあります。

```
/var/log/amzn-guardduty-agent
```

クラスターで実行されているタスクにタスク実行ロールがない場合はどうなりますか?

Fargate タスクでは、タスクは GuardDuty セキュリティエージェントのサイドカーコンテナなしで開始されます。GuardDuty ダッシュボードには、カバレッジ統計ダッシュボードにタスクが保護されていないことが表示されます。

ランタイムモニタリング対応のクラスターにタグを付けるための正しいアクセス許可を持っているかどうかはどうすればわかりますか?

クラスターにタグを付けるには、CreateCluster と UpdateCluster の両方に対する ecs:TagResource アクションが必要です。

以下はポリシーの例の一部です。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ecs:TagResource"
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
             "ecs:CreateAction" : "CreateCluster",
             "ecs:CreateAction" : "UpdateCluster",
          }
       }
    }
  ]
}
```

Amazon ECR に接続されていない場合はどうなりますか?

Fargate タスクでは、タスクは GuardDuty セキュリティエージェントのサイドカーコンテナなしで開始されます。GuardDuty ダッシュボードには、カバレッジ統計ダッシュボードにタスクが保護されていないことが表示されます。

ランタイムモニタリングを有効にした後、Fargate タスクのメモリ不足エラーに対処するにはどうすればよいですか?

GuardDuty セキュリティエージェントは軽量なプロセスです。しかし、プロセスはそれでもワークロードのサイズに応じてリソースを消費します。クラスターに GuardDuty のデプロイをステージングするには、Amazon CloudWatch Container Insights などのコンテナリソーストラッキングツールを使用することをお勧めします。このようなツールは、アプリケーションの GuardDuty セキュリティエージェントの消費プロファイルを確認するのに役立ちます。そして、必要に応じて Fargate タスクのサイズを調整して、潜在的なメモリ不足状態を回避できます。

ECS Exec を使用して Amazon ECS コンテナをモニタリングする

Amazon ECS Exec を使用すれば、最初にホストコンテナのオペレーティングシステムとやり取りしたり、インバウンドポートを開いたり、SSH キーを管理したりすることなく、コンテナと直接やり取りできます。ECS Exec を使用して、Amazon EC2 インスタンスまたは AWS Fargate で実行されているコンテナでコマンドを実行したり、シェルを取得したりできます。これにより、診断情報を収

集し、エラーを迅速にトラブルシューティングすることが容易になります。例えば、開発コンテキストでは、ECS を使用して、コンテナ内のさまざまなプロセスと簡単にやり取りし、アプリケーションのトラブルシューティングを行うことができます。また本番稼働シナリオでは、これを使用することで、コンテナへのブレークグラスアクセスを行って問題をデバッグできます。

Amazon ECS API、AWS Command Line Interface (AWS CLI)、AWS、SDK、または AWS Copilot CLI から ECS Exec を使用して、実行中の Linux または Windows コンテナでコマンドを実行できます。ECS Exec の使用方法と AWS Copilot CLI を使用した動画チュートリアルの詳細については、Copilot に関する GitHub ドキュメントを参照してください。

ECS Exec を使用すれば、より厳格なアクセスコントロールポリシーを維持することもできます。この機能を選択的に有効にすることで、コマンドを実行できるユーザーと、それらのコマンドを実行できるタスクを制御できます。各コマンドとその出力のログを使用すると、ECS Exec を使用して、実行されたタスクを確認したり、CloudTrail を使用して、コンテナにアクセスしたユーザーを監査したりできます。

考慮事項

このトピックでは、ECS Exec の使用に関する次の側面に精通している必要があります:

- ECS Exec は現在、AWS Management Console を使用してサポートされていません。

  クラスターの詳細ページには、ローカルクライアントとコンテナ間のデータの暗号化に使用されるログ記録とAWS KMS カスタマーマネージドキーが表示されます。
- ECS Exec は、Systems Manager がサポートしないオペレーティングシステムでの実行時に期待どおりに動作しない場合があります。サポートされているオペレーティングシステムについては、「AWS Systems Manager ユーザーガイド」で「オペレーティングシステムのタイプ」を参照してください。
- ECS Exec は、次のインフラストラクチャで実行されるタスクでサポートされています。
  - Amazon EC2 上の Linux コンテナを任意の Amazon ECS に最適化された AMI (Bottlerocketを含む)
  - 外部インスタンス (Amazon ECS Anywhere) 上の Linux および Windows コンテナ
  - AWS Fargate 上の Linux および Windows コンテナ
  - 次の Windows Amazon ECS に最適化された AMI 上のAmazon EC2 上の Windows コンテナ (コンテナエージェントバージョン 1.56 以降を使用) :
    - Amazon ECS に最適化された Windows Server 2022 Full AMI
    - Amazon ECS に最適化された Windows Server 2022 Core AMI

    - Amazon ECS に最適化された Windows Server 2019 Full AMI
    - Amazon ECS に最適化された Windows Server 2019 Core AMI
    - Amazon ECS に最適化された Windows Server 20H2 Core AMI
- タスクに HTTP プロキシを設定した場合は、EC2 インスタンスメタデータと IAM ロールトラフィックのプロキシをバイパスするために、`NO_PROXY` 環境変数を `"NO_PROXY=169.254.169.254,169.254.170.2"` に設定します。`NO_PROXY` 環境変数を設定しない場合、コンテナ内のメタデータエンドポイントからインスタンスメタデータまたは IAM ロールの認証情報を取得するときに失敗する可能性があります。`NO_PROXY` 環境変数を推奨として設定すると、`169.254.169.254 and 169.254.170.2` へのリクエストが `HTTP` プロキシを通過しないように、メタデータと IAM トラフィックがフィルタリングされます。
- ECS Exec および Amazon VPC
    - Amazon ECS にインターフェイス Amazon VPC エンドポイントを使用している場合は、Systems Manager Session Manager (`ssmmessages`) のインターフェイス Amazon VPC エンドポイントを作成する必要があります。Systems Manager VPC エンドポイントの詳細については、AWS Systems Manager ユーザーガイドの「Session Manager に VPC エンドポイントを設定するために AWS PrivateLink を使用する」を参照してください。
    - Amazon ECS にインターフェイス Amazon VPC エンドポイントを使用していて、暗号化に AWS KMS key を使用している場合には、AWS KMS key 用のインターフェイス Amazon VPC エンドポイントを作成する必要があります。詳細については、「AWS Key Management Service デベロッパーガイド」の「VPC エンドポイントを介した AWS KMS key への接続」を参照してください。
    - Amazon EC2 インスタンスで実行されるタスクがある場合は、`awsvpc` ネットワークモードを使用してください。NAT ゲートウェイを使用するように設定されていないなど、インターネットにアクセスできない場合は、Systems Manager Session Manager 用のインターフェイス Amazon VPC エンドポイント (`ssmmessages`) を作成する必要があります。`awsvpc` ネットワークモードに関する考慮事項の詳細については、「考慮事項」を参照してください。Systems Manager VPC エンドポイントの詳細については、AWS Systems Manager ユーザーガイドの「Session Manager に VPC エンドポイントを設定するために AWS PrivateLink を使用する」を参照してください。
- ECS Exec および SSM
    - ユーザーが ECS Exec を使用してコンテナ上でコマンドを実行すると、これらのコマンドは `root` ユーザーとして実行されます。コンテナにユーザー ID を指定しても、SSM エージェントとその子プロセスは root として実行されます。

  - SSM エージェントは、必要なディレクトリやファイルを作成するために、コンテナのファイルシステムに書き込みができる必要があります。したがって、`readonlyRootFilesystem`タスク定義パラメータ、またはその他の方法を使ってルートファイルシステムを読み取り専用にすることは、サポートされません。
  - `execute-command`アクション外部の SSM セッションを開始することは可能ですが、これにより、セッションはログに記録されず、セッション制限に対してカウントされません。IAM ポリシーを使用した `ssm:start-session`操作を拒否して、このアクセスを制限することをお勧めします。詳細については、「[Start Session (セッション開始)] 操作へのアクセス制限」を参照してください。
- 以下の機能はサイドカーコンテナとして実行されます。そのため、コマンドを実行するコンテナ名を指定する必要があります。
  - Runtime Monitoring
  - Service Connect
- ユーザーは、コンテナコンテキスト内で使用可能なすべてのコマンドを実行できます。一部の操作 (コンテナのメインプロセスの終了、コマンドエージェントの終了、依存関係の削除) によって、孤立プロセスとゾンビプロセスが発生する可能性があります。ゾンビプロセスをクリーンアップするには、タスク定義に `initProcessEnabled` フラグを追加することをお勧めします。
- ECS Exec はある程度の CPU とメモリを使用します。タスク定義で CPU とメモリリソースの割り当てを指定する場合は、この点を考慮する必要があります。
- AWS CLI バージョン `1.22.3` 以降、または AWS CLI バージョン `2.3.6` 以降を使用する必要があります。AWS CLI をアップデートする情報については、AWS Command Line Interface ユーザーガイドバージョン 2 の「AWS CLI の最新バージョンのインストールまたはアップデート」を参照してください。
- プロセス ID (PID) 名前空間ごとに作成できる ECS Exec セッションは 1 つのみです。タスク内で PID 名前空間を共有している場合は、1 つのコンテナ内でのみ ECS Exec セッションを開始できます。
- ECS Exec セッションのアイドルタイムアウト時間は 20 分です。この値は変更できません。
- 既存のタスクに対して ECS Exec をオンにすることはできません。新しいタスクに対してのみオンにできます。
- `run-task` を使用して、非同期配置でマネージドスケーリングを使用するクラスターでタスクを起動 (インスタンスなしでタスクを起動) する場合、ECS Exec は使用できません。
- Microsoft Nano Server コンテナに対しては ECS Exec を実行できません。

前提条件

ECS Exec の使用を開始する前に、次の操作が完了していることを確認してください。

- AWS CLI をインストールして設定します。詳細については、「AWS CLI の使用を開始する」を参照してください。
- AWS CLI のセッションマネージャープラグインをインストールします。詳細については、に セッション マネージャー プラグインのインストールAWS CLI を参照してください。
- ECS Exec の適切なアクセス許可のあるタスクロールを使用する必要があります。詳細については、「タスク IAM ロール」を参照してください。
- ECS Exec には、タスクが Amazon EC2 でホストされているか AWS Fargate でホストされているかに応じて、バージョン要件があります:
  - Amazon EC2 を使用している場合は、2021 年 1 月 20 日以降にリリースされた Amazon ECS 最適化 AMI を、エージェントバージョン 1.50.2 以上で使用する必要があります。詳細については、Amazon ECS 最適化 AMI を参照してください。
  - AWS Fargate を使用している場合、プラットフォームバージョン `1.4.0` 以上 (Linux) または `1.0.0` (Windows) を使用する必要があります。詳細については、の「AWS Fargateプラットフォームバージョン」を参照してください。

アーキテクチャ

ECS Exec は、AWS Systems Manager (SSM) セッションマネージャーを使用して実行中のコンテナとの接続を確立し、AWS Identity and Access Management (IAM) ポリシーを使用して実行中のコンテナで実行中のコマンドへのアクセスを制御します。これは、必要な SSM Agent バイナリをコンテナにバインドマウントすることによって実現されます。Amazon ECS または AWS Fargate エージェントは、アプリケーションコードと一緒にコンテナ内で SSM コアエージェントをスタートする責任があります。詳細については、 Systems Manager のセッションマネージャーを参照してください。

AWS CloudTrail の `ExecuteCommand` を使用してコンテナにアクセスしたユーザーを監査し、各コマンド (およびその出力) を Amazon S3 または Amazon CloudWatch Logs に記録できます。独自の暗号化キーを使用してローカルクライアントとコンテナ間のデータを暗号化するには、AWS Key Management Service (AWS KMS) キーを指定する必要があります。

ECS Exec の使用

オプションのタスク定義の変更

タスク定義パラメータ `initProcessEnabled` を `true` に設定すると、コンテナ内で init プロセスが開始されます。この結果、見つかったゾンビ SSM エージェントの子プロセスはすべて削除されます。以下に例を示します。

```
{
    "taskRoleArn": "ecsTaskRole",
    "networkMode": "awsvpc",
    "requiresCompatibilities": [
        "EC2",
        "FARGATE"
    ],
    "executionRoleArn": "ecsTaskExecutionRole",
    "memory": ".5 gb",
    "cpu": ".25 vcpu",
    "containerDefinitions": [
        {
            "name": "amazon-linux",
            "image": "amazonlinux:latest",
            "essential": true,
            "command": ["sleep","3600"],
            "linuxParameters": {
                "initProcessEnabled": true
            }
        }
    ],
    "family": "ecs-exec-task"
}
```

タスクとサービスに対する ECS Exec をオンにする

次の AWS CLI コマンド:(`create-service`、`update-service`、`start-task`、または `run-task`) のいずれかを使用するときに、`--enable-execute-command` フラグを指定することにより、サービスおよびスタンドアロンタスクの ECS Exec 機能をオンにすることができます。

例えば、次のコマンドを実行すると、ECS Exec 機能が Fargate で実行される新しく作成されたサービスに対してオンになります。サービス作成の詳細については、create-service を参照してください。

```
aws ecs create-service \
    --cluster cluster-name \
    --task-definition task-definition-name \
    --enable-execute-command \
    --service-name service-name \
    --launch-type FARGATE \
     --network-configuration
 "awsvpcConfiguration={subnets=[subnet-12344321],securityGroups=[sg-12344321],assignPublicIp=EN
 \
    --desired-count 1
```

タスクに対して ECS Exec をオンにしたら、次のコマンドを実行して、タスクが使用可能な状態であることを確認できます。ExecuteCommandAgent の lastStatus プロパティが RUNNING として表示され、enableExecuteCommand プロパティが true に設定されている場合、タスクの準備が整います。

```
aws ecs describe-tasks \
    --cluster cluster-name \
    --tasks task-id
```

以下の出力スニペットは、表示される可能性があるものの例です。

```
{
    "tasks": [
        {
            ...
            "containers": [
                {
                    ...
                    "managedAgents": [
                        {
                            "lastStartedAt": "2021-03-01T14:49:44.574000-06:00",
                            "name": "ExecuteCommandAgent",
                            "lastStatus": "RUNNING"
                        }
                    ]
                }
            ],
            ...
            "enableExecuteCommand": true,
            ...
        }
```

```
    ]
}
```

ECS Exec を使用してコマンド実行

ExecuteCommandAgent が実行されていることを確認したら、以下のコマンドを使用してコンテナ上でインタラクティブシェルを開くことができます。タスクに複数のコンテナが含まれている場合は、--containerフラグを使うコンテナ名を指定する必要があります。Amazon ECS はインタラクティブセッションの開始のみをサポートするため、--interactiveフラグを使用する必要があります。

次のコマンドでは、*task-id* という ID のタスクで、*container-name* という名前のコンテナに対して、インタラクティブな /bin/sh コマンドが実行されます。

task-id は、タスクの Amazon リソースネーム (ARN) です。

```
aws ecs execute-command --cluster cluster-name \
    --task task-id \
    --container container-name \
    --interactive \
    --command "/bin/sh"
```

ECS Exec を使用したログ記録

タスクとサービスでのログ記録を有効にする

> **Important**
>
> CloudWatch の料金の詳細については、 CloudWatch の料金をご覧ください。Amazon ECS は、追加料金なしで提供されているモニタリングメトリクスも提供します。詳細については、「CloudWatch を使用して Amazon ECS をモニタリングする」を参照してください。

Amazon ECS には、ECS Exec で実行されたコマンドのログ記録がデフォルトで有効になっています。デフォルトでは、タスク定義で設定されたログドライバーを使用して CloudWatch Logs に awslogs ログを送信します。カスタム構成を提供する場合、AWS CLI は create-cluster コマンドと update-cluster コマンドの両方に対して --configuration フラグをサポートします。コマンドログを Amazon S3 または CloudWatch Logs に正しくアップロードするには、コンテナ

イメージに script と cat をインストールする必要があります。クラスター作成の詳細については、create-cluster を参照してください。

> **Note**
>
> この設定では、execute-command セッションのログ記録のみを処理します。アプリケーションのログには影響しません。

以下の例では、クラスターを作成し、出力を cloudwatch-log-group-name という名前の CloudWatch Logs LogGroup と s3-bucket-name という名前の Amazon S3 バケットに記録します。

CloudWatchEncryptionEnabledオプションをtrueに設定した場合、ロググループの暗号化にAWS KMSカスタマーマネージドキーを使用する必要があります。ロググループを暗号化する方法については、「Amazon CloudWatch Logsユーザーガイド」のAWS Key Management Serviceを使用してCloudWatch Logsのログデータを暗号化するを参照してください。

```
aws ecs create-cluster \
    --cluster-name cluster-name \
    --configuration executeCommandConfiguration="{ \
        kmsKeyId=string, \
        logging=OVERRIDE, \
        logConfiguration={ \
            cloudWatchLogGroupName=cloudwatch-log-group-name, \
            cloudWatchEncryptionEnabled=true, \
            s3BucketName=s3-bucket-name, \
            s3EncryptionEnabled=true, \
            s3KeyPrefix=demo \
        } \
    }"
```

logging プロパティにより、ECS Exec のログ機能の動作が決まります:

- NONE: ログ記録はオフになっています。
- DEFAULT: ログは設定された awslogs ドライバーに送信されます。ドライバーが設定されていない場合、ログは保存されません。
- OVERRIDE: ログは、指定された Amazon CloudWatch Logs LogGroup、Amazon S3 バケット、またはその両方に送信されます。

Amazon CloudWatch Logs または Amazon S3 ロギングに必要な IAM アクセス許可

ログ記録を有効にするには、 タスク定義で参照されるAmazon ECSタスクロールに追加のアクセス許可が必要です。これらの追加アクセス許可は、ポリシーとしてタスクロールに追加することが可能です。ログの送信先が Amazon CloudWatch Logs と Amazon S3 のどちらであるかによって異なります。

Amazon CloudWatch Logs

次のポリシー例では、Amazon CloudWatch Logs について必須のアクセス許可を追加しています。

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
               "logs:CreateLogStream",
               "logs:DescribeLogStreams",
               "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:region:account-id:log-group:/aws/
ecs/cloudwatch-log-group-name:*"
        }
   ]
}
```

Amazon S3

次のインラインポリシー例では、Amazon S3 について必須のアクセス許可を追加しています。

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

```
        {
            "Effect": "Allow",
            "Action": [
               "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
        {
           "Effect": "Allow",
           "Action": [
               "s3:GetEncryptionConfiguration"
           ],
           "Resource": "arn:aws:s3:::s3-bucket-name"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::s3-bucket-name/*"
        }
    ]
   }
```

独自のAWS KMS key (KMS キー) を使用した暗号化に必要な IAM アクセス許可

デフォルトでは、ローカルクライアントとコンテナ間で転送されるデータは、AWS が提供する TLS 1.2 暗号化を使用します。独自の KMS キー を使用してデータをさらに暗号化するには、KMS キー を作成し、タスク IAM ロールに `kms:Decrypt` アクセス権限を追加する必要があります。このアクセス許可は、データを復号化するためにコンテナによって使用されます。KMS キーの 作成の詳細については、キーを作成する を参照してください。

AWS KMS アクセス許可を必要とするタスク IAM ロールに次のインラインポリシーを追加します。詳細については、「ECS Exec のアクセス許可」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
```

```
            ],
            "Resource": "kms-key-arn"
        }
    ]
}
```

独自の KMS キー を使用してデータを暗号化するには、execute-command アクションを使用するユーザーまたはグループに kms:GenerateDataKey アクセス許可が付与されている必要があります。

以下のユーザーまたはグループのポリシー例では、独自の KMS キー を使用するために必要なアクセス許可が含まれています。KMS キーのAmazon リソースネーム (ARN) を指定する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": "kms-key-arn"
        }
    ]
}
```

IAM ポリシーを使用して ECS Exec へのアクセスを制限する

次の IAM ポリシー条件キーの 1 つ以上を使用して、execute-command API アクションへのユーザーアクセスを制限します。

- aws:ResourceTag/*clusterTagKey*
- ecs:ResourceTag/*clusterTagKey*
- aws:ResourceTag/*taskTagKey*
- ecs:ResourceTag/*taskTagKey*
- ecs:container-name
- ecs:cluster
- ecs:task
- ecs:enable-execute-command

以下の IAM ポリシーの例では、ユーザーは environment キーと development 値を持つタグのあるタスク内で実行されているコンテナと、cluster-nameという名前のクラスターでコマンドを実行できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:ExecuteCommand",
                "ecs:DescribeTasks"
            ],
            "Resource": [
                "arn:aws:ecs:region:aws-account-id:task/cluster-name/*",
                "arn:aws:ecs:region:aws-account-id:cluster/cluster-name"
            ],
            "Condition": {
                "StringEquals": {
                    "ecs:ResourceTag/environment": "development"
                }
            }
        }
    ]
}
```

次の IAM ポリシーの例では、コンテナ名が production-app の場合、ユーザーは execute-command API を使用できません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ecs:ExecuteCommand"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:container-name": "production-app"
                }
```

```
            }
        }
    ]
}
```

次の IAM ポリシーを使用するユーザーは、ECS Exec がオフ状態の場合にのみタスクを起動できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:RunTask",
                "ecs:StartTask",
                "ecs:CreateService",
                "ecs:UpdateService"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:enable-execute-command": "false"
                }
            }
        }
    ]
}
```

> **Note**
>
> execute-command API 操作には、リクエスト内のタスクとクラスターリソースのみが含まれるため、クラスタータグとタスクタグのみが評価されます。

IAM ポリシー条件キーの詳細については、「Service Authorization Reference」の「Actions, resources, and condition keys for Amazon Elastic Container Service」を参照してください。

[Start Session (セッション開始)] 操作へのアクセス制限

ECS Exec の外部コンテナで SSM セッションを開始することは可能ですが、セッションがログに記録されない可能性があります。ECS Exec 以外で開始されたセッションも、セッションクォータに対してカウントされません。IAM ポリシーを使用して Amazon ECS タスクに対する `ssm:start-session` アクションを直接拒否することで、このアクセスを制限することをお勧めします。使用されているタグに基づいて、すべての Amazon ECS タスクまたは特定のタスクへのアクセスを拒否できます。

以下は、指定されたクラスター名を持つすべてのリージョンのタスクに対する `ssm:start-session`アクション へのアクセスを拒否する IAM ポリシーの例です。オプションで、*`cluster-name`* にワイルドカードを含めることができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ssm:StartSession",
            "Resource": [
                "arn:aws:ecs:region:aws-account-id:task/cluster-name/*"
        }
    ]
}
```

以下は、タグキー `Task-Tag-Key` とタグ値 `Exec-Task` でタグ付けされたすべてのリージョンのリソースに対する `ssm:start-session` アクションへのアクセスを拒否する IAM ポリシーの例です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ssm:StartSession",
            "Resource": "arn:aws:ecs:*:*:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Task-Tag-Key": "Exec-Task"
                }
            }
```

```
        }
    ]
}
```

Amazon ECS Exec の使用中に発生する可能性のある問題のヘルプについては、「Exec に関する問題のトラブルシューティング」を参照してください。

Amazon ECS に関する AWS Compute Optimizer 推奨事項

AWS Compute Optimizer は、Amazon ECS のタスクとコンテナのサイズに関する推奨事項を生成します。詳細については、『AWS Compute Optimizer ユーザーガイド』の「What is AWS Compute Optimizer? (とは ?)」 を参照してください。

AWS Fargate の Amazon ECS サービスでの、タスクとコンテナサイズに関する推奨事項

AWS Compute Optimizer は、AWS Fargate の Amazon ECS サービスについての推奨事項を生成します。 AWS Compute Optimizer からは、タスクの CPU とメモリサイズおよびコンテナの CPU、コンテナメモリ、およびその予約サイズに関する推奨事項が得られます。これらの推奨事項は、Compute Optimizer コンソールの以下のページにそれぞれ表示されます。

- [Fargate の Amazon ECS サービスに関する推奨事項] ページ
- [Fargate の Amazon ECS サービスの詳細] ページ

詳細については、「AWS Compute Optimizer ユーザーガイド」の「Fargate の Amazon ECS サービスに関する推奨事項の表示」を参照してください。

Amazon ECS トラブルシューティング

ロードバランサー、タスク、サービス、またはコンテナインスタンスの問題のトラブルシューティングが必要な場合があります。この章は、Amazon ECS コンソールで Amazon ECS コンテナエージェント、コンテナインスタンス上の Docker デーモン、サービスイベントログから診断情報を見つけるのに役立ちます。

停止したタスクの詳細については、次のいずれかを参照してください。

アクション	詳細はこちら
停止したタスクのエラーを解決します。	Amazon ECS の停止したタスクのエラーを表示する
停止したタスクのエラーを表示します。	Amazon ECS の停止したタスクのエラーを解決する
停止したタスクのエラーコードを確認します。	Amazon ECS の停止したタスクのエラーメッセージ
CannotPullContainer タスクのエラーを確認します。	Amazon ECS での CannotPullContainer タスクエラー
タスクの IAM ロールリクエストを表示します。	Amazon ECS タスクの IAM ロールリクエストの表示

サービスエラーの詳細については、次のいずれかを参照してください。

アクション	詳細はこちら
サービスイベントメッセージを表示します。	Amazon ECS のサービスイベントメッセージを表示する
サービスイベントメッセージを確認します。	Amazon ECS のサービスイベントメッセージ

アクション	詳細はこちら
ロードバランサーの問題を確認します。	Amazon ECS のサービスロードバランサーのトラブルシューティング
サービスの自動スケーリングの問題を確認します。	Amazon ECS のサービス自動スケーリングのトラブルシューティング

タスク定義のエラーの詳細については、次のいずれかを参照してください。

アクション	詳細はこちら
タスク定義のメモリエラーを解決します。	Amazon ECS タスク定義の無効な CPU またはメモリエラーをトラブルシューティングする

Amazon ECS エージェントのエラーの詳細については、次のいずれかを参照してください。

アクション	詳細はこちら
Amazon ECS コンテナエージェントログを表示します。	Amazon ECS コンテナエージェントログの表示
Amazon ECS ログを収集する方法について説明します。	Amazon ECS ログコレクターを使用したコンテナログの収集
Amazon ECS エージェントを使用して診断の詳細を取得します。	エージェントのイントロスペクションを使用して Amazon ECS 診断の詳細を取得する

Docker エラーの一般的な情報については、次のいずれかを参照してください。

アクション	詳細はこちら
Docker 診断を使用します。	Amazon ECS の Docker 診断
Docker デバッグモードを有効にします。	Amazon ECS の Docker デーモンからの詳細な出力の設定
Docker API エラー 500 のトラブルシューティングを実行します。	Amazon ECS の Docker API error (500): devmapper のトラブルシューティング

ECS Exec および Amazon ECS Anywhere のエラーの詳細については、次のいずれかを参照してください。

アクション	詳細はこちら
ECS Exec のトラブルシューティングを実行します。	Amazon ECS Exec に関する問題のトラブルシューティング
Amazon ECS Anywhere のトラブルシューティングを実行します。	Amazon ECS Anywhere に関する問題のトラブルシューティング

スロットリングの問題を解決するための情報については、次のいずれかを参照してください。

アクション	詳細はこちら
Fargate のスロットリングクォータについて説明します。	AWS Fargate スロットリングのクォータ
Amazon ECS スロットリングのベストプラクティスについて説明します。	Amazon ECS のスロットリングに関する問題を処理する

API エラーの詳細については、次のいずれかを参照してください。

アクション	詳細はこちら	
API エラーを解決します。	Amazon ECS での API エラーの原因	

Amazon ECS の停止したタスクのエラーを解決する

タスクの開始に失敗すると、コンソールと describe-tasks 出力パラメータ (stoppedReason および stoppedCode) にエラーメッセージが表示されます。

停止したタスクは、コンソールで 1 時間表示できます。停止したタスクを表示するには、フィルターオプションを変更する必要があります。詳細については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

次のページには、エラーコードに関する情報が記載されています。

- 停止したタスクのエラーメッセージの変更について説明します。

  Amazon ECS の停止したタスクのエラーメッセージの更新
- 停止したタスクを表示して、原因に関する情報を取得します。

  Amazon ECS の停止したタスクのエラーを表示する
- 停止したタスクのエラーメッセージと、考えられるエラーの原因について説明します。

  Amazon ECS の停止したタスクのエラーメッセージ
- 停止したタスク接続を検証し、エラーを修正する方法について説明します。

  Amazon ECS の停止したタスクの接続を検証する

Amazon ECS の停止したタスクのエラーメッセージの更新

2024 年 6 月 14 日より、Amazon ECS チームは、以下の表に示すように停止したタスクのエラーメッセージを変更します。stopCode の変更はありません。アプリケーションが正確なエラーメッセージ文字列に依存している場合は、新しい文字列でアプリケーションを更新する必要があります。ご質問や問題については、AWS サポート にお問い合わせください。

> **Note**
>
> このエラーメッセージは変更される可能性があるため、オートメーションではエラーメッセージに依存しないことをお勧めします。

CannotPullContainerError

以前のエラーメッセージ	新しいエラーメッセージ	
CannotPullContainerError: Error response from daemon: pull access denied for *repository* , repository does not exist or may require 'docker login': denied: User: *roleARN*	• CannotPullContainerError: The task can't pull the image. ロールにレジストリからイメージをプルするためのアクセス許可があることを確認します。Error response from daemon: pull access denied for *repository* , repository does not exist or may require 'docker login': denied: User: *roleARN* is not authorized to perform: ecr:BatchGetImage on resource: *image* because no identity-based policy allows the ecr:BatchGetImage action. • CannotPullContainerError: The task can't pull the image. イメージが存在することを確認します。Error response from daemon: pull access denied for *repository* , repository does not exist or may	

以前のエラーメッセージ	新しいエラーメッセージ	
	require 'docker login': denied: requested access to the resource is denied.	
CannotPullContainerError: Error response from daemon: Get *imageURI*: net/http: request canceled while waiting for connection	CannotPullContainerError: The task can't pull the image. ネットワーク設定を確認します。Error response from daemon: Get *image*: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)	
CannotPullContainerError: ref pull has been retried 5 time(s): failed to copy: httpReadSeeker: failed open: failed to do request: Get *registry-uri* : dial tcp <ip>:<port> i/o timeout	CannotPullContainerError: The task cannot pull *image-uri* from the registry *registry-uri* . There is a connection issue between the task and the registry. Check your task network configuration. : failed to copy: httpReadSeeker: failed open: failed to do request: Get *registry-uri* : dial tcp <ip>:<port> i/o timeout	

ResourceNotFoundException

以前のエラーメッセージ	新しいエラーメッセージ	
Fetching secret data from AWS Secrets Manager in region *region*: secret *sercretARN* : ResourceN	ResourceNotFoundException: The task can't retrieve the secret with ARN '*sercretARN* ' from AWS Secrets	

以前のエラーメッセージ	新しいエラーメッセージ	
otFoundException: Secrets Manager can't find the specified secret.	Manager. Check whether the secret exists in the specified Region. ResourceNotFoundException: Fetching secret data from AWS Secrets Manager in region *region*: secret *sercretARN* : ResourceNotFoundException: Secrets Manager can't find the specified secret.	

ResourceInitializationError

以前のエラーメッセージ	新しいエラーメッセージ	
ResourceInitializationError : unable to pull secrets or registry auth: execution resource retrieval failed: unable to retrieve ecr registry auth: service call has been retried 3 time(s): RequestError: send request failed caused by: Post "https://api.ecr.us-east-1.amazonaws.com/": dial tcp <ip>:<port>: i/o timeout. Please check your task network configuration.	ResourceInitializationError : unable to pull secrets or registry auth: The task cannot pull registry auth from Amazon ECR: There is a connection issue between the task and Amazon ECR. Check your task network configuration. RequestError: send request failed caused by: Post "https://api.ecr.us-east-1.amazonaws.com": dial tcp <ip>:<port>: i/o timeout	
ResourceInitializationError : unable to pull secrets or registry auth: execution resource retrieval failed: unable to retrieve secrets from	ResourceInitializationError : unable to pull secrets or registry auth: unable to retrieve secrets from ssm: The task cannot pull	

以前のエラーメッセージ	新しいエラーメッセージ	
ssm: service call has been retried 5 time(s): RequestCanceled: request context canceled caused by: context deadline exceeded	secrets from AWS Systems Manager. There is a connection issue between the task and AWS Systems Manager Parameter Store. Check your task network configuration. RequestCanceled: request context canceled caused by: context deadline exceeded	
ResourceInitializationError: failed to download env files: file download command: non empty error stream: RequestCanceled: request context canceled caused by: context deadline exceeded	ResourceInitializationError: failed to download env files: The task can't download the environment variable files from Amazon S3. There is a connection issue between the task and Amazon S3. Check your task network configuration. service call has been retried 5 time(s): RequestCanceled: request context canceled caused by: context deadline exceeded	
ResourceInitializationError : failed to validate logger args::signal:killed	ResourceInitializationError : failed to validate logger args: The task cannot find the Amazon CloudWatch log group defined in the task definition. There is a connection issue between the task and Amazon CloudWatch. Check your network configuration. : signal: killed	

以前のエラーメッセージ	新しいエラーメッセージ	
ResourceInitializationError : unable to pull secrets or registry auth: pull command failed: : signal: killed	ResourceInitializationError : unable to pull secrets or registry auth: Check your task network configuration. : signal: killed	

Amazon ECS の停止したタスクのエラーを表示する

タスクの開始に問題がある場合、アプリケーションエラーまたは設定エラーのためにタスクが停止している可能性があります。例えば、タスクを実行するとタスクが `PENDING` ステータスを表示して消えるとします。

タスクが Amazon ECS サービスによって作成された場合、Amazon ECS がサービスを維持するために行うアクションはサービスイベントで公開されます。イベントは、AWS Management Console、AWS CLI、AWS SDK、Amazon ECS API または SDK と API を使用するツールで表示できます。これらのイベントには、タスク内のコンテナの実行が停止したり、Elastic Load Balancing によるヘルスチェックに何度も失敗したりしたことが原因で、Amazon ECS が停止してタスクが置き換えられることが含まれます。

また、タスクが Amazon EC2 にあるコンテナインスタンスまたは外部コンピュータで実行された場合、コンテナランタイムと Amazon ECS エージェントのログを確認することもできます。これらのログは、ホスト Amazon EC2 インスタンスまたは外部コンピュータにあります。詳細については、「Amazon ECS コンテナエージェントログの表示」を参照してください。

手順

Console

AWS Management Console

次の手順に従って、コンソールを使用して停止されたタスクにエラーがないかどうかを確認することができます。停止したタスクを表示するには、フィルターオプションを変更する必要があります。

停止したタスクは 1 時間だけコンソールに表示されます。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。

2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. [Cluster: ***name***] (クラスター: 名前) ページで、[Tasks] (タスク) タブを選択します。
5. 停止済みのタスクを表示するようにフィルターを設定します。希望ステータスのフィルターでは、停止 を選択します。

   [停止済み] オプションには停止されたタスクが表示され、[任意の必要なステータス] にはすべてのタスクが表示されます。
6. 停止したタスクを選択して検査します。
7. 停止済みのタスクの行の [前回のステータス] 列で、[停止済み] を選択します。

   ポップアップウィンドウに停止した理由が表示されます。

AWS CLI

1. クラスターで停止したタスクを一覧表示します。出力には、タスクの Amazon リソースネーム (ARN) が含まれますが、この名前は、タスクを説明するものである必要があります。

```
aws ecs list-tasks \
     --cluster cluster_name \
     --desired-status STOPPED \
     --region region
```

2. 停止したタスクを記述して情報を取得します。詳細については、「AWS Command Line Interface リファレンス」の「describe-tasks」を参照してください。

```
aws ecs describe-tasks \
     --cluster cluster_name \
     --tasks arn:aws:ecs:region:account_id:task/cluster_name/task_ID \
     --region region
```

次の出力パラメータを使用します。

- `stopCode` - ResourceInitializationError などの停止コードは、タスクが停止された理由を示します。
- `StoppedReason` - タスクが停止した理由を示します。

- `reason` (`containers` 構造の場合) - 理由には、停止したコンテナに関するその他の詳細が含まれます。

次のステップ

停止したタスクを表示して、原因に関する情報を取得します。詳細については、「Amazon ECS の停止したタスクのエラーメッセージ」を参照してください。

Amazon ECS の停止したタスクのエラーメッセージ

タスクが予期せず停止した場合に表示される可能性のあるエラーメッセージは、以下のとおりです。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

停止したタスクのエラーコードには、「ResourceInitializationError」などのカテゴリが関連付けられています。各カテゴリの詳細については、以下を参照してください。

カテゴリ	詳細はこちら
TaskFailedToStart	Amazon ECS TaskFailedToStart エラーのトラブルシューティング
ResourceInitializationError	Amazon ECS での ResourceInitializationError エラーのトラブルシューティング
ResourceNotFoundException	Amazon ECS ResourceNotFoundException エラーのトラブルシューティング
SpotInterruptionError	Amazon ECS での SpotInterruption エラーのトラブルシューティング
InternalError	Amazon ECS での InternalError エラーのトラブルシューティング

カテゴリ	詳細はこちら
JVM OutOfMemoryError	Amazon ECS での OutOfMemoryError エラーのトラブルシューティング
ContainerRuntimeError	Amazon ECS での ContainerRuntimeError エラーのトラブルシューティング
ContainerRuntimeTimeoutError	Amazon ECS での ContainerRuntimeTimeoutError エラーのトラブルシューティング
CannotStartContainerError	Amazon ECS での CannotStartContainerError エラーのトラブルシューティング
CannotStopContainerError	Amazon ECS での CannotStopContainerError エラーのトラブルシューティング
CannotInspectContainerError	Amazon ECS での CannotInspectContainerError エラーのトラブルシューティング
CannotCreateVolumeError	Amazon ECS での CannotCreateVolumeError エラーのトラブルシューティング
CannotPullContainer	Amazon ECS での CannotPullContainer タスクエラー

Amazon ECS TaskFailedToStart エラーのトラブルシューティング

以下に、`TaskFailedToStart` エラーメッセージおよび、そのエラーを修正するために取れる措置を示します。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

Unexpected EC2 error while attempting to Create Network Interface with public IP assignment enabled in subnet '***subnet-id***

これは、aswsvpc ネットワークモードを使用し、パブリック IP アドレスを持つサブネットで実行される Fargate タスクにおいて、サブネットに十分な IP アドレスがない場合に発生します。

利用可能な IP アドレスの数は、Amazon EC2 コンソールのサブネットの詳細ページ、または `describe-subnets` を使用して確認できます。詳細については、Amazon VPC ユーザーガイドの「サブネットを表示する」を参照してください。

この問題を修正するには、タスクを実行するための新しいサブネットを作成します。

InternalError: ***<reason>***

このエラーは、ENI アタッチメントが要求されたときに発生します。Amazon EC2 は ENI のプロビジョニングを非同期で処理します。プロビジョニングプロセスには時間がかかります。Amazon ECS では、待ち時間が長かったり、エラーが報告されない場合に備えてタイムアウトを設けています。ENI がプロビジョニングされても、レポートは障害タイムアウト後に Amazon ECS に送られる場合があります。この場合、Amazon ECS は使用中の ENI で報告されたタスク障害を確認します。

The selected task definition is not compatible with the selected compute strategy

このエラーは、起動タイプがクラスターのキャパシティタイプと一致しないタスク定義を選択した場合に発生します。詳細については、「Amazon ECS 起動タイプ」を参照してください。クラスターに割り当てられたキャパシティープロバイダーと一致するタスク定義を選択する必要があります。

Unable to attach network interface to unused device index

このエラーは、awsvpc ネットワーキングタイプを使用しているときに、タスク用に十分な CPU/メモリがない場合に発生します。まず、インスタンスの CPU を確認します。詳細については、「Amazon EC2 インスタンスタイプ」の「Amazon EC2 インスタンスタイプの仕様」を参照してください。インスタンスの CPU 値をインスタンスの ENI の数で乗算します。その値をタスク定義で使用します。

AGENT

タスクを起動しようとしたコンテナインスタンスに、現在接続されていないエージェントがあります。タスク配置の待ち時間が長くならないように、リクエストは拒否されました。

切断されたエージェントをトラブルシューティングする方法については、「切断された Amazon ECS エージェントをトラブルシューティングするにはどうすればよいですか?」を参照してください。

Amazon ECS での ResourceInitializationError エラーのトラブルシューティング

以下に、`ResourceInitialization` エラーメッセージおよび、そのエラーを修正するために取れる措置を示します。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

エラー

- The task cannot pull registry authentication from Amazon ECR. There is a connection issue between the task and Amazon ECR. Check your task network configuration.
- The task can't download the environment variable files from Amazon S3. There is a connection issue between the task and Amazon S3. Check your task network configuration.
- The task cannot pull secrets from AWS Systems Manager Parameter Store. Check your network connection between the task and AWS Systems Manager.
- The task can’t pull secrets from AWS Secrets Manager. There is a connection issue between the task and Secrets Manager. Check your task network configuration.
- The task can’t pull the secret from Secrets Manager. The task can't retrieve the secret with ARN ‘secretARN' from Secrets Manager. Check whether the secret exists in the specified Region.
- pull command failed: unable to pull secrets or registry auth Check your task network configuration.
- The task cannot find the Amazon CloudWatch log group defined in the task definition. There is a connection issue between the task and Amazon CloudWatch. ネットワーク設定を確認します。
- failed to initialize logging driver
- failed to invoke EFS utils commands to set up EFS volumes

The task cannot pull registry authentication from Amazon ECR. There is a connection issue between the task and Amazon ECR. Check your task network configuration.

このエラーは、タスクが Amazon ECR に接続できないことを示します。

タスクと Amazon ECR との間の接続を確認してください。詳細については、Amazon ECS の停止したタスクの接続を検証する を参照してください。

The task can't download the environment variable files from Amazon S3. There is a connection issue between the task and Amazon S3. Check your task network configuration.

このエラーは、タスクが Amazon S3 から環境設定ファイルをダウンロードできない場合に発生します。

タスクと Amazon S3 VPC エンドポイントとの間の接続を確認してください。詳細については、Amazon ECS の停止したタスクの接続を検証する を参照してください。

The task cannot pull secrets from AWS Systems Manager Parameter Store. Check your network connection between the task and AWS Systems Manager.

このエラーは、タスクが Systems Manager の認証情報を使用して、タスク定義で定義されたイメージをプルできない場合に発生します。

タスクと Systems Manager VPC エンドポイントとの間の接続を確認してください。詳細については、Amazon ECS の停止したタスクの接続を検証する を参照してください。

The task can’t pull secrets from AWS Secrets Manager. There is a connection issue between the task and Secrets Manager. Check your task network configuration.

このエラーは、タスクが Secrets Manager の認証情報を使用して、タスク定義で定義されたイメージをプルできない場合に発生します。

エラーは、Systems Manager VPC エンドポイントとタスク間のネットワーク接続に問題があることを示します。

タスクとエンドポイント間の接続を確認する方法については、「Amazon ECS の停止したタスクの接続を検証する」を参照してください。

The task can’t pull the secret from Secrets Manager. The task can't retrieve the secret with ARN ‘***secretARN***' from Secrets Manager. Check whether the secret exists in the specified Region.

このエラーは、タスクが Secrets Manager の認証情報を使用して、タスク定義で定義されたイメージをプルできない場合に発生します。

この問題は、次のいずれかの理由によって発生します。

エラーの原因	手順	
Secrets Manager VPC エンドポイントとタスク間のネットワーク接続の問題 エラーメッセージに次のいずれかの文字列が表示されている場合、問題の原因はネットワークです。 • dial tcp • dial udp • <ip>:<port>: i/o timeout • net/http: TLS handshake timeout • read: connection timed out • Client.Timeout exceeded while awaiting headers • net/http: request canceled while waiting for connection • signal: killed • context deadline exceeded	タスクと Secrets Manager エンドポイント間の接続を確認します。詳細については、「Amazon ECS の停止したタスクの接続を検証する」を参照してください。	
タスク定義で定義されたタスク実行ロールに、Secrets Manager のアクセス許可がありません。	タスク実行ロールに、Secrets Manager に必要なアクセス許可を追加します。詳細については、「Secrets Manager または Systems Manager のアクセス許可」を参照してください。	
シークレット ARN が存在しません	Secrets Manager に ARN が存在することを確認します。イメージの表示については、「Secrets Manager デベロッ	

エラーの原因	手順	
	パーガイド」の「Find secrets in Secrets Manager」を参照してください。	

pull command failed: unable to pull secrets or registry auth Check your task network configuration.

このエラーは、タスクが Amazon ECR、Systems Manager、または Secrets Manager に接続できない場合に発生します。これはネットワークの設定ミスが原因です。

この問題を解決するには、タスクと Amazon ECR との間の接続を確認します。また、タスクとシークレットを保存するサービス (Systems Manager または Secrets Manager) との間の接続も確認する必要があります。詳細については、「Amazon ECS の停止したタスクの接続を検証する」を参照してください。

The task cannot find the Amazon CloudWatch log group defined in the task definition. There is a connection issue between the task and Amazon CloudWatch. ネットワーク設定を確認します。

このエラーは、タスクがタスク定義で定義した CloudWatch ロググループを見つけられない場合に発生します。

このエラーは、CloudWatch VPC エンドポイントとタスクとの間のネットワーク接続に問題があることを示します。

タスクとエンドポイント間の接続を確認する方法については、「Amazon ECS の停止したタスクの接続を検証する」を参照してください。

failed to initialize logging driver

このエラーは、タスクがタスク定義で定義した CloudWatch ロググループを見つけられない場合に発生します。

このエラーは、タスク定義内に CloudWatch グループが存在しないことを示します。

対象の CloudWatch を検索するには、次の手順を実行します。

1. 次のコマンドを実行して、タスク定義情報を取得します。

```
aws ecs describe-task-definition \
```

```
    --task-definition task-def-name
```

各コンテナの出力を見て、awslogs-group 値を書き留めます。

```
"logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-group": "/ecs/example-group",
                    "awslogs-create-group": "true",
                    "awslogs-region": "us-east-1",
                    "awslogs-stream-prefix": "ecs"
                },
```

2. このグループが CloudWatch に存在することを確認します。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「ロググループとログストリームの操作」を参照してください。

   この問題は、タスク定義で指定されたグループが正しくないことか、ロググループが存在しないことのいずれかです。

3. 問題を修正します。

問題	手順
タスク定義で正しくないロググループが指定されています。	コンテナ定義にロググループ設定が含まれるようにタスク定義を更新します。タスク定義の更新については、「Amazon Elastic Container Service API リファレンス」の「コンソールを使用した Amazon ECS タスク定義の更新」または「RegisterTaskDefinition」を参照してください。
ロググループが CloudWatch に存在しません	ロググループを作成します。詳細については、Amazon CloudWatch Logs ユーザー

問題	手順	
	ガイドの「CloudWatch Logs のロググループを作成する」を参照してください。	

failed to invoke EFS utils commands to set up EFS volumes

以下の問題により、タスクに Amazon EFS ボリュームをマウントできない可能性があります。

- Amazon EFS ファイルシステムが正しく設定されていません。
- タスクに必要なアクセス許可がありません。
- ネットワークおよび VPC 構成に関連する問題があります。

この問題をデバッグして修正する方法については、AWS re:Post の 「AWS Fargate タスクに Amazon EFS ボリュームをマウントできない理由」を参照してください。

Amazon ECS ResourceNotFoundException エラーのトラブルシューティング

以下に、 `ResourceNotFoundException` エラーメッセージおよび、そのエラーを修正するために取れる措置を示します。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

The task can't retrieve the secret with ARN '***sercretARN***' from AWS Secrets Manager. Check whether the secret exists in the specified Region.

このエラーは、タスクが Secrets Manager からシークレットを取得できない場合に発生します。つまり、タスク定義で指定されたシークレット (およびエラーメッセージに含まれるシークレット) は Secrets Manager に存在しないということです。

リージョンはエラーメッセージに含まれています。

Fetching secret data from AWS Secrets Manager in region *region*: secret *sercretARN*: ResourceNotFoundException: Secrets Manager can't find the specified secret.

シークレットの検索方法については、「AWS Secrets Manager ユーザーガイド」の「Find secrets in AWS Secrets Manager」を参照してください。

次の表を使用して、エラーを特定して対処します。

問題	アクション
シークレットは、タスク定義とは異なるリージョンにあります。	a. タスクと同じリージョンにシークレットを作成します。詳細については、「AWS Secrets Manager シークレットを作成する」を参照してください。 b. 新しいシークレットでタスク定義を更新します。詳細については、「Amazon Elastic Container Service API リファレンス」の「コンソールを使用した Amazon ECS タスク定義の更新」または「RegisterTaskDefinition」参照してください。
タスク定義に誤ったシークレット ARN が存在します。正しいシークレットは Secrets Manager に存在します。	正しいシークレットでタスク定義を更新します。詳細については、「Amazon Elastic Container Service API リファレンス」の「コンソールを使用した Amazon ECS タスク定義の更新」または「RegisterTaskDefinition」参照してください。
シークレットが存在しません。	a. タスクと同じリージョンにシークレットを作成します。詳細については、「AWS Secrets Manager シークレットを作成する」を参照してください。

問題	アクション	
	b. 新しいシークレットでタスク定義を更新します。詳細については、「Amazon Elastic Container Service API リファレンス」の「コンソールを使用した Amazon ECS タスク定義の更新」または「RegisterTaskDefinition」参照してください。	

Amazon ECS での SpotInterruption エラーのトラブルシューティング

`SpotInterruption` エラーの原因は、Fargate と EC2 の起動タイプによって異なります。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

Fargate 起動タイプ

`SpotInterruption` エラーは、Fargate Spot に容量がない場合や、Fargate がスポット容量を元に戻した場合に発生します。

タスクを複数のアベイラビリティーゾーンで実行することで、容量を増やすことができます。

EC2 起動タイプ

このエラーは、使用可能なスポットインスタンスがない場合や、EC2 がスポットインスタンスの容量を元に戻した場合に発生します。

インスタンスを複数のアベイラビリティーゾーンで実行することで、容量を増やすことができます。

Amazon ECS での InternalError エラーのトラブルシューティング

適用対象: Fargate 起動タイプ

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

`InternalError` エラーは、ランタイムに関連しない予期せぬ内部エラーがエージェントに発生した場合に発生します。

このエラーは、プラットフォームバージョン `1.4` 以降を使用の場合にのみ発生します。

この問題をデバッグして修正する方法については、AWS re:Post の「ECS クラスターで起動に失敗した Amazon ECS タスクをトラブルシューティングする方法」を参照してください。

Amazon ECS での OutOfMemoryError エラーのトラブルシューティング

以下は、OutOfMemoryError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

container killed due to memory usage

このエラーは、タスク定義で割り当てられているよりも多くのメモリをコンテナ内のプロセスで消費しているためにコンテナが終了したときに発生します。

Amazon ECS での ContainerRuntimeError エラーのトラブルシューティング

以下は、ContainerRuntimeError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

ContainerRuntimeError

このエラーは、エージェントが `containerd` がランタイム固有のオペレーションに関する予期しないエラーを受け取った場合に発生します。このエラーは通常、エージェントや `containerd` ランタイムの内部障害によって発生します。

このエラーは、プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) を使用している場合のみに発生します。

この問題をデバッグして修正する方法については、AWS re:Post の「Amazon ECS タスクが停止する理由」を参照してください。

Amazon ECS での ContainerRuntimeTimeoutError エラーのトラブルシューティング

以下は、ContainerRuntimeTimeoutError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

Could not transition to running; timed out after waiting 1m or Docker timeout error

このエラーは、タイムアウト期間内にコンテナが `RUNNING`または`STOPPED`のどちらかの状態に移行できなかった場合に発生します。理由とタイムアウト値は、エラーメッセージに表示されます。

Amazon ECS での CannotStartContainerError エラーのトラブルシューティング

以下は、CannotStartContainerError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

failed to get container status: ***<reason>***

このエラーは、コンテナをスタートできない場合に発生します。

コンテナは、ここで指定したメモリを超えようとすると、停止されます。コンテナに提供するメモリを増やしてください。これは、タスク定義の `memory` パラメータです。詳細については、「the section called “「メモリ」”」を参照してください。

Amazon ECS での CannotStopContainerError エラーのトラブルシューティング

以下は、CannotStopContainerError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

CannotStopContainerError

このエラーは、コンテナを停止できない場合に発生します。

この問題をデバッグして修正する方法については、AWS re:Post の「Amazon ECS タスクが停止する理由」を参照してください。

Amazon ECS での CannotInspectContainerError エラーのトラブルシューティング

以下は、CannotInspectContainerError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

CannotInspectContainerError

このエラーは、コンテナエージェントがコンテナランタイムを通してコンテナを説明できない場合に発生します。

プラットフォームバージョン `1.3` 以前を使用している場合、Amazon ECS エージェントは Docker から理由を返します。

プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) を使用している場合、Fargate エージェントは `containerd` から理由を返します。

この問題をデバッグして修正する方法については、AWS re:Post の「Amazon ECS タスクが停止する理由」を参照してください。

Amazon ECS での CannotCreateVolumeError エラーのトラブルシューティング

以下は、CannotCreateVolumeError のエラーメッセージと、エラーを修正するために実行できるアクションの一部です。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

CannotCreateVolumeError

このエラーは、エージェントがタスク定義に指定されているボリュームマウントを作成できない場合に発生します。

このエラーは、プラットフォームバージョン `1.4.0` 以降 (Linux) または `1.0.0` 以降 (Windows) を使用している場合のみに発生します。

この問題をデバッグして修正する方法については、AWS re:Post の「Amazon ECS タスクが停止する理由」を参照してください。

Amazon ECS での CannotPullContainer タスクエラー

次のエラーは、Amazon ECS が指定されたコンテナイメージを取得できないためにタスクを開始できなかったことを示しています。

> **Note**
>
> 1.4 Fargate プラットフォームバージョンでは、長いエラーメッセージが切り捨てられます。

停止したタスクのエラーメッセージを AWS Management Console で確認する方法については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

エラー

- The task can't pull the image. ロールにレジストリからイメージをプルするためのアクセス許可があることを確認します。
- The task cannot pull 'image-name' from the Amazon ECR repository 'repository URI'. There is a connection issue between the task and Amazon ECR. Check your task network configuration.
- The task can't pull the image. Check your network configuration
- API error (500): Get https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request canceled while waiting for connection
- API エラー
- write /var/lib/docker/tmp/GetImageBlob111111111: no space left on device
- ERROR: toomanyrequests: Too Many Requests or You have reached your pull rate limit.
- Error response from daemon: Get url: net/http: request canceled while waiting for connection
- ref pull has been retried 1 time(s): failed to copy: httpReaderSeeker: failed open: unexpected status code
- pull access denied
- pull command failed: panic: runtime error: invalid memory address or nil pointer dereference
- error pulling image conf/error pulling image configuration
- コンテキストがキャンセルされました

The task can't pull the image. ロールにレジストリからイメージをプルするためのアクセス許可があることを確認します。

このエラーは、アクセス許可の問題により、タスク定義で指定されたイメージをタスクがプルできないことを示します。

この問題を解決するには。

1. イメージが*#####*に存在することを確認してください。イメージの表示の詳細については、「Amazon Elastic Container Registry ユーザーガイド」の「Viewing image details in Amazon ECR」を参照してください。
2. *role-arn* にイメージをプルするための正しいアクセス許可があることを確認します。

   ロールを更新する方法については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。

   タスクには次のいずれかのロールを使用します。

   - Fargate 起動タイプのタスクの場合、これはタスク実行ロールになります。Amazon ECR の追加のアクセス許可については、「インターフェイスエンドポイントのアクセス許可によって Amazon ECR イメージをプルする Fargate タスクです。」を参照してください。
   - EC2 起動タイプのタスクの場合、これはコンテナインスタンスロールになります。Amazon ECR の追加のアクセス許可については、「Amazon ECR のアクセス許可」を参照してください。

The task cannot pull '***image-name***' from the Amazon ECR repository '***repository URI***'. There is a connection issue between the task and Amazon ECR. Check your task network configuration.

このエラーは、タスクが Amazon ECR に接続できないことを示します。*##### URI* リポジトリへの接続を確認してください。

これらの問題を検証および解決する方法の詳細については、「Amazon ECS の停止したタスクの接続を検証する」を参照してください。

The task can't pull the image. Check your network configuration

このエラーは、タスクが Amazon ECR に接続できないことを示します。

これらの問題を検証および解決する方法の詳細については、「Amazon ECS の停止したタスクの接続を検証する」を参照してください。

API error (500): Get https://111122223333.dkr.ecr.us-east-1.amazonaws.com/v2/: net/http: request canceled while waiting for connection

このエラーは、インターネットへのルートがないため、接続がタイムアウトしたことを示します。

この問題を解決するには、以下ができます。

- パブリックサブネットのタスクでは、タスクの起動時に [Auto-assign public IP] (自動割り当てパブリック IP)を [ENABLED] (有効)に指定する必要があります。詳細については、「Amazon ECS タスクとしてのアプリケーションの実行」を参照してください。
- プライベートサブネットのタスクでは、タスク起動時に [Auto-assign public IP] (自動割り当てパブリック IP) を [DISABLED] (無効) に指定し、VPC の NAT ゲートウェイを設定してリクエストをインターネットにルートします。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。

API エラー

このエラーは、Amazon ECR エンドポイントとの接続に問題があることを示します。

この問題を解決する方法については、サポート ウェブサイトの「Amazon ECS の Amazon ECR エラー "CannotPullContainerError: API error" を解決するには」を参照してください。

write /var/lib/docker/tmp/***GetImageBlob111111111***: no space left on device

このエラーは、ディスク容量が不足していることを示しています。

この問題を解決するには、ディスク容量を解放します。

Amazon ECS 最適化 AMI を使用している場合は、次のコマンドを使用してファイルシステムで 20 個の最大ファイルを取得できます。

```
du -Sh / | sort -rh | head -20
```

出力例:

```
5.7G    /var/lib/docker/
containers/50501b5f4cbf90b406e0ca60bf4e6d4ec8f773a6c1d2b451ed8e0195418ad0d2
1.2G    /var/log/ecs
594M    /var/lib/docker/devicemapper/mnt/
c8e3010e36ce4c089bf286a623699f5233097ca126ebd5a700af023a5127633d/rootfs/data/logs
```

```
...
```

場合によっては、実行中のコンテナによってルートボリュームがいっぱいになる可能性があります。コンテナが max-size 制限のないデフォルトの json-file ログドライバーを使用している場合、ログファイルが使用されているスペースの大半を占めている可能性があります。docker ps コマンドを使用して、上記の出力からコンテナ ID にディレクトリ名をマッピングすることによって、どのコンテナが容量を使用しているかを確認します。例:

```
CONTAINER ID   IMAGE                                COMMAND             CREATED
 STATUS              PORTS                               NAMES
50501b5f4cbf   amazon/amazon-ecs-agent:latest   "/agent"            4 days ago
 Up 4 days                                              ecs-agent
```

デフォルトでは、json-file ログドライバーを使用する場合、Docker はすべてのコンテナの標準出力 (および標準エラー) をキャプチャし、JSON 形式を使用してファイルに書き込みます。ログドライバーオプションとして max-size を設定できます。これにより、ログファイルの容量が大きくなりすぎるのを防ぐことができます。詳細については、Docker ドキュメントの「JSON ファイルロギングドライバー」を参照してください。

このオプションの使用方法を示すコンテナ定義のスニペットを次に示します。

```
{
    "log-driver": "json-file",
    "log-opts": {
        "max-size": "256m"
    }
}
```

コンテナログのディスク容量使用量が大きすぎる場合、awslogs ログドライバーを使用することもできます。awslogs ログドライバーがログを CloudWatch に送信します。これによりコンテナインスタンスのコンテナログに使用されるディスク容量が解放されます。詳細については、「Amazon ECS ログを CloudWatch に送信する 」を参照してください。

ERROR: toomanyrequests: Too Many Requests or You have reached your pull rate limit.

このエラーは、Docker Hub のレート制限があることを示します。

次のエラーのいずれかが表示された場合は、Docker Hub のレート制限に達している可能性があります。

Docker Hub のレート制限の詳細については、[Understanding Docker Hub rate limiting] (Docker ハブのレート制限を理解する) を参照してください。

Docker Hub のレート制限を上げ、コンテナインスタンスの Docker プルを認証する必要がある場合は、「Private registry authentication for container instances」を参照してください。

Error response from daemon: Get ***url***: net/http: request canceled while waiting for connection

このエラーは、インターネットへのルートがないため、接続がタイムアウトしたことを示します。

この問題を解決するには、以下ができます。

- パブリックサブネットのタスクでは、タスクの起動時に [Auto-assign public IP] (自動割り当てパブリック IP)を [ENABLED] (有効)に指定する必要があります。詳細については、「Amazon ECS タスクとしてのアプリケーションの実行」を参照してください。
- プライベートサブネットのタスクでは、タスク起動時に [Auto-assign public IP] (自動割り当てパブリック IP) を [DISABLED] (無効) に指定し、VPC の NAT ゲートウェイを設定してリクエストをインターネットにルートします。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。

ref pull has been retried 1 time(s): failed to copy: httpReaderSeeker: failed open: unexpected status code

このエラーは、イメージのコピー時に問題があったことを示します。

この問題を解決するには、次のいずれかの記事を確認してください。

- Fargate タスクについては、Fargate Amazon ECSタスクの「cannotpullcontainererror」エラーの解決方法を参照してください。
- その他のタスクについては、Amazon ECS タスクの「cannotpullcontainererror」エラーの解決方法を参照してください。

pull access denied

このエラーは、イメージにアクセスできないことを示します。

この問題を解決するには、Amazon ECR で Docker クライアントを認証する必要がある場合があります。詳細については、Amazon ECR ユーザーガイドの「プライベートレジストリ認証」を参照してください。

pull command failed: panic: runtime error: invalid memory address or nil pointer dereference

このエラーは、メモリアドレスが無効であるか、ポインターデリファレンスが nil であるため、イメージにアクセスできないことを示しています。

この問題を解決するには。

- Amazon S3 に到達するためのセキュリティグループのルールがあることを確認してください。
- ゲートウェイエンドポイントを使用するときは、エンドポイントにアクセスするためのルートをルートテーブルに追加する必要があります。

error pulling image conf/error pulling image configuration

このエラーは、レート制限に達したか、ネットワークエラーが発生したことを示します。

この問題を解決するには、「Amazon ECS EC2 起動タイプタスクで CannotPullContainerError エラーを解決する方法」を参照してください。

コンテキストがキャンセルされました

このエラーは、コンテキストがキャンセルされたことを示しています。

このエラーの一般的な原因は、タスクが使用している VPC にコンテナイメージを Amazon ECR から取得するルートがないためです。

Amazon ECS の停止したタスクの接続を検証する

ネットワーク接続の問題により、タスクが停止することがあります。断続的な問題である可能性がありますが、タスクがエンドポイントに接続できないことが原因である可能性が最も高いです。

タスクの接続をテストする

`AWSSupport-TroubleshootECSTaskFailedToStart` ランブックを使用して、タスクの接続をテストできます。ランブックを使用する場合は、次のリソースに関する情報が必要です。

- タスク ID

  最後に失敗したタスク のID を使用します。
- タスクが属していたクラスター

ランブックの使用方法については、「AWS Systems Manager Automation ランブックリファレンス」の「AWSSupport-TroubleshootECSTaskFailedToStart」を参照してください。

ランブックはタスクを分析します。タスクの開始を妨げる可能性のある次の問題については、「出力」セクションで結果を確認できます。

- 設定済みのコンテナレジストリーへのネットワーク接続
- VPC エンドポイント接続
- セキュリティグループのルール設定

VPC エンドポイントの問題を修正する

AWSSupport-TroubleshootECSTaskFailedToStart ランブックの結果に VPC エンドポイントの問題が表示された場合は、次の設定を確認します。

- エンドポイントを作成する VPC では、プライベート DNS を使用する必要があります。
- タスクが接続できないサービスの AWS PrivateLink エンドポイントが、タスクと同じ VPC 内にあることを確認してください。詳細については、以下のいずれかを参照してください。

サービス	サービスの VPC エンドポイント情報	
Amazon ECR	Amazon ECS およびインターフェイスの VPC エンドポイント (AWS PrivateLink)	
Systems Manager	Systems Manager のために VPC エンドポイントを使用して EC2 インスタンスのセキュリティを強化する	
Secrets Manager	AWS Secrets Manager VPC エンドポイントを使用する	
クラウドWatch	CloudWatch VPC エンドポイント	

サービス	サービスの VPC エンドポイント情報	
Amazon S3	Amazon S3 用 AWS PrivateLink	

- ポート 443 DNS (TCP) トラフィックで HTTPS を許可するタスクサブネットのアウトバウンドルールを設定します。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「セキュリティグループへのルールの追加」を参照してください。
- カスタムネームドメインサーバーを使用する場合は、DNS クエリの設定を確認します。クエリは、53 番ポートで外部への通信を行うことができ、UDP および TCP プロトコルを使用する必要があります。また、443 番ポートでの HTTPS 通信も必要です。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「セキュリティグループルールを構成する」を参照してください。
- サブネットにネットワーク ACL がある場合は、次の ACL ルールが必要です。
  - ポート 1024-65535 でトラフィックを許可するアウトバウンドルール
  - ポート 443 の TCP トラフィックを許可するインバウンドルール

  ルールの設定方法については、「Amazon Virtual Private Cloud ユーザーガイド」の「network ACLs」を参照してください。

ネットワークの問題を修正する

`AWSSupport-TroubleshootECSTaskFailedToStart` ランブックの結果にネットワークの問題が表示されたら、次の設定を確認します。

パブリックサブネットで awsvpc ネットワークモードを使用するタスク

ランブックに基づいて次の設定を実行します。

- パブリックサブネットのタスクでは、タスクの起動時に [Auto-assign public IP] (自動割り当てパブリック IP)を [ENABLED] (有効)に指定する必要があります。詳細については、「Amazon ECS タスクとしてのアプリケーションの実行」を参照してください。
- インターネットトラフィックを処理するにはゲートウェイが必要です。タスクサブネットのルートテーブルには、ゲートウェイへのトラフィック用のルートが必要です。

  詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「ルートテーブルのルートの追加と削除」を参照してください。

ゲートウェイタイプ	ルートテーブルの送信先	ルートテーブルのターゲット
NAT	0.0.0.0/0	NAT ゲートウェイ ID
インターネットゲートウェイ	0.0.0.0/0	インターネットゲートウェイ ID

- タスクサブネットにネットワーク ACL がある場合は、次の ACL ルールが必要です。
  - ポート 1024-65535 でトラフィックを許可するアウトバウンドルール
  - ポート 443 の TCP トラフィックを許可するインバウンドルール

  ルールの設定方法については、「Amazon Virtual Private Cloud ユーザーガイド」の「network ACLs」を参照してください。

プライベートサブネットで awsvpc ネットワークモードを使用するタスク

ランブックに基づいて次の設定を実行します。

- タスクの起動時に、[自動割り当てパブリック IP] で [無効] を選択します。
- リクエストがインターネットにルーティンされるように VPC の NAT ゲートウェイを設定します。詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「NAT ゲートウェイ」を参照してください。
- タスクサブネットのルートテーブルには、NAT ゲートウェイへのトラフィック用のルートが必要です。

  詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「ルートテーブルのルートの追加と削除」を参照してください。

ゲートウェイタイプ	ルートテーブルの送信先	ルートテーブルのターゲット
NAT	0.0.0.0/0	NAT ゲートウェイ ID

- タスクサブネットにネットワーク ACL がある場合は、次の ACL ルールが必要です。
  - ポート 1024-65535 でトラフィックを許可するアウトバウンドルール
  - ポート 443 の TCP トラフィックを許可するインバウンドルール

ルールの設定方法については、「Amazon Virtual Private Cloud ユーザーガイド」の「network ACLs」を参照してください。

パブリックサブネットで awsvpc ネットワークモードを使用しないタスク

ランブックに基づいて次の設定を実行します。

- クラスターの作成時に、[Amazon EC2 インスタンスのネットワーク] の [IP の自動割り当て] で、[オンにする] を選択します。

  このオプションにより、インスタンスのプライマリネットワークインターフェイスにパブリック IP アドレスを割り当てます。
- インターネットトラフィックを処理するにはゲートウェイが必要です。インスタンスサブネットのルートテーブルには、ゲートウェイへのトラフィック用のルートが必要です。

  詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「ルートテーブルのルートの追加と削除」を参照してください。

ゲートウェイタイプ	ルートテーブルの送信先	ルートテーブルのターゲット
NAT	0.0.0.0/0	NAT ゲートウェイ ID
インターネットゲートウェイ	0.0.0.0/0	インターネットゲートウェイ ID

- インスタンスサブネットにネットワーク ACL がある場合は、次の ACL ルールが必要です。
  - ポート 1024-65535 でトラフィックを許可するアウトバウンドルール
  - ポート 443 の TCP トラフィックを許可するインバウンドルール

  ルールの設定方法については、「Amazon Virtual Private Cloud ユーザーガイド」の「network ACLs」を参照してください。

プライベートサブネットで awsvpc ネットワークモードを使用しないタスク

ランブックに基づいて次の設定を実行します。

- クラスターの作成時に、[Amazon EC2 インスタンスのネットワーク] の [IP の自動割り当て] で、[オフにする] を選択します。

- リクエストがインターネットにルーティングされるように VPC の NAT ゲートウェイを設定します。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。
- インスタンスサブネットのルートテーブルには、NAT ゲートウェイへのトラフィック用のルートが必要です。

  詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「ルートテーブルのルートの追加と削除」を参照してください。

ゲートウェイタイプ	ルートテーブルの送信先	ルートテーブルのターゲット
NAT	0.0.0.0/0	NAT ゲートウェイ ID

- タスクサブネットにネットワーク ACL がある場合は、次の ACL ルールが必要です。
  - ポート 1024-65535 でトラフィックを許可するアウトバウンドルール
  - ポート 443 の TCP トラフィックを許可するインバウンドルール

  ルールの設定方法については、「Amazon Virtual Private Cloud ユーザーガイド」の「network ACLs」を参照してください。

Amazon ECS タスクの IAM ロールリクエストの表示

IAM ロールでタスク認証情報にプロバイダーを使用すると、プロバイダーは監査ログに保存されたものをリクエストします。監査ログは、コンテナエージェントログと同じログローテーション設定を継承します。コンテナエージェントの設定変数 `ECS_LOG_ROLLOVER_TYPE`、`ECS_LOG_MAX_FILE_SIZE_MB`、および `ECS_LOG_MAX_ROLL_COUNT` を設定して、監査ログの動作に影響を与えることもできます。詳細については、「Amazon ECS コンテナエージェントのログ設定パラメータ」を参照してください。

コンテナエージェントバージョン 1.36.0 以降の場合、監査ログは `/var/log/ecs/audit.log` にあります。ログがローテーションされると、*YYYY*-*MM*-*DD*-*HH* 形式のタイムスタンプがログファイル名の最後に追加されます。

コンテナエージェントバージョン 1.35.0 以前の場合、監査ログは `/var/log/ecs/audit.log.`*YYYY*-*MM*-*DD*-*HH* にあります。

ログエントリの形式は以下のとおりです。

- Timestamp

- HTTP レスポンスコード
- リクエスト元の IP アドレスとポート番号
- 認証情報プロバイダーの相対 URI
- リクエストを行ったユーザーエージェント
- リクエスト元のコンテナが属するタスクの ARN
- `GetCredentials` API 名とバージョン番号
- コンテナインスタンスが登録されている Amazon ECS クラスターの名前
- コンテナインスタンス ARN

ログファイルを表示するには、次のコマンドが使用できます。

```
cat /var/log/ecs/audit.log.2016-07-13-16
```

出力:

```
2016-07-13T16:11:53Z 200 172.17.0.5:52444 "/v1/credentials" "python-requests/2.7.0
 CPython/2.7.6 Linux/4.4.14-24.50.amzn1.x86_64" TASK_ARN GetCredentials
 1 CLUSTER_NAME CONTAINER_INSTANCE_ARN
```

Amazon ECS のサービスイベントメッセージを表示する

サービスの問題をトラブルシューティングする際、最初に診断情報を確認する必要があるのは、サービスイベントログです。サービスイベントは、`DescribeServices` API、AWS CLI、または AWS Management Console を使って表示できます。

Amazon ECS API を使用して、サービスイベントメッセージを表示する場合、サービススケジューラからのイベントのみが返されます。これには、最新のタスク配置とインスタンスの健全性イベントが含まれます。ただし、Amazon ECS コンソールには、次のソースからのサービスイベントが表示されます。

- Amazon ECS サービススケジューラからのタスク配置およびインスタンスのヘルスイベント。これらのイベントには、service ***(service-name)*** のプレフィックスがついています。このイベントビューが役立つ情報を提供するために、最新の 100 件のイベントのみを表示します。重複したサービスイベントメッセージは、原因が解決するか、6 時間が経過するまで表示されません。6 時間以内に原因が解決されない場合、その原因に関する別のサービスイベントメッセージが表示されます。

- サービスの自動スケーリングイベント。これらのイベントにはMessageというプレフィックスが付き、サービスが Application Auto Scaling スケーリングポリシーで構成されている場合にのみ発生します。

現在のサービスイベントメッセージを表示するには、次の手順を実行します。

Console

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで [Clusters] (クラスター) を選択します。
3. [Clusters] (クラスター) ページで、クラスターを選択します。
4. 検査するサービスを選択します。
5. [Events] (イベント) で [Deployments and events] (デプロイとイベント) を選択し、メッセージを表示します。

AWS CLI

指定したサービスのサービスイベントメッセージを表示するには、describe-service コマンドを使用します。

次の AWS CLI 例では、*default* クラスター内の *service-name* サービスが記述されます。ここには、最新のサービスイベントメッセージが表示されます。

```
aws ecs describe-services \
    --cluster default \
    --services service-name \
    --region us-west-2
```

Amazon ECS のサービスイベントメッセージ

以下は、Amazon ECS コンソールで確認できる可能性があるサービスイベントメッセージの例です。

サービス (*service-name*) が定常状態に達しました。

サービススケジューラは、サービスが正常で、必要な数のタスクが定常状態になったときに、service (*service-name*) has reached a steady state. サービスイベントを送信します。

サービススケジューラは定期的にステータスを報告するため、このメッセージを複数回受信する場合があります。

サービス (*service-name*) で、すべての要件を満たしたコンテナインスタンスがないため、タスクを配置できませんでした。

サービススケジューラは、別のタスクを追加するために利用可能なリソースが見つからなかったときに、このイベントメッセージを送信します。以下に示しているのは、その考えられる原因です。

クラスターにコンテナインスタンスが見つかなかった

タスクを実行しようとしているクラスターにコンテナインスタンスが登録されていない場合は、このエラーが返されます。コンテナインスタンスをクラスターに追加する必要があります。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

ポートが足りない

タスクで固定ホストポートマッピングを使用している場合 (タスクでウェブサーバーのホスト上のポート 80 を使用している場合など)、1 つのコンテナが一度に使用できるホストポートは 1 つのみであるため、タスクごとに 1 つ以上のコンテナインスタンスが必要です。コンテナインスタンスをクラスターに追加するか、タスクの必要数を減らす必要があります。

登録されたポートが多すぎる

タスク配置に最も近いコンテナインスタンスは、コンテナインスタンスごとに許可される最大予約ホストポート数である 100 を超えることはできません。ホストポートの動的マッピングを使用すると、問題を解決できる場合があります。

ポートは既に使用中です

このタスクのタスク定義は、選択されたコンテナインスタンスで既に実行されているタスクと同じポートをポートマッピングで使用します。サービスイベントメッセージは、以下のメッセージの一部としてコンテナインスタンス ID を本来選択していました。

```
The closest matching container-instance is already using a port required by your
 task.
```

メモリが足りない

タスク定義で 1,000 MiB のメモリを指定しており、クラスター内の各コンテナインスタンスのメモリが 1,024 MiB の場合、コンテナインスタンスごとにこのタスクのコピーを 1 つのみ実行できます。タスク定義でメモリを減らしてコンテナインスタンスごとに複数のタスクを起動できるようにするか、クラスターで起動するコンテナインスタンスを増やすことができます。

> **Note**
>
> リソースの使用率を最大化することを目的に、特定のインスタンスタイプにおいて、タスクにできるだけ多くのメモリを提供する場合には、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

CPU が足りない

コンテナインスタンスには、CPU コアごとに 1,024 個の CPU ユニットがあります。タスク定義で 1,000 個の CPU ユニットを指定しており、クラスター内の各コンテナインスタンスの CPU ユニットが 1,024 個である場合、コンテナインスタンスごとにこのタスクのコピーを 1 つのみ実行できます。タスク定義で CPU ユニット数を減らしてコンテナインスタンスごとに複数のタスクを起動できるようにするか、クラスターで起動するコンテナインスタンスを増やすことができます。

十分な数の ENI アタッチメントポイントを利用できない

`awsvpc` ネットワークモードを使用するタスクには、それぞれ独自の Elastic Network Interface (ENI) が提供されます。この ENI は、ENI をホストするコンテナインスタンスに添付されています。Amazon EC2 インスタンスは添付できる ENI の数には制限があり、クラスター内に利用可能なENI 容量があるコンテナインスタンスはありません。

個別のコンテナインスタンスの ENI 制限は、以下の条件によって異なります。

- `awsvpcTrunking` アカウント設定をオプトインしていない場合、各コンテナインスタンスの ENI 制限は、インスタンスタイプによって異なります。詳細については、Amazon EC2 ユーザーガイドの「各インスタンスタイプのネットワークインターフェイスあたりの IP アドレス」を参照してください。
- `awsvpcTrunking` アカウント設定をオプトインしているが、オプトイン後にサポートされているインスタンスタイプを使用して新しいコンテナインスタンスを起動していない場合、各コンテナインスタンスの ENI 制限はデフォルト値のままです。詳細については、Amazon EC2

ユーザーガイドの「各インスタンスタイプのネットワークインターフェイスあたりの IP アドレス」を参照してください。

- awsvpcTrunking アカウント設定をオプトインしていて、かつオプトイン後にサポートされているインスタンスタイプを使用して新しいコンテナインスタンスを起動している場合、追加の ENI オプトインを利用できます。詳細については、「Amazon ECS コンテナネットワークインターフェイスの増加でサポートされるインスタンス」を参照してください。

awsvpcTrunking アカウント設定のオプトインの詳細については、「Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす」を参照してください。

クラスターにコンテナインスタンスを追加することで、利用できるネットワークアダプタの数を増やすことができます。

コンテナインスタンスに必須の属性がない

一部のタスク定義パラメータでは、特定バージョンの Docker リモート API をコンテナインスタンスにインストールする必要があります。ロギングドライバーオプションなどのその他のパラメータでは、コンテナインスタンスに ECS_AVAILABLE_LOGGING_DRIVERS エージェント設定変数を使用して、それらのロギングドライバーを登録する必要があります。タスク定義に特定のコンテナインスタンス属性を必要とするパラメータが含まれており、この要件を満たすことができるコンテナインスタンスがない場合、そのタスクは配置できません。

このエラーの一般的な原因は、サービスが awsvpc ネットワークおよび EC2 起動タイプを使用している場合です。指定したクラスターには、サービスの作成時に awsvpcConfiguration で指定されたものと同じサブネットにコンテナインスタンスが登録されていません。

トラブルシューティングには、AWSSupport-TroubleshootECSContainerInstance ランブックを使用できます。ランブックでは、インスタンスのユーザーデータに正しいクラスター情報が含まれているかどうか、インスタンスプロファイルに必要なアクセス権限が含まれているかどうか、およびネットワーク設定の問題が確認されます。詳細については、「AWS Systems Manager オートメーションランブックリファレンスユーザーガイド」の「AWSSupport-TroubleshootECSContainerInstance」を参照してください。

特定のタスク定義パラメータとエージェント設定変数に必要な属性の詳細については、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」と「Amazon ECS コンテナエージェントの設定」を参照してください。

サービス (*service-name*) で、すべての要件を満たしたコンテナインスタンスがないため、タスクを配置できませんでした。container-instance-id に最も近い *container-instance-id* には、使用可能な CPU ユニットがありません。

タスク配置に最も一致するコンテナインスタンスに、タスク定義の要件を満たす十分な CPU ユニットがありません。タスク定義のタスクサイズとコンテナ定義の両方のパラメータで、CPU の要件を確認します。

サービス (*service-name*) で、すべての要件を満たしたコンテナインスタンスがないため、タスクを配置できませんでした。container-instance-id に最も近い *container-instance-id* で、エラー「AGENT」が発生しました。

タスク配置に最も一致するコンテナインスタンス上の Amazon ECS コンテナエージェントが切断されています。コンテナインスタンスに SSH で接続できる場合は、エージェントログを調べることができます。詳細については、「Amazon ECS コンテナエージェントのログ設定パラメータ」を参照してください。エージェントがインスタンスで実行されていることも確認する必要があります。Amazon ECS に最適化された AMI を使用している場合、次のコマンドでエージェントを停止して再開始する試みができます。

- Amazon ECS に最適化された Amazon Linux 2 AMI および Amazon ECS に最適化された Amazon Linux 2023 AMI の場合

```
sudo systemctl restart ecs
```

- Amazon ECS に最適化された Amazon Linux AMI の場合:

```
sudo stop ecs && sudo start ecs
```

サービス (*service-name*) (instance *instance-id*) は、 (理由 インスタンスが、少なくとも UnhealthyThreshold 回のヘルスチェックに連続して失敗した。) のため、(elb *elb-name*) で正常ではありません

このサービスはロードバランサーに登録されており、ロードバランサーのヘルスチェックは失敗しています。詳細については、「Amazon ECS のサービスロードバランサーのトラブルシューティング」を参照してください。

サービス (*service-name*) は、一貫してタスクを正常に開始できません。

このサービスには、連続して試行された後開始に失敗したタスクがあります。この時点で、サービススケジューラによって再試行間隔が段階的に増加し始めます。タスクの起動に失敗している理由をトラブルシューティングする必要があります。詳細については、「Amazon ECS サービスのスロットルロジック」を参照してください。

更新されたタスク定義などでサービスが更新された後、サービススケジューラは正常な動作を再開します。

サービス (*service-name*) オペレーションは抑制されています。後で再試行します。

このサービスは、API スロットルの制限により、これ以上のタスクを起動できません。サービススケジューラが追加のタスクを起動できるようになると、再開します。

API レート制限クォータの引き上げをリクエストするには、[AWS サポート Center (センター)] の ページを開き、必要に応じてサインインし、[Create case (ケースを作成する)] を選択します。[Service Limit increase] (サービス制限の緩和) を選択します。フォームに入力して送信します。

サービス (*service-name*) は、サービスデプロイメント構成のため、デプロイメント中にタスクを停止または開始できませんでした。minimumHealthyPercent または maximumPercent の値を更新してから、もう一度試してください。

このサービスは、デプロイメント構成であるため、サービスのデプロイメント中にタスクを停止または開始できません。デプロイ設定は、サービスの作成時に定義される `minimumHealthyPercent` 値と `maximumPercent` 値で構成されます。これらの値は既存のサービスでも更新できます。

`minimumHealthyPercent` は、デプロイ中またはコンテナインスタンスがドレインしているときに、サービスに対して実行する必要があるタスク数の下限を表します。これは、サービスに必要なタスク数に対するパーセンテージです。この値は切り上げられます。例えば、最小正常率が `50` で、必要なタスク数が 4 の場合、スケジューラは 2 つの新しいタスクを開始する前に既存のタスクを 2 つ停止できます。同様に、最小正常率が 75% で、必要なタスク数が 2 の場合、結果の値も 2 であるため、スケジューラはタスクを停止できません。

`maximumPercent` は、デプロイ中またはコンテナインスタンスがドレインしているときに、サービスに対して実行する必要があるタスク数の上限を表します。これは、サービスに必要なタスク数に対するパーセンテージです。この値は切り捨てられます。例えば、最大パーセンテージが `200` で、目的のタスク数が 4 の場合、スケジューラは既存のタスクを 4 つ停止する前に 4 つの新しいタスクを開始できます。同様に、最大比率が `125` で、必要なタスク数が 3 の場合、結果の値も 3 であるため、スケジューラはタスクを開始できません。

最小正常率または最大正常率を設定するときは、デプロイメントがトリガーされたときにスケジューラが 1 つ以上のタスクを停止または開始できることを確認する必要があります。

サービス [*service-name(####-#)*] がタスクを配置できませんでした。理由: 同時に実行できるタスク数の上限に達しました

エラーの原因となったリソースに対して、クォータの引き上げをリクエストすることができます。詳細については、「Service Quotas」を参照してください。クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

サービス [*service-name(####-#)*] がタスクを配置できませんでした。理由: 内部エラー。

このエラーが表示される理由として考えられるものは、次のとおりです。

あるサブネットがサポートされていないアベイラビリティーゾーンにあるため、サービスはタスクを開始できません。

サポートされた Fargate リージョンおよびアベイラビリティーゾーンの情報については、the section called “AWS Fargate リージョン” を参照してください。

サブネットのアベイラビリティーゾーンを確認する方法については、「Amazon VPC ユーザーガイド」の「サブネットの確認」を参照してください。

サービス [*service-name(####-#)*] がタスクを配置できませんでした。理由:リクエストされた CPU 構成が制限を超えています。

エラーの原因となったリソースに対して、クォータの引き上げをリクエストすることができます。詳細については、「Service Quotas」を参照してください。クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

サービス [*service-name(####-#)*] がタスクを配置できませんでした。理由:リクエストされたメモリ構成が制限を超えています。

エラーの原因となったリソースに対して、クォータの引き上げをリクエストすることができます。詳細については、「Service Quotas」を参照してください。クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「クォータ引き上げリクエスト」を参照してください。

サービス [*service-name(####-#)*] がタスクを配置できませんでした。理由: 同時に実行できる vCPU の上限数に達しました

AWS Fargate は、タスク数ベースのクォータから vCPU ベースのクォータに移行しています。

Fargate の vCPU ベースの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」を参照してください。Fargate クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「Requesting a quota increase」(クォータ引き上げリクエスト) を参照してください。

タスクセット (*taskSet-ID*) がスケールインできなかったため、サービス (*service-name*) は定常状態に到達できませんでした。理由: 保護されているタスクの数が、必要なタスク数を超えています

サービスに、必要なタスク数よりも多くの保護タスクがあります。次のいずれかを行うことができます。

- 現在のタスクの保護が期限切れになり、タスクを終了できるようになるまでお待ちください。
- どのタスクを停止できるかを判断し、UpdateTaskProtection API で protectionEnabled オプションを false に設定し、これらのタスクに対する保護を設定解除します。
- サービスの必要なタスク数を増やして、保護されているタスクの数よりも多くします。

サービス (*service-name*) が定常状態に到達できませんでした。理由:キャパシティープロバイダーにコンテナインスタンスが見つかりませんでした。

サービススケジューラは、別のタスクを追加するために利用可能なリソースが見つからなかったときに、このイベントメッセージを送信します。以下に示しているのは、その考えられる原因です。

クラスターに関連付けられたキャパシティプロバイダーがありません

クラスターにキャパシティプロバイダーが関連付けられていることを確認するには、describe-services を使用します。サービスのキャパシティプロバイダー戦略を更新できます。

キャパシティプロバイダーに利用可能なキャパシティがあることを確認します。EC2 起動タイプの場合は、コンテナインスタンスがタスク定義の要件を満たしていることを確認してください。

クラスターにコンテナインスタンスが見つかなかった

タスクを実行しようとしているクラスターにコンテナインスタンスが登録されていない場合は、このエラーが返されます。コンテナインスタンスをクラスターに追加する必要があります。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。

ポートが足りない

タスクで固定ホストポートマッピングを使用している場合 (タスクでウェブサーバーのホスト上のポート 80 を使用している場合など)、タスクごとに 1 つ以上のコンテナインスタンスが必要です。一度に 1 つのホストポートを使用できるコンテナは 1 つだけです。コンテナインスタンスをクラスターに追加するか、タスクの必要数を減らす必要があります。

登録されたポートが多すぎる

タスク配置に最も近いコンテナインスタンスは、コンテナインスタンスごとに許可される最大予約ホストポート数である 100 を超えることはできません。ホストポートの動的マッピングを使用すると、問題を解決できる場合があります。

ポートは既に使用中です

このタスクのタスク定義は、選択されたコンテナインスタンスで既に実行されているタスクと同じポートをポートマッピングで使用します。サービスイベントメッセージは、以下のメッセージの一部としてコンテナインスタンス ID を本来選択していました。

```
The closest matching container-instance is already using a port required by your
 task.
```

メモリが足りない

タスク定義で 1,000 MiB のメモリを指定しており、クラスター内の各コンテナインスタンスのメモリが 1,024 MiB の場合、コンテナインスタンスごとにこのタスクのコピーを 1 つのみ実行できます。タスク定義でメモリを減らしてコンテナインスタンスごとに複数のタスクを起動できるようにするか、クラスターで起動するコンテナインスタンスを増やすことができます。

> **Note**
>
> 特定のインスタンスタイプでタスクにできるだけ多くのメモリを提供してリソースの使用率を最大限に高めるには、「Amazon ECS Linux コンテナインスタンスのメモリを予約する」を参照してください。

十分な数の ENI アタッチメントポイントを利用できない

awsvpc ネットワークモードを使用するタスクには、それぞれ独自の Elastic Network Interface (ENI) が提供されます。この ENI は、ENI をホストするコンテナインスタンスに添付されています。Amazon EC2 インスタンスにアタッチできる ENI の数には制限があり、クラスターには利用可能な ENI 容量があるコンテナインスタンスはありません。

個別のコンテナインスタンスの ENI 制限は、以下の条件によって異なります。

- awsvpcTrunking アカウント設定をオプトインしていない場合、各コンテナインスタンスの ENI 制限は、インスタンスタイプによって異なります。詳細については、Amazon EC2 ユーザーガイドの「各インスタンスタイプのネットワークインターフェイスあたりの IP アドレス」を参照してください。
- awsvpcTrunking アカウント設定をオプトインしているが、オプトイン後にサポートされているインスタンスタイプを使用して新しいコンテナインスタンスを起動していない場合、各コンテナインスタンスの ENI 制限はデフォルト値のままです。詳細については、Amazon EC2 ユーザーガイドの「各インスタンスタイプのネットワークインターフェイスあたりの IP アドレス」を参照してください。
- awsvpcTrunking アカウント設定をオプトインしていて、かつオプトイン後にサポートされているインスタンスタイプを使用して新しいコンテナインスタンスを起動している場合、追加の ENI オプトインを利用できます。詳細については、「Amazon ECS コンテナネットワークインターフェイスの増加でサポートされるインスタンス」を参照してください。

awsvpcTrunking アカウント設定のオプトインの詳細については、「Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす」を参照してください。

クラスターにコンテナインスタンスを追加することで、利用できるネットワークアダプタの数を増やすことができます。

コンテナインスタンスに必須の属性がない

一部のタスク定義パラメータでは、特定バージョンの Docker リモート API をコンテナインスタンスにインストールする必要があります。ロギングドライバーオプションなどのその他のパラメータでは、コンテナインスタンスに ECS_AVAILABLE_LOGGING_DRIVERS エージェント設定変数を使用して、それらのロギングドライバーを登録する必要があります。タスク定義に特定のコンテナインスタンス属性を必要とするパラメータが含まれており、この要件を満たすことができるコンテナインスタンスがない場合、そのタスクは配置できません。

このエラーの一般的な原因は、サービスが awsvpc ネットワークモードを使用するタスクを使用していて、EC2 起動タイプと指定したクラスターに、サービスの作成時に

awsvpcConfiguration で指定された同じサブネットにコンテナインスタンスが登録されていない場合です。

トラブルシューティングには、AWSSupport-TroubleshootECSContainerInstance ランブックを使用できます。ランブックでは、インスタンスのユーザーデータに正しいクラスター情報が含まれているかどうか、インスタンスプロファイルに必要なアクセス権限が含まれているかどうか、およびネットワーク設定の問題が確認されます。詳細については、「AWS Systems Manager オートメーションランブックリファレンスユーザーガイド」の「AWSSupport-TroubleshootECSContainerInstance」を参照してください。

特定のタスク定義パラメータとエージェント設定変数に必要な属性の詳細については、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」と「Amazon ECS コンテナエージェントの設定」を参照してください。

サービス [*service-name(####-#)*] がタスクを配置できませんでした。理由: 現在、容量は使用できません。後でもう一度試すか、別のアベイラビリティーゾーンで試してください。

現在、サービスを実行できる容量がありません。

次のいずれかを行うことができます。

- Fargate 容量または EC2 コンテナインスタンスが使用可能になるまでお待ちください。
- サービスを再起動し、追加のサブネットを指定します。

サービス (*service-name*) のデプロイに失敗しました:タスクを開始できませんでした。

サービスのタスクが開始できませんでした。

停止タスクをデバッグする方法については、「Amazon ECS の停止したタスクのエラーメッセージ」を参照してください。

サービス (*service-name*) が、Amazon ECS エージェントの開始を待ってタイムアウトになりました。/var/log/ecs/ecs-agent.log でログを確認してください。"

タスク配置に最も一致するコンテナインスタンス上の Amazon ECS コンテナエージェントが切断されています。コンテナインスタンスに SSH で接続できる場合は、エージェントログを調べるこ

とができます。詳細については、「Amazon ECS コンテナエージェントの設定パラメータ」を参照してください。エージェントがインスタンスで実行されていることも確認する必要があります。Amazon ECS に最適化された AMI を使用している場合、次のコマンドでエージェントを停止して再開始する試みができます。

- Amazon ECS に最適化された Amazon Linux 2 AMI の場合

```
sudo systemctl restart ecs
```

- Amazon ECS に最適化された Amazon Linux AMI の場合:

```
sudo stop ecs && sudo start ecs
```

TARGET GROUP IS NOT FOUND が原因で、ターゲットグループ (***target-group-ARN***) 内のサービス (***service-name***) のタスクセット (***TaskSet-ID***) に異常があります。

ターゲットグループが見つからなかったため、サービスのタスクセットはヘルスチェックに合格できません。サービスを削除して再作成してください。対応する Amazon ECS サービスが既に削除されていない限り、Elastic Load Balancing のターゲットグループを削除しないでください。

TARGET IS NOT FOUND が原因で、ターゲットグループ (***target-group-ARN***) 内のサービス (***service-name***) のタスクセット (***TaskSet-ID***) に異常があります。

ターゲットが見つからなかったため、サービスのタスクセットはヘルスチェックに合格できません。

Amazon ECS アベイラビリティーゾーンサービスの再調整サービスイベントメッセージ

以下は、表示される可能性があるサービスイベントメッセージの例です。

サービス (***service-name***) は、***Availability Zone 1*** の ***number-tasks*** タスク、***Availability Zone 2*** の ***number-tasks*** タスク、***Availability Zone 3*** の ***number-tasks*** タスクで AZ が調整されていません。AZ の再調整は進行中です。

サービススケジューラは、タスク数がアベイラビリティーゾーン間で均等に分散されていない場合、`service (service-name) is not AZ balanced` サービスイベントを送信します。実行するアクションはありません。これは情報イベントです。

サービス (*service-name*) は、*Availability Zone 1* の *number-tasks* タスク、*Availability Zone 2* の *number-tasks* タスク、*Availability Zone 3* の *number-tasks* タスクで AZ が調整されています。

サービススケジューラは、アベイラビリティーゾーンのサービスの再調整が完了すると、service (*service-name*) is AZ balanced サービスイベントを送信します。実行するアクションはありません。これは情報イベントです。

service-name は、AZ の再調整のために *Availability Zone* の *number-tasks* タスクを開始しました: *task-ids*。

サービススケジューラは、サービスの再調整のためにアベイラビリティーゾーンのタスクを開始したときに、*service-name*/*task-set-name* が *Availability Zone* の *number* タスクを開始したというサービスイベントを送信します。実行するアクションはありません。これは情報イベントです。

service-name は、AZ の再調整のために *Availability Zone* の実行中の *number-tasks* タスクを停止しました: *task-ids*。

サービススケジューラは、サービスの再調整のためにアベイラビリティーゾーンのタスクを停止したときに、*service-name*/*task-set-name* が *Availability Zone* の *number* タスクを開始したというサービスイベントを送信します。実行するアクションはありません。これは情報イベントです。

サービス (*service-name*) で、すべての要件を満たしたコンテナインスタンスがないため、*Availability Zone* にタスクを配置できません。

サービススケジューラは、すべての要件を満たしたコンテナインスタンスがないため、*service-name* で *Availability Zone* にタスクを配置できないというサービスイベントを送信します。問題に対処するには、アベイラビリティーゾーンでインスタンスを起動します。

サービス (*service-name*) で、*Availability Zone* にタスクを配置できません。

サービススケジューラは、Fargate 起動タイプを使用していて利用可能なキャパシティがないと、*service-name* で *Availability Zone* にタスクを配置できないというサービスイベントを送信します。

追加のキャパシティを取得するには、エラーメッセージでアベイラビリティーゾーンにサブネットを追加するか、サポートにお問い合わせください。

サービス (*service-name*) で、*task-set-name* が *reason* によりスケールインできなかったため、AZ を再調整できませんでした。

サービススケジューラは、タスクスケールイン保護を使用するときに、*task-set-name* が *reason* によりスケールインできなかったため、*service-name* で AZ を再調整できなかったというサービスイベントを送信します。

次のいずれかを行うことができます。

- 現在のタスクの保護が期限切れになり、タスクを終了できるようになるまでお待ちください。
- どのタスクを停止できるかを判断し、UpdateTaskProtection API で protectionEnabled オプションを false に設定し、これらのタスクに対する保護を設定解除します。
- サービスの必要なタスク数を増やして、保護されているタスクの数よりも多くします。

サービス (*service-name*) が AZ の再調整を停止しました。

サービススケジューラは、アベイラビリティーゾーンの再調整オペレーションが停止すると、*service-name* が AZ の再調整を停止したというサービスイベントを送信します。これは情報イベントです。Amazon ECS は、詳細情報を提供する追加のイベントを送信します。

Amazon ECS のサービスロードバランサーのトラブルシューティング

Amazon ECS サービスは、Elastic Load Balancing のロードバランサーにタスクを登録することができます。ロードバランサーの設定エラーは、タスクが停止された一般的な原因です。ロードバランサーを使用するサービスによって停止されたタスクが開始された場合は、以下の原因が考えられます。

Amazon ECS サービスにリンクされたロールは存在しません

Amazon ECS サービスにリンクされたロールを使用すると、Amazon ECS サービスが Elastic Load Balancing ロードバランサーにコンテナインスタンスを登録できます。サービスにリンクされたロールはアカウントに作成される必要があります。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。

コンテナインスタンスのセキュリティグループ

コンテナがコンテナインスタンスのポート 80 にマッピングされている場合、コンテナインスタンスのセキュリティグループでは、ロードバランサーのヘルスチェックに合格するように、ポート 80 上の受信トラフィックを許可する必要があります。

一部のアベイラビリティゾーンで、Elastic Load Balancing ロードバランサーが設定されていません

リージョン内のすべてのアベイラビリティーゾーンを使用するように、または少なくとも、コンテナインスタンスが存在するすべてのアベイラビリティーゾーンを使用するように、ロードバランサーが設定されている必要があります。サービスでロードバランサーを使用し、ロードバランサーを使用するように設定されていないアベイラビリティーゾーンにあるコンテナインスタンスでタスクが開始されると、そのタスクはヘルスチェックに合格できません。これにより、タスクは強制終了されます。

Elastic Load Balancing ロードバランサー ヘルスチェックが正しく設定されていません

ロードバランサーのヘルスチェックパラメータが過度に制限されているか、存在しないリソースを指している可能性があります。コンテナインスタンスが異常であると判断されると、そのコンテナインスタンスはロードバランサーから削除されます。以下のパラメータがサービスロードバランサーに対して正しく設定されていることを確認してください。

ping ポート

ロードバランサーのヘルスチェックの [Ping Port (ping ポート)] 値は、ロードバランサーが正常であるかどうかを判断するために確認するコンテナインスタンス上のポートです。このポートの設定が正しくないと、多くの場合、ロードバランサーからコンテナインスタンスが登録解除されます。このポートは、ヘルスチェックで使用しているサービスのタスク定義内のコンテナで `hostPort` 値を使用するように設定する必要があります。

ping パス

これはロードバランサーのヘルスチェックの一部です。これは、アプリケーションが正常な場合に、成功のステータスコード (200 など) を返すことができる、アプリケーション上のエンドポイントです。この値はよく `index.html` に設定されることがありますが、サービスがそのリクエストに応答しない場合、ヘルスチェックは失敗します。コンテナに `index.html` ファイルがない場合は、これを `/` に設定して、コンテナインスタンスのベース URL をターゲットにすることができます。

応答タイムアウト

これは、コンテナがヘルスチェック ping に対する応答を返す必要のある時間です。この値が応答に必要な時間よりも短い場合、ヘルスチェックは失敗します。

ヘルスチェック間隔

これは、ヘルスチェック ping 間の時間です。ヘルスチェックの間隔が短くなるほど、コンテナインスタンスが [Unhealthy Threshold (非正常のしきい値)] に達するのが速くなります。

非正常のしきい値

これは、コンテナインスタンスが異常と見なされるまでに、ヘルスチェックが失敗できる回数です。異常と見なされるまでのしきい値が 2、ヘルスチェックの間隔が 30 秒の場合、コンテナインスタンスが異常と見なされるまでに、タスクはヘルスチェック ping に 60 秒間応答します。異常と見なされるまでのしきい値を増やすか、ヘルスチェックの間隔を長くすると、タスクが ping に応答する時間が長くなります。

servicename サービスを更新できません: タスク定義でロードバランサーのコンテナ名またはポートが変更されました

サービスでロードバランサーを使用している場合は、AWS CLI または SDK を使用してロードバランサーの設定を変更できます。設定の変更方法の詳細については、「Amazon Elastic Containers サービス API リファレンス」の UpdateService を参照してください。サービスのタスク定義を更新する場合は、ロードバランサー設定で指定されたコンテナ名とコンテナポートはタスク定義のままにしておく必要があります。

同時に実行できるタスク数の上限に達しました。

新しいアカウントの場合、クォータがサービスクォータよりも低くなることがあります。Service Quotas コンソールでは、アカウントのサービスクォータを表示できます。クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。

Amazon ECS のサービス自動スケーリングのトラブルシューティング

Amazon ECS デプロイの進行中、Application Auto Scaling はスケールインプロセスをオフにします。このプロセスは、デプロイの完了後に再開されます。ただし、スケールアウトプロセスは、中断しない限り、デプロイ中に引き続き発生します。詳細については、「Application Auto Scaling のスケーリングの中断と再開」を参照してください。

Amazon ECS タスク定義の無効な CPU またはメモリエラーをトラブルシューティングする

Amazon ECS API または AWS CLI を使用してタスク定義を登録する場合、無効なcpuまたはmemory値を指定すると、以下のエラーが返されます。

```
An error occurred (ClientException) when calling the RegisterTaskDefinition operation:
 Invalid 'cpu' setting for task.
```

> **Note**
>
> Terraform の使用時に、以下のエラーが返される可能性があります。
>
> ```
> Error: ClientException: No Fargate configuration exists for given values.
> ```

この問題を解決するには、タスク定義でタスクの CPU とメモリにサポートされている値を指定する必要があります。cpu 値はタスク定義で、CPU ユニットまたは vCPU で表すことができます。タスク定義が登録されると、CPU ユニットを示す整数に変換されます。memory 値はタスク定義で、MiB または GB で表すことができます。タスク定義が登録されると、MiB を示す整数に変換されます。

requiresCompatibilities パラメータに FARGATE を指定しているタスク定義については (EC2 も指定されている場合も)、次の表のいずれかの値を使用する必要があります。これらの値によって、CPU とメモリのパラメータでサポートされる値の範囲が決まります。

Fargate でホストされるタスクの場合、次の表に有効な CPU とメモリの組み合わせを示します。JSON ファイルのメモリ値は MiB 単位で指定されます。この値に 1024 を掛けると、GB 値を MiB に変換できます。例えば、1 GB = 1024 MiB です。

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
256 (.25 vCPU)	512 MiB、1 GB、2 GB	リナックス
512 (.5 vCPU)	1 GB、2 GB、3 GB、4 GB	リナックス
1,024 (1 vCPU)	2 GB、3 GB、4 GB、5 GB、6 GB、7 GB、8 GB	Linux、Windows

CPU の値	メモリの値	AWS Fargate でサポートされるオペレーティングシステム
2,048 (2 vCPU)	4 GB ～ 16 GB (1 GB のインクリメント)	Linux、Windows
4,096 (4 vCPU)	8 GB ～ 30 GB (1 GB のインクリメント)	Linux、Windows
8192 (8 vCPU) **Note** このオプションには Linux プラットフォーム 1.4.0 以降が必要です。	16 GB ~ 60 GB (4 GB のインクリメント)	リナックス
16384 (16vCPU) **Note** このオプションには Linux プラットフォーム 1.4.0 以降が必要です。	32 GB ~ 120 GB (8 GB のインクリメント)	リナックス

Amazon EC2 でホストされているタスクでサポートされるタスク CPU の値は、0.25 vCPU ～ 192 vCPU です。

Amazon ECS は、CPU 期間と CPU クォータを使用して、タスクサイズの CPU ハード制限を制御します。タスク定義で vCPU を指定すると、Amazon ECS は `cgroup` に適用される CPU 期間と CPU クォータの設定に値を変換します。

CPU クォータは、特定の CPU 期間中に `cgroup` に付与される CPU 時間を制御します。どちらの設定も、マイクロ秒単位で表されます。CPU クォータが CPU 期間と等しい場合、`cgroup` は 1 つの vCPU で最大 100% (または複数の vCPU の場合は合計で 100% になる割合) まで実行できま

す。CPU クォータは最大 1,000,000 マイクロ秒で、CPU 期間は最小 1 ミリ秒です。これらの値を使用して CPU 数の制限を設定できます。CPU クォータを変更せずに CPU 期間を変更する場合、有効になる制限はタスク定義で指定した制限とは異なります。

100 ミリ秒の期間では、0.125 ~ 10 の vCPU を使用できます。

> **Note**
>
> タスクレベル CPU およびメモリのパラメータは Windows コンテナでは無視されます。

Amazon ECS コンテナエージェントログの表示

Amazon ECS によってログはコンテナインスタンスの `/var/log/ecs` フォルダに保存されます。Amazon ECS コンテナエージェントから得られるログと、コンテナインスタンスのエージェントの状態 (スタート/停止) を制御する `ecs-init` サービスから得られるログがあります。これらのログファイルは、コンテナインスタンスに SSH で接続することにより表示できます。

> **Note**
>
> コンテナインスタンスのログをすべて収集する方法がわからない場合は、Amazon ECS ログコレクターを使用できます。詳細については、「Amazon ECS ログコレクターを使用したコンテナログの収集」を参照してください。

Linux オペレーティングシステム

`ecs-init` プロセスはログを `/var/log/ecs/ecs-init.log` に保存します。

`ecs-init.log` ファイルには、コンテナエージェントのライフサイクル管理、設定、ブートストラップに関する情報が含まれています。

ログファイルを表示するには、次のコマンドが使用できます。

```
cat /var/log/ecs/ecs-init.log
```

出力:

```
2018-02-16T18:13:54Z [INFO] pre-start
2018-02-16T18:13:56Z [INFO] start
```

```
2018-02-16T18:13:56Z [INFO] No existing agent container to remove.
2018-02-16T18:13:56Z [INFO] Starting Amazon Elastic Container Service Agent
```

Windows オペレーティングシステム

Windows 用の Amazon ECS ログコレクターを使用できます。詳細については、Github の「Amazon ECS Logs Collector For Windows」を参照してください。

1. インスタンスに接続します。
2. PowerShell を開き、管理者権限で次のコマンドを実行します。このコマンドは、スクリプトをダウンロードし、ログを収集します。

   ```
   Invoke-WebRequest -OutFile ecs-logs-collector.ps1 https://
   raw.githubusercontent.com/awslabs/aws-ecs-logs-collector-for-windows/master/ecs-
   logs-collector.ps1
   .\ecs-logs-collector.ps1
   ```

Amazon ECS エージェントおよび Docker デーモンのデバッグログを有効にできます。このオプションを使用すると、スクリプトはデバッグモードを有効にする前にログを収集できます。スクリプトは Docker デーモンと Amazon ECS エージェントを再起動し、インスタンスで実行されているすべてのコンテナを終了します。次のコマンドを実行する前に、コンテナインスタンスをドレインし、重要なタスクを他のコンテナインスタンスに移動します。

次のコマンドを実行して、ログ記録をオンにします。

```
.\ecs-logs-collector.ps1 -RunMode debug
```

Amazon ECS ログコレクターを使用したコンテナログの収集

コンテナインスタンスのさまざまなログをすべて収集する方法がわからない場合は、Amazon ECS ログコレクターを使用できます。Linux 用と Windows 用のいずれも GitHub で入手できます。スクリプトは一般的なオペレーティングシステムログおよび Docker と Amazon ECS コンテナエージェントログを収集します。これらは、AWS サポート ケースのトラブルシューティングに役立ちます。次に、収集された情報が、診断目的で簡単に共有することができる 1 つのファイルに圧縮およびアーカイブされます。また、Docker デーモン、および Amazon Linux バリアントで Amazon ECS コンテナエージェント (Amazon ECS 最適化 AMI など) に対してデバッグモードを有効にすることもできます。現在、Amazon ECS ログコレクターでは以下のオペレーティングシステムがサポートしています:

- Amazon Linux
- Red Hat Enterprise Linux 7
- Debian 8
- Ubuntu 14.04
- Ubuntu 16.04
- Ubuntu 18.04
- Windows Server 2016

> **Note**
>
> Amazon ECS ログコレクターのソースコードは、Linux 用と Windows 用の両方を GitHub で入手できます。含めることを希望する変更について、プルリクエストを送信することをお勧めします。ただし、現在、Amazon Web Service では、このソフトウェアの変更されたコピーの実行をサポートしていません。

LinuxにAmazon ECS ログコレクターをダウンロードして実行するには

1. コンテナインスタンスに接続します。
2. Amazon ECS ログ コレクタースクリプトをダウンロードします。

```
curl -O https://raw.githubusercontent.com/awslabs/ecs-logs-collector/master/ecs-logs-collector.sh
```

3. スクリプトを実行してログを収集し、アーカイブを作成します。

> **Note**
>
> Docker デーモンと Amazon ECS コンテナエージェントに対してデバッグモードを有効にするには、次のコマンドに `--mode=enable-debug` オプションを追加します。これにより、Docker デーモンが再起動され、インスタンスで実行されているすべてのコンテナが強制終了されます。デバッグモードを有効にする前に、コンテナインスタンスをドレインし、重要なタスクを他のコンテナインスタンスに移動することを検討してください。詳細については、「Amazon ECS コンテナインスタンスをドレインする」を参照してください。

```
[ec2-user ~]$ sudo bash ./ecs-logs-collector.sh
```

> **Important**
>
> ログを編集し、ファイルからすべての機密データを削除することをお勧めします。既知のデータを検索でき、ファイル内の AWS_ACCESS_KEY_ID、AWS_SECRET_ACCESS_KEY、AWS_SESSION_TOKEN などの環境変数も検索できます。

スクリプトを実行した後、スクリプトによって作成された collect フォルダに収集されたログを調べることができます。collect.tgz ファイルはすべてのログの圧縮アーカイブであり、AWS サポートと共有することで診断に役立ちます。

WindowsでAmazon ECS ログコレクターをダウンロードして実行するには

1. コンテナインスタンスに接続します。詳細については、「Amazon EC2 ユーザーガイド」の「RDP を使用した Windows インスタンスへの接続」を参照してください。
2. PowerShell を使用して、Amazon ECSログコレクターのスクリプトをダウンロードします。

```
Invoke-WebRequest -OutFile ecs-logs-collector.ps1 https://
raw.githubusercontent.com/awslabs/aws-ecs-logs-collector-for-windows/master/ecs-
logs-collector.ps1
```

3. スクリプトを実行してログを収集し、アーカイブを作成します。

> **Note**
>
> Docker デーモンと Amazon ECS コンテナエージェントに対してデバッグモードを有効にするには、次のコマンドに -RunMode debug オプションを追加します。これにより、Docker デーモンが再起動され、インスタンスで実行されているすべてのコンテナが強制終了されます。デバッグモードを有効にする前に、コンテナインスタンスをドレインし、重要なタスクを他のコンテナインスタンスに移動することを検討してください。詳細については、「Amazon ECS コンテナインスタンスをドレインする」を参照してください。

```
.\ecs-logs-collector.ps1
```

> **Important**
>
> ログを編集し、ファイルからすべての機密データを削除することをお勧めします。既知のデータを検索でき、ファイル内の AWS_ACCESS_KEY_ID、AWS_SECRET_ACCESS_KEY、AWS_SESSION_TOKEN などの環境変数も検索できます。

スクリプトを実行した後、スクリプトによって作成された collect フォルダに収集されたログを調べることができます。collect.tgz ファイルはすべてのログの圧縮アーカイブであり、診断に役立つように AWS サポートと共有できます。

エージェントのイントロスペクションを使用して Amazon ECS 診断の詳細を取得する

Amazon ECS エージェントのイントロスペクション API は、Amazon ECS エージェントとコンテナインスタンスの全体的な状態に関する情報を提供します。

エージェントのイントロスペクション API を使用して、タスク内のコンテナの Docker ID を取得できます。コンテナインスタンスに SSH で接続することにより、エージェントイントロスペクション API を使用できます。

> **Important**
>
> イントロスペクション API に到達するには、コンテナインスタンスにAmazon ECS にアクセスできる IAM ロールが必要です。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

次の例では、2 つのタスクを示しています。1 つは現在実行中のタスク、もう 1 つは停止されたタスクです。

> **Note**
>
> 次のコマンドは、読みやすくするために python -mjson.tool によりパイプされています。

```
curl http://localhost:51678/v1/tasks | python -mjson.tool
```

出力:

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1095  100  1095    0     0   117k      0 --:--:-- --:--:-- --:--:--  133k
{
    "Tasks": [
        {
            "Arn": "arn:aws:ecs:us-west-2:aws_account_id:task/090eff9b-1ce3-4db6-848a-
a8d14064fd24",
            "Containers": [
                {
                    "DockerId":
 "189a8ff4b5f04affe40e5160a5ffadca395136eb5faf4950c57963c06f82c76d",
                    "DockerName": "ecs-console-sample-app-static-6-simple-
app-86caf9bcabe3e9c61600",
                    "Name": "simple-app"
                },
                {
                    "DockerId":
 "f7f1f8a7a245c5da83aa92729bd28c6bcb004d1f6a35409e4207e1d34030e966",
                    "DockerName": "ecs-console-sample-app-static-6-busybox-
ce83ce978a87a890ab01",
                    "Name": "busybox"
                }
            ],
            "Family": "console-sample-app-static",
            "KnownStatus": "STOPPED",
            "Version": "6"
        },
        {
            "Arn": "arn:aws:ecs:us-west-2:aws_account_id:task/1810e302-eaea-4da9-
a638-097bea534740",
            "Containers": [
                {
```

```
                    "DockerId":
 "dc7240fe892ab233dbbcee5044d95e1456c120dba9a6b56ec513da45c38e3aeb",
                    "DockerName": "ecs-console-sample-app-static-6-simple-app-
f0e5859699a7aecfb101",
                    "Name": "simple-app"
                },
                {
                    "DockerId":
 "096d685fb85a1ff3e021c8254672ab8497e3c13986b9cf005cbae9460b7b901e",
                    "DockerName": "ecs-console-sample-app-static-6-
busybox-92e4b8d0ecd0cce69a01",
                    "Name": "busybox"
                }
            ],
            "DesiredStatus": "RUNNING",
            "Family": "console-sample-app-static",
            "KnownStatus": "RUNNING",
            "Version": "6"
        }
    ]
}
```

上記の例では、停止されたタスク (*090eff9b-1ce3-4db6-848a-a8d14064fd24*) には 2 つのコンテナがあります。docker inspect ***container-ID*** を使用して、各コンテナの詳細情報を表示できます。詳細については、「Amazon ECS コンテナの詳細分析」を参照してください。

Amazon ECS の Docker 診断

Docker には、コンテナやタスクに関する問題のトラブルシューティングに役立つ診断ツールがいくつか用意されています。使用できるすべての Docker コマンドラインユーティリティの詳細については、Docker ドキュメントの Docker CLI リファレンスを参照してください。コンテナインスタンスに SSH で接続することにより、Docker コマンドラインユーティリティにアクセスできます。

Docker コンテナからレポートされる終了コードからも診断情報を得られます (例えば、終了コード 137 は、コンテナが SIGKILL 信号を受信したことを意味します)。詳細については、Docker ドキュメントの「終了ステータス」を参照してください。

Amazon ECS の Docker コンテナを一覧表示する

コンテナインスタンスの docker ps コマンドを使用して、実行中のコンテナを一覧表示できます。次の例では、Amazon ECS コンテナエージェントのみが実行されています。詳細については、Docker ドキュメントの「docker ps」を参照してください。

```
docker ps
```

出力:

```
CONTAINER ID        IMAGE                            COMMAND             CREATED
      STATUS              PORTS                          NAMES
cee0d6986de0        amazon/amazon-ecs-agent:latest   "/agent"            22 hours ago
      Up 22 hours         127.0.0.1:51678->51678/tcp   ecs-agent
```

docker ps -a コマンドを使用して、すべてのコンテナ (停止されたコンテナまたは強制終了されたコンテナも含む) を表示できます。この情報は、予期せず停止されたコンテナを一覧表示するために役立ちます。以下の例では、コンテナ f7f1f8a7a245 は 9 秒前に終了したため、-a フラグのない docker ps 出力には表示されません。

```
docker ps -a
```

出力:

```
CONTAINER ID        IMAGE                                              COMMAND
 CREATED             STATUS                          PORTS                         NAMES
db4d48e411b1        amazon/ecs-emptyvolume-base:autogenerated   "not-applicable"
  19 seconds ago                                                                    ecs-
console-sample-app-static-6-internalecs-emptyvolume-source-c09288a6b0cba8a53700
f7f1f8a7a245        busybox:buildroot-2014.02                   "\"sh -c '/bin/sh -c
  22 hours ago        Exited (137) 9 seconds ago                                    ecs-
console-sample-app-static-6-busybox-ce83ce978a87a890ab01
189a8ff4b5f0        httpd:2                                     "httpd-foreground"
  22 hours ago        Exited (137) 40 seconds ago                                   ecs-
console-sample-app-static-6-simple-app-86caf9bcabe3e9c61600
0c7dca9321e3        amazon/ecs-emptyvolume-base:autogenerated   "not-applicable"
  22 hours ago                                                                      ecs-
console-sample-app-static-6-internalecs-emptyvolume-source-90fefaa68498a8a80700
```

```
cee0d6986de0        amazon/amazon-ecs-agent:latest              "/agent"
  22 hours ago        Up 22 hours                    127.0.0.1:51678->51678/tcp   ecs-
agent
```

Amazon ECS で Docker ログを表示する

docker logs コマンドを使用して、コンテナの STDOUT および STDERR ストリームを表示できます。この例では、ログは *dc7240fe892a* コンテナのものが表示され、見やすくするために head コマンドによりパイプされています。詳細については、Docker ドキュメントの「Docker ログ」を参照してください。

> **Note**
>
> デフォルトの json ログドライバーを使用している場合、Docker ログはコンテナインスタンスのみで利用できます。awslogs ログドライバーを使用するようにタスクを設定している場合には、コンテナログは CloudWatch Logs で使用できます。詳細については、「Amazon ECS ログを CloudWatch に送信する 」を参照してください。

```
docker logs dc7240fe892a | head
```

出力:

```
AH00558: httpd: Could not reliably determine the server's fully qualified domain name,
 using 172.17.0.11. Set the 'ServerName' directive globally to suppress this message
AH00558: httpd: Could not reliably determine the server's fully qualified domain name,
 using 172.17.0.11. Set the 'ServerName' directive globally to suppress this message
[Thu Apr 23 19:48:36.956682 2015] [mpm_event:notice] [pid 1:tid 140327115417472]
 AH00489: Apache/2.4.12 (Unix) configured -- resuming normal operations
[Thu Apr 23 19:48:36.956827 2015] [core:notice] [pid 1:tid 140327115417472] AH00094:
 Command line: 'httpd -D FOREGROUND'
10.0.1.86 - - [23/Apr/2015:19:48:59 +0000] "GET / HTTP/1.1" 200 348
10.0.0.154 - - [23/Apr/2015:19:48:59 +0000] "GET / HTTP/1.1" 200 348
10.0.1.86 - - [23/Apr/2015:19:49:28 +0000] "GET / HTTP/1.1" 200 348
10.0.0.154 - - [23/Apr/2015:19:49:29 +0000] "GET / HTTP/1.1" 200 348
10.0.1.86 - - [23/Apr/2015:19:49:50 +0000] "-" 408 -
10.0.0.154 - - [23/Apr/2015:19:49:50 +0000] "-" 408 -
10.0.1.86 - - [23/Apr/2015:19:49:58 +0000] "GET / HTTP/1.1" 200 348
10.0.0.154 - - [23/Apr/2015:19:49:59 +0000] "GET / HTTP/1.1" 200 348
10.0.1.86 - - [23/Apr/2015:19:50:28 +0000] "GET / HTTP/1.1" 200 348
```

```
10.0.0.154 - - [23/Apr/2015:19:50:29 +0000] "GET / HTTP/1.1" 200 348
time="2015-04-23T20:11:20Z" level="fatal" msg="write /dev/stdout: broken pipe"
```

Amazon ECS で Docker コンテナを検査する

コンテナの Docker ID がある場合は、docker inspect コマンドを使用してコンテナを検査できます。コンテナを検査すると、コンテナが起動された環境の最も詳細なビューを得られます。詳細については、Docker ドキュメントの「Docker の検査」を参照してください。

```
docker inspect dc7240fe892a
```

出力:

```
[{
    "AppArmorProfile": "",
    "Args": [],
    "Config": {
        "AttachStderr": false,
        "AttachStdin": false,
        "AttachStdout": false,
        "Cmd": [
            "httpd-foreground"
        ],
        "CpuShares": 10,
        "Cpuset": "",
        "Domainname": "",
        "Entrypoint": null,
        "Env": [
            "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/
local/apache2/bin",
            "HTTPD_PREFIX=/usr/local/apache2",
            "HTTPD_VERSION=2.4.12",
            "HTTPD_BZ2_URL=https://www.apache.org/dist/httpd/httpd-2.4.12.tar.bz2"
        ],
        "ExposedPorts": {
            "80/tcp": {}
        },
        "Hostname": "dc7240fe892a",
...
```

Amazon ECS の Docker デーモンからの詳細な出力の設定

Docker コンテナまたはイメージに問題がある場合は、Docker デーモンに対してデバッグモードをオフにすることができます。デバッグを使用すると、デーモンからより詳細な出力が得られます。これを使用して、Amazon ECR などのコンテナレジストリから送信されるエラーメッセージを取得できます。

> **Important**
>
> この手順は、Amazon ECS 最適化 Amazon Linux AMI 用に書かれています。他のオペレーティングシステムについては、Docker ドキュメントの「デバッグの有効化」と「systemd による Docker の制御と設定」を参照してください。

Amazon ECS に最適化された Amazon Linux AMI で Docker デーモンのデバッグモードを使用するには

1. コンテナインスタンスに接続します。
2. Docker options ファイルを vi などのテキストエディタで開きます。Amazon ECS 最適化 Amazon Linux AMI の場合、Docker options ファイルは`/etc/sysconfig/docker`にあります。
3. Docker options ステートメントを見つけ、引用符の中の文字列に `-D` オプションを追加します。

   > **Note**
   >
   > Docker options ステートメントが `#` で始まっている場合、その文字を削除してそのステートメントをコメント解除し、オプションを有効にします。

   Amazon ECS 最適化 Amazon Linux AMI では、Docker options ステートメントを `OPTIONS` と呼びます。例:

   ```
   # Additional startup options for the Docker daemon, for example:
   # OPTIONS="--ip-forward=true --iptables=true"
   # By default we limit the number of open files per container
   OPTIONS="-D --default-ulimit nofile=1024:4096"
   ```

4. ファイルを保存し、テキストエディタを終了します。

5. Docker デーモンを再び開始します。

```
sudo service docker restart
```

出力は次のとおりです。

```
Stopping docker:                                           [  OK  ]
Starting docker: .                                    [  OK  ]
```

6. Amazon ECS エージェントを再び開始します。

```
sudo service ecs restart
```

これで、Docker ログにはより詳細な出力が表示されます。

```
time="2015-12-30T21:48:21.907640838Z" level=debug msg="Unexpected response from
 server: \"{\\\"errors\\\":[{\\\"code\\\":\\\"DENIED\\\",\\\"message\\\":\\\"User:
 arn:aws:sts::1111:assumed-role/ecrReadOnly/i-abcdefg is not authorized to perform:
 ecr:InitiateLayerUpload on resource: arn:aws:ecr:us-east-1:1111:repository/nginx_test
\\\"}]}\\n\" http.Header{\"Connection\":[]string{\"keep-alive\"}, \"Content-Type\":
[]string{\"application/json; charset=utf-8\"}, \"Date\":[]string{\"Wed, 30 Dec 2015
 21:48:21 GMT\"}, \"Docker-Distribution-Api-Version\":[]string{\"registry/2.0\"},
 \"Content-Length\":[]string{\"235\"}}"
```

Amazon ECS の Docker **API error (500): devmapper** のトラブルシューティング

以下の Docker エラーは、コンテナインスタンスのシンプールストレージがいっぱいで、Docker デーモンが新しいコンテナを作成できないことを示しています。

```
CannotCreateContainerError: API error (500): devmapper: Thin Pool has 4350 free data
 blocks which is less than minimum required 4454 free data blocks. Create more free
 space in thin pool or use dm.min_free_space option to change behavior
```

デフォルトでは、バージョン 2015.09.d以降の Amazon ECS 最適化 Amazon Linux AMIs は、/dev/xvdaに添付されファイルシステムのルートとしてマウントされたオペレーティングシステム用の8 GiB ボリュームで起動します。また、Docker がイメージとメタデータの保存に使用する /dev/

xvdczに添付された22 GiB のボリュームが追加されています。このストレージ領域がいっぱいになると、Docker デーモンは新しいコンテナを作成できません。

コンテナインスタンスにストレージを追加する最も簡単な方法は、既存のインスタンスを終了し、サイズを増加したデータストレージボリュームで新しいインスタンスを起動することです。ただし、この方法を実行できない場合は、「Amazon ECS に最適化された Linux AMI」の手順に従って、Docker が使用するボリュームグループにストレージを追加し、その論理ボリュームを拡張できます。

コンテナインスタンスストレージがあまりにも速くいっぱいになる場合は、以下のいくつかの対処方法があります。

- thin poll情報を表示するには、コンテナインスタンスで次のコマンドを実行します。

  ```
  docker info
  ```

- (Amazon ECS コンテナエージェント 1.8.0 以降) 停止または終了したコンテナがコンテナインスタンスに残る時間を短縮できます。ECS_ENGINE_TASK_CLEANUP_WAIT_DURATION エージェント設定変数で、タスクが停止されてから Docker コンテナが削除されるまでの時間を設定します (デフォルトでは、この値は 3 時間です)。これにより Docker コンテナのデータは削除されます。この値が低すぎると、ログを削除するまでは停止したコンテナを検査したり、ログを表示したりすることができない場合があります。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。
- 実行されていないコンテナと未使用のイメージをコンテナインスタンスから削除できます。次のコマンドの例を使用して、停止したコンテナと未使用のイメージを手動で削除することができます。削除されたコンテナを後から検査することはできませんので、削除されたイメージは、新しいコンテナをスタートする前に、再度プルする必要があります。

  実行中ではないコンテナを削除するには、コンテナインスタンスで以下のコマンドを実行します。

  ```
  docker rm $(docker ps -aq)
  ```

  使用しないイメージを削除するには、コンテナインスタンスで以下のコマンドを実行します。

  ```
  docker rmi $(docker images -q)
  ```

- コンテナ内で使用されていないデータブロックは削除できます。以下のコマンドを使用して、実行中のコンテナで fstrim を実行し、コンテナファイルシステムによって使用されていないデータブロックを破棄できます。

```
sudo sh -c "docker ps -q | xargs docker inspect --format='{{ .State.Pid }}' | xargs -IZ fstrim /proc/Z/root/"
```

Amazon ECS Exec に関する問題のトラブルシューティング

ECS Exec の使用時にエラーが発生する理由を診断するトラブルシューティングに関する注意事項を以下に示します。

Execチェッカーを使用して検証する

ECS Exec チェッカー スクリプトを使用すると、Amazon ECS クラスターとタスクが ECS Exec 機能を使用するための前提条件を満たしていることを確認および検証できます。ECS Exec チェッカースクリプトは、AWS CLI 環境およびクラスターを両方認証し、お客様に代わってさまざまな API を呼び出すことで、タスクが ECS Exec に対応できるようにします。このツールには、AWS CLI の最新バージョンとjqが利用可能であることが必要です。詳細については、GitHub で「ECS Exec チェッカー」を参照してください。

`execute-command` 呼び出し時のエラー

`The execute command failed` エラーが発生した場合は、以下の原因が考えられます。

- タスクに必要なアクセス許可がありません。タスクの起動に使用されるタスク定義にタスク IAM のロールが定義されていること、およびロールに必要なアクセス許可があることを確認します。詳細については、「ECS Exec のアクセス許可」を参照してください。
- SSM エージェントがインストールされていないか、実行されていません。
- Amazon ECS 用のインターフェイス Amazon VPC エンドポイントはありますが、システムマネージャーセッションマネージャー用のエンドポイントはありません。

Amazon ECS Anywhere に関する問題のトラブルシューティング

Amazon ECS Anywhere は、オンプレミスサーバーや仮想マシン (VM) などの外部インスタンスを Amazon ECS クラスターに登録するためのサポートを提供します。以下は、発生する可能性のある一般的な問題と、一般的なトラブルシューティングの推奨事項です。

トピック

外部インスタンス登録の問題

Amazon ECS クラスターに外部インスタンスを登録する場合、次の要件を満たす必要があります:

- アクティベーション ID およびアクティベーションコードで構成される、AWS Systems Manager のアクティベーションを取得する必要があります。Systems Manager マネージドインスタンスとして、外部 インスタンスを登録するために使用します。Systems Manager の有効化が要求されたら、登録制限と有効期限を指定します。登録制限は、アクティベーションを使用して登録できるインスタンスの最大数を指定します。登録制限のデフォルト値は 1 instance です。有効期限は、アクティベーションが期限切れになる日付です。デフォルト値は 24 時間です。外部インスタンスの登録に使用している Systems Manager のアクティベーションが有効でない場合は、新しいものをリクエストします。詳細については、「Amazon ECS クラスターに外部インスタンスを登録する」を参照してください。
- IAM ポリシーは、外部インスタンスが AWS API 操作との通信に必要なアクセス許可を提供するために使用されます。このマネージド ポリシーが正しく作成されず、必要なアクセス権限が含まれていない場合、外部インスタンスの登録は失敗します。詳細については、「Amazon ECS Anywhere IAM ロール」を参照してください。
- Amazon ECS には、Docker、Amazon ECS コンテナエージェント、および Systems Manager Agent を外部インスタンスにインストールするインストールスクリプトが用意されています。インストールスクリプトが失敗した場合、エラーが発生しなくても、同じインスタンスでスクリプトを再実行できない可能性があります。このような場合は、クリーンアッププロセスに従ってAWSリソースをインスタンスから削除して、再度インストールスクリプトを実行できます。詳細については、「Amazon ECS 外部インスタンスの登録を解除する」を参照してください。

> **Note**
>
> インストールスクリプトが Systems Manager のアクティベーションを正常に要求し、使用した場合、インストールスクリプトを 2 回実行すると Systems Manager のアクティベーションが再び使用されることに注意してください。これにより、順番にアクティベーションの登録制限に達する可能性があります。この制限に達した場合、新しいアクティベーションを作成する必要があります。

- GPU ワークロードの外部インスタンスでインストールスクリプトを実行するときに、NVIDIA ドライバが検出されない、または正しく設定されていない場合、エラーが発生します。インストールスクリプトは `nvidia-smi` コマンドを実行して、NVIDIA ドライバの存在を確認します。

外部インスタンスネットワークの問題

変更内容を伝えるには、外部インスタンスはAWSにネットワーク接続が必要です。外部インスタンスがAWSへのネットワーク接続が切断された場合、マニュアルで停止しない限り、インスタンスで実行されているタスクは、引き続き実行されます。AWS への接続後が復元されると、外部インスタンスの Amazon ECS コンテナエージェントと Systems Manager Agent によって使用される AWS 認証情報は自動的に更新されます。外部インスタンスとAWSの間の通信に使用されるAWSドメインの詳細については、「ネットワーク」を参照してください。

外部インスタンスでのタスクの実行に関する問題

タスクまたはコンテナが外部インスタンスで実行されない場合、最もよくある原因はネットワークまたはアクセス許可に関連しています。コンテナがAmazon ECRからイメージを引き出している場合や、コンテナのログをCloudWatch Logsに送信するように設定されている場合は、タスク定義で有効なタスク実行IAMロールを指定する必要があります。有効なタスク実行 IAM ロールがない場合、コンテナは起動しません。ネットワーク関連の問題の詳細については、「外部インスタンスネットワークの問題」を参照してください。

> **Important**
>
> Amazon ECS には、Amazon ECS ログ収集ツールが用意されています。これを使用して、トラブルシューティングの目的で外部インスタンスからログを収集することができます。詳細については、「Amazon ECS ログコレクターを使用したコンテナログの収集」を参照してください。

AWS Fargate スロットリングのクォータ

AWS Fargate は、リージョンごとに各 AWS アカウントのトークンバケットアルゴリズムを使用して、Amazon ECS タスクと Amazon EKS ポッドの起動レートをクォータ (以前は制限と呼ばれていました) に制限します。このアルゴリズムでは、アカウントには、特定の数のトークンを保持するバケットがあります。バケット内のトークンの数は、特定の秒におけるレートクォータを表します。各カスタマーアカウントには、タスクとポッドのトークンバケットがあり、カスタマーアカウントが起

動したタスクとポッドの数に応じて枯渇していきます。このトークンバケットは、定期的により多くのリクエストを行うことができるバケットの最大値と、必要に応じて一定数のリクエストを維持できるリフィルレートを持ちます。

例えば、Fargate カスタマーアカウントのタスクとポッドトークンのバケットサイズは 100 トークンで、リフィルレートは毎秒 20 トークンです。したがって、カスタマーアカウントごとに最大 100 の Amazon ECS タスクと Amazon EKS ポッドをすぐに起動できます。持続的な起動レートは、1 秒あたり 20 の Amazon ECS タスクと Amazon EKS ポッドです。

アクション	バケット最大容量 (またはバーストレート)	バケット補充率 (または持続率)
オンデマンドの Amazon ECS タスクおよび Amazon EKS ポッドの Fargate リソースレートクォータ[1]	100	20
スポット Amazon ECS タスクの Fargate リソースレートクォータ	100	20

[1]Amazon EKS ポッドのみを起動するアカウントのバーストレートは 20 で、Amazon EKS プラットフォームバージョンで呼び出されるプラットフォームバージョンを使用する場合、1 秒あたりの持続的なポッド起動レートは 20 です。

Fargate での **RunTask** API のスロットリング

さらに、Fargate は Amazon ECS RunTask API を使用したタスクの起動時に、別のクォータを使用してリクエストレートを制限します。Fargate は、リージョンごとに、各 AWS アカウントの Amazon ECS RunTask API リクエストを制限します。各リクエストは、バケットから 1 つのトークンが削除されます。これは、サービスのパフォーマンスを向上し、Fargate のすべてのお客様に平等にご利用いただくために行います。API コールは、呼び出し元が Amazon Elastic Container Service コンソール、コマンドラインツール、サードパーティーアプリケーションのどれであるかに関係なく、リクエストクォータの対象となります。Amazon ECS RunTask API への呼び出しのレートクォータは毎秒 20 コール (バーストおよび持続的) です。ただし、この API を呼び出すたびに、最大 10 のタスクを起動できます。つまり、この API に 10 回の呼び出しを行い、各呼び出しで 10 のタスクを起動するように要求することで、1 秒で 100 のタスクを起動できます。同様に、この API に 20 回の呼び出しを行い、各呼び出しで 5 つのタスクを起動するように要求することもできま

す。Amazon ECS RunTask API の API スロットリングの詳細については、Amazon ECS API リファレンスの「API リクエストのスロットリング」を参照してください。

実際には、タスクやポッドの起動レートは、ダウンロードおよび解凍するコンテナイメージ、ヘルスチェック、タスクやポッドをロードバランサーに登録するなどの統合を有効にする他の考慮事項にも依存します。お客様が有効にした機能により、以前のクォータに比べるとタスクとポッドの起動レートにばらつきが見られます。

Fargate でのレートクォータの調整

AWS アカウントの Fargate レートスロットリングクォータの増加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」(クォータ引き上げのリクエスト) を参照してください。

Amazon ECS のスロットリングに関する問題を処理する

スロットリングエラーは、同期スロットリングと非同期スロットリングの 2 つの主要なカテゴリに分類されます。

同期スロットリング

同期スロットリングが発生すると、すぐに Amazon ECS からエラーレスポンスが届きます。このカテゴリは通常、タスクの実行中またはサービスの作成中に Amazon ECS API を呼び出すと発生します。影響を受けるスロットリングと関連するスロットリング制限の詳細については、「Amazon ECS API リクエストのスロットリング」を参照してください。

アプリケーションが、AWS CLI、AWS SDK などを使用して API リクエストを開始すると、API スロットリングを修正できます。そのためには、エラーを処理するようにアプリケーションを設計するか、API コールの再試行ロジックを使用してエクスポネンシャルバックオフとジッター戦略を実装します。詳細については、「タイムアウト、リトライ、ジッターによるバックオフ」を参照してください。

AWS SDK を使用する場合、自動再試行ロジックは組み込まれており、設定可能です。

非同期スロットリング

非同期スロットリングは、Amazon ECS または AWS CloudFormation がユーザーに代わって API を呼び出してリソースをプロビジョニングする非同期ワークフローが原因で発生する場合がありま

す。Amazon ECS がユーザーに代わって呼び出す AWS API がどれなのかを知ることは重要です。たとえば、CreateNetworkInterface API は awsvpc ネットワークモードを使用するタスクに対して呼び出され、DescribeTargetHealth API はロードバランサーに登録されたタスクのヘルスチェックを実行するときに呼び出されます。

ワークロードがかなり大きくなると、これらの API オペレーションがスロットリングされる可能性があります。つまり、Amazon ECS や呼び出される AWS のサービス による制限を超えるほどスロットリングされる可能性があります。たとえば、数百のサービスをデプロイし、それぞれが awsvpc ネットワークモードを使用する数百のタスクを同時に実行する場合、Amazon ECS は CreateNetworkInterface などの EC2 API 操作および RegisterTarget、DescribeTargetHealth などの Elastic Load Balancing API 操作を呼び出し、それぞれエラスティックネットワーク、ロードバランサーを登録します。これらの API コールが API の制限を超えると、スロットリングエラーが発生する可能性があります。以下は、サービスイベントメッセージに含まれる Elastic Load Balancing スロットリングエラーの例です。

```
{
   "userIdentity":{
      "arn":"arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForECS/ecs-service-
scheduler",
      "eventTime":"2022-03-21T08:11:24Z",
      "eventSource":"elasticloadbalancing.amazonaws.com",
      "eventName":" DescribeTargetHealth ",
      "awsRegion":"us-east-1",
      "sourceIPAddress":"ecs.amazonaws.com",
      "userAgent":"ecs.amazonaws.com",
      "errorCode":"ThrottlingException",
      "errorMessage":"Rate exceeded",
      "eventID":"0aeb38fc-229b-4912-8b0d-2e8315193e9c"
   }
}
```

これらの API コールがアカウント内の他の API トラフィックと制限を共有している場合、サービスイベントとして送信されても監視が難しい場合があります。

スロットリングを監視する

どの API リクエストがスロットリングされ、誰がリクエストを発行したかを特定することが重要です。AWS CloudTrail を使用すると、スロットリングを監視し、CloudWatch、Amazon Athena、Amazon EventBridge と統合できます。CloudWatch Logs にイベントを送信するように CloudTrail を設定することができます。CloudWatch Logs のログインサイトはイベントを解析して分

析します。これにより、呼び出しを行ったユーザーや IAM ロール、行われた API コールの数など、スロットリングイベントの詳細が特定されます。詳細については、「Amazon CloudWatch Logs で CloudTrail ログファイルを監視する」を参照してください。

CloudWatch Logs Insights の詳細および、ログファイルのクエリ方法については、「CloudWatch Logs Insights を使用したログデータの分析」を参照してください。

Amazon Athena では、標準 SQL を使用してクエリを作成し、データを分析できます。たとえば、Athena テーブルを作成して CloudTrail イベントを解析することができます。詳細については、「CloudTrail コンソールを使用して CloudTrail ログ用 Athena テーブルを作成する」を参照してください。

Athena テーブルを作成すると、次のような SQL クエリを使用して ThrottlingException エラーを調査できます。

user-input を独自の値に置き換えます。

```
select eventname, errorcode,eventsource,awsregion, useragent,COUNT(*) count
FROM cloudtrail_table-name
where errorcode = 'ThrottlingException'
AND eventtime between '2024-09-24T00:00:08Z' and '2024-09-23T23:15:08Z'
group by errorcode, awsregion, eventsource, useragent, eventname
order by count desc;
```

Amazon ECS は、Amazon EventBridge にもイベント通知を送信します。リソース状態変更イベントおよびサービスアクションイベントがあります。これらには、ECS_OPERATION_THROTTLED、SERVICE_DISCOVERY_OPERATION_THROTTLED などの API スロットリングイベントが含まれます。詳細については、「Amazon ECS サービスアクションイベント」を参照してください。

これらのイベントは、応答アクションを実行する目的で、AWS Lambda などのサービスによって利用される可能性があります。詳細については、「Amazon ECS イベントの処理」を参照してください。

スタンドアロンタスクを実行する場合、RunTask などの一部の API 操作は非同期となり、再試行操作は自動的に実行されません。このような場合は、EventBridge と統合している AWS Step Functions などのサービスを使用して、スロットリングされた操作や失敗した操作を再試行できます。詳細については、「コンテナタスクの管理 (Amazon ECS、Amazon SNS)」を参照してください。

CloudWatch を使用してスロットリングを監視する

CloudWatch では、[AWS リソース別] で Usage ネームスペースの API 使用状況をモニタリングできます。これらのメトリクスは タイプ [API]、メトリック名 [CallCount] で記録されます。これらのメトリクスが特定のしきい値に達するたびに開始するアラームを作成できます。詳細については、「サービスクォータの視覚化とアラームの設定」を参照してください。

CloudWatch には異常検出機能もあります。この機能は、機械学習を使用して、有効にしたメトリクスの特定の動作に基づいて分析し、ベースラインを確立します。異常な API アクティビティが発生した場合は、この機能を CloudWatch アラームと合わせて使用できます。詳細については、「CloudWatch の異常検出の使用方法」を参照してください。

スロットリングエラーをプロアクティブにモニタリングすることで、サポート に連絡することで、関連するスロットリング制限を引き上げたり、アプリケーション固有のニーズに関するガイダンスを受けたりできます。

Amazon ECS での API エラーの原因

Amazon ECS API、コンソール、または AWS CLI でトリガーした API アクションが failures エラーメッセージを表示して終了した場合、以下が原因のトラブルシューティングに役立つことがあります。失敗すると、その理由と、その失敗に関連付けられたリソースの Amazon リソースネーム (ARN) が返されます。

多くのリソースはリージョン固有であるため、コンソールを使用するときは、リソースに正しいリージョンを設定してください。AWS CLI コマンドを使用するときは、AWS CLI コマンドが --region *region* パラメータで正しいリージョンに送信されるようにします。

Failureデータ型の構造の詳細については、「Amazon Elastic Container サービス API リファレンス」の[Failure(失敗)]を参照してください。

次の内容は、API コマンド実行時に受信する場合がある障害メッセージの例です。

API アクション	[失敗] の理由または [停止] の理由	原因
DescribeClusters	MISSING	指定されたクラスターは見つかりませんでした。クラスター名が正しく入力されているか確認します。

API アクション	[失敗] の理由または [停止] の理由	原因
DescribeInstances	MISSING	指定されたコンテナインスタンスは見つかりませんでした。コンテナインスタンスが登録されているクラスターを指定したこと、およびコンテナインスタンスの ARN または ID の両方が正しいことを確認します。
DescribeServices	MISSING	指定されたサービスは見つかりませんでした。正しいクラスターまたはリージョンが指定されていること、サービス ARN またはサービス名が有効であることを確認します。
DescribeTasks	MISSING	指定されたタスクは見つかりませんでした。正しいクラスターまたはリージョンが指定されており、タスク ARN または ID の両方が有効であることを確認します。

API アクション	[失敗] の理由または [停止] の理由	原因
DescribeTasks	TaskFailedToStart: RESOURCE:*	RESOURCE:CPU エラーの場合、タスクによって要求された CPU の数がコンテナインスタンスで利用できません。これは通常、タスク定義の CPU ユニット要件が、キャパシティプロバイダーにマッピングされた Auto Scaling グループで定義される Amazon EC2 インスタンスの CPU サイズよりも大きい場合に発生します。キャパシティプロバイダーの設定を確認する必要があります。 RESOURCE:MEMORY エラーの場合、タスクによって要求されたメモリの量がコンテナインスタンスで利用できません。これは通常、タスク定義のメモリ量要件が、キャパシティプロバイダーにマッピングされた Auto Scaling グループで定義される Amazon EC2 インスタンスでサポートされているメモリよりも大きい場合に発生します。キャパシティプロバイダーの設定を確認する必要があります。

API アクション	[失敗] の理由または [停止] の理由	原因
	TaskFailedToStart: AGENT	タスクを起動しようとしたコンテナインスタンスに、現在接続されていないエージェントがあります。タスク配置の待ち時間が長くならないように、リクエストは拒否されました。 切断されたエージェントをトラブルシューティングする方法については、「切断された Amazon ECS エージェントをトラブルシューティングするにはどうすればよいですか?」を参照してください。
	TaskFailedToStart: MemberOf placement constraint unsatisfied	タスク定義で定義された配置制約を満たすコンテナインスタンスがありません。

API アクション	[失敗] の理由または [停止] の理由	原因
	`TaskFailedToStart: ATTRIBUTE`	タスク定義に、コンテナインスタンスで使用できない特定のコンテナインスタンス属性が必要なパラメータが含まれています。例えば、awsvpc ネットワークモードを使用するタスクであるものの、指定したサブネット内に、`ecs.capability.task-eni` 属性を持つインスタンスがありません。特定のタスク定義パラメータとエージェント設定変数に必要な属性の詳細については、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」と「Amazon ECS コンテナエージェントの設定」を参照してください。
	`TaskFailedToStart: NO ACTIVE INSTANCES`	キャパシティプロバイダーにアクティブなインスタンスがありません。Auto Scaling グループの管理方法については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループ」を参照してください。

API アクション	[失敗] の理由または [停止] の理由	原因
	`TaskFailedToStart: EMPTY CAPACITY PROVIDER`	クラスターにはインスタンスはありません。これは、キャパシティープロバイダーが空であるか、キャパシティープロバイダーのインスタンスがクラスターに登録されていないことが原因と考えられます。Auto Scaling グループの管理方法については、「Amazon EC2 Auto Scaling ユーザーガイド」の「Auto Scaling グループ」を参照してください。
`GetTaskProtection`	`MISSING`	指定されたタスクは見つかりませんでした。クラスター名または ARN、タスク ARN または ID が有効であることを確認します。
	`TASK_NOT_VALID`	指定されたタスクは、Amazon ECS サービスの一部ではありません。保護できるのは Amazon ECS サービスの管理対象タスクだけです。タスク ARN または ID を確認して、もう一度お試しください。

API アクション	[失敗] の理由または [停止] の理由	原因
RunTask、または StartTask	RESOURCE:*	タスクでリクエストされたリソースまたは複数のリソースは、クラスターのコンテナインスタンスで使用できません。リソースが CPU、メモリ、ポート、または Elastic Network Interface の場合は、クラスターへのその他のコンテナインスタンスを追加する必要がある場合があります。 RESOURCE:ENI エラーの場合、awsvpc ネットワークモードを使用するタスクで必要な Elastic Network Interface アタッチメントポイントが、クラスターで利用できません。Amazon EC2 インスタンスには、アタッチできるネットワークインターフェイスの数には制限があり、プライマリネットワークインターフェイスも 1 つ分としてカウントされます。各インスタンスタイプでサポートされるネットワークインターフェイスの数の詳細については、「Amazon EC2 ユーザーガイド」の「各インスタンスタイプのネットワークインターフェイスあたりの IP アドレス数」を参照してください。

API アクション	[失敗] の理由または [停止] の理由	原因
		RESOURCE:GPU エラーの場合、タスクでリクエストされた GPU 数が利用できないため、クラスターへ GPU 対応のコンテナインスタンスの追加が必要になる場合があります。詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。
	AGENT	タスクを起動しようとしたコンテナインスタンスに、現在接続されていないエージェントがあります。タスク配置の待ち時間が長くならないように、リクエストは拒否されました。 切断されたエージェントをトラブルシューティングする方法については、「切断された Amazon ECS エージェントをトラブルシューティングするにはどうすればよいですか?」を参照してください。
	LOCATION	タスクを起動しようとしたコンテナインスタンスが、awsVpcConfiguration で指定したサブネットと異なるアベイラビリティーゾーンにあります。

API アクション	[失敗] の理由または [停止] の理由	原因
	ATTRIBUTE	タスク定義に、コンテナインスタンスで使用できない特定のコンテナインスタンス属性が必要なパラメータが含まれています。例えば、awsvpc ネットワークモードを使用するタスクであるものの、指定したサブネット内に、ecs.capability.task-eni 属性を持つインスタンスがありません。特定のタスク定義パラメータとエージェント設定変数に必要な属性の詳細については、「Fargate 起動タイプでの Amazon ECS タスク定義パラメータ」と「Amazon ECS コンテナエージェントの設定」を参照してください。
StartTask	MISSING	タスクを起動しようとした対象のコンテナインスタンスが見つかりません。間違ったクラスターまたはリージョンが指定されていたり、コンテナインスタンスの ARN または ID が正しく記述されていなかったりしないかを確認してください。
	INACTIVE	タスクを起動しようとしたコンテナインスタンスは、Amazon ECS ですでに登録解除されており、使用できません。

API アクション	[失敗] の理由または [停止] の理由	原因
TagResource	InvalidParameterException	タグ付けするサービスの ARN は短い形式です。長い形式に移行する必要があります。移行方法についての詳細は、「Amazon ECS の短いサービス ARN を長い ARN に移行する」を参照してください。
UpdateTaskProtection	DEPLOYMENT_BLOCKED	1 つ以上の保護されたタスクが原因で、サービスのデプロイが安定した状態に移行できず、タスク保護を設定できません。既存のタスクに対するタスク保護の設定を解除するか、タスク保護の有効期限が切れるまでお待ちください。
	MISSING	指定されたタスクは見つかりませんでした。クラスター名または ARN、タスク ARN または ID が有効であることを確認します。
	TASK_NOT_VALID	指定されたタスクは、Amazon ECS サービスの一部ではありません。保護できるのは Amazon ECS サービスの管理対象タスクだけです。タスク ARN または ID を確認して、もう一度お試しください。

> **Note**
>
> ここで説明した障害シナリオの他に、API 操作が例外によってエラーとなり、エラー応答が発生することもあります。このような例外のリストについては、「一般的なエラー」を参照してください。

Amazon Elastic Container Service のセキュリティ

「AWS」 ではクラウドセキュリティが最優先事項です。セキュリティを最も重視する組織の要件を満たすために構築された 「AWS」 のデータセンターとネットワークアーキテクチャは、お客様に大きく貢献します。

セキュリティは、「AWS」 と顧客の間の責任共有です。責任共有モデルでは、この責任がクラウドのセキュリティおよびクラウド内のセキュリティとして説明されています。

- クラウドのセキュリティ - 「AWS」 は、「AWS」 クラウドで 「AWS」 の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を負います。また、「AWS」 は、使用するサービスを安全に提供します。「AWS」 コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon Elastic Container Service, に適用されるコンプライアンスプログラムについては、コンプライアンスプログラムによる対象範囲内のAWSサービス」を参照してください。
- クラウド内のセキュリティ - ユーザーの責任は、使用する 「AWS」 のサービスに応じて異なります。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、Amazon ECS 使用時における責任共有モデルの適用法を理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目的を満たすように Amazon ECS を設定する方法について説明します。Amazon ECS リソースのモニタリングやセキュリティ確保に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- Amazon Elastic コンテナサービスのアイデンティティ とアクセス管理
- Amazon Elastic Container Service でのログとモニタリング
- Amazon Elastic Container Service でのコンプライアンス検証
- AWS Fargate 連邦情報処理標準 (FIPS-140)
- Amazon Elastic Container Service におけるインフラストラクチャセキュリティ
- Amazon ECS の AWS 責任共有モデル。
- Amazon ECS のネットワークセキュリティのベストプラクティス
- Amazon ECS タスクおよびコンテナのセキュリティのベストプラクティス

Amazon Elastic コンテナサービスのアイデンティティ とアクセス管理

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するために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に Amazon ECS 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、追加費用なしで使用できる AWS のサービスです。

トピック

対象者

AWS Identity and Access Management (IAM) の用途は、Amazon ECS で行う作業によって異なります。

サービスユーザー – ジョブを実行するために Amazon ECS サービスを使用する場合は、管理者から必要なアクセス許可と認証情報が与えられます。さらに多くの Amazon ECS 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。Amazon ECS の機能にアク

セスできない場合は、「Amazon Elastic Container Service のアイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の Amazon ECS リソースを担当している場合は、通常、Amazon ECS へのフルアクセスがあります。サービスのユーザーがどの Amazon ECS 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 Amazon ECS を使用して IAM を利用する方法の詳細については、「IAM を使用する Amazon Elastic Container Service」を参照してください。

IAM 管理者 – 管理者は、 Amazon ECS 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 Amazon ECS 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、「Amazon Elastic Container Service のアイデンティティベースのポリシーの例」を参照してください。

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWSにサインインする方法です。ユーザーは、AWS アカウントのルートユーザー、IAM ユーザーとして、または IAM ロールを引き受けることによって、認証される (AWSにサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。AWS IAM Identity Centerフェデレーティッドアイデンティティの例としては、(IAM アイデンティティセンター) ユーザー、貴社のシングルサインオン認証、Google または Facebook の認証情報などがあります。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。フェデレーションを使用して AWSにアクセスする場合、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。AWS へのサインインの詳細については、AWS サインインユーザーガイドの「AWS アカウントにサインインする方法」を参照してください。

プログラムを使用して AWS にアクセスする場合、AWSは Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) 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、AWS 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 のルートユーザー

AWS アカウント を作成する場合は、このアカウントのすべての AWS のサービス とリソースに対して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。このアイデンティティは 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によってアクセスできます。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。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに対し、ID プロバイダーとのフェデレーションを使用して、一時的な認証情報の使用により、AWS のサービスにアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリのユーザーか、または ID ソースから提供された認証情報を使用して AWS のサービス にアクセスするユーザーです。フェデレーティッド ID が AWS アカウントにアクセスすると、ロールが継承され、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、AWS IAM Identity Centerを使用することをお勧めします。IAM アイデンティティセンター でユーザーとグループを作成するか、すべての AWS アカウント とアプリケーションで使用するために、独自の ID ソースで一連のユーザーとグループに接続して同期することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Centerユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) 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 1 つのアプリケーションに対して特定の許可を持つ AWS アカウント 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 ユーザーのユースケース」を参照してください。

IAM ロール

IAM ロールは、特定の許可を持つ、AWS アカウント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。AWS Management Console で IAM ロールを一時的に引き受けるには、ユーザーから IAM ロール に切り替える (コンソール) ことができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、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 AWS のサービ

ス では、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。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権 - 一部の AWS のサービス では、他の AWS のサービス の機能を使用します。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 AWS でアクションを実行するユーザーは、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、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。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、AWS のサービス にリンクされたサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント 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 - EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。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。AWS ロールを EC2 インスタンスに割り当て、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、インスタンスに添付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権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS 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、これらのポリシーを評価します。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。大半のポリシーは JSON ドキュメントとして AWS 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 AWS JSON ポリシーを使用して、だれ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んなリソースにどんな条件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。このポリシーがあるユーザーは、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。ID ベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「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ます。マネージドポリシーは、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマーマネージドポリシーがあります。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、フェデレーションユーザー、または AWS のサービス を含めることができます。

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は使用できません。

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、ACL をサポートするサービスの例です。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 では、他の一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCP) - SCP は、AWS Organizations で組織や組織単位 (OU) の最大許可を指定する JSON ポリシーです。AWS Organizations は、お客様が所有する複数の AWS

アカウントをグループ化し、一元的に管理するサービスです。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 はメンバーアカウントのエンティティに対する権限を制限します (各 AWS アカウントのルートユーザー など)。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許可を制限し、組織に属す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 のための有効な許可に影響を及ぼす可能性があります。RCP をサポートする AWS のサービス のリストを含む Organizations と RCP の詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、「IAM ユーザーガイド」の「ポリシーの評価ロジック」を参照してください。

IAM を使用するAmazon Elastic Container Service

IAM を使用して Amazon ECS へのアクセスを管理する前に、Amazon ECS で使用できる IAM 機能について理解しておく必要があります。

IAM の機能	Amazon ECS サポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ

IAM の機能	Amazon ECS サポート
ポリシーアクション	はい
ポリシーリソース	部分的
ポリシー条件キー	Yes
ACL	いいえ
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	はい
サービスリンクロール	あり

大部分の IAM 機能が Amazon ECS および、その他のサービスでどのように機能するかに関するおおまかな説明については、AWS IAM ユーザーガイドの「IAM と連携する AWS のサービス」を参照してください。

Amazon ECS のアイデンティティベースの ポリシー

ID ベースのポリシーのサポート: あり

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。ID ベースの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。

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、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Amazon ECS の ID ベースのポリシー例

Amazon ECS でのアイデンティティベースのポリシーの例は、「Amazon Elastic Container Service のアイデンティティベースのポリシーの例」でご確認ください。

Amazon ECS 内のリソースベースのポリシー

リソースベースのポリシーのサポート: なし

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、フェデレーションユーザー、または AWS のサービス を含めることができます。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる AWS アカウント にある場合、信頼できるアカウントの IAM 管理者は、リソースにアクセスするための権限をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

Amazon ECS のポリシーアクション

ポリシーアクションのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれ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。

Amazon ECS アクションのリストを確認するには、「Service Authorization Reference」の「Actions defined by Amazon Elastic Container Service」を参照してください。

Amazon ECS のポリシーアクションは、アクションの前に以下のプレフィックスを使用します。

```
ecs
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "ecs:action1",
      "ecs:action2"
         ]
```

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、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": "ecs:Describe*"
```

Amazon ECS でのアイデンティティベースのポリシーの例は、「Amazon Elastic Container Service のアイデンティティベースのポリシーの例」でご確認ください。

Amazon ECS のポリシーリソース

ポリシーリソースのサポート: 一部

管理者は AWS JSON ポリシーを使用して、だれ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んなリソースにどんな条件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、アマゾン 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": "*"
```

Amazon ECS リソースタイプとその ARN のリストを確認するには、「Service Authorization Reference」の「Resources defined by Amazon Elastic Container Service」を参照してください。各リソースの ARN を指定できるアクションについては、「Amazon Elastic Container Service で定義されるアクション」を参照してください。

複数のリソースをサポートする Amazon ECS API アクションもあります。例えば、`DescribeClusters` API アクションを呼び出すときに複数のクラスターを参照できます。複数リソースを単一ステートメントで指定するには、ARN をカンマで区切ります。

```
"Resource": [
      "EXAMPLE-RESOURCE-1",
      "EXAMPLE-RESOURCE-2"
```

例えば、Amazon ECS クラスターリソースの ARN は次のようになります。

```
arn:${Partition}:ecs:${Region}:${Account}:cluster/${clusterName}
```

次の ARN を使用して、ステートメントで `my-cluster-1` および `my-cluster-2` クラスタを指定します。

```
"Resource": [
         "arn:aws:ecs:us-east-1:123456789012:cluster/my-cluster-1",
         "arn:aws:ecs:us-east-1:123456789012:cluster/my-cluster-2"
```

特定のアカウントに属するすべてのクラスターを指定するには、ワイルドカード (*) を使用します。

```
"Resource": "arn:aws:ecs:us-east-1:123456789012:cluster/*"
```

タスク定義では、最新のリビジョンまたは特定のリビジョンを指定できます。

タスク定義のすべてのリビジョンを指定するには、ワイルドカード (*) を使用します。

```
"Resource:arn:${Partition}:ecs:${Region}:${Account}:task-definition/
${TaskDefinitionFamilyName}:*"
```

特定のタスク定義リビジョンを指定する場合は、${TaskDefinitionRevisionNumber} を使用します。

```
"Resource:arn:${Partition}:ecs:${Region}:${Account}:task-definition/
${TaskDefinitionFamilyName}:${TaskDefinitionRevisionNumber}"
```

Amazon ECS でのアイデンティティベースのポリシーの例は、「Amazon Elastic Container Service のアイデンティティベースのポリシーの例」でご確認ください。

Amazon ECS のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれ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んなリソースにどんな条件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。単一の条件キーに複数の値を指定する場合、AWS では OR 論理演算子を使用して条件を評価します。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。

Amazon ECS は、以下のサービス固有の条件キーをサポートしており、IAM ポリシーのきめ細かいフィルタリングの提供に使用することができます。

条件キー	説明	評価の種類
aws:RequestTag/${TagKey}	コンテキストキーは "aws:RequestTag/ *tag-key*":"*tag-value* " という形式です。ここで *tag-key* および *tag-value* はタグキーと値のペアです。 タグキーと値のペアが AWS リクエストに含まれていることを確認します。例えば、リクエストに「"Dept"」タグキーが含まれ、「"Accounting" 」という値が含まれているかどうかを確認できます。	String
aws:ResourceTag/${TagKey}	コンテキストキーは "aws:ResourceTag/ *tag-key*":"*tag-value* " という形式です。ここで *tag-key* および *tag-value* はタグキーと値のペアです。 リソース (ユーザーまたはロール) を識別するためにアタッチされたタグが、指定されたキーの名前および値と一致するかどうかをチェックします。	String
aws:TagKeys	このコンテキストキーは "aws:TagKeys":" *tag-key*" という形式であり、ここで *tag-key* は値 (["Dept","Cost-Center"] など) のないタグキーのリストです。 AWS リクエストに存在するタグキーをチェックします。	String
ecs:ResourceTag/${TagKey}	コンテキストキーは "ecs:ResourceTag/ *tag-key*":"*tag-value* " という形式です。ここで *tag-key* および *tag-value* はタグキーと値のペアです。 リソース (ユーザーまたはロール) を識別するためにアタッチされたタグが、指定されたキーの名前および値と一致するかどうかをチェックします。	String
ecs:cluster	コンテキストキーは "ecs:cluster":" *cluster-arn* " という形式です。ここで *cluster-arn* は、Amazon ECS クラスターの ARN です。	ARN、Null

条件キー	説明	評価の種類
ecs:container-instances	コンテキストキーは "ecs:container-instances":" *container-instance-arns* " という形式です。ここで *container-instance-arns* は、1 つ以上のコンテナインスタンス ARN です。	ARN、Null
ecs:container-name	コンテキストキーは "ecs:container-name":" *container-name* " 形式で、*container-instan-* は、タスク定義で定義されている Amazon ECS コンテナの名前です。	String
ecs:enable-execute-command	コンテキストキーは"ecs:enable-execute-command":" *value*" 形式であり、*value-* は「true」または「false」です。	String
ecs:enable-service-connect	コンテキストキーは "ecs:enable-service-connect":" *value*" 形式であり、*value* は "true" または "false" です。	String
ecs:enable-ebs-volumes	コンテキストキーは "ecs:enable-ebs-volumes":" *value*" 形式であり、*value* は "true" または "false" です。	String
ecs:namespace	コンテキストキーは "ecs:namespace":" *namespace-arn* " 形式であり、*namespace-arn* は AWS Cloud Map 名前空間の ARN です。	ARN、Null
ecs:service	コンテキストキーは "ecs:service":" *service-arn* " という形式です。ここで *service-arn* は、Amazon ECS サービスの ARN です。	ARN、Null
ecs:task-definition	コンテキストキーは "ecs:task-definition":" *task-definition-arn* " という形式です。ここで *task-definition-arn* は、Amazon ECS タスク定義の ARN です。	ARN、Null

条件キー	説明	評価の種類
ecs:account-setting	コンテキストキーは "ecs:account-setting":" *account-setting* " という形式で、*account-setting* は Amazon ECS アカウント設定の名前です。	String

Amazon ECS 条件キーのリストを確認するには、「Service Authorization Reference」の「Condition keys for Amazon Elastic Container Service」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、「Amazon Elastic Container Service で定義するアクション」を参照してください。

Amazon ECS でのアイデンティティベースのポリシーの例は、「Amazon Elastic Container Service のアイデンティティベースのポリシーの例」でご確認ください。

Amazon ECS アクセスコントロールリスト (ACL)

ACL のサポート: なし

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 ECS での属性ベースのアクセスコントロール (ABAC)

> **Important**
>
> Amazon ECS は、すべての Amazon ECS リソースに対して属性ベースのアクセスコントロールをサポートしています。属性を使用してアクションの範囲を設定できるかどうかを判断するには、「サービス許可リファレンス」の「Amazon Elastic Container Service で定義されるアクション」の表を参照してください。まず、リソース列にリソースがあることを確認します。次に、[条件キー]列を使用して、アクションとリソースの組み合わせのキーを確認します。

ABAC (ポリシー内のタグ) のサポート: あり

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。AWS では、属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、お

よび多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws: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。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

Amazon ECS リソースのタグ付けの詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。

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、「タグに基づき、Amazon ECS サービスを記述する」を参照してください。

Amazon ECS での一時的な認証情報の使用

一時的な認証情報のサポート: あり

AWS のサービスには、一時的な認証情報を使用してサインインしても機能しないものがあります。一時的な認証情報を利用できる AWS のサービス を含めた詳細情報については、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

ユーザー名とパスワード以外の方法で AWS Management Console にサインインする場合は、一時的な認証情報を使用していることになります。例えば、会社のシングルサインオン (SSO) リンクを使用して AWS にアクセスすると、そのプロセスは自動的に一時認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時認証情報は、AWS CLI または AWS API を使用して手動で作成できます。作成後、一時認証情報を使用して AWS にアクセスできるようになります。AWSは、長期的なアクセスキーを使用する代わりに、一時認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Amazon ECS のフォワードアクセスセッション

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルとみなされます。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、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。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。

Amazon ECS のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス に許可を委任するロールを作成する」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Amazon ECS の機能が破損する可能性があります。Amazon ECS が指示する場合以外は、サービスロールを編集しないでください。

Amazon ECS のサービスにリンクされたロール

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。

サービスにリンクされたロールは、AWS アカウント 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 ECS でのサービスにリンクされたロールの作成または管理の詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。

Amazon Elastic Container Service のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーおよびロールにはAmazon ECS リソースを作成または変更する許可はありません。また、AWS Management Console、AWS Command Line Interface (AWS CLI)、または AWS API を使用してタスクを実行することもできません。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継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、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「IAM ポリシーを作成する (コンソール)」を参照してください。

Amazon ECS が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「Service Authorization Reference」の「Actions, resources, and condition keys for Amazon Elastic Container Service」を参照してください。

トピック

- Amazon ECS ポリシーのベストプラクティス
- 自分のアクセス許可の表示を Amazon ECS ユーザーに許可する
- Amazon ECS クラスターの例
- Amazon ECS コンテナインスタンスの例
- Amazon ECS タスク定義の例
- Amazon ECS タスク実行の例
- Amazon ECS タスク開始の例
- Amazon ECS のタスクの例を一覧表示して説明する
- Amazon ECS サービス作成の例
- Amazon ECS サービス更新の例

- タグに基づき、Amazon ECS サービスを記述する
- Amazon ECS Service Connect 名前空間の上書き拒否の例

Amazon ECS ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウント内で誰かが Amazon ECS 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 マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケース別に AWS カスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込む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。また、AWS CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用して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。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 – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。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。

自分のアクセス許可の表示を Amazon ECS ユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI か AWS API を使用してプログラム的に、このアクションを完了する権限が含まれています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

Amazon ECS クラスターの例

次の IAM ポリシーでは、クラスターを作成し、記載したアクセス権限を付与します。CreateCluster と ListClusters のアクションはリソースを受け入れないため、すべてのリソースでリソース定義は * に設定されます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:CreateCluster",
                "ecs:ListClusters"
            ],
            "Resource": ["*"]
        }
    ]
}
```

次の IAM ポリシーでは、特定のクラスターに記述、および削除するアクセス権限を付与します。DescribeClusters と DeleteCluster のアクションはリソースとしてクラスター ARN を使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DescribeClusters",
                "ecs:DeleteCluster"
            ],
            "Resource": ["arn:aws:ecs:us-east-1:<aws_account_id>:cluster/
<cluster_name>"]
        }
    ]
```

```
}
```

次の IAM ポリシーは、ユーザーまたはグループが特定のクラスターでのオペレーションの実行のみを許可するユーザーまたはグループにアタッチできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ecs:Describe*",
                "ecs:List*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "ecs:DeleteCluster",
                "ecs:DeregisterContainerInstance",
                "ecs:ListContainerInstances",
                "ecs:RegisterContainerInstance",
                "ecs:SubmitContainerStateChange",
                "ecs:SubmitTaskStateChange"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ecs:us-east-1:<aws_account_id>:cluster/default"
        },
        {
            "Action": [
                "ecs:DescribeContainerInstances",
                "ecs:DescribeTasks",
                "ecs:ListTasks",
                "ecs:UpdateContainerAgent",
                "ecs:StartTask",
                "ecs:StopTask",
                "ecs:RunTask"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "ArnEquals": {"ecs:cluster": "arn:aws:ecs:us-
east-1:<aws_account_id>:cluster/default"}
```

```
            }
        }
    ]
}
```

Amazon ECS コンテナインスタンスの例

コンテナインスタンス登録は、Amazon ECS エージェントによって処理されますが、ユーザーがクラスターからインスタンスを手動で登録解除を許可する場合があります。コンテナインスタンスを間違ったクラスターに登録、または実行中のタスクがあるインスタンスを誤って終了してしまうかもしれません。

次に示す IAM ポリシーでは、ユーザーが指定したクラスターでコンテナインスタンスをリストし、登録を解除することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DeregisterContainerInstance",
                "ecs:ListContainerInstances"
            ],
            "Resource": ["arn:aws:ecs:<region>:<aws_account_id>:cluster/
<cluster_name>"]
        }
    ]
}
```

次の IAM ポリシーでは、ユーザーが指定したクラスターに指定コンテナインスタンスを記述することができます。このアクセス権限をクラスター内のすべてのコンテナインスタンスに開放するためには、コンテナインスタンスの UUID を * に置き換えることができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:DescribeContainerInstances"],
            "Condition": {
```

```
                "ArnEquals": {"ecs:cluster":
 "arn:aws:ecs:<region>:<aws_account_id>:cluster/<cluster_name>"}
            },
            "Resource": ["arn:aws:ecs:<region>:<aws_account_id>:container-instance/
<cluster_name>/<container_instance_UUID>"]
        }
    ]
}
```

Amazon ECS タスク定義の例

タスク定義 IAM ポリシーは、リソースレベルのアクセス権限をサポートしていませんが、次の IAM ポリシーでは、ユーザーがタスク定義を登録、一覧表示、および記述することができます。

コンソールを使用する場合は、CloudFormation: CreateStack を Action として追加する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:RegisterTaskDefinition",
                "ecs:ListTaskDefinitions",
                "ecs:DescribeTaskDefinition"
            ],
            "Resource": ["*"]
        }
    ]
}
```

Amazon ECS タスク実行の例

RunTask のリソースは、タスク定義です。ユーザーがタスク定義を実行できるクラスターを制限するには、Condition ブロックで指定します。この方法には、適切なアクセス権を許可するためにリソースでタスク定義とクラスターの両方をリストする必要がないという利点があります。いずれか、または両方を適用できます。

次の IAM ポリシーでは、特定のクラスターで特定のタスク定義の変更を実行するアクセス権限を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:RunTask"],
            "Condition": {
                "ArnEquals": {"ecs:cluster":
 "arn:aws:ecs:<region>:<aws_account_id>:cluster/<cluster_name>"}
            },
            "Resource": ["arn:aws:ecs:<region>:<aws_account_id>:task-definition/
<task_family>:*"]
        }
    ]
}
```

Amazon ECS タスク開始の例

StartTask のリソースは、タスク定義です。ユーザーがタスク定義を開始できるクラスターとコンテナインスタンスを制限するには、Condition ブロックでそれらを指定します。この方法には、適切なアクセス権を許可するためにリソースでタスク定義とクラスターの両方をリストする必要がないという利点があります。いずれか、または両方を適用できます。

次の IAM ポリシーでは、特定のクラスターおよび特定のコンテナインスタンスで特定のタスク定義の変更を開始するアクセス許可を付与します。

> **Note**
>
> この例では、AWS CLI または別の AWS SDK で StartTask API を呼び出すときに、Resource マッピングが一致するようにタスク定義リビジョンを指定する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:StartTask"],
            "Condition": {
                "ArnEquals": {
```

```
                    "ecs:cluster": "arn:aws:ecs:<region>:<aws_account_id>:cluster/
<cluster_name>",
                    "ecs:container-instances":
 ["arn:aws:ecs:<region>:<aws_account_id>:container-instance/<cluster_name>/
<container_instance_UUID>"]
                }
            },
            "Resource": ["arn:aws:ecs:<region>:<aws_account_id>:task-definition/
<task_family>:*"]
        }
    ]
}
```

Amazon ECS のタスクの例を一覧表示して説明する

次の IAM ポリシーでは、ユーザーが指定したクラスターのためのタスクをリストできるようにします。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:ListTasks"],
            "Condition": {
                "ArnEquals": {"ecs:cluster":
 "arn:aws:ecs:<region>:<aws_account_id>:cluster/<cluster_name>"}
            },
            "Resource": ["*"]
        }
    ]
}
```

次の IAM ポリシーでは、ユーザーが指定したクラスターに指定タスクを記述することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:DescribeTasks"],
            "Condition": {
```

```
                "ArnEquals": {"ecs:cluster":
 "arn:aws:ecs:<region>:<aws_account_id>:cluster/<cluster_name>"}
            },
            "Resource": ["arn:aws:ecs:<region>:<aws_account_id>:task/<cluster_name>/
<task_UUID>"]
        }
    ]
}
```

Amazon ECS サービス作成の例

次の IAM; ポリシーでは、ユーザーが AWS Management Console で Amazon ECS サービスを作成することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:Describe*",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ecs:List*",
                "ecs:Describe*",
                "ecs:CreateService",
                "elasticloadbalancing:Describe*",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRoles",
                "iam:ListGroups",
                "iam:ListUsers"
            ],
            "Resource": ["*"]
        }
    ]
}
```

Amazon ECS サービス更新の例

次の IAM ポリシーでは、ユーザーが AWS Management Console で Amazon ECS サービスを更新することができます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:Describe*",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ecs:List*",
                "ecs:Describe*",
                "ecs:UpdateService",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRoles",
                "iam:ListGroups",
                "iam:ListUsers"
            ],
            "Resource": ["*"]
        }
    ]
}
```

タグに基づき、Amazon ECS サービスを記述する

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 Amazon ECS リソースへのアクセスをコントロールできます。この例では、サービスを表示できるポリシーを作成する方法を示します。ただし、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": "DescribeServices",
            "Effect": "Allow",
            "Action": "ecs:DescribeServices",
            "Resource": "*"
        },
        {
            "Sid": "ViewServiceIfOwner",
            "Effect": "Allow",
            "Action": "ecs:DescribeServices",
            "Resource": "arn:aws:ecs:*:*:service/*",
            "Condition": {
                "StringEquals": {"ecs:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

このポリシーをアカウントの IAM ユーザーにアタッチできます。richard-roe という名前のユーザーが Amazon ECS サービスを表示する場合は、サービスに Owner=richard-roe または owner=richard-roe とタグ付けする必要があります。それ以外の場合、アクセスは拒否されます。条件キー名では大文字と小文字が区別されないため、条件タグキー Owner は Owner と owner の両方に一致します。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 条件」を参照してください。

Amazon ECS Service Connect 名前空間の上書き拒否の例

以下の IAM ポリシーは、サービス設定のデフォルトの Service Connect 名前空間をユーザーが上書きすることを拒否します。デフォルトの名前空間はクラスターに設定されます。ただし、サービス設定内ではそれを上書きできます。一貫性を保つため、新しいサービスはすべて同じ名前空間を使用するように設定することを検討してください。サービスに特定の名前空間を使用するように要求するには、以下のコンテキストキーを使用します。以下の例で、<region>、<aws_account_id>、<cluster_name>、<namespace_id> を独自のものに置き換えます。

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

```
            "Effect": "Allow",
            "Action": [
                "ecs:CreateService",
                "ecs:UpdateService"
            ],
            "Condition": {
                "ArnEquals": {
                    "ecs:cluster": "arn:aws:ecs:<region>:<aws_account_id>:cluster/
<cluster_name>",
                    "ecs:namespace":
 "arn:aws:servicediscovery:<region>:<aws_account_id>:namespace/<namespace_id>"
                }
            },
            "Resource": "*"
        }
    ]
}
```

Amazon Elastic Container Service に関する AWS 管理ポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには自分でポリシーを作成するよりも、AWS マネージドポリシーを使用する方が簡単です。チームに必要な権限のみを提供する IAM カスタマーマネージドポリシーを作成するには時間と専門知識が必要です。すぐに使用を開始するために、AWS マネージドポリシーを使用できます。これらのポリシーは一般的なユースケースを対象範囲に含めており、AWS アカウントで利用できます。AWS マネージドポリシーの詳細については「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 のサービスはAWS マネージドポリシーを維持および更新します。AWS マネージドポリシーの許可を変更することはできません。サービスでは新しい機能を利用できるようにするために、AWS マネージドポリシーに権限が追加されることがあります。この種類の更新はポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスがAWS マネージドポリシーを更新する可能性が最も高くなります。サービスはAWS マネージドポリシーから権限を削除しないため、ポリシーの更新によって既存の権限が破棄されることはありません。

さらに、AWS は複数のサービスにまたがるジョブ機能の特徴に対するマネージドポリシーもサポートしています。例えば、ReadOnlyAccess AWS マネージドポリシーではすべての AWS のサービ

スおよびリソースへの読み取り専用アクセスを許可します。サービスが新しい機能を起動する場合、AWS は新たなオペレーションとリソース用に、読み取り専用の許可を追加します。ジョブ機能ポリシーのリストと説明については、IAM ユーザーガイドのジョブ機能の AWS 管理ポリシーを参照してください。

Amazon ECS および Amazon ECR では、ユーザー、グループ、ロール、Amazon EC2 インスタンス、および Amazon ECS タスクにアタッチして、リソースや API オペレーションで異なる制御レベルを使用できる複数の管理ポリシーと信頼関係を提供しています。これらのポリシーを直接適用することも、独自のポリシーを作成する開始点として使用することもできます。Amazon ECR 管理ポリシーの詳細については、「Amazon ECR 管理ポリシー」を参照してください。

AmazonECS_FullAccess

`AmazonECS_FullAccess` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、Amazon ECS リソースへの管理アクセスを許可し、IAM ID(ユーザー、グループ、ロールなど)にAWSサービスは、Amazon ECS のすべての機能を使用するために統合されています。このポリシーを使用すると、AWS Management Console で利用可能な Amazon ECS のすべての機能にアクセスできます。これらの機能は、。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonECS_FullAccess」を参照してください。

AmazonECSInfrastructureRolePolicyForVolumes

`AmazonECSInfrastructureRolePolicyForVolumes` マネージドポリシーを IAM エンティティにアタッチできます。

ポリシーは、Amazon ECS がユーザーに変わって AWS API コールを行うのに必要なアクセス許可を付与します。このポリシーは、Amazon ECS のタスクとサービスを起動するときにボリューム設定で指定する IAM ロールにアタッチできます。このロールにより、Amazon ECS はタスクにアタッチされたボリュームを管理できます。詳細については、「Amazon ECS インフラストラクチャの IAM ロール」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonECSInfrastructureRolePolicyForVolumes」を参照してください。

AmazonEC2ContainerServiceforEC2Role

`AmazonEC2ContainerServiceforEC2Role` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、ユーザーに代わって AWS に呼び出すことを Amazon ECS コンテナインスタ

ンスに許可する管理権限を付与します。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

Amazon ECS は、Amazon EC2 インスタンスまたは外部インスタンスに対して、ユーザーに代わってアクションを実行することを Amazon ECS に許可するサービスロールにこのポリシーをアタッチします。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonEC2ContainerServiceforEC2Role」を参照してください。

考慮事項

AmazonEC2ContainerServiceforEC2Role が管理する IAM ポリシーを使用するときは、次の推奨事項と考慮事項を検討する必要があります。

- 最小権限を付与する標準のセキュリティアドバイスに従って、AmazonEC2ContainerServiceforEC2Role 管理ポリシーを変更して、特定のニーズに合わせることができます。管理ポリシーで付与されたアクセス許可のいずれかがユースケースに必要でない場合、カスタムポリシーを作成し、必要なアクセス許可のみを追加します。例えば、UpdateContainerInstancesState アクセス許可は、スポットインスタンスのドレインに提供されます。その権限がユースケースに必要ない場合、カスタムポリシーを使用して除外します。
- コンテナインスタンスで実行しているコンテナは、インスタンスのメタデータを通じてコンテナインスタンスのロールに提供されているすべての権限にアクセスできます。コンテナインスタンスのロールのアクセス許可は、以下に提供されるマネージド型 AmazonEC2ContainerServiceforEC2Role ポリシーのアクセス許可のミニマリストに制限することをお勧めします。タスクのコンテナでリストされていない追加のアクセス許可が必要な場合は、独自の IAM ロールを使用してタスクを提供することをお勧めします。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。

  コンテナを防ぐには、docker0 ブリッジからコンテナインスタンスロールに指定されたアクセス許可にアクセスしないようにします。これは、次の iptables コマンドをコンテナインスタンスで実行することで Amazon ECS タスクの IAM ロール が提供するアクセス許可を許可して、コンテナは、有効なこのルールでインスタンスメタデータをクエリできません。このコマンドはデフォルトの Docker のブリッジ設定を前提としており、host ネットワークモードを使用してコンテナでは動作しません。詳細については、「ネットワークモード」を参照してください。

  ```
  sudo yum install -y iptables-services; sudo iptables --insert DOCKER USER 1 --in-interface docker+ --destination 169.254.169.254/32 --jump DROP
  ```

再起動後も有効にするには、コンテナインスタンスでこの iptables ルールを保存する必要があります。Amazon ECS 最適化 AMI の場合は、次のコマンドを使用します。他のオペレーティングシステムについては、その OS のドキュメントを参照してください。

- Amazon ECS に最適化された Amazon Linux 2 AMI の場合:

```
sudo iptables-save | sudo tee /etc/sysconfig/iptables && sudo systemctl enable --now iptables
```

- Amazon ECS に最適化された Amazon Linux AMI の場合:

```
sudo service iptables save
```

AmazonEC2ContainerServiceEventsRole

`AmazonEC2ContainerServiceEventsRole` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、Amazon EventBridge(旧 CloudWatch Events)がユーザーに代わってタスクを実行できるようにするアクセス権限を付与します。このポリシーは、スケジュールされたタスクの作成時に指定された IAM ロールにアタッチできます。詳細については、「Amazon ECS EventBridge IAM ロール」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonEC2ContainerServiceEventsRole」を参照してください。

AmazonECSTaskExecutionRolePolicy

`AmazonECSTaskExecutionRolePolicy` 管理 IAM ポリシーは、Amazon ECS コンテナエージェントおよび AWS Fargate コンテナエージェントに必要なアクセス権限を付与し、ユーザーに代わって AWS API コールを作成します。このポリシーは、タスク実行 IAM ロールに追加できます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonECSTaskExecutionRolePolicy」を参照してください。

AmazonECSServiceRolePolicy

`AmazonECSServiceRolePolicy` マネージド IAM ポリシーにより、Amazon Elastic Container Service でクラスターを管理できるようになります。このポリシーは、タスク実行 IAM ロールに追加できます。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonECSServiceRolePolicy」を参照してください。

AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecur

IAM エンティティに AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity ポリシーをアタッチできます。このポリシーは、お客様に代わって Amazon ECS Service Connect TLS 機能を管理するために必要な AWS Private Certificate Authority、Secrets Manager、およびその他の AWS サービスへの管理アクセスを提供します。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity」を参照してください。

AWSApplicationAutoscalingECSServicePolicy

IAM エンティティに AWSApplicationAutoscalingECSServicePolicy をアタッチすることはできません。このポリシーは、ユーザーに代わって Application Auto Scaling がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、「Application Auto Scaling のサービスにリンクされたロール」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSApplicationAutoscalingECSServicePolicy」を参照してください。

AWSCodeDeployRoleForECS

IAM エンティティに AWSCodeDeployRoleForECS をアタッチすることはできません。このポリシーは、ユーザーに代わって CodeDeploy がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、AWS CodeDeploy ユーザーガイドの「CodeDeploy のサービスロールを作成する」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSCodeDeployRoleForECS」を参照してください。

AWSCodeDeployRoleForECSLimited

IAM エンティティに AWSCodeDeployRoleForECSLimited をアタッチすることはできません。このポリシーは、ユーザーに代わって CodeDeploy がアクションを実行することを許可する、サービスにリンクされたロールにアタッチされます。詳細については、AWS CodeDeploy ユーザーガイドの「CodeDeploy のサービスロールを作成する」を参照してください。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AWSCodeDeployRoleForECSLimited」を参照してください。

AmazonECSInfrastructureRolePolicyForVpcLattice

IAM エンティティに AmazonECSInfrastructureRolePolicyForVpcLattice ポリシーをアタッチできます。このポリシーは、ユーザーに代わって Amazon ECS ワークロードの VPC Lattice 機能を管理するために必要な他の AWS サービスリソースへのアクセスを提供します。

このポリシーのアクセス許可を確認するには、「AWS マネージドポリシーリファレンス」の「AmazonECSInfrastructureRolePolicyForVpcLattice」を参照してください。

ユーザーに代わって Amazon ECS ワークロードの VPC Lattice 機能を管理するために必要な他の AWS サービスリソースへのアクセスを提供します。

Amazon ECS での AWS 管理ポリシーに関する更新

Amazon ECS 向けの AWS 管理ポリシーについて、このサービスがこれらの変更の追跡を開始して以降行われた更新の詳細情報を示します。このページの変更に関する自動通知を入手するには、Amazon ECS ドキュメントの履歴ページから、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
新しい AmazonECSInfrastructureRolePolicyForVpcLattice の追加	ユーザーに代わって Amazon ECS ワークロードの VPC Lattice 機能を管理するために必要な他の AWS サービスリソースへのアクセスを提供します。	2024 年 11 月 18 日
AmazonECSInfrastructureRolePolicyForVolumes へのアクセス許可を追加する	AmazonECSInfrastructureRolePolicyForVolumes ポリシーが更新され、お客様がスナップショットから Amazon EBS ボリュームを作成できるようになりました。	2024 年 10 月 10 日

変更	説明	日付
アクセス許可を the section called “AmazonECS_FullAccess” に追加しました。	AmazonECS_FullAccess ポリシーが更新され、ecsInfrastructureRole という名前のロールの IAM ロールの iam:PassRole アクセス許可が追加されました。これは、AWS Management Console によって作成されたデフォルトの IAM ロールで、Amazon ECS が ECS タスクにアタッチされた Amazon EBS ボリュームを管理できる ECS インフラストラクチャロールとして使用されることを目的としています。	2024 年 8 月 13 日
新しく、AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity ポリシーを追加しました。	新しく、AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity ポリシーを追加しました。これは AWS KMS、AWS Private Certificate Authority、Secrets Manager に管理アクセスを付与し、Amazon ECS Service Connect TLS 機能が正常に動作できるようにするものです。	2024 年 1 月 22 日

変更	説明	日付
新しいポリシー AmazonECSInfrastructureRolePolicyForVolumes を追加しました。	AmazonECSInfrastructureRolePolicyForVolumes ポリシーが追加されました。このポリシーにより、Amazon ECS が AWS API コールを行い、Amazon ECS ワークロードに関連付けられた Amazon EBS ボリュームを管理するために必要な権限が付与されます。	2024 年 1 月 11 日
AmazonECSServiceRolePolicy にアクセス許可を追加する	AmazonECSServiceRolePolicy マネージド IAM ポリシーが更新され、新しい events アクセス許可および、追加権限 autoscaling 、autoscaling-plans が追加されました。	2023 年 12 月 4 日
許可を AmazonEC2ContainerServiceEventsRole に追加する	AmazonECSServiceRolePolicy マネージド IAM ポリシーが AWS Cloud Map DiscoverInstancesRevision API 操作へのアクセスを許可するように更新されました。	2023 年 10 月 4 日
許可を AmazonEC2ContainerServiceforEC2Role に追加する	AmazonEC2ContainerServiceforEC2Role ポリシーが変更され、新しく作成されたクラスターと登録されたコンテナインスタンスのみに許可を制限する条件を含む ecs:TagResource 許可が追加されました。	2023 年 3 月 6 日

変更	説明	日付
the section called “AmazonECS_FullAccess” へのアクセス許可を追加する	AmazonECS_FullAccess ポリシーが変更され、elasticloadbalancing:AddTags 権限が追加されました。これには、新しく作成されたロードバランサー、ターゲットグループ、ルール、および作成されたリスナーのみにアクセス許可を制限する条件が含まれています。この権限では、既に作成されている Elastic Load Balancing リソースにタグを追加することはできません。	2023 年 1 月 4 日
Amazon ECS が変更の追跡を開始しました。	Amazon ECS が AWS 管理ポリシーの変更の追跡を開始しました。	2021 年 6 月 8 日

AWS Amazon Elastic Container Service の マネージド IAM ポリシーを段階的に廃止します。

以下の AWS 管理 IAM ポリシーは段階的に廃止されます。これらのポリシーは、更新されたポリシーに置き換えられます。ユーザーまたはロールを更新して、更新されたポリシーを使用することをお勧めします。

AmazonEC2ContainerServiceFullAccess

> **Important**
>
> AmazonEC2ContainerServiceFullAccess 管理 IAM ポリシーは、2021 年 1 月 29 日に段階的に廃止されました。これは、iam:passRole 許可で発見されたセキュリティへの対応です。このアクセス許可は、アカウント内のロールへの認証情報を含むすべてのリソースへのアクセスを許可します。ポリシーが廃止されると、新しいユーザーまたはロールにポリシーをアタッチできなくなります。ポリシーがアタッチされているユーザーまたは

ロールは、そのポリシーを引き続き使用できます。ただし、ユーザーまたはロールを更新して、AmazonECS_FullAccess 管理ポリシーを代わりに使用することをお勧めします 詳細については、「AmazonECS_FullAccess 管理ポリシーへの移行」を参照してください。

AmazonEC2ContainerServiceRole

> **Important**
>
> AmazonEC2ContainerServiceRole マネージド IAM ポリシーは段階的に廃止されます。これで Amazon ECS サービスリンクロールに置き換えられます。詳細については、「Amazon ECS のサービスリンクロールの使用」を参照してください。

AmazonEC2ContainerServiceAutoscaleRole

> **Important**
>
> AmazonEC2ContainerServiceAutoscaleRole マネージド IAM ポリシーは段階的に廃止されます。これは、Amazon ECS の Application Auto Scaling サービスリンクロールに置き換えられました。詳細については、「Application Auto Scaling ユーザーガイド」の「Application Auto Scaling 用のサービスリンクロール」を参照してください。

AmazonECS_FullAccess 管理ポリシーへの移行

AmazonEC2ContainerServiceFullAccess 管理 IAM ポリシーは、2021 年 1 月 29 日に段階的に廃止されました。これは、iam:passRole アクセス許可で発見されたセキュリティへの対応です。このアクセス許可は、アカウント内のロールへの認証情報を含むすべてのリソースへのアクセスを許可します。ポリシーが廃止されると、新しいグループ、ユーザー、またはロールにポリシーをアタッチできなくなります。すでにポリシーがアタッチされているグループ、ユーザー、またはロールは、引き続きそのポリシーを使用できます。ただし、グループ、ユーザー、またはロールを更新して、AmazonECS_FullAccess が管理するポリシーを代わりに使用することをお勧めします。

AmazonECS_FullAccess によって付与される許可には、ECS を管理者として使用するために必要なアクセス許可の完全なリストが含まれます。AmazonECS_FullAccess ポリシーにはない AmazonEC2ContainerServiceFullAccess ポリシーによって付与されているアクセス許可を現

在使用している場合、それらをインラインポリシーステートメントに追加できます。詳細については、「Amazon Elastic Container Service に関する AWS 管理ポリシー」を参照してください。

現在 AmazonEC2ContainerServiceFullAccess 管理 IAM ポリシーを使用しているグループ、ユーザー、またはロールがあるかを判断するには、次のステップを使用します。次に、これらのポリシーを更新して以前のポリシーをデタッチし、AmazonECS_FullAccess ポリシーをアタッチします。

AmazonECS_FullAccess ポリシーを使用するようにグループ、ユーザー、またはロールを更新するには (AWS Management Console)

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで [Policies] を選択し、AmazonEC2ContainerServiceFullAccess ポリシーを検索して選択します。
3. [Policy usage (ポリシーの使用)] タブを選択すると、現在このポリシーを使用している IAM ロールが表示されます。
4. 現在 AmazonEC2ContainerServiceFullAccess ポリシーを使用している IAM ロールごとに、ロールを選択し、次の手順を使用して段階的廃止されるポリシーをデタッチし、AmazonECS_FullAccess ポリシーをアタッチします。

    a. [Permissions] (許可) タブで、AmazonEC2ContainerServiceFullAccess ポリシーの横にある X を選択します。

    b. [Add permissions (許可の追加)] を選択します。

    c. [Attach existing policies directly] を選択し、AmazonECS_FullAccess ポリシーを検索してクリックして、[Next: Review] を選択します。

    d. 変更を確認し、[Add permissions] を選択します。

    e. AmazonEC2ContainerServiceFullAccess ポリシーを使用しているグループ、ユーザー、またはロールごとに、これらの手順を繰り返します。

AmazonECS_FullAccess ポリシーを使用するようにグループ、ユーザー、またはロールを更新するには (AWS CLI)

1. generate-service-last-accessed-details コマンドを使用して、段階的に廃止されたポリシーが最後に使用された日時に関する詳細を含むレポートを生成します。

```
aws iam generate-service-last-accessed-details \
```

```
    --arn arn:aws:iam::aws:policy/AmazonEC2ContainerServiceFullAccess
```

出力例:

```
{
    "JobId": "32bb1fb0-1ee0-b08e-3626-ae83EXAMPLE"
}
```

2. get-service-last-accessed-details コマンドを使用して、前回の出力のジョブ ID を指定すると、サービスの最終アクセスレポートを取得できます。このレポートには、段階的に廃止されたポリシーを最後に使用した IAM エンティティの Amazon リソースネーム (ARN) が表示されます。

```
aws iam get-service-last-accessed-details \
    --job-id 32bb1fb0-1ee0-b08e-3626-ae83EXAMPLE
```

3. グループ、ユーザー、またはロールから AmazonEC2ContainerServiceFullAccess ポリシーをデタッチするには、次のコマンドのいずれかを使用します。

   - detach-group-policy
   - detach-role-policy
   - detach-user-policy

4. AmazonECS_FullAccess ポリシーをグループ、ユーザー、またはロールにアタッチするには、次のコマンドのいずれかを使用します。

   - attach-group-policy
   - attach-role-policy
   - attach-user-policy

Amazon ECS のサービスリンクロールの使用

Amazon Elastic Container Service は、AWS Identity and Access Management (IAM) のサービスにリンクされたロールを使用します。サービスリンクロールは、Amazon ECS に直接リンクされた特殊なタイプの IAM ロールです。サービスリンクロールは Amazon ECS によって事前に定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要な、すべての許可が含まれています。

サービスにリンクされたロールを使用すると、必要な許可を手動で追加する必要がないため、Amazon ECS のセットアップが簡単になります。サービスリンクロールの許可は Amazon ECS

が定義し、特に定義されない限り、Amazon ECS 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サポートする他のサービスについては、「IAM と連動する AWS のサービス」を参照し、[Service-linked role (サービスリンクロール)] の列内で [Yes (はい)] と表記されたサービスを確認してください。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、[Yes] (はい) リンクを選択します。

Amazon ECS のサービスリンクロール許可

Amazon ECS は、[AWSServiceRoleForECS] 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。

サービスにリンクされたロール AWSServiceRoleForECS は、次のサービスを信頼してロールを引き受けます。

- `ecs.amazonaws.com`

AmazonECSServiceRolePolicy という名前のロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを Amazon ECS に許可します。

- アクション: `awsvpc` Amazon ECS タスクのネットワークモードを使用する場合、Amazon ECS はタスクに関連するエラスティックネットワークインターフェイスのライフサイクルを管理します。これには、Amazon ECS がエラスティックネットワークインターフェイスに追加するタグも含まれます。
- アクション: Amazon ECS サービスでロードバランサーを使用する場合、Amazon ECS は、ロードバランサーへのリソースの登録と登録解除を管理します。
- アクション: Amazon ECS サービス検出を使用する場合、Amazon ECS は必要な Route 53 を管理し、AWS Cloud Map サービス検出が機能するためのリソース
- アクション: Amazon ECS サービスのオートスケーリングを使用する場合、Amazon ECS は必要な Auto Scaling リソースを管理します。
- アクション: Amazon ECS は、Amazon ECS リソースのモニタリングに役立つ CloudWatch アラームとログストリームを作成および管理します。
- アクション: Amazon ECS Exec を使用する場合、Amazon ECS Exec セッションを開始するために必要なタスクへのアクセス権限は Amazon ECS が管理します。

- アクション: Amazon ECS Service Connect を使用する場合、その機能を使用するために必要な AWS Cloud Map リソースは Amazon ECS が管理します。
- アクション: Amazon ECS キャパシティープロバイダーを使用する場合、Auto Scaling グループとその Amazon EC2 インスタンスを変更するために必要なアクセス権限は Amazon ECS が管理します。

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 User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスにリンクされたロールのアクセス権限) を参照してください。

Amazon ECS のサービスリンクロールの作成

ほとんどの場合、サービスにリンクされた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 でクラスターを作成したり、サービスを作成または更新したりすると、Amazon ECS によってサービスにリンクされたロールが自動的に作成されます。クラスターを作成した後に AWSServiceRoleForECS ロールが表示されない場合は、以下を実行して問題を解決してください。

- Amazon ECS がユーザーに代わってサービスにリンクされたロールを作成、編集、または削除できるようにするためのアクセス許可を確認して設定します。詳細については、 IAM ユーザーガイド の「サービスリンクロールのアクセス許可」を参照してください。
- クラスター作成操作を再試行するか、サービスにリンクされたロールを手動で作成してください。

  IAM コンソールを使用して、AWSServiceRoleForECS サービスにリンクされたロールを作成できます。AWS CLI または AWS API では、`ecs.amazonaws.com` サービス名を使用してサービスにリンクされたロールを作成します。詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。

> **Important**
>
> このサービスリンク役割はこの役割でサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。

このサービスリンク役割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役割を再作成できます。クラスターを作成したり、サービスを作成または更新したりすると、Amazon ECS によってサービスにリンクされたロールが自動的に作成されます。

このサービスにリンクされたロールを削除する場合、この同じ IAM プロセスを使用して、もう一度ロールを作成できます。

Amazon ECS のサービスリンクロールの編集

Amazon ECS では、AWSServiceRoleForECS サービスリンクロールを編集できません。サービスにリンクされた役割を作成すると、多くのエンティティによって役割が参照される可能性があるため、役割名を変更することはできません。ただし、IAM を使用した役割の説明の編集はできます。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を更新する」を参照してください。

Amazon ECS のサービスリンクロールの削除

サービスリンク役割が必要な機能またはサービスが不要になった場合にはその役割を削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守さ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、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除しようとしたときに Amazon ECS サービスがロールを使用している場合は、削除が失敗する可能性があります。失敗した場合は数分待ってから操作を再試行してください。

サービスにリンクされたロールがアクティブなセッションを持っているかどうかを確認するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. ナビゲーションペインで、[Roles] (ロール) を選択し、AWSServiceRoleForECS の名前を選択します。(チェックボックスではなく)
3. Summary] (概要) ページで Access Advisor] (アクセスアドバイザー) を選択し、サービスにリンクされたロールの最新のアクティビティを確認します。

> **Note**
>
> Amazon ECS が AWSServiceRoleForECS ロールを使用しているかどうか不明な場合は、ロールを削除してみてください。サービスがロールを使用している場合、削除は失敗し、ロールが使用されているリージョンを表示できます。ロールが使用されている場合は、ロールを削除する前にセッションが終了するのを待つ必要があります。サービスにリンクされたロールのセッションを取り消すことはできません。

AWSServiceRoleForECS サービスリンクロールが使用している Amazon ECS リソースを削除するには

AWSServiceRoleForECS ロールを削除する前に、AWS リージョンすべての Amazon ECS クラスターを削除する必要があります。

1. すべての Amazon ECS サービスをすべてのリージョンで必要数 0 に縮小してから、サービスを削除します。詳細については、コンソールを使用した Amazon ECS サービスの更新およびコンソールを使用して Amazon ECS サービスの削除を参照してください。
2. すべてのリージョンですべてのクラスターからすべてのコンテナインスタンスを登録解除します。詳細については、「Amazon ECS コンテナインスタンスの登録を解除する」を参照してください。
3. すべてのリージョンですべての Amazon ECS クラスターを削除します。詳細については、「Amazon ECS クラスターを削除する」を参照してください。

サービスリンクロールを IAM で手動削除するには

IAM コンソール、AWS CLI、または AWS API を使用して、サービスにリンクされたロールである AWSServiceRoleForECS 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。

Amazon ECS サービスリンクロールがサポートされるリージョン

Amazon ECS 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ます。詳細については、「AWS リージョンとエンドポイント」を参照してください。

Amazon ECS の IAM ロール

IAM ロールは、特定の許可があり、 アカウントで作成できる IAM アイデンティティです。Amazon ECS では、コンテナやサービスなどの Amazon ECS リソースにアクセス許可を付与するロールを作成できます。

Amazon ECS が必要とするロールは、タスク定義の起動タイプと使用する機能によって異なります。次の表を参照して、Amazon ECS に必要な IAM ロールを決定します。

ロール	定義	必要な場合	詳細情報
タスク実行ロール	このロールにより、Amazon ECS がお客様に代わって他の AWS サービスを利用できるようにします。	タスクは AWS Fargate または外部インスタンスホストされています。また、 • Amazon ECR プライベートリポジトリからコンテナイメージをプルします。 • タスクを実行するアカウントとは別のアカウントの Amazon ECR プライベートリポジトリからコンテナイメージをプルします。 • `awslogs` ログドライバーを使用して CloudWatch Logs にコンテナログを送信します。 タスクは、AWS Fargate または	Amazon ECS タスク実行IAM ロール

ロール	定義	必要な場合	詳細情報
		Amazon EC2 インスタンスでホストされています。また、 • プライベートレジストリの認証を使用します。 • Runtime Monitoring を使用します。 • タスク定義は、Secrets Manager のシークレットまたは AWS Systems Manager Parameter Store のパラメータを使用して機密データを参照します。	
タスクロール	このロールにより、(コンテナ上の) アプリケーションコードが他の AWS サービスを使用できるようになります。	アプリケーションは、Amazon S3 などの他の AWS サービスにアクセスします。	Amazon ECS タスクの IAM ロール
コンテナインスタンスのロール	このロールにより、EC2 インスタンスまたは外部インスタンスをクラスターに登録できます。	タスクは Amazon EC2 インスタンスまたは外部インスタンスでホストされています。	Amazon ECS コンテナインスタンスの IAM ロール

ロール	定義	必要な場合	詳細情報
Amazon ECS Anywhere ロール	このロールにより、外部インスタンスが AWS API にアクセスできるようになります。	タスクは外部インスタンスでホストされています。	Amazon ECS Anywhere IAM ロール
Amazon ECS CodeDeploy ロール	このロールにより、CodeDeploy はサービスを更新できます。	CodeDeploy のブルー/グリーンデプロイタイプを使用して、サービスをデプロイします。	Amazon ECS CodeDeploy IAM ロール
Amazon ECS EventBridge ロール	このロールにより、EventBridge はサービスを更新できます。	EventBridge のルールとターゲットを使用してタスクをスケジュールします。	Amazon ECS EventBridge IAM ロール

ロール	定義	必要な場合	詳細情報
Amazon ECS インフラストラクチャロール	このロールにより、Amazon ECS はクラスター内のインフラストラクチャリソースを管理できます。	• Amazon EBS ボリュームを Fargate または EC2 起動タイプの Amazon ECS タスクにアタッチできます。インフラストラクチャロールにより、Amazon ECS はタスクの Amazon EBS ボリュームを管理できます。 • Amazon ECS Service Connect サービス間のトラフィックを暗号化するには、Transport Layer Security (TLS) を使用します。 • VPC Lattice ターゲットグループを作成する場合。	Amazon ECS インフラストラクチャ IAM ロール

Amazon ECS での IAM ロールのベストプラクティス

タスクロールを割り当てることをお勧めします。このロールは、それが実行されている Amazon EC2 インスタンスのロールと区別することができます。各タスクにロールを割り当てることは、最小権限アクセスの原則に沿っており、アクションとリソースをよりきめ細かく制御できます。

タスクに IAM ロールを割り当てるときは、次の信頼ポリシーを使用して、EC2 インスタンスが使用する IAM ロールとは異なるロールを各タスクが引き受けるようにする必要があります。この方法では、タスクは EC2 インスタンスのロールを継承しません。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ecs-tasks.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

タスクロールをタスク定義に追加すると、Amazon ECS コンテナエージェントはタスク用の固有の認証情報 ID (例: 12345678-90ab-cdef-1234-567890abcdef) を持つトークンを自動的に作成します。その後、このトークンとロール認証情報はエージェントの内部キャッシュに追加されます。エージェントは、コンテナ内の環境変数 AWS_CONTAINER_CREDENTIALS_RELATIVE_URI に認証情報 ID の URI (例: /v2/credentials/12345678-90ab-cdef-1234-567890abcdef) を入力します。

Amazon ECS コンテナエージェントの IP アドレスに環境変数を追加し、結果の文字列に対して curl コマンドを実行することで、コンテナ内から一時的なロール認証情報を手動で取得できます。

```
curl 169.254.170.2$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI
```

予想される出力は次のようになります。

```
{
 "RoleArn": "arn:aws:iam::123456789012:role/SSMTaskRole-SSMFargateTaskIAMRole-
DASWWSF2WGD6",
 "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
 "Token": "IQoJb3JpZ2luX2VjEEM/Example==",
 "Expiration": "2021-01-16T00:51:53Z"
}
```

新しいバージョンの AWS SDK では、AWS API 呼び出しを行うと、これらの認証情報が AWS_CONTAINER_CREDENTIALS_RELATIVE_URI 環境変数から自動的に取得されます。認証情報を更新する方法については、rePost の「AWS 認証情報の更新」を参照してください。

出力には、シークレットアクセスキー ID で構成されるアクセスキーペアと、アプリケーションが AWS リソースにアクセスするために使用するシークレットキーが含まれます。また、認証情報が有効であることを確認するために AWS が使用するトークンも含まれています。デフォルトでは、タスクロールを使用してタスクに割り当てられた認証情報は6 時間有効です。その後は、Amazon ECS コンテナエージェントによって自動的にローテーションされます。

タスク実行ロール

タスク実行ロールは、ユーザーに代わって特定の AWS API アクションを呼び出すためのアクセス許可を Amazon ECS コンテナエージェントに付与するのに使用されます。たとえば、AWS Fargate を使用する場合、Fargate には Amazon ECR からイメージをプルして CloudWatch Logs にログを書き込むことができる IAM ロールが必要です。IAM ロールは、イメージプルシークレットなど、AWS Secrets Manager に保存されているシークレットをタスクが参照する場合にも必要です。

> **Note**
>
> 認証されたユーザーとしてイメージをプルする場合、Docker Hub のプルレート制限が変更されても、影響を受ける可能性は低くなります。詳細については、「コンテナインスタンスのプライベートレジストリの認証」を参照してください。
> Amazon ECR と Amazon ECR パブリックを使用することで、Docker によって課せられる制限を回避できます。Amazon ECR からイメージをプルすると、ネットワークのプル時間を短縮し、トラフィックが VPC を離れる際のデータ転送の変更を減らすのにも役立ちます。

> **Important**
>
> Fargate を使用するときは、`repositoryCredentials` を使用してプライベートイメージレジストリの認証を行う必要があります。Amazon ECS コンテナエージェントの環境変数である `ECS_ENGINE_AUTH_TYPE` および `ECS_ENGINE_AUTH_DATA` を設定したり、Fargate でホストされているタスクの `ecs.config` ファイルを変更したりすることはできません。詳細については、「タスクのプライベートレジストリの認証」を参照してください。

コンテナインスタンスのロール

`AmazonEC2ContainerServiceforEC2Role` 管理 IAM ポリシーには以下のアクセス許可が含まれています。最小権限を付与する標準のセキュリティアドバイスに従って、`AmazonEC2ContainerServiceforEC2Role` 管理ポリシーをガイドとして使用できます。

ユースケースの管理ポリシーで付与されているアクセス許可が不要な場合、カスタムポリシーを作成し、必要なアクセス許可のみを追加します。

- `ec2:DescribeTags` – (任意) Amazon EC2 インスタンスに関連付けられているタグをプリンシパルが記述できるようになります。このアクセス許可は、リソースタグの伝播をサポートするために Amazon ECS コンテナエージェントによって使用されます。詳細については、「リソースのタグ付け方法」を参照してください。
- `ecs:CreateCluster` – (任意) プリンシパルが Amazon ECS クラスターを作成できるようになります。このアクセス許可は、Amazon ECS コンテナエージェントによって `default` クラスターが存在しない場合、このクラスタを作成するために使用されます。
- `ecs:DeregisterContainerInstance` – (任意) プリンシパルがクラスターから Amazon ECS コンテナインスタンスを登録解除できるようになります。Amazon ECS コンテナエージェントはこの API 操作を呼び出しませんが、このアクセス許可は後方互換性を確保するために維持されます。
- `ecs:DiscoverPollEndpoint` – (必須) このアクションは、Amazon ECS コンテナエージェントが更新のポーリングに使用するエンドポイントを返します。
- `ecs:Poll` – (必須) Amazon ECS コンテナエージェントが Amazon ECS コントロールプレーンと通信し、タスクの状態の変更を報告できるようになります。
- `ecs:RegisterContainerInstance` – (必須) プリンシパルがコンテナインスタンスをクラスターに登録できるようになります。このアクセス許可は、Amazon ECS コンテナエージェントが Amazon EC2 インスタンスをクラスターに登録し、リソースタグの伝播をサポートするために使用されます。
- `ecs:StartTelemetrySession` – (任意) Amazon ECS コンテナエージェントが Amazon ECS コントロールプレーンと通信し、各コンテナおよびタスクのヘルス情報とメトリクスをレポートできるようになります。

  このアクセス許可は必須ではありませんが、コンテナインスタンスのメトリクスがスケールアクションを開始できるようにし、ヘルスチェックコマンドに関連するレポートを受信できるようにするために、これを追加することをお勧めします。
- `ecs:TagResource` – (任意) Amazon ECS コンテナエージェントが、作成時にクラスターにタグ付けしたり、コンテナインスタンスがクラスターに登録されたときにタグ付けしたりできるようになります。
- `ecs:UpdateContainerInstancesState` — プリンシパルが Amazon ECS コンテナインスタンスのステータスを変更できるようにします。このアクセス許可は、スポットインスタンスのドレイン用に Amazon ECS コンテナエージェントによって使用されます。

- ecs:Submit* – (必須) これには API アクション SubmitAttachmentStateChanges、SubmitContainerStateChange、および SubmitTaskStateChange が含まれています。これらは、Amazon ECS コンテナエージェントによって使用され、各リソースの状態変化を Amazon ECS コントロールプレーンに報告します。SubmitContainerStateChange アクセス許可は、Amazon ECS コンテナエージェントによって使用されなくなりますが、後方互換性を確保するために維持されます。
- ecr:GetAuthorizationToken – (オプション) プリンシパルに認可トークンの取得を許可します。認可トークンは IAM 認証情報を表し、IAM プリンシパルによってアクセスされる Amazon ECR レジストリへのアクセスに使用できます。受け取る認可トークンは 12 時間有効です。
- ecr:BatchCheckLayerAvailability – (任意) コンテナイメージが Amazon ECR プライベートリポジトリにプッシュされると、各イメージレイヤーに対してすでにプッシュされているかどうかが確認されます。その場合、そのイメージレイヤーはスキップされます。
- ecr:GetDownloadUrlForLayer – (任意) コンテナイメージが Amazon ECR プライベートリポジトリからプルされると、この API が、まだキャッシュされていない各イメージレイヤーに対して 1 回呼び出されます。
- ecr:BatchGetImage – (任意) コンテナイメージが Amazon ECR プライベートリポジトリからプルされると、この API が 1 回呼び出されてイメージマニフェストが取得されます。
- logs:CreateLogStream – (任意) プリンシパルが、指定したロググループの CloudWatch Logs ログストリームを作成できるようになります。
- logs:PutLogEvents – (任意) プリンシパルが、指定したログストリームにログイベントのバッチをアップロードできるようになります。

次のポリシーは必須のアクセス許可を含んでいます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecs:DiscoverPollEndpoint",
                "ecs:Poll",
                "ecs:RegisterContainerInstance",
                "ecs:UpdateContainerInstancesState",
                "ecs:Submit*"
            ],
            "Resource": "*"
```

```
        }
    ]
}
```

サービスにリンクされた役割

Amazon ECS のサービス連動ロールを使用して、Amazon ECS サービスに他のサービス API を代理で呼び出す許可を付与できます。Amazon ECS には、ネットワークインターフェイスの作成と削除、ターゲットグループへのターゲットの登録と登録解除を行う許可が必要です。また、スケーリングポリシーの作成と削除に必要な許可も必要です。これらの許可は、サービスにリンクされたロールによって付与されます。このロールは、サービスを初めて使用するときに、ユーザーに代わって作成されます。

> **Note**
>
> サービスにリンクされたロールを誤って削除してしまった場合は、ロールを再作成できます。手順については、「サービスにリンクされたロールの作成」を参照してください。

ロールの推奨事項

タスクの IAM ロールとポリシーを設定するときは、以下を行うことをお勧めします。

Amazon EC2 メタデータへのアクセスをブロックする

Amazon EC2 インスタンスでタスクを実行する場合、Amazon EC2 メタデータへのアクセスをブロックして、それらのインスタンスに割り当てられたロールをコンテナが継承しないようにすることを強くお勧めします。アプリケーションが AWS API アクションを呼び出す必要がある場合は、代わりに IAM ロールをタスクに使用してください。

ブリッジモードで実行されているタスクが Amazon EC2 メタデータにアクセスしないようにするには、次のコマンドを実行するか、インスタンスのユーザーデータを更新します。インスタンスのユーザーデータを更新する方法の詳細については、このAWS サポート記事を参照してください。タスク定義ブリッジモードについて詳しくは、「タスク定義ネットワークモード」を参照してください。

```
sudo yum install -y iptables-services; sudo iptables --insert FORWARD 1 --in-interface
 docker+ --destination 169.254.169.254/32 --jump DROP
```

再起動後もこの変更が持続するようにするには、Amazon マシンイメージ (AMI) 固有の次のコマンドを実行します。

- Amazon Linux 2

```
sudo iptables-save | sudo tee /etc/sysconfig/iptables && sudo systemctl enable --now
 iptables
```

- Amazon Linux

```
sudo service iptables save
```

awsvpc ネットワークモードを使用するタスクでは、/etc/ecs/ecs.config ファイル内の環境変数 ECS_AWSVPC_BLOCK_IMDS を true に設定します。

host ネットワーク内で実行されているコンテナが Amazon EC2 メタデータにアクセスできないように、ecs-agent config ファイルの ECS_ENABLE_TASK_IAM_ROLE_NETWORK_HOST 変数を false に設定する必要があります。

awsvpc ネットワークモードを使用する

awsvpc ネットワークモードを使用して、異なるタスクの間、またはタスクと Amazon VPC 内で実行される他のサービスとの間のトラフィックの流れを制限します。これにより、セキュリティの追加レイヤーが追加されます。awsvpc ネットワークモードは、Amazon EC2 で実行されるタスクをタスクレベルでネットワーク分離します。これは AWS Fargate のデフォルトモードであり、タスクにセキュリティグループを割り当てるのに使用できる唯一のネットワークモードです。

最終アクセス時間情報を使用してロールを絞り込む

一度も使用されていないか、しばらく使用されていないアクションは、削除することをお勧めします。そうすることで、望ましくないアクセスが発生するのを防ぐことができます。これを行うには、IAM によって提供される最終アクセス時間情報を確認し、使用されたことがない、または最近使用されていないアクションを削除します。これを行うには、次のステップに従ってください。

次のコマンドを実行して、参照されたポリシーの最終アクセス情報を示すレポートを生成します。

```
aws iam generate-service-last-accessed-details --arn arn:aws:iam::123456789012:policy/
ExamplePolicy1
```

出力に表示されていた JobId を使用して、次のコマンドを実行します。これを実行すると、レポートの結果を表示できます。

```
aws iam get-service-last-accessed-details --job-id 98a765b4-3cde-2101-2345-example678f9
```

詳細については、「最終アクセス情報を使用して AWS のアクセス許可を調整する」を参照してください。

AWS CloudTrail に不審なアクティビティがないか監視する

AWS CloudTrail に不審なアクティビティがないか監視することができます。ほとんどの AWS API 呼び出しは AWS CloudTrail イベントとして記録されます。これらは AWS CloudTrail Insights によって分析され、`write` API 呼び出しに関連する疑わしい動作があればアラートが表示されます。これには、呼び出しの急増が含まれる場合があります。これらのアラートには、異常なアクティビティが発生した時間や、API に寄与した上位のアイデンティティ ARN などの情報が含まれます。

IAM ロールが割り当てられているタスクが実行するアクションは、AWS CloudTrail でイベントの `userIdentity` プロパティを調べることで特定できます。次の例では、`arn` に引き受けたロールの名前 `s3-write-go-bucket-role` が含まれ、その後にタスクの名前 `7e9894e088ad416eb5cab92afExample` が続きます。

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA36C6WWEJ2YEXAMPLE:7e9894e088ad416eb5cab92afExample",
    "arn": "arn:aws:sts::123456789012:assumed-role/s3-write-go-bucket-
role/7e9894e088ad416eb5cab92afExample",
    ...
}
```

> **Note**
>
> ロールを引き受けるタスクが Amazon EC2 コンテナインスタンスで実行されると、リクエストは Amazon ECS コンテナエージェントによって、`/var/log/ecs/audit.log.YYYY-MM-DD-HH` フォーマットのアドレスにあるエージェントの監査ログに記録されます。詳細については、「タスクの IAM ロール ログ」と「証跡のインサイトイベントの記録」を参照してください。

Amazon ECS タスク実行IAM ロール

タスク実行ロールは、ユーザーに代わって AWS API コールを実行するためのアクセス許可を Amazon ECS コンテナと Fargate エージェントに付与します。タスク実行 IAM ロールは、タスクの

要件に応じて必要です。さまざまな目的とサービスのタスク実行ロールを、アカウントに複数関連付けることができます。

> **Note**
>
> これらのアクセス許可は、タスク内のコンテナからはアクセスできません。アプリケーションの実行に必要な IAM 許可については、「Amazon ECS タスクの IAM ロール」を参照してください。

以下に示しているのは、タスク実行 IAM ロールの一般的なユースケースです。

- タスクは AWS Fargate または外部インスタンスでホストされています。また、
  - Amazon ECR プライベートリポジトリからコンテナイメージをプルします。
  - タスクを実行するアカウントとは別のアカウントの Amazon ECR プライベートリポジトリからコンテナイメージをプルします。
  - `awslogs` ログドライバーを使用して CloudWatch Logs にコンテナログを送信します。詳細については、「Amazon ECS ログを CloudWatch に送信する 」を参照してください。
- タスクは、AWS Fargate または Amazon EC2 インスタンスでホストされています。また、
  - プライベートレジストリの認証を使用します。詳細については、「プライベートレジストリ認証のアクセス許可」を参照してください。
  - Runtime Monitoring を使用します。
  - タスク定義は、Secrets Manager のシークレットまたは AWS Systems Manager Parameter Store のパラメータを使用して機密データを参照します。詳細については、「Secrets Manager または Systems Manager のアクセス許可」を参照してください。

> **Note**
>
> タスク実行ロールは Amazon ECS コンテナエージェントバージョン 1.16.0 以降でサポートされています。

Amazon ECS は、上記の一般的なユースケースに必要なアクセス許可を含む、AmazonECSTaskExecutionRolePolicy という管理ポリシーを提供しています。詳細については、「AWS Managed Policy リファレンスガイド」の「AmazonECSTaskExecutionRolePolicy」を参

照してください。特殊なユースケースでは、タスク実行ロールにインラインポリシーを追加する必要がある可能性があります。

Amazon ECS コンソールで、ECS タスク実行ロールを作成します。追加の機能や機能強化が導入された場合に Amazon ECS がそのアクセス許可を追加できるように、タスクのマネージド IAM ポリシーを手動でアタッチすることができます。IAM コンソールの検索を使用して `ecsTaskExecutionRole` を検索すると、アカウントにすでにタスク実行ロールがあるかどうかを確認できます。詳細については、IAM ユーザーガイドの「IAM コンソールの検索」を参照してください。

認証されたユーザーとしてイメージをプルすると、Docker Hub のプルレート制限が変更された場合でも、影響を受ける可能性が低くなります。詳細については、「コンテナインスタンスのプライベートレジストリの認証」を参照してください。

Amazon ECR と Amazon ECR パブリックを使用することで、Docker によって課せられる制限を回避できます。Amazon ECR からイメージをプルすると、ネットワークのプル時間を短縮し、トラフィックが VPC を離れる際のデータ転送の変更を減らすのにも役立ちます。

Fargate を使用するときは、`repositoryCredentials` を使用してプライベートイメージレジストリの認証を行う必要があります。Amazon ECS コンテナエージェントの環境変数である `ECS_ENGINE_AUTH_TYPE` および `ECS_ENGINE_AUTH_DATA` を設定したり、Fargate でホストされているタスクの `ecs.config` ファイルを変更したりすることはできません。詳細については、「タスクのプライベートレジストリの認証」を参照してください。

タスク実行 ロールの作成

アカウントにまだタスク実行ロールがない場合は、次のステップに従ってロールを作成します。

AWS Management Console

Elastic Container Service のサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] で [エラスティックコンテナサービス] を選択し、次に [エラスティックコンテナのサービスタスク] を選択します。
5. [Next] を選択します。

6. [アクセス許可の追加] セクションで [AmazonECSTaskExecutionRolePolicy] を検索し、ポリシーを選択します。
7. [Next] を選択します。
8. [ロール名] に [ECSTaskExecutionRole] と入力します。
9. ロールを確認したら、[ロールを作成] を選択します。

AWS CLI

すべての *[######]* は、お客様の情報で置き換えてください。

1. IAM ロールに使用する信頼ポリシーが含まれている ecs-tasks-trust-policy.json という名前のファイルを作成します。ファイルには次の内容が含まれます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ecs-tasks.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 前のステップで作成した信頼ポリシーを使用した ecsTaskExecutionRole という名前の IAM ロールを作成します。

```
aws iam create-role \
      --role-name ecsTaskExecutionRole \
      --assume-role-policy-document file://ecs-tasks-trust-policy.json
```

3. AWS 管理 AmazonECSTaskExecutionRolePolicy ポリシー ecsTaskExecutionRole をロールにアタッチします。

```
aws iam attach-role-policy \
      --role-name ecsTaskExecutionRole \
```

```
      --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonECSTaskExecutionRolePolicy
```

ロールを作成したら、次の機能のアクセス許可をロールに追加します。

機能	追加のアクセス許可
Secrets Manager の認証情報を使用してコンテナイメージのプライベートリポジトリにアクセスする	プライベートレジストリ認証のアクセス許可
Systems Manager または Secrets Manager を使用して機密データを渡す	Secrets Manager または Systems Manager のアクセス許可
Fargate タスクが、インターネットエンドポイントを介して Amazon ECR イメージをプルできるようにする	インターフェイスエンドポイントのアクセス許可によって Amazon ECR イメージをプルする Fargate タスクです。
設定ファイルを Amazon S3 バケットでホストする	Amazon S3 ファイルストレージのアクセス許可
Amazon ECS ライフサイクルイベントを表示するように Container Insights を設定する	Amazon ECS ライフサイクルイベントを表示するには、Container Insights を設定するために必要なアクセス権限が必要です。
Container Insights に Amazon ECS ライフサイクルイベントを表示する	Amazon ECS ライフサイクルイベントを Container Insights で表示するには、以下のアクセス許可が必要です。

プライベートレジストリ認証のアクセス許可

作成したシークレットにアクセスできるようにするには、以下のアクセス許可を、インラインポリシーとしてタスクの実行ロール追加します。詳細については、「IAM ポリシーの追加と削除」を参照してください。

- `secretsmanager:GetSecretValue`

- `kms:Decrypt` - カスタムの KMS キーを使用するが、デフォルトのキーは使用しない場合にのみ必須。カスタムキーの Amazon リソースネーム (ARN) は、リソースとして追加する必要があります。

次の例では、インラインポリシーによりアクセス許可を追加しています。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
                "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
            ]
        }
    ]
}
```

Secrets Manager または Systems Manager のアクセス許可

コンテナエージェントが必要な AWS Systems Manager または Secrets Manager のリソースをプルできるようにするためのアクセス許可です。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。

Secrets Manager の使用

作成した Secrets Manager シークレットにアクセスできるようにするには、タスクの実行ロールに対し、以下のアクセス許可を手動により追加します。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 ID のアクセス許可の追加および削除」を参照してください。

- `secretsmanager:GetSecretValue` – Secrets Manager シークレットを参照する場合に必須です。Secrets Manager からシークレットを取得するための許可を追加します。

次のポリシーの例では、必須のアクセス許可を追加します。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name"
      ]
    }
  ]
}
```

Systems Manager の使用

> **Important**
>
> EC2 起動タイプを使用するタスクの場合、この機能を使用するには ECS エージェント設定変数 `ECS_ENABLE_AWSLOGS_EXECUTIONROLE_OVERRIDE=true` を使用する必要があります。コンテナインスタンスの作成時に `./etc/ecs/ecs.config` ファイルに追加するか、既存のインスタンスに追加して ECS エージェントを再起動できます。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

作成した Systems Manager Parameter Store のパラメータにアクセスできるようにするには、タスク実行ロールに対し、以下のアクセス許可を手動で追加する必要があります。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 ID のアクセス許可の追加および削除」を参照してください。

- `ssm:GetParameters` – Systems Manager Parameter Store のパラメータをタスク定義で参照している場合は必須です。Systems Manager パラメータを取得するための許可を追加します。
- `secretsmanager:GetSecretValue` – Secrets Manager シークレットをユーザーが直接参照している、あるいは、Systems Manager Parameter Store のパラメータが、タスク定義で Secrets Manager シークレットを参照している場合は必須です。Secrets Manager からシークレットを取得するための許可を追加します。
- `kms:Decrypt` – シークレットが、デフォルトのキーではなく、カスタマーマネージドのキーを使用している場合にのみ必須です。そのカスタムキーの ARN はリソースとして追加されている必要があります。カスタマーマネージドキーを復号するための許可を追加します。

次の例のポリシーでは、必須のアクセス許可を追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:ssm:region:aws_account_id:parameter/parameter_name",
        "arn:aws:secretsmanager:region:aws_account_id:secret:secret_name",
        "arn:aws:kms:region:aws_account_id:key/key_id"
      ]
    }
  ]
}
```

インターフェイスエンドポイントのアクセス許可によって Amazon ECR イメージをプルする Fargate タスクです。

Amazon ECR がインターフェイス VPC エンドポイントを使用するように設定されているときに、Amazon ECR からイメージをプルする Fargate 起動タイプを使用するタスクを起動するときは、特定の VPC または VPC エンドポイントへのアクセスにタスクを制限できます。この操作を行うには、IAM 条件キーを使用するタスクのタスク実行ロールを作成します。

次の IAM グローバル条件キーを使用して、特定の VPC または VPC エンドポイントへのアクセスを制限します。詳細については、「AWSvグローバル条件コンテキストキー」を参照してください。

- `aws:SourceVpc` - 特定の VPC へのアクセスを制限します。タスクとエンドポイントをホストする VPC に制限できます。
- `aws:SourceVpce` - 特定の VPC エンドポイントへのアクセスを制限します。

次のタスク実行ロールポリシーは、条件キーを追加する方法の例を示しています。

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

```
        {
            "Effect": "Allow",
            "Action": [
                "ecr:GetAuthorizationToken",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:GetDownloadUrlForLayer",
                "ecr:BatchGetImage"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpce": "vpce-xxxxxx",
                    "aws:sourceVpc": "vpc-xxxxx"
                }
            }
        }
    ]
}
```

Amazon S3 ファイルストレージのアクセス許可

Amazon S3 でホストされる設定ファイルを指定する場合、タスク実行ロールには、設定ファイルに対する `s3:GetObject` アクセス許可と、ファイルが格納されている Amazon S3 バケットでの `s3:GetBucketLocation` アクセス許可が含まれている必要があります。詳細については、「Amazon Simple Storage Service ユーザーガイド」の「Amazon S3 のポリシーアクション」を参照してください。

次のポリシーの例では、Amazon S3 からファイルを取得するために必要なアクセス許可を追加します。Amazon S3 バケットの名前と設定ファイル名を指定します。

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

```
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/folder_name/config_file_name"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket"
      ]
    }
  ]
}
```

Amazon ECS ライフサイクルイベントを表示するには、Container Insights を設定するために必要なアクセス権限が必要です。

ライフサイクルイベントを設定するには、タスクロールで以下のアクセス許可が必要です。

- events:PutRule
- events:PutTargets
- logs:CreateLogGroup

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "events:PutRule",
        "events:PutTargets",
        "logs:CreateLogGroup"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

Amazon ECS ライフサイクルイベントを Container Insights で表示するには、以下のアクセス許可が必要です。

ライフサイクルイベントを表示するには、以下のアクセス権限が必要です。次のアクセス許可をインラインポリシーとしてタスク実行ロールに追加します。詳細については、「IAM ポリシーの追加と削除」を参照してください。

- events:DescribeRule
- events:ListTargetsByRule
- logs:DescribeLogGroups

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "events:DescribeRule",
        "events:ListTargetsByRule",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon ECS タスクの IAM ロール

Amazon ECS タスクには IAM ロールを関連付けることができます。IAM ロールで付与される許可は、タスクで実行されているコンテナによって引き受けられます。このロールにより、(コンテナ上の) アプリケーションコードが他の AWS サービスを使用できるようになります。タスクロールは、アプリケーションが Amazon S3 などの他の AWS サービスにアクセスするときに必要です。

> **Note**
>
> これらのアクセス許可は、Amazon ECS コンテナと Fargate エージェントからはアクセスされません。Amazon ECS がコンテナイメージをプルしてタスクを実行するために必要な IAM 許可については、「Amazon ECS タスク実行IAM ロール」を参照してください。

タスクロールを使用する利点は次のとおりです。

- 認証情報の分離: コンテナは、コンテナが属するタスク定義で定義された IAM ロールの認証情報のみを取得できます。コンテナは、別のタスクに属する別のコンテナを対象にした認証情報にアクセスすることはありません。
- 認可: 認可されていないコンテナは、他のタスク用に定義された IAM ロール認証情報にアクセスできません。
- 監査: CloudTrail にアクセスしイベントのログ記録を利用することで、遡及的な監査を確実に行えます。タスクの認証情報には、セッションにアタッチされている `taskArn` のコンテキストがあるため、CloudTrail ログではどのタスクがどのロールを使用しているかを表示できます。

> **Note**
>
> タスク用の IAM ロールを指定すると、そのタスクのコンテナ内の AWS CLI または他の SDK は、タスクロールによって提供された AWS 認証情報を排他的に使用し、Amazon EC2 または外部インスタンスで実行されていて、それらから IAM 許可を継承しなくなります。

タスクの IAM ロールを作成する

タスクで使用する IAM ポリシーを作成するときは、そのポリシーはタスクのコンテナが引き受けるタスクの許可を含める必要があります。既存の AWS マネージドポリシーを使用することも、特定のニーズを満たすカスタムポリシーを最初から作成することもできます。詳細についてはIAM ユーザーガイド の「IAM ポリシーの作成」を参照してください。

> **Important**
>
> Amazon ECS タスク (すべての起動タイプ) では、タスクに IAM ポリシーとロールを使用することをお勧めします。これらの認証情報により、タスクは `sts:AssumeRole` を呼び出してタスクに既に関連付けられているのと同じロールを引き受けることなく、AWS API リクエ

ストを行うことができます。タスクでロールがそれ自体を引き受けることが必要な場合、そのロールがそれ自体を引き受けることを明示的に許可する信頼ポリシーを作成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「ロール信頼ポリシーの更新」を参照してください。

IAM ポリシーを作成した後、Amazon ECS タスク定義で参照するポリシーを含む IAM ロールを作成できます。IAM コンソールで [Elastic Container Service Task] (Elastic Container Service タスク) ユースケースを使用してロールを作成できます。その後、タスクのコンテナに必要なアクセス許可を付与するロールに特定の IAM ポリシーをアタッチできます。次の手順では、これを行う方法について説明します。

IAM のアクセス許可を必要とする複数のタスク定義またはサービスがある場合は、各タスクに提供するアクセスを最小限に抑えるために、タスクを操作するために必要な最小限のアクセス許可で特定のタスク定義またはサービスごとにロールを作成することを検討してください。

リージョンのサービスエンドポイントの詳細については、Amazon Web Services 全般のリファレンス ガイドの「サービスエンドポイント」を参照してください。

IAM タスクロールは、`ecs-tasks.amazonaws.com` サービスを特定する信頼ポリシーが必要です。`sts:AssumeRole` 許可は、Amazon EC2 インスタンスが使用するロールとは異なる IAM ロールをタスクに引き受けられるようにします。これにより、タスクは Amazon EC2 インスタンスに関連付けられたロールを継承しません。以下に示しているのは、信頼ポリシーの例です。リージョン識別子を置き換えて、タスク起動時に使用する AWS アカウント番号を特定します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":[
               "ecs-tasks.amazonaws.com"
            ]
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "ArnLike":{
            "aws:SourceArn":"arn:aws:ecs:us-west-2:111122223333:*"
            },
            "StringEquals":{
```

```
                "aws:SourceAccount":"111122223333"
            }
         }
      }
   ]
}
```

> **Important**
>
> タスク IAM ロールを作成するときは、信頼関係またはロールに関連付けられた IAM ポリシーで aws:SourceAccount または aws:SourceArn のいずれかの条件キーを使用してアクセス許可のスコープを詳細にし、複雑な副セキュリティ問題を防止します。特定のクラスターを指定する aws:SourceArn 条件キーの使用は現在サポートされていません。ワイルドカードを使用してすべてのクラスターを指定する必要があります。混乱した代理の問題と、お客様の AWS アカウントの保護方法の詳細について学ぶためには、[The confused deputy problem] (IAM ユーザーガイド) の[IAM User Guide] (混乱した代理の問題) を参照してください。

以下の手順では、Amazon S3 からオブジェクトを取得するポリシーを作成する方法を、ポリシー例とともに説明します。すべての######を自分の値に置き換えてください。

AWS Management Console

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

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

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

```
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::my-task-secrets-bucket/*"
         ],
         "Condition":{
            "ArnLike":{
            "aws:SourceArn":"arn:aws:ecs:region:123456789012:*"
            },
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            }
         }
      }
   ]
}
```

6. [次へ] をクリックします。

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

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

AWS CLI

すべての######を自分の値に置き換えてください。

1. s3-policy.json というファイルを次の内容で作成します。

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::my-task-secrets-bucket/*"
         ],
         "Condition":{
            "ArnLike":{
            "aws:SourceArn":"arn:aws:ecs:region:123456789012:*"
            },
            "StringEquals":{
               "aws:SourceAccount":"123456789012"
            }
         }
      }
   ]
}
```

2. JSON ポリシードキュメントファイルを使用して IAM ポリシーを作成するには、次のコマンドを使用します。

```
aws iam create-policy \
      --policy-name taskRolePolicy \
      --policy-document file://s3-policy.json
```

以下の手順では、作成した IAM ポリシーをアタッチすることでタスクの IAM ロール を作成する方法を示しています。

AWS Management Console

Elastic Container Service のサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。

4. [サービスまたはユースケース] で [エラスティックコンテナサービス] を選択し、次に [エラスティックコンテナのサービスタスク] を選択します。
5. [Next] を選択します。
6. [アクセス許可の追加] で、作成したポリシーを検索し、選択します。
7. [Next] を選択します。
8. ロール名 に、ロールの名前を入力します。この例では、AmazonECSTaskS3BucketRole と入力してロールに名前を付けます。
9. ロールを確認したら、[ロールを作成] を選択します。

AWS CLI

すべての######を自分の値に置き換えてください。

1. タスク IAM ロールに使用する信頼ポリシーが含まれている ecs-tasks-trust-policy.json という名前のファイルを作成します。ファイルには次の内容が含まれます。リージョン識別子を置き換えて、タスク起動時に使用する AWS アカウント番号を特定します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":[
               "ecs-tasks.amazonaws.com"
            ]
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "ArnLike":{
            "aws:SourceArn":"arn:aws:ecs:us-west-2:111122223333:*"
            },
            "StringEquals":{
               "aws:SourceAccount":"111122223333"
            }
         }
      }
   ]
```

```
}
```

2. 前のステップで作成した信頼ポリシーを使用した ecsTaskRole という名前の IAM ロールを作成します。

```
aws iam create-role \
      --role-name ecsTaskRole \
      --assume-role-policy-document file://ecs-tasks-trust-policy.json
```

3. 次のコマンドを使用して、作成した IAM ポリシーの ARN を取得します。*taskRolePolicy* は、作成したポリシーの名前に置き換えます。

```
aws iam list-policies --scope Local --query 'Policies[?
PolicyName==`taskRolePolicy`].Arn'
```

4. 作成した IAM ポリシーを、ecsTaskRole ロールにアタッチします。policy-arn を、作成したポリシーの ARN に置き換えます。

```
aws iam attach-role-policy \
      --role-name ecsTaskRole \
      --policy-arn arn:aws:iam:111122223333:aws:policy/taskRolePolicy
```

ロールを作成したら、次の機能のアクセス許可をロールに追加します。

機能	追加のアクセス許可
ECS Exec を使用する	ECS Exec のアクセス許可
EC2 インスタンスを使用する (Windows および Linux)	Amazon EC2 インスタンスの追加設定
外部インスタンスを使用する	外部インスタンスの追加設定
EC2 Windows インスタンスを使用する	Amazon EC2 Windows インスタンスの追加設定

ECS Exec のアクセス許可

ECS Exec 機能には、マネージド型 SSM エージェント (execute-command エージェント) と SSM サービス間の通信に必要なアクセス許可をコンテナに付与するためのタスク IAM ロールが必要です。次のアクセス許可をタスク IAM ロールに追加し、タスク定義にタスク IAM ロールを含める必要があります。詳細については、IAM ユーザーガイドのIAM ポリシーの追加と削除を参照してください。

タスク IAM ロールに次のポリシーを使用して、必要な SSM アクセス許可を追加します。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
       "Effect": "Allow",
       "Action": [
            "ssmmessages:CreateControlChannel",
            "ssmmessages:CreateDataChannel",
            "ssmmessages:OpenControlChannel",
            "ssmmessages:OpenDataChannel"
       ],
      "Resource": "*"
      }
   ]
}
```

Amazon EC2 インスタンスの追加設定

コンテナインスタンスのロールの許可は、以下に提供されるマネージド型 AmazonEC2ContainerServiceforEC2Role IAM ポリシーの許可のミニマリストに制限することをお勧めします。

Amazon EC2 インスタンスは、タスクのロールを使用するために、コンテナエージェントのバージョン 1.11.0 以上が必要です。ただし、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。Amazon ECS に最適化された AMI を使用している場合、インスタンスには、ecs-init パッケージの 1.11.0-1 以降が必要です。インスタンスが最新 Amazon ECS に最適化された AMI を使用している場合、コンテナエージェントおよび ecs-init の必要なバージョンが含まれます。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

コンテナインスタンスで Amazon ECS に最適化された AMI を使用していない場合、エージェントを開始する `--net=host` コマンドと、目的の設定に次のエージェント設定変数に docker run オプションを追加してください (詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください)。

`ECS_ENABLE_TASK_IAM_ROLE=true`

`bridge` および `default` のネットワークモードに設定されたコンテナのタスク用の、IAM ロールを使用します。

`ECS_ENABLE_TASK_IAM_ROLE_NETWORK_HOST=true`

`host` ネットワークモードに設定されたコンテナのタスク用の、IAM ロールを使用します。この変数はエージェントバージョン 1.12.0 以降でのみサポートされています。

実行コマンドの例の詳細については、「Amazon ECS コンテナエージェントの手動更新 (Amazon ECS 最適化以外の AMI の場合)」を参照してください。また、タスクのコンテナが AWS 認証情報を取得できるよう、次のネットワーキングコマンドをコンテナインスタンスで設定する必要があります。

```
sudo sysctl -w net.ipv4.conf.all.route_localnet=1
sudo iptables -t nat -A PREROUTING -p tcp -d 169.254.170.2 --dport 80 -j DNAT --to-
destination 127.0.0.1:51679
sudo iptables -t nat -A OUTPUT -d 169.254.170.2 -p tcp -m tcp --dport 80 -j REDIRECT --
to-ports 51679
```

再起動後も有効にするには、コンテナインスタンスにこれらの iptables ルールを保存する必要があります。iptables-save および iptables-restore コマンドを使用して、iptables ルールを保存し、起動時にそのルールを復元します。詳細については、特定のオペレーティングシステムのドキュメントを参照してください。

`awsvpc` ネットワークモードを使用するタスクで実行されたコンテナが、Amazon EC2 のインスタンスプロファイルに入力されている認証情報にアクセスを防止するためには (タスクロールで指定されている許可は有効)、エージェントの設定 ファイルで `ECS_AWSVPC_BLOCK_IMDS` エージェント設定変数を `true` に設定し、そのエージェントを再起動します。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。

`bridge` ネットワークモードを使用するタスクで実行されたコンテナが、Amazon EC2 のインスタンスプロファイルに入力されている認証情報にアクセスを防止するためには (タスクロールで指定されている許可は有効)、Amazon EC2 インスタンスで次の iptables コマンドを実行します。このコマ

ンドは、host または awsvpc ネットワークモードを使用するタスク内のコンテナに影響を与えることはありません。詳細については、「ネットワークモード」を参照してください。

- ```
  sudo yum install -y iptables-services; sudo iptables --insert DOCKER-USER 1 --in-interface docker+ --destination 169.254.169.254/32 --jump DROP
  ```

  再起動後も有効にするには、Amazon EC2 インスタンスでこの iptables ルールを保存する必要があります。Amazon ECS に最適化された AMI を使用する場合は、次のコマンドを使用します。他のオペレーティングシステムの場合、そのオペレーティングシステムのドキュメントを参照してください。

  ```
  sudo iptables-save | sudo tee /etc/sysconfig/iptables && sudo systemctl enable --now iptables
  ```

外部インスタンスの追加設定

外部インスタンスは、タスクの IAM ロールを使用にするために、コンテナエージェントのバージョン 1.11.0 以上が必要ですが、最新のコンテナエージェントのバージョンを使用することをお勧めします。エージェントのバージョンの確認と最新バージョンへの更新については、「Amazon ECS コンテナエージェントをアップデートする」を参照してください。Amazon ECS に最適化された AMI を使用している場合、インスタンスは、1.11.0-1 パッケージの ecs-init バージョン以降が必要です。インスタンスが最新 Amazon ECS に最適化された AMI を使用している場合、コンテナエージェントおよび ecs-init の必要なバージョンが含まれます。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。

コンテナインスタンスで Amazon ECS に最適化された AMI を使用していない場合、エージェントを開始する --net=host コマンドと、目的の設定に次のエージェント設定変数に docker run オプションを追加してください (詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください)。

ECS_ENABLE_TASK_IAM_ROLE=true

bridge および default のネットワークモードに設定されたコンテナのタスク用の、IAM ロールを使用します。

ECS_ENABLE_TASK_IAM_ROLE_NETWORK_HOST=true

host ネットワークモードに設定されたコンテナのタスク用の、IAM ロールを使用します。この変数はエージェントバージョン 1.12.0 以降でのみサポートされています。
  ```

実行コマンドの例の詳細については、「Amazon ECS コンテナエージェントの手動更新 (Amazon ECS 最適化以外の AMI の場合)」を参照してください。また、タスクのコンテナが AWS 認証情報を取得できるよう、次のネットワーキングコマンドをコンテナインスタンスで設定する必要があります。

```
sudo sysctl -w net.ipv4.conf.all.route_localnet=1
sudo iptables -t nat -A PREROUTING -p tcp -d 169.254.170.2 --dport 80 -j DNAT --to-
destination 127.0.0.1:51679
sudo iptables -t nat -A OUTPUT -d 169.254.170.2 -p tcp -m tcp --dport 80 -j REDIRECT --
to-ports 51679
```

再起動後も有効にするには、コンテナインスタンスにこれらの iptables ルールを保存する必要があります。iptables-save および iptables-restore コマンドを使用して、iptables ルールを保存し、起動時にそのルールを復元します。詳細については、特定のオペレーティングシステムのドキュメントを参照してください。

Amazon EC2 Windows インスタンスの追加設定

> **Important**
>
> これは、タスクロールを使用する EC2 上にある Windows コンテナにのみ適用されます。

Windows 機能を使用するタスクロールには EC2 での追加設定が必要です。

- コンテナインスタンスを起動する際に、コンテナインスタンスのユーザーデータスクリプトの `-EnableTaskIAMRole` オプションを設定して、この機能を有効にする必要があります。`EnableTaskIAMRole`は、タスクの Task IAM ロール機能をオンにします。例:

  ```
  <powershell>
  Import-Module ECSTools
  Initialize-ECSAgent -Cluster 'windows' -EnableTaskIAMRole
  </powershell>
  ```

- Amazon ECS コンテナブートストラップスクリプト に提供されているネットワーキングコマンドを使用してコンテナをブートストラップする必要があります。
- タスク用の IAM ロールとポリシーを作成する必要があります。詳細については、「タスクの IAM ロールを作成する」を参照してください。

- タスク認証情報プロバイダーの IAM ロールは、コンテナインスタンスのポート 80 を使用します。したがって、コンテナインスタンスでタスクの IAM ロールを設定にすると、コンテナはポートマッピングのホストポートにポート 80 を使用できません。コンテナをポート 80 で公開するには、負荷分散を使用するサービスをコンテナ用に設定することをお勧めします。ロードバランサーのポート 80 を使用できます。これにより、コンテナインスタンス上の別のホストポートにトラフィックをルーティングできます。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。
- Windows インスタンスが再起動された場合は、プロキシインターフェイスを削除して、Amazon ECS コンテナエージェントを再度初期化し、認証情報プロキシを元に戻す必要があります。

Amazon ECS コンテナブートストラップスクリプト

コンテナからコンテナインスタンスの認証情報プロキシにアクセスする前に、必要なネットワーキングコマンドを使用してコンテナをブートストラップする必要があります。起動時にコンテナで次のコードのサンプルスクリプトを実行する必要があります。

> **Note**
>
> Windows で awsvpc ネットワークモードを使用している場合は、このスクリプトを実行する必要はありません。

Powershell を含む Windows コンテナを実行する場合は、次のスクリプトを使用します。

```
# Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the "License"). You may
# not use this file except in compliance with the License. A copy of the
# License is located at
#
# http://aws.amazon.com/apache2.0/
#
# or in the "license" file accompanying this file. This file is distributed
# on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either
# express or implied. See the License for the specific language governing
# permissions and limitations under the License.

$gateway = (Get-NetRoute | Where { $_.DestinationPrefix -eq '0.0.0.0/0' } | Sort-Object
 RouteMetric | Select NextHop).NextHop
```

```
$ifIndex = (Get-NetAdapter -InterfaceDescription "Hyper-V Virtual Ethernet*" | Sort-
Object | Select ifIndex).ifIndex
New-NetRoute -DestinationPrefix 169.254.170.2/32 -InterfaceIndex $ifIndex -NextHop
 $gateway -PolicyStore ActiveStore # credentials API
New-NetRoute -DestinationPrefix 169.254.169.254/32 -InterfaceIndex $ifIndex -NextHop
 $gateway -PolicyStore ActiveStore # metadata API
```

コマンドシェルのみを持つ Windows コンテナを実行する場合は、次のスクリプトを使用します。

```
# Copyright Amazon.com Inc. or its affiliates. All Rights Reserved.
#
# Licensed under the Apache License, Version 2.0 (the "License"). You may
# not use this file except in compliance with the License. A copy of the
# License is located at
#
# http://aws.amazon.com/apache2.0/
#
# or in the "license" file accompanying this file. This file is distributed
# on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either
# express or implied. See the License for the specific language governing
# permissions and limitations under the License.

for /f "tokens=1" %i  in ('netsh interface ipv4 show interfaces ^| findstr /x /r
 ".*vEthernet.*"') do set interface=%i
for /f "tokens=3" %i  in ('netsh interface ipv4 show addresses %interface% ^| findstr /
x /r ".*Default.Gateway.*"') do set gateway=%i
netsh interface ipv4 add route prefix=169.254.170.2/32 interface="%interface%"
 nexthop="%gateway%" store=active # credentials API
netsh interface ipv4 add route prefix=169.254.169.254/32 interface="%interface%"
 nexthop="%gateway%" store=active # metadata API
```

Amazon ECS コンテナインスタンスの IAM ロール

Amazon ECS コンテナインスタンス (Amazon EC2 と外部インスタンスの両方を含む) では、Amazon ECS コンテナエージェントを実行し、エージェントがユーザーに属していることをサービスに伝える IAM ロールが必要です。コンテナインスタンスを起動してクラスターに登録する前に、使用するコンテナインスタンス用の IAM ロールを作成する必要があります。ロールは、コンソールへのログインまたは AWS CLI コマンドの実行に使用するアカウントで作成されます。

> **Important**
>
> クラスターに外部インスタンスを登録する場合、使用する IAM ロールには Systems Manager のアクセス許可も必要です。詳細については、「Amazon ECS Anywhere IAM ロール」を参照してください。

Amazon ECS では、AmazonEC2ContainerServiceforEC2Role 管理 IAM ポリシーを提供し、これには Amazon ECS の完全な機能セットを使用するために必要なアクセス権限が含まれます。この管理ポリシーは、IAM ロールにアタッチし、コンテナインスタンスに関連付けることができます。または、使用するカスタムポリシーを作成するときに、管理ポリシーをガイドとして使用することもできます。コンテナインスタンスロールには、Amazon ECS コンテナエージェントと Docker デーモンがユーザーに変わって AWS API を呼び出すために必要な許可があります。管理ポリシーの詳細については、「AmazonEC2ContainerServiceforEC2Role」を参照してください。

Amazon ECS は、サポートされている Amazon EC2 インスタンスタイプを使用して、ENI 密度が高いコンテナインスタンスの起動をサポートします。この機能を使用する場合は、2 つのコンテナインスタンスロールを作成することをお勧めします。1 つのロールで awsvpcTrunking アカウント設定を有効にし、そのロールを ENI トランキングを必要とするタスクに使用します。awsvpcTrunking アカウント設定については、「アカウント設定による Amazon ECS 機能へのアクセス」を参照してください。

コンテナインスタンスロールを作成する

> **Important**
>
> クラスターに外部インスタンスを登録する場合は、Amazon ECS Anywhere IAM ロール を参照してください。

機能や機能強化が今後導入されたときに Amazon ECS がそれらに対するアクセス許可を追加できるように、手動でロールを作成し、その IAM 管理ポリシーをコンテナインスタンスにアタッチできます。必要に応じて、以下の手順を使用してマネージド IAM ポリシーをアタッチします。

AWS Management Console

Elastic Container Service のサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] で [エラスティックコンテナサービス] を選択し、次に [エラスティックコンテナサービスのユースケースの EC2 ロール] を選択します。
5. [Next] を選択します。
6. [アクセス許可ポリシー] セクションで、[AmazonEC2ContainerServiceforEC2Role] ポリシーが選択されていることを確認します。

> **Important**
>
> AmazonEC2ContainerServiceforEC2Role 管理ポリシーは、コンテナインスタンス IAM ロールにアタッチする必要があります。アタッチされていない場合、AWS Management Console をクリックして、クラスターを作成します。

7. [Next] を選択します。
8. [ロール名] には、[ecsInstanceRole] と入力します。
9. ロールを確認したら、[ロールを作成] を選択します。

AWS CLI

すべての######を自分の値に置き換えてください。

1. `instance-role-trust-policy.json` というファイルを次の内容で作成します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

2. 信頼ポリシードキュメントを使用してインスタンスの IAM ロールを作成するには、次のコマンドを使用します。

```
aws iam create-role \
    --role-name ecsInstanceRole \
    --assume-role-policy-document file://instance-role-trust-policy.json
```

3. create-instance-profile コマンドを使用して、ecsInstanceRole-profile という名前のインスタンスプロファイルを作成します。

```
aws iam create-instance-profile --instance-profile-name ecsInstanceRole-profile
```

レスポンスの例

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2022-04-12T23:53:34.093Z",
        "InstanceProfileName": "ecsInstanceRole-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/ecsInstanceRole-
profile"
    }
}
```

4. *ecsInstanceRole* インスタンスプロファイルに *ecsInstanceRole-profile* ロールを追加します。

```
aws iam add-role-to-instance-profile \
    --instance-profile-name ecsInstanceRole-profile \
    --role-name ecsInstanceRole
```

5. 次のコマンドを使用して、AmazonEC2ContainerServiceRoleForEC2Role マネージドポリシーをロールにアタッチします。

```
aws iam attach-role-policy \
```

```
    --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonEC2ContainerServiceforEC2Role \
    --role-name ecsInstanceRole
```

ロールを作成したら、次の機能のアクセス許可をロールに追加します。

機能	追加のアクセス許可
Amazon ECR でコンテナイメージを取得する	Amazon ECR のアクセス許可
CloudWatch Logs でコンテナインスタンスをモニタリングする	コンテナインスタンスのモニタリングに必要なアクセス許可
設定ファイルを Amazon S3 バケットでホストする	Amazon S3 への読み取り専用アクセス

Amazon ECR のアクセス許可

コンテナインスタンスで使用する Amazon ECS コンテナインスタンスロールには、Amazon ECR に対する以下の IAM ポリシーのアクセス許可が必要です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ecr:BatchCheckLayerAvailability",
                "ecr:BatchGetImage",
                "ecr:GetDownloadUrlForLayer",
                "ecr:GetAuthorizationToken"
            ],
            "Resource": "*"
        }
    ]
}
```

コンテナインスタンスに AmazonEC2ContainerServiceforEC2Role 管理ポリシーを使用すると、ロールに適切なアクセス権限が付与されます。ロールが Amazon ECR をサポートすることを確

認するには、Amazon Elastic Container Service デベロッパーガイドの「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

Amazon S3 への読み取り専用アクセス

設定情報を Amazon S3 のプライベートバケットに保存し、コンテナインスタンスの IAM ロールに読み取り専用アクセス権限を付与するのが、コンテナインスタンスの起動時に設定を許可する安全で便利な方法です。`ecs.config` ファイルのコピーをプライベートバケットに保存し、Amazon EC2 ユーザーデータを使用して AWS CLI をインストールします。その後、インスタンスの起動時に設定情報を `/etc/ecs/ecs.config` にコピーします。

`ecs.config` ファイルの作成と Amazon S3 への保存、およびこの構成を使用したインスタンスの起動の詳細については、「Amazon S3 に Amazon ECS コンテナインスタンスの設定を保存する」を参照してください。

次の AWS CLI コマンドを使用すると、Amazon S3 の読み取り専用アクセス許可をコンテナインスタンスのロールに許可できます。前に作成したロールの名前で *ecsInstanceRole* を置き換えます。

```
aws iam attach-role-policy \
      --role-name ecsInstanceRole \
      --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
```

IAM コンソールを使用して、Amazon S3 の読み取り専用アクセス許可 (`AmazonS3ReadOnlyAccess`) をロールに追加することもできます。詳細については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。

コンテナインスタンスのモニタリングに必要なアクセス許可

コンテナインスタンスが CloudWatch Logs にログデータを送信する前に、Amazon ECS エージェントがお客様のアプリケーションログを CloudWatch に書き込むことを許可する IAM ポリシーを作成する必要があります (通常は `awslogs` ドライバーを介して処理されます)。作成が完了したポリシーは、`ecsInstanceRole` にアタッチします。

AWS Management Console

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

2. 左側のナビゲーションペインで、[ポリシー] を選択します。

   初めて [ポリシー] を選択する場合には、[管理ポリシーにようこそ] ページが表示されます。[今すぐ始める] を選択します。

3. ページの上部で、[ポリシーを作成] を選択します。

4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。

5. 次の JSON ポリシードキュメントを入力します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": ["arn:aws:logs:*:*:*"]
        }
    ]
}
```

6. [次へ] をクリックします。

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

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

8. [ポリシーの作成] をクリックして、新しいポリシーを保存します。

ポリシーを作成したら、そのポリシーをコンテナインスタンスロールにアタッチします。ポリシーをロールにアタッチする方法については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。

AWS CLI

1. `instance-cw-logs.json` というファイルを次の内容で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogStreams"
            ],
            "Resource": ["arn:aws:logs:*:*:*"]
        }
    ]
}
```

2. JSON ポリシードキュメントファイルを使用して IAM ポリシーを作成するには、次の コマンドを使用します。

```
aws iam create-policy \
      --policy-name cwlogspolicy \
      --policy-document file://instance-cw-logs.json
```

3. 次のコマンドを使用して、作成した IAM ポリシーの ARN を取得します。*cwlogspolicy* は、作成したポリシーの名前に置き換えます。

```
aws iam list-policies --scope Local --query 'Policies[?
PolicyName==`cwlogspolicy`].Arn'
```

4. ポリシー ARN を使用してコンテナインスタンスの IAM ロールにポリシーをアタッチするには、次のコマンドを使用します。

```
aws iam attach-role-policy \
      --role-name ecsInstanceRole \
```

```
    --policy-arn arn:aws:iam:111122223333:aws:policy/cwlogspolicy
```

Amazon ECS Anywhere IAM ロール

オンプレミスサーバーまたは仮想マシン (VM) をクラスタ-に登録する場合、サーバーまたは VM は AWS APIと通信するために IAM ロールを必要とします。IAM ロールの作成は AWS アカウントごとに一度のみ行う必要があります。ただし、この IAM ロールは、クラスターに登録する各サーバーまたは VM に関連付ける必要があります。このロールはECSAnywhereRole。このロールを手動で作成することもできます。または、Amazon ECS は、AWS Management Console に外部インスタンスを登録するときに、ユーザーに代わってロールを作成することもできます。IAM コンソールの検索を使用して ecsAnywhereRole を検索すると、アカウントにすでにそのロールがあるかどうかを確認できます。詳細については、IAM ユーザーガイドの「IAM コンソールの検索」を参照してください。

AWSには、ECS Anywhere IAM ロールの作成時に使用できる 2 つの管理対象 IAM ポリシー、AmazonSSMManagedInstanceCoreおよびAmazonEC2ContainerServiceforEC2Roleポリシーが用意されています。AmazonEC2ContainerServiceforEC2Roleポリシーには、必要以上に多くのアクセスを提供するアクセス許可が含まれています。したがって、特定のユースケースに応じて、必要なポリシーからのアクセス許可のみを追加するカスタムポリシーを作成することをお勧めします。詳細については、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。

タスク実行 IAM ロールは、ユーザーに代わって AWS API コールを実行するアクセス許可を Amazon ECS コンテナエージェントに付与します。タスク実行 IAM ロールを使用する場合は、タスク定義で指定する必要があります。詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

次のいずれかの条件が適用される場合は、タスクの実行ロールが必要です。

- コンテナログを CloudWatch Logs に送信するには、awslogsログドライバーを使用します。
- タスク定義では、Amazon ECR プライベートリポジトリでホストされるコンテナイメージを指定します。ただし、外部インスタンスに関連付けられている ECSAnywhereRole ロールに、Amazon ECR からイメージをプルするために必要なアクセス許可が含まれている場合は、タスク実行ロールにそれらを含める必要はありません。

Amazon ECS Anywhere ロールを作成する

すべての *[######]* は、お客様の情報で置き換えてください。

1. 以下のポリシーを持つ、ssm-trust-policy.json という名前のローカルファイルを作成します。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"Service": [
      "ssm.amazonaws.com"
    ]},
    "Action": "sts:AssumeRole"
  }
}
```

2. 次の AWS CLI コマンドを使用して、ロールを作成し、信頼ポリシーをアタッチします。

```
aws iam create-role --role-name ecsAnywhereRole --assume-role-policy-document
 file://ssm-trust-policy.json
```

3. 次のコマンドを使用して AWS マネージドポリシーをアタッチします。

```
aws iam attach-role-policy --role-name ecsAnywhereRole --policy-arn
 arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
aws iam attach-role-policy --role-name ecsAnywhereRole --policy-arn
 arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role
```

IAM のカスタム信頼ポリシーワークフローを使用してロールを作成することもできます。詳細については、IAM ユーザーガイドの「カスタム信頼ポリシーを使用してロールを作成する (コンソール)」を参照してください。

Amazon ECS インフラストラクチャ IAM ロール

Amazon ECS インフラストラクチャ IAM ロールを使用すると、Amazon ECS はユーザーに代わってクラスター内のインフラストラクチャリソースを管理できます。次の場合に使用します。

- Amazon EBS ボリュームを Fargate または EC2 起動タイプの Amazon ECS タスクにアタッチできます。インフラストラクチャロールにより、Amazon ECS はタスクの Amazon EBS ボリュームを管理できます。
- Amazon ECS Service Connect サービス間のトラフィックを暗号化するには、Transport Layer Security (TLS) を使用します。

- Amazon VPC Lattice ターゲットグループを作成する場合。

Amazon ECS がこの役割を引き受け、ユーザーに代わってアクションを実行すると、イベントが AWS CloudTrail に表示されます。Amazon ECS がそのロールを使用してタスクにアタッチされた Amazon EBS ボリュームを管理する場合、CloudTrail ログ `roleSessionName` は `ECSTaskVolumesForEBS` となります。ロールを使用して Service Connect サービス間のトラフィックを暗号化する場合、CloudTrail ログ `roleSessionName` は `ECSServiceConnectForTLS` になります。ロールを使用して VPC Lattice のターゲットグループを作成する場合、CloudTrail ログ `roleSessionName` は `ECSNetworkingWithVPCLattice` になります。この名前を使用して、[ユーザー名]でフィルタリングすることで CloudTrail コンソールでイベントを検索できます。

Amazon ECS では、ボリュームのアタッチメントと TLS に必要なアクセス許可を含むマネージドポリシーを提供しています。詳細については、「AWS マネージドポリシーリファレンスガイド」の「AmazonECSInfrastructureRolePolicyForVolumes」、「AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity」、および「AmazonECSInfrastructureRolePolicyForVpcLattice」を参照してください。

Amazon ECS インフラストラクチャロールを作成する

すべての *[######]* は、お客様の情報で置き換えてください。

1. IAM ロールに使用する信頼ポリシーが含まれている `ecs-infrastructure-trust-policy.json` という名前のファイルを作成します。ファイルには次の内容が含まれます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToECSForInfrastructureManagement",
      "Effect": "Allow",
      "Principal": {
        "Service": "ecs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 前のステップで作成した信頼ポリシーを使用して、`ecsInfrastructureRole` という名前のロールを作成するには、次の AWS CLI コマンドを使用します。

```
aws iam create-role \
      --role-name ecsInfrastructureRole \
      --assume-role-policy-document file://ecs-infrastructure-trust-policy.json
```

3. ユースケースに応じて、AWS マネージド AmazonECSInfrastructureRolePolicyForVolumes、AmazonECSInfrastructureRolePolic または AmazonECSInfrastructureRolePolicyForVpcLattice ポリシーを ecsInfrastructureRole ロールにアタッチします。

```
aws iam attach-role-policy \
      --role-name ecsInfrastructureRole \
      --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonECSInfrastructureRolePolicyForVolumes
```

```
aws iam attach-role-policy \
      --role-name ecsInfrastructureRole \
      --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity
```

IAM コンソールの[カスタム信頼ポリシー]ワークフローを使用してロールを作成することもできます。詳細については、IAM ユーザーガイドの「カスタム信頼ポリシーを使用してロールを作成する (コンソール)」を参照してください。

> **Important**
>
> Amazon ECS がタスクにアタッチされた Amazon EBS ボリュームを管理するために ECS インフラストラクチャロールを使用している場合は、Amazon EBS ボリュームを使用するタスクを停止する前に、次の点を確認してください。
>
> - ロールが削除されていません。
> - ロールの信頼ポリシーは、Amazon ECS アクセス (ecs.amazonaws.com) を削除するように変更されていません。
> - マネージドポリシー AmazonECSInfrastructureRolePolicyForVolumes は削除されていません。ロールのアクセス許可を変更する必要がある場合は、ボリュームを削除するために、少なくとも ec2:DetachVolume、ec2:DeleteVolume、ec2:DescribeVolumes を残してください。

Amazon EBS ボリュームがアタッチされたタスクを停止する前にロールを削除または変更すると、タスクが DEPROVISIONING で停止し、関連する Amazon EBS ボリュームは削除されません。Amazon ECS は、必要なアクセス許可が回復するまで、定期的に自動的に再試行してタスクを停止し、ボリュームを削除します。DescribeTasks API を使用して、タスクのボリュームアタッチ状態と関連するステータス理由を表示できます。

ファイルを作成したら、Amazon ECS にロールを渡すためのアクセス許可をユーザーに付与する必要があります。

インフラストラクチャロールを Amazon ECS に渡すためのアクセス許可

ECS インフラストラクチャの IAM ロールを使用するには、そのロールを Amazon ECS に渡すためのユーザー権限を付与する必要があります。ユーザーに、次の iam:PassRole 権限をアタッチします。前に作成したインフラストラクチャロールの名前で *ecsInfrastructureRole* を置き換えます。

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

        {
            "Action": "iam:PassRole",
            "Effect": "Allow",
            "Resource": ["arn:aws:iam::*:role/ecsInfrastructureRole"],
            "Condition": {
                "StringEquals": {"iam:PassedToService": "ecs.amazonaws.com"}
            }
        }
    ]
}
```

iam:Passrole およびユーザーの権限の更新について詳しくは、AWS Identity and Access Management ユーザーガイドの「AWS サービスにロールを渡すためのアクセス許可の付与」と「IAM ユーザーの権限の変更」を参照してください。

Amazon ECS CodeDeploy IAM ロール

Amazon ECS で CodeDeploy ブルー/グリーンデプロイタイプを使用するには、ユーザーの代わりに Amazon ECS サービスを更新するためのアクセス許可を事前に CodeDeploy サービスに付与しておく必要があります。これらのアクセス権限は、CodeDeploy IAM ロール (`ecsCodeDeployRole`) によって付与されます。

> **Note**
>
> ユーザーには CodeDeploy を使用するアクセス許可も必要です。これらの権限については、「必要な IAM 許可」で説明しています。

2 つの管理ポリシーが用意されています。詳細については、「AWS マネージドポリシーリファレンスガイド」で、次のいずれかを参照してください。

- AWSCodeDeployRoleForECS - 関連付けられたアクションを使用して、リソースを更新するためのアクセス許可を CodeDeploy に付与します。
- AWSCodeDeployRoleForECSLimited - より制限されたアクセス許可を CodeDeploy に付与します。

CodeDeploy ロールの作成

以下の手順を使用して、Amazon ECS 用 CodeDeploy ロールを作成できます。

AWS Management Console

CodeDeploy のサービスロールを作成するには (IAM コンソール)

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. IAM コンソールのナビゲーションペインで、[ロール]、[ロールを作成] を選択します。
3. 信頼できるエンティティタイプ で、AWS のサービス を選択します。
4. [サービスまたはユースケース] で [CodeDeploy] を選択し、次に [CodeDeploy - ECS] ユースケースを選択します。
5. [Next] を選択します。
6. 「[アクセス許可ポリシーをアタッチする]」セクションで、[AWSCodeDeployRoleForECS] ポリシーが選択されていることを確認します。

7. [Next] を選択します。
8. [ロール名] に [ECSodeDeployRole] と入力します。
9. ロールを確認したら、[ロールを作成] を選択します。

AWS CLI

すべての *[######]* は、お客様の情報で置き換えてください。

1. CodeDeploy IAM ロールに使用する信頼ポリシーを含む、codedeploy-trust-policy.json という名前のファイルを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": ["codedeploy.amazonaws.com"]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 前のステップで作成した信頼ポリシーを使用した ecsCodedeployRole という名前の IAM ロールを作成します。

```
aws iam create-role \
      --role-name ecsCodedeployRole \
      --assume-role-policy-document file://codedeploy-trust-policy.json
```

3. AWSCodeDeployRoleForECS または AWSCodeDeployRoleForECSLimited マネージドポリシー を ecsTaskRole ロールにアタッチします。

```
aws iam attach-role-policy \
      --role-name ecsCodedeployRole \
      --policy-arn arn:aws:iam::aws:policy/AWSCodeDeployRoleForECS
```

```
aws iam attach-role-policy \
```

```
    --role-name ecsCodedeployRole \
    --policy-arn arn:aws:iam::aws:policy/AWSCodeDeployRoleForECSLimited
```

サービス内のタスクにタスク実行ロールが必要な場合は、各タスク実行ロールまたはタスクロールの上書きの iam:PassRole アクセス許可を、ポリシーとして CodeDeploy ロールに追加する必要があります。

タスク実行ロールのアクセス許可

サービス内のタスクにタスク実行ロールが必要な場合は、各タスク実行ロールまたはタスクロールの上書きの iam:PassRole アクセス許可を、ポリシーとして CodeDeploy ロールに追加する必要があります。詳細については、Amazon ECS タスク実行IAM ロールおよびAmazon ECS タスクの IAM ロールを参照してください。次に、そのポリシーを CodeDeploy ロールにアタッチします。

ポリシーの作成

AWS Management Console

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": ["arn:aws:iam::<aws_account_id>:role/
<ecsCodeDeployRole>"]
        }
```

```
    ]
}
```

6. [次へ] をクリックします。

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

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

ポリシーを作成したら、そのポリシーを CodeDeploy ロールにアタッチします。ポリシーをロールにアタッチする方法については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。

AWS CLI

すべての *[######]* は、お客様の情報で置き換えてください。

1. `blue-green-iam-passrole.json` というファイルを次の内容で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": ["arn:aws:iam::<aws_account_id>:role/
<ecsCodeDeployRole>"]
        }
    ]
}
```

2. JSON ポリシードキュメントファイルを使用して IAM ポリシーを作成するには、次の コマンドを使用します。

```
aws iam create-policy \
      --policy-name cdTaskExecutionPolicy \
      --policy-document file://blue-green-iam-passrole.json
```

3. 次のコマンドを使用して、作成した IAM ポリシーの ARN を取得します。

```
aws iam list-policies --scope Local --query 'Policies[?
PolicyName==`cdTaskExecutionPolicy`].Arn'
```

4. 次のコマンドを使用して、ポリシーを CodeDeploy IAM ロールにアタッチします。

```
aws iam attach-role-policy \
      --role-name ecsCodedeployRole \
      --policy-arn arn:aws:iam:111122223333:aws:policy/cdTaskExecutionPolicy
```

Amazon ECS EventBridge IAM ロール

Amazon ECS でスケジュールされたタスクを EventBridge のルールとターゲットで送信するには、ユーザーの代わりに Amazon ECS タスクを実行するためのアクセス許可が EventBridge サービスに必要です。これらのアクセス許可は、EventBridge IAM ロール (`ecsEventsRole`) によって付与されます。

`AmazonEC2ContainerServiceEventsRole` のポリシーを次に示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ecs:RunTask"],
            "Resource": ["*"]
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": ["*"],
            "Condition": {
                "StringLike": {"iam:PassedToService": "ecs-tasks.amazonaws.com"}
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ecs:TagResource",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:CreateAction": ["RunTask"]
                }
            }
        }
    ]
}
```

スケジュールされたタスクでタスク実行ロールの使用、タスクロール、またはタスクロール上書きが必要な場合、タスク実行ロール、タスクロール、またはタスクロール上書きごとに `iam:PassRole` アクセス許可を EventBridge IAM ロールに追加する必要があります。タスクの実行ロールの詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。

> **Note**
>
> タスク実行ロールまたはタスクロール上書きの完全 ARN を指定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": ["arn:aws:iam::<aws_account_id>:role/
<ecsTaskExecutionRole_or_TaskRole_name>"]
        }
    ]
}
```

スケジュールされたタスクを設定するときに、AWS Management Console が EventBridge ロールを作成するようにすることができます。詳細については、「Amazon EventBridge スケジューラを使用して Amazon ECS タスクをスケジュールする 」を参照してください。

Amazon ECS EventBridge ロールを作成する

すべての *[######]* は、お客様の情報で置き換えてください。

1. IAM ロールに使用する信頼ポリシーが含まれている eventbridge-trust-policy.json という名前のファイルを作成します。ファイルには次の内容が含まれます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 前のステップで作成した信頼ポリシーを使用して、ecsEventsRole という名前の IAM ロールを作成するには、次のコマンドを使用します。

```
aws iam create-role \
      --role-name ecsEventsRole \
      --assume-role-policy-document file://eventbridge-trust-policy.json
```

3. 次のコマンドを使用して、AWS マネージド AmazonEC2ContainerServiceEventsRole を ecsEventsRole ロールにアタッチします。

```
aws iam attach-role-policy \
      --role-name ecsEventsRole \
      --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonEC2ContainerServiceEventsRole
```

IAM コンソールの[カスタム信頼ポリシーワークフロー] (https://console.aws.amazon.com/iam/) を使用してロールを作成することもできます。詳細については、IAM ユーザーガイドの「カスタム信頼ポリシーを使用してロールを作成する (コンソール)」を参照してください。

`ecsEventsRole` ロールへのポリシーのアタッチ

以下の手順を使用して、タスク実行ロールのアクセス許可を EventBridge IAM ロールに追加できます。

AWS Management Console

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": ["arn:aws:iam::<aws_account_id>:role/
<ecsTaskExecutionRole_or_TaskRole_name>"]
        }
    ]
}
```

6. [次へ] をクリックします。

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

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

ポリシーを作成したら、そのポリシーを EventBridge ロールにアタッチします。ポリシーをロールにアタッチする方法については、「AWS Identity and Access Management ユーザーガイド」の「ロールに対するアクセス許可を更新する」を参照してください。

AWS CLI

すべての *[######]* は、お客様の情報で置き換えてください。

1. ev-iam-passrole.json というファイルを次の内容で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": ["arn:aws:iam::<aws_account_id>:role/
<ecsTaskExecutionRole_or_TaskRole_name>"]
        }
    ]
}
```

2. JSON ポリシードキュメントファイルを使用して IAM ポリシーを作成するには、次の AWS CLI コマンドを使用します。

```
aws iam create-policy \
      --policy-name eventsTaskExecutionPolicy \
      --policy-document file://ev-iam-passrole.json
```

3. 次のコマンドを使用して、作成した IAM ポリシーの ARN を取得します。

```
aws iam list-policies --scope Local --query 'Policies[?
PolicyName==`eventsTaskExecutionPolicy`].Arn'
```

4. ポリシー ARN を使用して EventBridge の IAM ロールにポリシーをアタッチするには、次のコマンドを使用します。

```
aws iam attach-role-policy \
      --role-name ecsEventsRole \
      --policy-arn arn:aws:iam:111122223333:aws:policy/eventsTaskExecutionPolicy
```

Amazon ECS コンソールに必要なアクセス許可

最小権限の付与のベストプラクティスに従い、AmazonECS_FullAccess 管理ポリシーを、独自のカスタムポリシーを作成するためのテンプレートとして使用できます。これにより、特定の要件に基づいて、管理ポリシーに権限を追加し、管理ポリシーから権限を追加、または権限を取り上げることができます。詳細については、「AWS マネージドポリシーリファレンス」の「AmazonECS_FullAccess」を参照してください。

IAM ロールを作成するための許可

以下のアクションでは、操作を完了するために追加のアクセス許可が必要です。

- 外部インスタンスの登録 - 詳細は、Amazon ECS Anywhere IAM ロール を参照してください。
- タスク定義の登録 - 詳細は、Amazon ECS タスク実行IAM ロール を参照してください。
- タスクのスケジューリングに使用する EventBridge ルールの作成 - 詳細は、Amazon ECS EventBridge IAM ロール を参照してください。

Amazon ECS コンソールで使用する前に IAM でロールを作成することで、これらのアクセス許可を追加できます。ロールを作成しない場合、Amazon ECS コンソールがユーザーに代わってロールを作成します。

外部インスタンスをクラスターに登録するために必要なアクセス許可

外部インスタンスをクラスターに登録し、新しい外部インスタンス (ecsExternalInstanceRole) ロールを作成する場合は、追加のアクセス許可が必要です。

以下に示す追加のアクセス許可が必要です。

- iam — プリンシパルが IAM ロールとそれにアタッチするポリシーを作成し、一覧表示できるようにします。
- ssm — プリンシパルが外部インスタンスを Systems Manager に登録できるようにします。

> **Note**
>
> 既存の ecsExternalInstanceRole を選択するには、iam:GetRole および iam:PassRole のアクセス許可が必要です。

次のポリシーには必要なアクセス許可が含まれており、アクションは ecsExternalInstanceRole ロールに限定されます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
            "Action": [
              "iam:AttachRolePolicy",
              "iam:CreateRole",
              "iam:CreateInstanceProfile",
              "iam:AddRoleToInstanceProfile",
              "iam:ListInstanceProfilesForRole",
              "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/ecsExternalInstanceRole"
        },
        {
            "Effect": "Allow",
            "Action": ["iam:PassRole","ssm:CreateActivation"],
            "Resource": "arn:aws:iam::*:role/ecsExternalInstanceRole"
        }
    ]
}
```

タスク定義を登録するために必要なアクセス許可

タスク定義を登録し、新しいタスク実行 (ecsTaskExecutionRole) ロールを作成する場合は、追加のアクセス許可が必要です。

以下に示す追加のアクセス許可が必要です。

- iam — プリンシパルが IAM ロールとそれにアタッチするポリシーを作成し、一覧表示できるようにします。

> **Note**
>
> 既存の ecsTaskExecutionRole を選択するには、iam:GetRole のアクセス許可が必要です。

次のポリシーには必要なアクセス許可が含まれており、アクションは ecsTaskExecutionRole ロールに限定されます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
            "Action": [
              "iam:AttachRolePolicy",
              "iam:CreateRole",
              "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/ecsTaskExecutionRole"
        }
    ]
}
```

スケジュールされたタスクの EventBridge ルールを作成するために必要なアクセス許可

タスクをスケジュールし、新しい CloudWatch Events ロール (ecsEventsRole) ロールを作成する場合は、追加のアクセス許可が必要です。

以下に示す追加のアクセス許可が必要です。

- iam — プリンシパルが IAM ロールとそれにアタッチするポリシーを作成して一覧表示し、Amazon ECS がそのロールを他のサービスに渡してロールを引き継ぐことができるようにします。

> **Note**
>
> 既存の ecsEventsRole を選択するには、iam:GetRole および iam:PassRole のアクセス許可が必要です。

次のポリシーには必要なアクセス許可が含まれており、アクションは ecsEventsRole ロールに限定されます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
            "Action": [
              "iam:AttachRolePolicy",
              "iam:CreateRole",
              "iam:GetRole",
              "iam: PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/ecsEventsRole"
        }
    ]
}
```

サービスデプロイを表示するために必要なアクセス許可

最小権限のベストプラクティスに従うと、コンソールでサービスデプロイを表示するには、アクセス許可を追加する必要があります。

次のアクションへのアクセスが必要です。

- ListServiceDeployments
- DescribeServiceDeployments
- DescribeServiceRevisions

次のリソースへのアクセスが必要です。

- サービス
- サービスデプロイ
- サービスリビジョン

次のポリシー例には必要なアクセス許可が含まれており、アクションは指定されたサービスに限定されます。

account、cluster-name、および service-name を独自の値に置き換えます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
            "Action": [
              "ecs:ListServiceDeployments",
              "ecs:DescribeServiceDeployments",
              "ecs:DescribeServiceRevisions"
            ],
            "Resource": [
             "arn:aws:ecs:us-east-1:123456789012:service/cluster-name/service-name",
             "arn:aws:ecs:us-east-1:123456789012:service-deployment/cluster-name/
service-name/*",
             "arn:aws:ecs:us-east-1:123456789012:service-revision/cluster-name/service-
name/*"
            ]
        }
    ]
}
```

AWS CloudFormation を使用する Amazon ECS コンソールに必要なアクセス許可

Amazon ECS コンソールは AWS CloudFormation を利用しているため、以下の場合には追加の IAM アクセス許可が必要になります。

- クラスターの作成
- サービスの作成
- キャパシティープロバイダーの作成

追加のアクセス許可のポリシーを作成して、コンソールへのアクセスに使用する IAM ロールにアタッチできます。詳細についてはIAM ユーザーガイド の「IAM ポリシーの作成」を参照してください。

クラスターを作成するために必要なアクセス許可

コンソールでクラスターを作成するときには、AWS CloudFormation スタックを管理するための追加のアクセス許可が必要です。

以下に示す追加のアクセス許可が必要です。

- cloudformation — プリンシパルの作成と管理を許可する AWS CloudFormation スタック。これは、AWS Management Console を使用して Amazon ECS クラスターを作成し、それらのクラスターのその後の管理に必要です。
- ssm – AWS CloudFormation が最新の Amazon ECS 最適化 AMI を参照できるようにします。これは、AWS Management Console を使用して Amazon ECS クラスターを作成するときに必要です。

次のポリシーには必要な AWS CloudFormation アクセス許可が含まれており、アクションは Amazon ECS コンソールで作成されたリソースに限定されます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStack*",
                "cloudformation:UpdateStack"
             ],
            "Resource": [
                "arn:*:cloudformation:*:*:stack/Infra-ECS-Cluster-*"
            ]
      },
      {
          "Effect": "Allow",
          "Action": "ssm:GetParameters",
          "Resource": [
            "arn:aws:ssm:*:*:parameter/aws/service/ecs/optimized-ami/amazon-linux-2*/
*",
            "arn:aws:ssm:*:*:parameter/aws/service/ecs/optimized-ami/amazon-
linux-2023*/*"
          ]
      }
   ]
}
```

Amazon ECS コンテナインスタンスロール (ecsInstanceRole) をまだ作成していない状態で Amazon EC2 インスタンスを使用するクラスターを作成する場合は、コンソールがユーザーに代わってロールを作成します。

さらに、Auto Scaling グループを使用する場合は、クラスターの自動スケーリング機能を使用する際にコンソールが Auto Scaling グループにタグを追加できるようにするための追加のアクセス許可が必要です。

以下に示す追加のアクセス許可が必要です。

- `autoscaling` — コンソールが Amazon EC2 Auto Scaling グループにタグ付けできるようにします。これは、クラスターのオートスケーリング機能を使用する場合、Amazon EC2 Auto Scaling グループを管理する場合に必要です。このタグは、ECS によって管理され、コンソールで作成されたことを示すためにコンソールによって自動的にグループに追加されます。
- `iam` — プリンシパルに IAM ロールとアタッチされたポリシーの一覧表示を許可します。プリンシパルは、Amazon EC2 インスタンスで利用できるインスタンスプロファイルを一覧表示することもできます。

次のポリシーには必要な IAM アクセス許可が含まれており、アクションは `ecsInstanceRole` ロールに限定されます。

自動スケーリング許可は制限されません。

```
{
  "Statement": [
      {
          "Effect": "Allow",
            "Action": [
              "iam:AttachRolePolicy",
              "iam:CreateRole",
              "iam:CreateInstanceProfile",
              "iam:AddRoleToInstanceProfile",
              "iam:ListInstanceProfilesForRole",
              "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/ecsInstanceRole"
        },
        {
            "Effect": "Allow",
            "Action": "autoscaling:CreateOrUpdateTags",
            "Resource": "*"
        }
    ]
}
```

サービスを作成するために必要なアクセス許可

コンソールでサービスを作成するときには、AWS CloudFormation スタックを管理するための追加のアクセス許可が必要です。以下に示す追加のアクセス許可が必要です。

- `cloudformation` — プリンシパルの作成と管理を許可する AWS CloudFormation スタック。これは、AWS Management Console を使用して Amazon ECS サービスを作成する際に、またその後それらのサービスを管理する際に必要です。

次のポリシーには必要なアクセス許可が含まれており、アクションは Amazon ECS コンソールで作成されたリソースに限定されます。

```
{
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStack*",
                "cloudformation:UpdateStack"
             ],
            "Resource": [
                "arn:*:cloudformation:*:*:stack/ECS-Console-V2-Service-*"
            ]
      }
   ]
}
```

Amazon ECS のサービス自動スケーリングに必要な IAM アクセス許可

Service Auto Scalingは、Amazon ECS、Amazon CloudWatch、およびアプリケーション Auto Scaling API の組み合わせによって可能になります。サービスは Amazon ECS で作成および更新され、アラームは CloudWatch で作成され、スケーリングポリシーは Application Auto Scaling で作成されます。

サービスの作成および更新のための標準の IAM アクセス許可に加えて、以下のポリシー例に示されているように、Service Auto Scaling 設定の操作には次のアクセス許可が必要です。

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ecs:DescribeServices",
                "ecs:UpdateService",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": ["*"]
        }
    ]
}
```

「Amazon ECS サービス作成の例」および「Amazon ECS サービス更新の例」の IAM ポリシー例に、AWS Management Consoleでサービスの自動スケーリングを使用するために必要なアクセス許可が示されています。

Application Auto Scaling サービスには、Amazon ECS サービスおよび CloudWatch アラームを記述するアクセス許可が必要です。また、ユーザーの代わりにサービスの必要タスク数を変更するアクセス許可も必要です。`sns:` 権限は、しきい値を超えたときに CloudWatch が Amazon SNS トピックに送信する通知を対象とするものです。Amazon ECS サービスの自動スケーリングを使用にする場合、サービスにリンクされたロールが `AWSServiceRoleForApplicationAutoScaling_ECSService` という名前で作成されます。このサービスにリンクされたロールでは、ポリシーのアラームを記述し、サービスの現在実行中のタスクの数をモニタリングし、サービスの必要なタスクの数を変更するアクセス許可を Application Auto Scaling に付与します。Application Auto Scaling の元のマネージド型の Amazon ECS ロールは `ecsAutoscaleRole` ですが、これは不要になりました。サービスにリンクされたロール

は、Application Auto Scaling のデフォルトロールです。詳細については、「Application Auto Scaling ユーザーガイド」の「Application Auto Scaling 用のサービスリンクロール」を参照してください。

CloudWatch メトリクスが Amazon ECS で使用可能になる前に Amazon ECS コンテナインスタンスロールを作成した場合は、このアクセス `ecs:StartTelemetrySession` 許可の追加が必要になることがあります。詳細については、「考慮事項」を参照してください。

リソース作成時にタグ付けするための許可を付与する

次の作成時のタグ付けの Amazon ECS API アクションを使用すると、リソースの作成時にタグを指定できます。リソース作成アクションでタグが指定されている場合、AWS は追加の認可を実行して、タグを作成するための正しい許可が割り当てられていることを検証します。

- `CreateCapacityProvider`
- `CreateCluster`
- `CreateService`
- `CreateTaskSet`
- `RegisterContainerInstance`
- `RegisterTaskDefinition`
- `RunTask`
- `StartTask`

リソースタグを使用して、属性ベースの制御 (ABAC) を実装できます。詳細については、the section called “リソースタグを使用して Amazon ECS リソースへのアクセスを制御する”および リソースのタグ付けを参照してください。

作成時のタグ付けを許可するには、ポリシーを作成または変更して、`ecs:CreateCluster` や `ecs:RunTask` などのリソースを作成するアクションと `ecs:TagResource` アクションを使用するための両方の許可を含めます。

次の例は、ユーザーがクラスターを作成し、クラスター作成時にタグを追加できるポリシーを示しています。ユーザーには既存のリソースへのタグ付けが許可されません (`ecs:TagResource` アクションを直接呼び出すことはできません)。

```
{
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
         "ecs:CreateCluster"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ecs:TagResource"
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
                  "ecs:CreateAction": [
                      "CreateCluster",
                      "CreateCapacityProvider",
                      "CreateService",
                      "CreateTaskSet",
                      "RegisterContainerInstance",
                      "RegisterTaskDefinition",
                      "RunTask",
                      "StartTask"
                  ]
          }
       }
    }
  ]
}
```

ecs:TagResource アクションはタグがリソース作成アクション時に適用された場合のみ評価されます。したがって、リクエストでタグが指定されていない場合、リソースを作成するアクセス許可を持っているユーザー (タグ付け条件がないと仮定) にはecs:TagResource アクションを実行するアクセス許可は必要ありません。ただし、ユーザーがタグを使用してリソースを作成しようとした場合、ユーザーが ecs:TagResource アクションを使用するアクセス許可を持っていない場合はリクエストに失敗します。

特定のタグへの Amazon ECS アクセス制御

IAM ポリシーの Condition 要素で追加の条件を使用して、リソースに適用できるタグキーとタグ値を制御できます。

次の条件キーは前のセクションの例で使用できます。

- aws:RequestTag: 特定のタグキーまたはタグキーと値がリクエストに存在している必要があることを指定する場合に使用します。リクエストでは他のタグも指定できます。
  - StringEquals 条件演算子とともに使用して、特定のタグキーと値の組み合わせを適用します。例えば、タグ cost-center=cc123: を適用します。

```
"StringEquals": { "aws:RequestTag/cost-center": "cc123" }
```

  - StringLike 条件演算子とともに使用して、リクエストで特定のタグキーを適用します。例えば、タグキー purpose を適用します。

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- aws:TagKeys: リクエストで使用されるタグキーを適用する場合に使用します。
  - リクエストにタグが指定されている場合はForAllValues 修飾子を使用して特定のタグキーのみを適用します (リクエストにタグが指定されている場合、特定のタグキーのみが許可されます。他のタグは許可されません)。例えば、タグキー environment または cost-center が適用されます:

```
"ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
```

  - ForAnyValue 修飾子とともに使用して、指定されたタグキーの少なくとも 1 つがリクエストに存在することを要求します。例えば、タグキー environment または webserver のうち少なくとも 1 つがリクエストに存在している必要があります。

```
"ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
```

これらの条件キーは、ecs:TagResource アクションだけでなく、タグ付けをサポートするリソース作成アクションにも適用できます。Amazon ECS API アクションがタグ付けをサポートしているかどうかについては、「Amazon ECS のアクション、リソース、および条件キー」を参照してください。

リソースの作成時にタグを指定するようにユーザーに強制するにはリソース作成アクションで aws:RequestTag 修飾子とともに aws:TagKeys 条件キーまたは ForAnyValue 条件キーを使用する必要があります。ユーザーがリソース作成アクションのタグを指定しない場合、ecs:TagResource アクションは評価されません。

条件においては条件キーでは大文字と小文字が区別されず、条件値では大文字と小文字が区別されます。したがって、タグキーの大文字と小文字を区別するには条件の値としてタグキーが指定される aws:TagKeys 条件キーを使用します。

複数値条件の詳細については、「IAM ユーザーガイド」の「複数のコンテキストキーまたは値による条件」を参照してください。

リソースタグを使用して Amazon ECS リソースへのアクセスを制御する

Amazon ECS リソースを使用するための許可をユーザーに付与する IAM ポリシーを作成する場合、ポリシーの Condition 要素にタグ情報を含めることで、タグに基づいてアクセスをコントロールできます。これは属性ベースのアクセス制御 (ABAC) と呼ばれます。ABAC を使用すると、ユーザーが変更、使用、または削除できるリソースをより適切に制御できます。詳細についてはAWS の ABAC とはを参照してください。

例えば、ユーザーによるクラスターの削除を許可するが、クラスターにタグ environment=production がある場合はそのアクションを拒否するポリシーを作成できます。これを行うにはaws:ResourceTag 条件キーを使用し、リソースにアタッチされているタグに基づいてリソースへのアクセスを許可または拒否します。

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Amazon ECS API アクションが aws:ResourceTag 条件キーを使用したアクセスの制御をサポートしているかどうかについては、「Amazon ECS のアクション、リソース、および条件キー」を参照してください。Describe アクションはリソースレベルのアクセス権限をサポートしないため、条件のない別のステートメントでそれらのアクセス権限を指定する必要があることに注意してください。

IAM ポリシーの例はAmazon ECS ポリシーの例 を参照してください。

タグに基づいてリソースへのユーザーのアクセスを許可または拒否する場合はユーザーが同じリソースに対してそれらのタグを追加または削除することを明示的に拒否することを検討する必要があります。そうしないと、ユーザーはそのリソースのタグを変更することで、制限を回避してリソースにアクセスできてしまいます。

Amazon ECS ポリシーの例

IAM ポリシーを使用して、Amazon ECS コンソールで特定のリソースを表示、および操作するための許可をユーザーに付与することができます。上記のセクションのサンプルポリシーを使用すること

はできますが、これらは AWS CLI または AWS SDK で作成されたリクエスト向けに設計されています。

例: タグに基づいてユーザーが Amazon ECS クラスターを削除するのを許可する

次のポリシーは、タグに「Purpose/Testing」のキー/値のペアがある場合、ユーザーがクラスターを削除することを許可します。

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ecs:DeleteCluster"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ecs:region:account-id:cluster/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Amazon Elastic Container Service 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、Amazon ECS と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Amazon ECS でアクションを実行する権限がない
- iam:PassRole を実行する権限がありません
- 自分の AWS アカウント 以外のユーザーに Amazon ECS リソースへのアクセスを許可したい
- その他のトラブルシューティングリソース

Amazon ECS でアクションを実行する権限がない

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なecs:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ecs:GetWidget on resource: my-example-widget
```

この場合、ecs:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Amazon ECS にロールを渡せるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールやサービスリンクロールを作成せずに、既存のロールをサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、marymajor という IAM ユーザーがコンソールを使用して Amazon ECS でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

自分の AWS アカウント 以外のユーザーに Amazon ECS リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Amazon ECS がこれらの機能をサポートしているかどうかについては、「IAM を使用するAmazon Elastic Container Service」を参照してください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「所有している別の AWS アカウントへのアクセス権を IAM ユーザーに提供」を参照してください。
- サードパーティーの AWS アカウント にリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「サードパーティーが所有する AWS アカウント へのアクセス権を付与する」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。

その他のトラブルシューティングリソース

次のページに、エラーコードに関する情報が記載されています。

- Amazon ECS の停止したタスクのエラーメッセージ
- Amazon ECS のサービスイベントメッセージを表示する

Amazon ECS の IAM ベストプラクティス

AWS Identity and Access Management (IAM) を使用すると、認証と認可を目的としたルールベースのポリシーを通じて、AWS のサービスとリソースへのアクセスの管理と制御を行うことができます。具体的には、このサービスを通じてユーザー、グループ、またはロールに適用されるポリシー

を使用して、AWS リソースへのアクセスを制御します。この 3 つのうち、ユーザーはリソースにアクセスできるアカウントです。また、IAM ロールは、認証された ID が引き受けることができる一連のアクセス許可であり、IAM 外の特定の ID には関連付けられていません。詳細については、「Amazon ECS overview of access management: Permissions and policies」を参照してください。

最小権限アクセスのポリシーに従う

ユーザーが所定の仕事を遂行できるようにポリシーの範囲を設定してください。たとえば、開発者が定期的にタスクを停止する必要がある場合、その特定のアクションのみを許可するポリシーを作成します。次の例では、特定の Amazon リソースネーム (ARN) を持つクラスター上の　特定の `task_family` に属するタスクを停止させることができます。リソースレベルのアクセス許可を使用する別の例として、条件で ARN を参照することが挙げられます。リソースレベルのアクセス許可を使用して、アクションを適用するリソースを指定できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:StopTask"
      ],
      "Condition": {
        "ArnEquals": {
          "ecs:cluster": "arn:aws:ecs:region:account_id:cluster/cluster_name"
        }
      },
      "Resource": [
        "arn:aws:ecs:region:account_id:task-definition/task_family:*"
      ]
    }
  ]
}
```

クラスターリソースを管理上の境界として使用する

ポリシーの範囲が狭すぎると、ロールが急増し、管理オーバーヘッドが増える可能性があります。特定のタスクやサービスのみを対象とするロールを作成するのではなく、クラスターを対象とするロールを作成し、そのクラスターを主要な管理上の境界として使用してください。

自動パイプラインを作成して API からエンドユーザーを隔離する

アプリケーションを自動的にパッケージ化して Amazon ECS クラスターにデプロイするパイプラインを作成することで、ユーザーが使用できるアクションを制限できます。これにより、タスクを作成、更新、削除するジョブをパイプラインに効果的に委任することができます。詳細については、「AWS CodePipeline ユーザーガイド」の「チュートリアル: CodePipeline を使用した Amazon ECS 標準デプロイ」を参照してください。

ポリシー条件を使用してセキュリティをより一層強化する

セキュリティを強化する必要がある場合は、ポリシーに条件を追加します。これは、権限のある操作を実行する場合や、特定のリソースに対して実行できるアクションを制限する必要がある場合に役立ちます。以下は、クラスターを削除する際に多要素認可を必要とするポリシーの例です。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DeleteCluster"
      ],
      "Condition": {
        "Bool": {
          "aws:MultiFactorAuthPresent": "true"
        }
      },
    "Resource": ["*"]
    }
  ]
}
```

サービスに適用されたタグは、そのサービスに含まれるすべてのタスクに反映されます。したがって、特定のタグを使用して Amazon ECS リソースを対象とするロールを作成できます。次のポリシーでは、タグキーが `Department` でタグ値が `Accounting` であるすべてのタスクを IAM プリンシパルが開始および停止します。

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

```
            "Effect": "Allow",
            "Action": [
                "ecs:StartTask",
                "ecs:StopTask",
                "ecs:RunTask"
            ],
            "Resource": "arn:aws:ecs:*",
            "Condition": {
                "StringEquals": {"ecs:ResourceTag/Department": "Accounting"}
            }
        }
    ]
}
```

API へのアクセスを定期的に監査する

ユーザーがロールを変更する場合があります。ロールを変更した後、以前に付与されていたアクセス許可が適用されなくなる場合があります。どのユーザーが Amazon ECS API にアクセスでき、そのアクセスが引き続き保証されているかどうかを必ず監査してください。ユーザーが組織を離れると自動的にアクセス権を取り消すユーザーライフサイクル管理ソリューションと IAM を統合することを検討してください。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS セキュリティ監査のガイドライン」を参照してください。

Amazon Elastic Container Service でのログとモニタリング

モニタリングは、Amazon Elastic Container Service および AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、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必要があります。AWS には、Amazon ECS リソー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複数のツールが用意されています。

Amazon CloudWatch アラーム

指定した期間にわたって単一のメトリクスを監視し、複数の期間にわたり特定のしきい値に関連するメトリクス値に基づいて 1 つ以上のアクションを実行します。アクションは、Amazon Simple Notification Service (Amazon SNS) のトピックまたは Amazon EC2 Auto Scaling のポリシーに送信される通知です。CloudWatch アラームは、特定の状態にあるという理由だけでアクションを呼び出すことはありません。状態が変更され、指定された期間維持されている必要があります。詳細については、「CloudWatch を使用して Amazon ECS をモニタリングする」を参照してください。

Fargate 起動タイプを使用するタスクがあるサービスでは、CloudWatch アラームを使用して、CPU やメモリの使用率などの CloudWatch メトリクスに基づいてサービス内のタスクをスケールインおよびスケールアウトできます。詳細については、「Amazon ECS サービスを自動的にスケールする」を参照してください。

EC2 起動タイプを使用するタスクまたはサービスがあるクラスターでは、CloudWatch アラームを使用して、クラスターのメモリ使用率などの CloudWatch メトリクスに基づいてコンテナインスタンスをスケールインおよびスケールアウトできます。

Amazon CloudWatch Logs

Amazon ECS タスク定義で `awslogs` ログドライバーを指定することで、Amazon ECS タスクのコンテナからの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、「awslogs ログドライバーを使用する」を参照してください。

Amazon ECS コンテナインスタンスからのオペレーティングシステムおよび Amazon ECS コンテナエージェントのログファイルをモニタリング、保存、アクセスすることもできます。この方法を使用したログへのアクセスは、EC2 起動タイプを使用するコンテナの場合で使うことができます。

Amazon CloudWatch Events

イベントを一致させ、イベントを 1 つ以上のターゲット関数やストリームにルーティングして、変更を加えたり、状態情報を取得したり、修正アクションを実行したりします。詳細については、このガイドの「EventBridge を使用して Amazon ECS エラーへの対応を自動化する」および「Amazon EventBridge ユーザーガイド」の「EventBridge is the evolution of Amazon CloudWatch Events」を参照してください。

AWS CloudTrail ログ

CloudTrail では、Amazon ECS のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を確認できます。CloudTrail で収集された情報を使用して、Amazon ECS に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「AWS CloudTrail を使用して Amazon ECS API コールをログに記録する」を参照してください。

AWS Trusted Advisor

Trusted Advisor は、AWS の数十万のお客様にサービスを提供することにより得られた、運用実績から学んだベストプラクティスを活用しています。Trusted Advisor はお客様の AWS 環境を検査し、システムの可用性とパフォーマンスを向上させたりセキュリティギャップを埋めたりする機会がある場合には、推奨事項を作成します。すべての AWS のお客様は、Trusted Advisor の 5

つのチェックにアクセスできます。ビジネスまたはエンタープライズサポートプランをご利用のお客様は、すべての Trusted Advisor チェックを表示できます。

詳細については、サポート ユーザーガイドの AWS Trusted Advisor をご参照ください。

AWS Compute Optimizer

AWS Compute Optimizer は、AWS リソースの設定と使用率のメトリクスを分析するサービスです。Compute Optimizer は、リソースが最適かどうかを報告し、最適化に関するレコメンデーションを生成してコストを削減およびワークロードのパフォーマンスを改善します。

詳細については、「Amazon ECS に関する AWS Compute Optimizer 推奨事項」を参照してください。

Amazon ECS のモニタリングでもう 1 つ重要な点は、CloudWatch のアラームの対象外の項目を手動でモニタリングすることです。Trusted Advisor、CloudWatch、その他の AWS コンソールのダッシュボードには、AWS 環境の状態が一目でわかるように表示されます。コンテナインスタンスおよびタスクのコンテナのログファイルも確認することをお勧めします。

Amazon Elastic Container Service でのコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの対象であるかどうかを確認するには、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」で、関心のあるコンプライアンスプログラムを選択してください。一般的な情報については、「AWSコンプライアンスプログラム」を参照してください。

AWS Artifact 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。詳細については、「AWS Artifact でレポートをダウンロードする」を参照してください。

AWS のサービス を使用する際のユーザーのコンプライアンス責任は、ユーザーのデータの機密性や貴社のコンプライアンス目的、適用される法律および規制によって決まります。AWS では、コンプライアンスに役立つ次のリソースを提供しています。

- 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。すべての AWS のサービスが HIPAA 適格であるわけではありません。

- 「AWS コンプライアンスのリソース」 – このワークブックおよびガイドのコレクションは、顧客の業界と拠点に適用されるものである場合があります。
- AWS Customer Compliance Guide - コンプライアンスの観点から見た責任共有モデルを理解できます。このガイドは、AWS のサービスを保護するためのベストプラクティスを要約したものであり、複数のフレームワーク (米国標準技術研究所 (NIST)、ペイメントカード業界セキュリティ標準評議会 (PCI)、国際標準化機構 (ISO) など) にわたるセキュリティ統制へのガイダンスがまとめられています。
- 「AWS Config デベロッパーガイド」の「ルールでのリソースの評価」 - AWS Config サービスは、自社のプラクティス、業界ガイドライン、および規制に対するリソースの設定の準拠状態を評価します。
- AWS Security Hub – この AWS のサービス は、AWS 内のセキュリティ状態の包括的なビューを提供します。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 – この AWS のサービスは、環境をモニタリングして、疑わしい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、AWS アカウント、ワークロード、コンテナ、データに対する潜在的な脅威を検出します。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 - この AWS のサービスは、AWS の使用状況を継続的に監査して、リスクの管理方法や、規制および業界標準へのコンプライアンスの管理方法を簡素化するために役立ちます。

Amazon ECS のセキュリティとコンプライアンスのベストプラクティス

Amazon ECS を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性や貴社のコンプライアンス目的、適用可能な法律および規制によって決定されます。

AWS では、コンプライアンスに役立つ、次のリソースを提供しています。

- セキュリティおよびコンプライアンスのクイックスタートガイド: これらのデプロイメントガイドでは、アーキテクチャー上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境を AWS にデプロイするための手順を説明します。

- HIPAA のセキュリティとコンプライアンスに関するホワイトペーパーを作成する: このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- コンプライアンスプログラム対象範囲内の AWS サービス:これには、特定のコンプライアンスプログラムの対象となる AWS のサービスが一覧表示されています。詳細については、「AWS コンプライアンスプログラム」を参照してください。

決済カード業界のデータセキュリティ基準 (PCI DSS)

PCI DSS を順守する際には、環境内のカード所有者データ (CHD) の流れ全体を理解することが重要です。CHD フローは PCI DSS の適用性を決定し、カード会員データ環境 (CDE) の境界と構成要素を定義し、PCI DSS 評価の範囲を定義します。PCI DSS の範囲を正確に決定することは、セキュリティ体制を定義し、最終的に評価を成功させるための鍵となります。範囲の完全性を保証し、範囲からの変更や逸脱を検出する範囲決定手順は、お客様で用意する必要があります。

コンテナ化されたアプリケーションは一時的な性質を持つため、構成の監査がさらに複雑になります。そのため、コンテナのライフサイクルの全段階でコンプライアンス要件に対応できるよう、お客様はコンテナのすべての設定パラメータを常に把握しておく必要があります。

Amazon ECS での PCI DSS コンプライアンスの達成方法の詳細については、次のホワイトペーパーを参照してください。

- Amazon ECS での PCI DSS コンプライアンスに向けたアーキテクチャ構築
- AWS での PCI DSS の範囲とセグメンテーションのためのアーキテクチャ構築

HIPAA (米国の医療保険の相互運用性と説明責任に関する法令)

Amazon ECS で保護対象医療情報 (PHI) を処理するワークロードを使用する場合、追加の設定は不要です。Amazon ECS は、Amazon EC2 でのコンテナの起動を調整するオーケストレーションサービスとして機能します。オーケストレーション対象のワークロード内のデータに対して動作したり、データに基づいて動作したりすることはありません。HIPAA 規制および AWS ビジネスアソシエイト補遺に従い、Amazon ECS で起動されたコンテナが PHI にアクセスする場合は、転送中も保存中も暗号化する必要があります。

AWS ストレージオプションごとに Amazon S3、Amazon EBS、AWS KMS など、保存時の暗号化のためのさまざまなメカニズムを利用できます。オーバーレイネットワーク (VNS3 や Weave Net など) をデプロイして、コンテナ間で転送される PHI を完全に暗号化したり、暗号化の冗長レイ

ヤーを提供したりすることもできます。ログも完全に有効にし、すべてのコンテナログが Amazon CloudWatch に送信されるようにしてください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには「セキュリティの柱 - AWS 適切なアーキテクチャを備えたフレームワーク」の「インフラストラクチャの保護」を参照してください。

AWS Security Hub

AWS Security Hub を使用して、セキュリティのベストプラクティスに関連して Amazon ECS の使用状況をモニタリングできます。Security Hub は、コントロールを使用してリソース設定とセキュリティ標準を評価し、お客様がさまざまなコンプライアンスフレームワークに準拠できるようサポートします。Security Hub を使用して Amazon ECS リソースを評価する方法の詳細については、「AWS Security Hub ユーザーガイド」の「Amazon ECS のコントロール」を参照してください。

Amazon ECS Runtime Monitoring を使用した Amazon GuardDuty

Amazon GuardDuty は、AWS 環境内のアカウント、コンテナ、ワークロード、データを保護する脅威検知サービスです。GuardDuty は、機械学習（ML）モデル、異常および脅威検出機能を使用して、さまざまなログソースとランタイムアクティビティを継続的に監視し、環境内の潜在的なセキュリティリスクと悪意のあるアクティビティを特定して優先順位を付けます。

GuardDuty のランタイムモニタリングを使用して、悪意のある、または不正な動作を特定します。ランタイムモニタリングは、AWS ログとネットワークアクティビティを継続的に監視して悪意のある動作や不正な動作を特定することで、Fargate および EC2 で実行されているワークロードを保護します。ランタイムモニタリングは、軽量でフルマネージド型の GuardDuty セキュリティエージェントを使用して、ファイルアクセス、プロセス実行、ネットワーク接続などのホスト上動作を分析します。これは、Amazon EC2 インスタンスおよびコンテナワークロードでの権限の昇格、流出した認証情報の使用、悪意のある IP アドレスやドメインとの通信、マルウェアの存在などの問題に対応しています。詳細については、「GuardDuty ユーザーガイド」の「GuardDuty ランタイムモニタリング」を参照してください。

コンプライアンスに関する推奨事項

関連するコンプライアンスプログラムを成功させるには、早めに社内のコンプライアンスプログラムの所有者に働きかけ、AWS 責任共有モデルを使用してコンプライアンス統制の所有権を特定する必要があります。

AWS Fargate 連邦情報処理標準 (FIPS-140)

連邦情報処理標準 (FIPS)。FIPS-140 は、機密情報を保護する暗号モジュールのセキュリティ要件を規定する米国およびカナダ政府の標準です。FIPS-140 は、転送中のデータと保管中のデータの暗号化に使用できる、一連の検証済みの暗号化関数を定めています。

FIPS-140 コンプライアンスをオンにすると、FIPS-140 に準拠した態様で Fargate でワークロードを実行できます。FIPS-140 コンプライアンスの詳細については、「連邦情報処理標準 (FIPS) 140-2」を参照してください。

AWS Fargate FIPS-140 に関する考慮事項

Fargate で FIPS-140 コンプライアンスを使用する場合は、次の点を考慮してください。

- FIPS-140 コンプライアンスは、AWS GovCloud (US) リージョンでのみ利用できます。
- FIPS-140 コンプライアンスは、デフォルトでオフになっています。オンにする必要があります。
- タスクでは、FIPS-140 コンプライアンスのために次の設定を使用する必要があります。
  - `operatingSystemFamily` は `LINUX` でなければなりません。
  - `cpuArchitecture` は `X86_64` でなければなりません。
  - Fargate プラットフォームバージョンは `1.4.0` 以降である必要があります。

Fargate で FIPS を使用する

Fargate で FIPS-140 コンプライアンスを使用するには、次の手順を実行します。

1. FIPS-140 コンプライアンスをオンにします。詳細については、「the section called “AWS Fargate 連邦情報処理標準 (FIPS-140) コンプライアンス”」を参照してください。
2. オプションで、ECS Exec を使用して次のコマンドを実行し、クラスターの FIPS-140 コンプライアンスステータスを検証できます。

   `cluster-name` をクラスターの名前に、*`task-id`* をタスクの ID または ARN に、*`container-name`* をコマンドを実行するタスク内のコンテナ名に置き換えます。

   戻り値「1」は、FIPS が使用されていることを示します。

```
aws ecs execute-command \
    --cluster cluster-name \
    --task task-id \
```

```
    --container container-name \
    --interactive \
    --command "cat /proc/sys/crypto/fips_enabled"
```

Fargate FIPS-140 監査に CloudTrail を使用する

CloudTrail は、アカウント作成時に AWS で有効になります。Amazon ECS で API およびコンソール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] で AWS のその他のサービスのイベントとともに CloudTrail イベントにレコードされます。最近のイベントは、AWSアカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrailイベント履歴でのイベントの表示」を参照してください。

Amazon ECS のイベントを含む、AWS アカウントでのイベントを継続的に記録するために、CloudTrail がログファイルを Amazon S3 バケットに配信する際に使用する証跡を作成します。デフォルトでは、コンソールで追跡を作成するときに、追跡がすべてのリージョンに適用されます。証跡は、AWSパーティション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 ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、「the section called “AWS CloudTrail を使用して Amazon ECS API コールをログに記録する”」を参照してください。

PutAccountSettingDefault API アクションを示す CloudTrail ログエントリの例を次に示します。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIV5AJI5LXF5EXAMPLE",
         "arn": "arn:aws:iam::123456789012:user/jdoe",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIPWIOFC3EXAMPLE",
    },
    "eventTime": "2023-03-01T21:45:18Z",
    "eventSource": "ecs.amazonaws.com",
    "eventName": "PutAccountSettingDefault",
    "awsRegion": "us-gov-east-1",
    "sourceIPAddress": "52.94.133.131",
    "userAgent": "aws-cli/2.9.8 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
ecs.put-account-setting",
```

```
    "requestParameters": {
        "name": "fargateFIPSMode",
        "value": "enabled"
    },
    "responseElements": {
        "setting": {
            "name": "fargateFIPSMode",
            "value": "enabled",
            "principalArn": "arn:aws:iam::123456789012:user/jdoe"
        }
    },
    "requestID": "acdc731e-e506-447c-965d-f5f75EXAMPLE",
    "eventID": "6afced68-75cd-4d44-8076-0beEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "ecs-fips.us-gov-east-1.amazonaws.com"
    }
}
```


Amazon Elastic Container Service におけるインフラストラクチャセキュリティ

マネージドサービスとして、Amazon Elastic Container Service は AWS グローバルネットワークセキュリティによって保護されています。AWS セキュリティサービスと AWS がインフラストラクチャを保護する方法については「AWS クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには「セキュリティの柱 - AWS 適切なアーキテクチャを備えたフレームワーク」の「インフラストラクチャの保護」を参照してください。

AWS が公開している API コールを使用し、ネットワーク経由で Amazon ECS にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。

- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードはJava 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。またはAWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

これらの API オペレーションは任意のネットワークの場所から呼び出すことができます。Amazon ECS は、リソースベースのアクセスポリシーをサポートしており、送信元 IP アドレスに基づく制限を含めることができるため、ポリシーがネットワークロケーションの IP アドレスを考慮していることを確認してください。また、Amazon ECS ポリシーを使用して、特定の Amazon Virtual Private Cloud エンドポイントまたは特定の VPC からのアクセスを制御することもできます。これにより、実質的に AWS ネットワーク内の特定の VPC からの特定の Amazon ECS リソースへのネットワークアクセスが分離されます。詳細については、「Amazon ECS とインターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

Amazon ECS とインターフェイス VPC エンドポイント (AWS PrivateLink)

インターフェイス VPC エンドポイントを使用するように Amazon ECS を設定することで、VPC のセキュリティ体制を強化できます。インターフェイスエンドポイントは、AWS PrivateLink (プライベート IP アドレスを使用した Amazon ECS API へのプライベートなアクセスを可能にするテクノロジ) により動作しています。AWS PrivateLink は、VPC とAmazon ECS 間のすべてのネットワークトラフィックを、Amazon ネットワークに制限します。インターネットゲートウェイ、NAT デバイス、または仮想プライベートゲートウェイは必要ありません。

AWS PrivateLink および VPC エンドポイントの詳細については、「Amazon VPC ユーザーガイド」の「Amazon VPC エンドポイント」を参照してください。

考慮事項

2023 年 12 月 23 日以降に導入されたリージョンのエンドポイントに関する考慮事項

Amazon ECS 用のインターフェイス VPC エンドポイントを設定する前に、以下の考慮事項に注意してください：

- 次のリージョン固有の VPC エンドポイントが必要です。

> **Note**
>
> すべてのエンドポイントを設定しなかった場合、トラフィックが経由するのは VPC エンドポイントではなく、パブリックエンドポイントになります。

- `com.amazonaws.region.ecs-agent`
- `com.amazonaws.region.ecs-telemetry`
- `com.amazonaws.region.ecs`

例えば、カナダ西部 (カルガリー) (ca-west-1) リージョンでは、次の VPC エンドポイントが必要です。

- `com.amazonaws.ca-west-1.ecs-agent`
- `com.amazonaws.ca-west-1.ecs-telemetry`
- `com.amazonaws.ca-west-1.ecs`

- テンプレートを使用して新しいリージョンに AWS リソースを作成する際に、2023 年 12 月 23 日以前に導入されたリージョンのテンプレートをコピーした場合は、コピー元のリージョンに応じて次のいずれかの操作を実行してください。

  例えば、コピー元のリージョンが米国東部 (バージニア北部) (us-east-1) であるとします。コピー先のリージョンは、カナダ西部 (カルガリー) (ca-west-1) です。

設定	アクション
コピー元のリージョンには VPC エンドポイントがありません。	新しいリージョンの 3 つの VPC エンドポイントをすべて作成します (例: `com.amazonaws.ca-west-1.ecs-agent`)。
コピー元のリージョンに、リージョン固有の VPC エンドポイントが含まれています。	a. 新しいリージョンの 3 つの VPC エンドポイントをすべて作成します (例: `com.amazonaws.ca-west-1.ecs-agent`)。

設定	アクション	
	b. コピー元のリージョンの 3 つの VPC エンドポイントをすべて削除します (例: `com.amazonaws.us-east-1.ecs-agent`)。	

Fargate 起動タイプの Amazon ECS VPC エンドポイントに関する考慮事項

Fargate タスクがデプロイされているのと同じ VPC に `ecr.dkr` および `ecr.api` の VPC エンドポイントがある場合は、その VPC エンドポイントが使用されます。VPC エンドポイントがない場合は、Fargate インターフェースが使用されます。

Amazon ECS 用のインターフェイス VPC エンドポイントを設定する前に、以下の考慮事項に注意してください：

- Fargate 起動タイプを使用するタスクでは、Amazon ECS 用のインターフェイス VPC エンドポイントは必要ありませんが、以下のように Amazon ECR のインターフェース VPC エンドポイント、Secrets Manager、または Amazon CloudWatch Logsが必要になる場合があります。
  - Amazon ECR からプライベートイメージをプルできるようにするには、Amazon ECR 用のインターフェイス VPC エンドポイントを 作成する必要があります。詳細については、Amazon Elastic Container Registry ユーザーガイドの「インターフェイス VPC エンドポイント (AWS PrivateLink)」を参照してください。

    > **Important**
    >
    > インターフェイス VPC エンドポイントを使用するよう Amazon ECR を設定する場合、特定の VPC または VPC エンドポイントへのアクセスを制限する条件キーを含むタスク実行ロールを作成できます。詳細については、「インターフェイスエンドポイントのアクセス許可によって Amazon ECR イメージをプルする Fargate タスクです。」を参照してください。

  - タスクで Secrets Manager から機密データをプルできるようにするには、Secrets Manager 用のインターフェイス VPC エンドポイントを作成する必要があります。詳細については、AWS Secrets Managerユーザーガイドの「VPC エンドポイントで Secrets Manager を作成する」を参照してください。

  - VPC にインターネットゲートウェイがなく、タスクで `awslogs` ログドライバーを使用してログ情報を CloudWatch Logs に送信する場合は、CloudWatch Logs 用のインターフェイス VPC エンドポイントを作成する必要があります。詳細については、Amazon CloudWatch Logs ユーザーガイドの「インターフェイス VPC エンドポイントでの CloudWatch Logs の使用」を参照してください。
- 現在、VPC エンドポイントはクロスリージョンリクエストをサポートしていません。Amazon ECS に対して API コールを発行するリージョンと同じリージョンにエンドポイントを作成してください。 例えば、タスクを米国東部 (バージニア北部) で実行することを考えてみます。その場合、Amazon ECS VPC エンドポイントは、米国東部 (バージニア北部) に作成する必要があります。他のリージョンで作成された Amazon ECS VPC エンドポイントは、米国東部 (バージニア北部) 内のタスクを実行できません。
- VPC エンドポイントでは、Amazon Route 53 を介して Amazon 提供の DNS のみがサポートされています。独自の DNS を使用したい場合は、条件付き DNS 転送を使用できます。詳細については、Amazon VPC ユーザーガイドのDHCP Options Setsを参照してください。
- VPCエンドポイントにアタッチされたセキュリティグループは、VPCのプライベートサブネットからの着信接続をポート 443 で許可する必要があります。
- Envoy プロキシの Service Connect 管理では、`com.amazonaws.region.ecs-agent` VPC エンドポイントを使用します。VPC エンドポイントを使用しない場合、Envoy プロキシの Service Connect 管理は、そのリージョンの `ecs-sc` エンドポイントを使用します。各リージョンの Amazon ECS エンドポイントのリストについては、「Amazon ECS のエンドポイントとクォータ」を参照してください。

EC2 起動タイプの Amazon ECS VPC エンドポイントに関する考慮事項

Amazon ECS 用のインターフェイス VPC エンドポイントを設定する前に、以下の考慮事項に注意してください：

- EC2 起動タイプを使用するタスクでは、起動されたコンテナインスタンスが Amazon ECS コンテナエージェントのバージョン `1.25.1` 以降を実行する必要があります。詳細については、「Amazon ECS Linux コンテナインスタンスの管理」を参照してください。
- タスクで Secrets Manager から機密データをプルできるようにするには、Secrets Manager 用のインターフェイス VPC エンドポイントを作成する必要があります。詳細については、AWS Secrets Managerユーザーガイドの「VPC エンドポイントで Secrets Manager を作成する」を参照してください。

- VPC にインターネットゲートウェイがなく、タスクで awslogs ログドライバーを使用してログ情報を CloudWatch Logs に送信する場合は、CloudWatch Logs 用のインターフェイス VPC エンドポイントを作成する必要があります。詳細については、Amazon CloudWatch Logs ユーザーガイドの「インターフェイス VPC エンドポイントでの CloudWatch Logs の使用」を参照してください。
- 現在、VPC エンドポイントはクロスリージョンリクエストをサポートしていません。Amazon ECS に対して API コールを発行するリージョンと同じリージョンにエンドポイントを作成してください。 例えば、タスクを米国東部 (バージニア北部) で実行することを考えてみます。その場合、Amazon ECS VPC エンドポイントは、米国東部 (バージニア北部) に作成する必要があります。他のリージョンで作成された Amazon ECS VPC エンドポイントは、米国東部 (バージニア北部) 内のタスクを実行できません。
- VPC エンドポイントでは、Amazon Route 53 を介して Amazon 提供の DNS のみがサポートされています。独自の DNS を使用したい場合は、条件付き DNS 転送を使用できます。詳細については、Amazon VPC ユーザーガイドのDHCP Options Setsを参照してください。
- VPCエンドポイントにアタッチされたセキュリティグループは、VPCのプライベートサブネットからの着信接続をポート 443 で許可する必要があります。

Amazon ECS 用の VPC エンドポイントの作成

Amazon ECS サービス用の VPC エンドポイントを作成するには、「Amazon VPC ユーザーガイド」の「インターフェイスVPCエンドポイント AWS のサービス を使用して にアクセスする」の手順を使用して、以下のエンドポイントを作成します。VPC 内に既存のコンテナインスタンスがある場合は、一覧表示されている順にエンドポイントを作成する必要があります。VPC エンドポイントが作成された後にコンテナインスタンスを作成する場合、順序は関係ありません。

> **Note**
>
> すべてのエンドポイントを設定しなかった場合、トラフィックが経由するのは VPC エンドポイントではなく、パブリックエンドポイントになります。
> エンドポイントを作成すると、Amazon ECS はエンドポイントのプライベート DNS 名も作成します。例えば、ecs-agent の `ecs-a.region.amazonaws.com` とecs-telemetry の `ecs-t.region.amazonaws.com` です。

- `com.amazonaws.region.ecs-agent`
- `com.amazonaws.region.ecs-telemetry`

- com.amazonaws.*region*.ecs

> **Note**
>
> *region* は、米国東部 (オハイオ) リージョンの us-east-2 のように、Amazon ECS でサポートされている AWS リージョンのリージョン識別子を表します。

ecs-agent エンドポイントは ecs:poll API を使用し、ecs-telemetry エンドポイントは ecs:poll および ecs:StartTelemetrySession API を使用します。

EC2 起動タイプを使用する既存のタスクがある場合は、VPC エンドポイントを作成した後に、各コンテナインスタンスで新しい設定が選択される必要があります。そのためには、各コンテナインスタンスを再起動するか、各コンテナインスタンスで Amazon ECS コンテナエージェントを再起動する必要があります。コンテナエージェントを再起動するには、以下を実行します。

Amazon ECS コンテナエージェントを再起動するには

1. SSH 経由でコンテナインスタンスにログインします。
2. コンテナエージェントを停止します。

```
sudo docker stop ecs-agent
```

3. コンテナエージェントを開始します。

```
sudo docker start ecs-agent
```

VPC エンドポイントを作成し、各コンテナインスタンスで Amazon ECS コンテナエージェントを再起動したら、新しく起動されるすべてのタスクで新しい設定が選択されます。

Amazon ECS 用の VPC エンドポイントポリシーの作成

VPC エンドポイントに Amazon ECS へのアクセスをコントロールするエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル。
- 実行可能なアクション。

- アクションを実行できるリソース。

詳細については、Amazon VPC ユーザーガイドの「VPC エンドポイントによるサービスのアクセスコントロール」を参照してください。

例: Amazon ECS アクションの VPC エンドポイントポリシー

Amazon ECS のエンドポイントポリシーの例を次に示します。このポリシーは、エンドポイントに接続すると、クラスターの作成や一覧表示が行えるようにアクセスを許可します。CreateCluster と ListClusters のアクションはリソースを受け入れないため、すべてのリソースでリソース定義は * に設定されます。

```
{
   "Statement":[
    {
      "Effect": "Allow",
      "Action": [
        "ecs:CreateCluster",
        "ecs:ListClusters"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Amazon ECS の AWS 責任共有モデル。

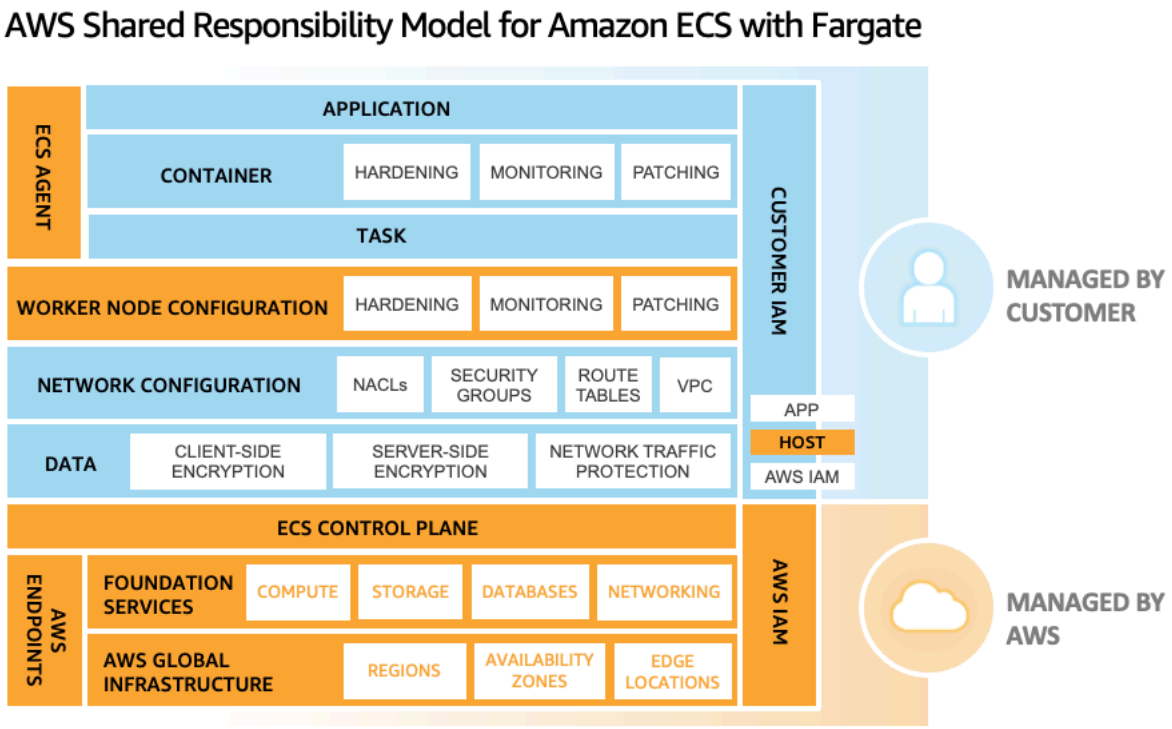
セキュリティとコンプライアンスに関して、AWS とお客様の間で責任を共有します。この共有モデルにより、ホストオペレーティングシステムや仮想化レイヤーからサービスが運用されている施設の物理的なセキュリティに至るまで、さまざまなコンポーネントを AWS が運用、管理、制御するため、お客様の運用の負担が軽減されます。お客様は、AWS が提供するセキュリティグループのファイアウォール設定に加えて、ゲストオペレーティングシステム (更新やセキュリティパッチを含む) およびその他の関連アプリケーションソフトウェアを管理し、責任を持って管理する必要があります。お客様の責任範囲は、使用するサービス、IT 環境へのサービス統合、適用される法規制に応じて異なります。このため、お客様は選択するサービスを注意深く検討する必要があります。この責任共有モデルの性質によって柔軟性が得られ、お客様はデプロイを統制できます。

Fargate 起動タイプ

次の図は、Fargate 起動タイプの責任共有モデルを示しています。Fargate は分離されたハードウェア仮想化環境で各ワークロードを実行します。その結果、各タスクは専用のインフラストラクチャキャパシティを取得します。Fargate で実行されているコンテナ化されたワークロードは、オペレーティングシステム、Linux カーネル、ネットワークインターフェイス、エフェメラルストレージ、CPU、またはメモリを他のタスクと共有しません。Fargate を使用する場合、お客様はコンテナを実行するコンピューティングインフラストラクチャのセキュリティを管理する責任を負いません。Fargate は、お客様のワークロードを実行するインフラストラクチャをプロビジョニングしてパッチを適用します。詳細については、「AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス」を参照してください。

お客様は次のリソースを管理する責任があります。

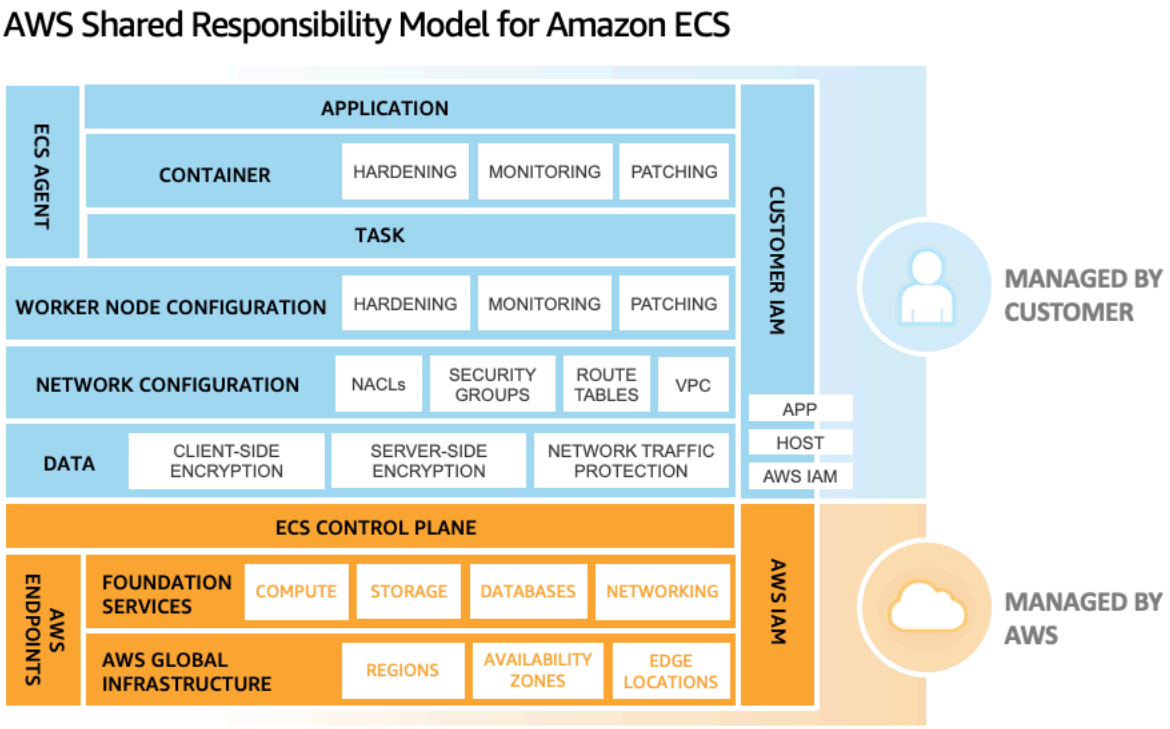
- VPC、NACL、セキュリティグループ、ルートテーブルなどのネットワーク設定
- クライアントとサービスストレージの暗号化。詳細については、「Amazon ECS タスクのストレージオプション」を参照してください。
- コンテナイメージ 詳細については、「Amazon ECS タスクおよびコンテナのセキュリティのベストプラクティス」を参照してください。
- タスクロールを使用したアプリケーションの IAM アクセス許可。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。



EC2 起動タイプ

次の図は、EC2 起動タイプの責任共有を示しています。EC2 インスタンスでタスクを実行する場合、次のリソースに加えて EC2 インスタンスを保守する責任があります。

- Amazon ECS エージェント。
- • パッチ適用と強化を含む EC2 インスタンス AMI。
- VPC、NACL、セキュリティグループ、ルートテーブルなどのネットワーク設定。
- クライアントとサービスストレージの暗号化。詳細については、「Amazon ECS タスクのストレージオプション」を参照してください。
- コンテナイメージ 詳細については、「Amazon ECS タスクおよびコンテナ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。
- タスクロールを使用したアプリケーションの IAM アクセス許可。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。



Amazon ECS のネットワークセキュリティのベストプラクティス

ネットワークセキュリティは、いくつかのサブトピックを含む幅広いトピックです。これには、転送中の暗号化、ネットワークのセグメンテーションと分離、ファイアウォール、トラフィックルーティング、オブザーバビリティなどが含まれます。

転送中の暗号化

ネットワークトラフィックを暗号化することで、データがネットワーク経由で送信されるときに、権限のないユーザーにデータを傍受されて読み取られることを防ぎます。Amazon ECS では、次のいずれかの方法でネットワーク暗号化を実装できます。

- Nitro インスタンスを使用する:

  デフォルトでは、C5n、G4、I3en、M5dn、M5n、P3dn、R5dn、R5n の Nitro インスタンスタイプ間のトラフィックは自動的に暗号化されます。トラフィックがトランジットゲートウェイ、ロードバランサー、または同様の仲介を経由する場合、トラフィックは暗号化されません。

  - 転送時の暗号化
  - 2019年の新発表
  - 「リ・インフォース 2019」からの会話

- Application Load Balancer で Server Name Indication (SNI) を使用する

  Application Load Balancer (ALB) と Network Load Balancer (NLB) は、Server Name Indication (SNI) をサポートします。SNI を使用すると、複数の安全なアプリケーションを 1 つのリスナーのバックグラウンドに配置できます。そのため、各リスナーには独自の TLS 証明書があります。AWS Certificate Manager (ACM) を使用してロードバランサーの証明書をプロビジョニングし、リスナーの証明書リストに追加することをお勧めします。AWS ロードバランサーは、SNI を使用するスマート証明書の選択アルゴリズムを使用します。クライアントから提供されたホスト名と一致する証明書がリスト内にひとつだけある場合、ロードバランサーはこの証明書を選択します。クライアントが提供するホスト名と一致する証明書がリスト内に複数ある場合、ロードバランサーはクライアントがサポートできる証明書を選択します。例として、自己署名証明書や ACM を通じて生成された証明書などがあげられます。

  - Application Load Balancer で SNI を使用する
  - Network Load Balancer で SNI を使用する
- TLS 証明書を使用したエンドツーエンド暗号化:

  これには、タスクとともに TLS 証明書をデプロイすることが含まれます。自己署名証明書でも、信頼できる認証局からの証明書でもかまいません。証明書のシークレットを参照することで証明書を取得できます。それ以外の場合は、ACM に証明書署名リクエスト (CSR) を発行し、その結果得られたシークレットを共有ボリュームにマウントするコンテナを実行することもできます。

  - Amazon ECS でNetwork Load Balancer を使用してコンテナまでトランスポートレイヤーのセキュリティを維持する (パート 1)
  - コンテナまで Transport Layer Security (TLS) を維持する (パート 2): AWS Private Certificate Authority を使用する

タスクネットワーク

以下の推奨事項は Amazon ECS の仕組みに関する考慮したものです。Amazon ECS はオーバーレイネットワークを使用しません。代わりに、タスクは異なるネットワークモードで動作するように設定されます。たとえば、`bridge` モードを使用するように設定されたタスクは、各ホストで実行される Docker ネットワークからルーティングできない IP アドレスを取得します。`awsvpc` ネットワークモードを使用するように設定されたタスクは、ホストのサブネットから IP アドレスを取得します。`host` ネットワークを使用して構成されたタスクはホストのネットワークインターフェースを使用します。`awsvpc` が推奨ネットワークモードです。これは、タスクにセキュリティグループを割り当てるのに使用できる唯一のモードであるため推奨されます。また、Amazon ECS の AWS Fargate タスクで使用できる唯一のモードでもあります。

タスクのセキュリティグループ

awsvpc ネットワークモードを使用するようにタスクを設定することをお勧めします。このモードを使用するようにタスクを設定すると、Amazon ECS エージェントは自動的に Elastic Network Interface (ENI) をプロビジョニングしてタスクにアタッチします。ENI がプロビジョニングされると、タスクは AWS セキュリティグループに登録されます。セキュリティグループは、インバウンドトラフィックとアウトバウンドトラフィックをコントロールするための仮想ファイアウォールとして機能します。

AWS PrivateLink および Amazon ECS

AWS PrivateLink は Amazon ECS を含むさまざまな AWS サービスのプライベートエンドポイントを作成できるようにするネットワーク技術です。エンドポイントは、Amazon VPC に Internet Gateway (IGW) が接続されておらず、インターネットへの代替ルートもないサンドボックス環境で必要となります。AWS PrivateLink を使用することで、Amazon ECS サービスへの呼び出しが Amazon VPC 内にとどまり、インターネットを経由しないことが保証されます。Amazon ECS およびその他の関連サービスの AWS PrivateLink エンドポイントを作成する方法については、「Amazon ECS インターフェイス Amazon VPC エンドポイント」を参照してください。

> **Important**
>
> AWS Fargate タスクには Amazon ECS の AWS PrivateLink エンドポイントは必要ありません。

Amazon ECR と Amazon ECS はどちらもエンドポイントポリシーをサポートしています。これらのポリシーにより、サービスの API へのアクセスを絞り込むことができます。たとえば、特定の AWS アカウントのレジストリにのみイメージをプッシュすることを許可する Amazon ECR のエンドポイントポリシーを作成できます。このようなポリシーは、コンテナイメージを通じてデータが流出するのを防ぎつつ、ユーザーが許可された Amazon ECR レジストリにプッシュできるようにするために使用できます。詳細については、「VPC エンドポイントポリシーの使用」を参照してください。

以下のポリシーでは、アカウントのすべての AWS プリンシパルが Amazon ECR リポジトリに対してのみ、すべてのアクションを実行できるようにします。

```
{
  "Statement": [
    {
```

```
      "Sid": "LimitECRAccess",
      "Principal": "*",
      "Action": "*",
      "Effect": "Allow",
      "Resource": "arn:aws:ecr:region:account_id:repository/*"
    },
  ]
}
```

新しい PrincipalOrgID プロパティを使用する条件を設定することで、これをさらに強化できます。これにより、ユーザーの AWS Organizations の一部ではない IAM プリンシパルによるイメージのプッシュやプルを防ぐことができます。詳細については、「aws:PrincipalOrgID」を参照してください。

com.amazonaws.*region*.ecr.dkr と com.amazonaws.*region*.ecr.api エンドポイントの両方に同じポリシーを適用することをお勧めします。

コンテナエージェントの設定

Amazon ECS コンテナエージェント設定ファイルには、ネットワークセキュリティに関連する複数の環境変数が含まれています。ECS_AWSVPC_BLOCK_IMDS と ECS_ENABLE_TASK_IAM_ROLE_NETWORK_HOST は、Amazon EC2 メタデータへのタスクのアクセスをブロックするために使用されます。HTTP_PROXY は、HTTP プロキシを経由してインターネットに接続するようにエージェントを設定するために使用されます。エージェントと Docker ランタイムをプロキシ経由でルーティングするように設定する方法については、「HTTP プロキシ設定」を参照してください。

> **Important**
>
> AWS Fargate を使用する場合は、これらの設定を使用することはできません。

ネットワークセキュリティに関する推奨事項

Amazon VPC、ロードバランサー、ネットワークを設定するときは、次のことを行うことをお勧めします。

Amazon ECS で必要に応じてネットワーク暗号化を使用する

必要に応じてネットワーク暗号化を使用してください。PCI DSS などの特定のコンプライアンスプログラムでは、データにカード所有者のデータが含まれている場合、転送中のデータを暗号化する必要があります。ワークロードに同様の要件がある場合は、ネットワーク暗号化を設定してください。

最新のブラウザでは、安全でないサイトに接続するとユーザーに警告が表示されます。公開されているロードバランサーがサービスのフロントエンドで使用されている場合は、TLS/SSL を使用してクライアントのブラウザーからロードバランサーへのトラフィックを暗号化し、必要に応じてバックエンドで再暗号化します。

`awsvpc` ネットワークモードとセキュリティグループを使用して、Amazon ECS のタスクと他のリソース間のトラフィックを制御する

タスク間のトラフィック、またはタスクと他のネットワークリソース間のトラフィックを制御する必要がある場合は、`awsvpc` ネットワークモードとセキュリティグループを使用してください。サービスが ALB の背後にある場合は、セキュリティグループを使用して、ALB と同じセキュリティグループを使用する他のネットワークリソースからのインバウンドトラフィックのみを許可します。アプリケーションが NLB の背後にある場合は、Amazon VPC CIDR 範囲からのインバウンドトラフィックと NLB に割り当てられた静的 IP アドレスのみを許可するようにタスクのセキュリティグループを設定します。

セキュリティグループは、タスクと Amazon VPC 内の他のリソース (Amazon RDS データベースなど) との間のトラフィックを制御するためにも使用する必要があります。

ネットワークトラフィックを厳密に分離する必要がある場合に、別の Amazon VPC に Amazon ECS クラスターを作成する

ネットワークトラフィックを厳密に分離する必要がある場合は、別の Amazon VPC にクラスターを作成してください。セキュリティ要件が厳しいワークロードを、その要件を満たす必要のないワークロードを含むクラスターで実行することは避けてください。ネットワークの厳密な分離が必須の場合は、別の Amazon VPC にクラスターを作成し、Amazon VPC エンドポイントを使用して他の Amazon VPC にサービスを選択的に公開します。詳細については、「VPC エンドポイント」を参照してください。

Amazon ECS で必要に応じて AWS PrivateLink エンドポイントを設定する

AWS PrivateLink エンドポイントは、必要に応じて設定してください。セキュリティポリシーにより Amazon VPC にインターネットゲートウェイ (IGW) をアタッチできない場合は、Amazon

ECS や Amazon ECR、AWS Secrets Manager、Amazon CloudWatch などの他のサービスの AWS PrivateLink エンドポイントを設定します。

Amazon VPC フローログを使用して、Amazon ECS の長時間実行されるタスクとの間のトラフィックを分析する

長時間実行されるタスクとの間のトラフィックを分析するには、Amazon VPC フローログを使用してください。awsvpc ネットワークモードを使用するタスクには独自の ENI が割り当てられます。これにより、Amazon VPC フローログを使用して個々のタスクに出入りするトラフィックをモニタリングできます。Amazon VPC フローログ (v3) の最新アップデートでは、VPC ID、サブネット ID、インスタンス ID などのトラフィックメタデータがログに追加されました。このメタデータを使用して、調査を絞り込むことができます。詳細については、「Amazon VPC フローログ」を参照してください。

> **Note**
>
> コンテナは一時的な性質を持つため、フローログは、異なるコンテナの間やコンテナとその他のネットワークリソースの間のトラフィックパターンを分析するうえで必ずしも効果的な方法であるとは限りません。

Amazon ECS タスクおよびコンテナのセキュリティのベストプラクティス

コンテナイメージは、攻撃に対する防御の最前線と見なしてください。安全性が低く、構築が不十分なイメージがあると、攻撃者はコンテナの境界を抜け出し、ホストにアクセスできるようになる可能性があります。これが発生するリスクを軽減するには、次のことを行う必要があります。

タスクとコンテナを設定するときは、次のことを行うことをお勧めします。

最小限のイメージを作成するか、distroless のイメージを使用する

まず、コンテナイメージから不要なバイナリをすべて削除します。Amazon ECR Public Gallery にある見慣れないイメージを使用している場合は、そのイメージを調べてコンテナの各レイヤーの内容を参照してください。これには Dive などのアプリケーションを使用できます。

あるいは、アプリケーションとそのランタイム依存関係のみを含む distroless イメージを使用することもできます。パッケージマネージャーやシェルは含まれません。Distroless イメージは、「スキャ

ナーの信号対雑音比を向上させ、必要なものだけを調達する負担を軽減する」ことができます。詳細については、GitHub の distroless に関するドキュメントを参照してください。

Docker には、scratch と呼ばれる、予約済みの最小限のイメージからイメージを作成するメカニズムがあります。詳細については、Docker ドキュメントの「scratch を使用した単純な親イメージの作成」を参照してください。Go などの言語では、静的にリンクされたバイナリを作成して Dockerfile で参照できます。以下の例で、その方法を示します。

```
############################
# STEP 1 build executable binary
############################
FROM golang:alpine AS builder
# Install git.
# Git is required for fetching the dependencies.
RUN apk update && apk add --no-cache git
WORKDIR $GOPATH/src/mypackage/myapp/
COPY . .
# Fetch dependencies.
# Using go get.
RUN go get -d -v
# Build the binary.
RUN go build -o /go/bin/hello
############################
# STEP 2 build a small image
############################
FROM scratch
# Copy our static executable.
COPY --from=builder /go/bin/hello /go/bin/hello
# Run the hello binary.
ENTRYPOINT ["/go/bin/hello"]
This creates a container image that consists of your application and nothing else,
 making it extremely secure.
```

前の例も、マルチステージビルドの例です。これらのタイプのビルドは、コンテナレジストリにプッシュされる最終イメージのサイズを最小限に抑えることができるため、セキュリティの観点からは魅力的です。コンテナイメージからビルドツールやその他の無関係なバイナリを省くことで、イメージのアタックサーフェスが減り、セキュリティ対策を強化することができます。マルチステージビルドの詳細については、Docker ドキュメントの「Multi-stage builds」を参照してください。

イメージをスキャンして脆弱性がないか調べる

対応する仮想マシンと同様に、コンテナイメージには脆弱性のあるバイナリやアプリケーションライブラリが含まれていたり、時間の経過とともに脆弱性が生じたりする可能性があります。エクスプロイトから保護する最善の方法は、イメージスキャナーでイメージを定期的にスキャンすることです。

Amazon ECR に保存されている画像は、プッシュまたはオンデマンド (24 時間に 1 回) でスキャンできます。Amazon ECR のベーシックスキャンでは、オープンソースのイメージスキャンソリューションである Clair を使用します。Amazon ECR の拡張スキャンでは、Amazon Inspector を使用します。イメージがスキャンされると、その結果は Amazon EventBridge の Amazon ECR イベントストリームにログが残ります。また、Amazon ECR コンソール内から、あるいは DescribeImageScanFindings API を呼び出して、スキャンの結果を確認することもできます。脆弱性が `HIGH` または `CRITICAL` のイメージは、削除するか再構築する必要があります。デプロイされたイメージに脆弱性が生じた場合は、できるだけ早く交換する必要があります。

Docker Desktop Edge バージョン 2.3.6.0 以降では、ローカルイメージをスキャンできます。スキャンはアプリケーションセキュリティサービスの Snyk によって行われます。脆弱性が発見されると、Snyk は Dockerfile 内の脆弱性のあるレイヤーと依存関係を識別します。また、脆弱性が少なく、よりスリムなベースイメージを使用したり、特定のパッケージを新しいバージョンにアップグレードしたりするなど、安全な代替手段も推奨します。Docker スキャンを使用すれば、開発者はイメージをレジストリにプッシュする前に、潜在的なセキュリティ問題を解決できます。

- Amazon ECR と AWS Security Hub を使用してイメージコンプライアンスを自動化するでは、AWS Security Hub の Amazon ECR から脆弱性情報を検出し、脆弱なイメージへのアクセスをブロックすることで修復を自動化する方法について説明します。

イメージから特別な権限を削除する

アクセス権フラグ`setuid` と `setgid` は、実行ファイルの所有者またはグループの権限で実行できるようにします。これらのアクセス権限を持つバイナリは権限昇格に利用される可能性があるため、イメージからすべてのバイナリを削除してください。悪意のある目的に使用される可能性のある、`nc` や `curl` などのシェルやユーティリティをすべて削除することを検討してください。次のコマンドを使用すると `setuid` および `setgid` アクセス権のあるファイルを見つけることができます。

```
find / -perm /6000 -type f -exec ls -ld {} \;
```

これらのファイルから、これらの特別な権限を削除するには、以下のディレクティブをコンテナイメージに追加します。

```
RUN find / -xdev -perm /6000 -type f -exec chmod a-s {} \; || true
```

キュレーションされたイメージのセットを作成する

開発者が独自のイメージを作成できるようにするのではなく、組織内のさまざまなアプリケーションスタック用に、検証済みのイメージセットを作成することができます。そうすることで、開発者は Dockerfile の作成方法を学ぶ必要がなくなり、コードの記述に集中できます。変更がコードベースにマージされると、CI/CD パイプラインがアセットを自動的にコンパイルし、アーティファクトリポジトリに保存できます。最後に、アーティファクトを適切なイメージにコピーしてから、Amazon ECR などの Docker レジストリにプッシュします。少なくとも、開発者が独自の Dockerfile を作成できるようなベースイメージのセットを作成する必要があります。Docker Hub からイメージをプルすることは避けてください。イメージに何が入っているかを常に把握できるわけではなく、上位 1000 個のイメージの約 5 分の 1 に脆弱性があります。これらのイメージとその脆弱性のリストは https://vulnerablecontainers.org/ で確認できます。

アプリケーションパッケージとライブラリをスキャンして脆弱性がないか調べる

オープンソースライブラリの使用は今や一般的になっています。オペレーティングシステムや OS パッケージと同様に、これらのライブラリには脆弱性が潜んでいる可能性があります。開発ライフサイクルの一環として、重大な脆弱性が見つかった場合は、これらのライブラリをスキャンして更新する必要があります。

Docker Desktop は Snyk を使用してローカルスキャンを実行します。また、オープンソースライブラリの脆弱性や潜在的なライセンス問題の検出にも使用できます。開発者のワークフローに直接統合できるため、オープンソースライブラリがもたらすリスクを軽減できます。詳細については、以下の各トピックを参照してください。

- オープンソースのアプリケーションセキュリティツールには、アプリケーションの脆弱性を検出するためのツールのリストが含まれています。

静的コード分析を行う

コンテナイメージを構築する前に、静的コード分析を実行する必要があります。これはソースコードに対して実行され、コーディングエラーや、フォールトインジェクションなどの悪意のある攻撃者に悪用される可能性のあるコードの特定に使用されます。Amazon Inspector を使用できます。詳細については、「Amazon Inspector ユーザーガイド」の「Amazon Inspector による Amazon ECR コンテナイメージのスキャン」を参照してください。

非ルートユーザーとしてコンテナを実行する

コンテナを実行するときは、非ルートユーザーとして実行してください。デフォルトでは、Dockerfile に USER ディレクティブが含まれていない限り、コンテナは `root` ユーザーとして実行されます。Docker によって割り当てられるデフォルトの Linux 機能では、`root` として実行できるアクションが制限されますが、制限されるのはごくわずかです。例えば、`root` として実行しているコンテナは、デバイスにアクセスすることがまだできません。

CI/CD パイプラインの一部として、Dockerfiles をリントして USER ディレクティブを探し、見つからない場合はビルドを失敗させる必要があります。詳細については、以下の各トピックを参照してください。

- Dockerfile-lint は RedHat のオープンソースツールで、ファイルがベストプラクティスに準拠しているかどうかを確認するために使用できます。
- Hadolint も、ベストプラクティスに準拠した Docker イメージを構築するためのツールです。

読み取り専用のルートファイルシステムを使用する

読み取り専用のルートファイルシステムを使用してください。コンテナのルートファイルシステムは、デフォルトでは書き込み可能です。コンテナに RO (読み取り専用) ルートファイルシステムを設定すると、データを保存できる場所を明示的に定義する必要性が生じます。これにより、権限が具体的に付与されない限りコンテナのファイルシステムに書き込みができなくなるため、アタックサーフェスが減少します。

> **Note**
>
> ルートファイルシステムが読み取り専用であると、そのファイルシステムへの書き込みが可能であることを想定している特定の OS パッケージで問題が発生する可能性があります。読

み取り専用のルートファイルシステムを使用する予定がある場合は、事前に十分にテストしてください。

CPU とメモリの制限を設定してタスクを設定する (Amazon EC2)

以下のリスクを最小限に抑えるには、CPU とメモリの制限を設定してタスクを設定する必要があります。タスクのリソース制限は、タスク内のすべてのコンテナで予約できる CPU とメモリの量の上限を設定します。制限が設定されていない場合、タスクはホストの CPU とメモリにアクセスできます。これにより、共有ホストにデプロイされたタスクが他のタスクのシステムリソースを枯渇させるという問題が発生する可能性があります。

> **Note**
>
> Amazon ECS on AWS Fargate Tasks では CPU とメモリの制限を指定する必要があります。これらの値は請求目的で使用されるためです。Amazon ECS Fargate では、1 つのタスクがすべてのシステムリソースを占有しても問題にはなりません。各タスクは専有インスタンスで実行されるからです。メモリ制限を指定しない場合、Amazon ECS は各コンテナに最低 4MB を割り当てます。同様に、タスクに CPU 制限が設定されていない場合、Amazon ECS コンテナエージェントはタスクに最低 2 つの CPU を割り当てます。

Amazon ECR でイミュータブルタグを使用する

Amazon ECR では、イミュータブルタグを使用してイメージを設定することができるので、これを使用するようにしてください。これにより、変更または更新されたバージョンの画像が、同一のタグで画像リポジトリにプッシュされるのを防ぐことができます。また、攻撃者が侵害されたバージョンのイメージを同じタグが付いたイメージにプッシュすることを防ぐことができます。イミュータブルタグを使用すれば、変更するたびに異なるタグが付いた新しいイメージを効果的にプッシュできます。

コンテナを特権として実行することは避けてください (Amazon EC2)

コンテナを特権として実行することは避けてください。バックグラウンドでは、`privileged` として実行されるコンテナは、ホスト上で拡張された権限でされます。つまり、ホスト上で `root` に割り当てられた Linux 機能がすべてコンテナに継承されるということです。その使用は厳しく制限するか禁止してください。Amazon ECS コンテナエージェント環境変数 `ECS_DISABLE_PRIVILEGED` を `true` に設定して、`privileged` が必要がない場合はコンテナが `privileged` として特定のホスト

で実行されないようにすることをお勧めします。あるいは、AWS Lambda を使用してタスク定義をスキャンして `privileged` パラメータを使用することもできます。

> **Note**
>
> AWS Fargate 上の Amazon ECS では、コンテナを `privileged` として実行することはサポートされていません。

不要な Linux 機能をコンテナから削除する

Docker コンテナに割り当てられているデフォルトの Linux 機能のリストを以下に示します。各機能の詳細については、「Linux 機能の概要」を参照してください。

```
CAP_CHOWN, CAP_DAC_OVERRIDE, CAP_FOWNER, CAP_FSETID, CAP_KILL,
CAP_SETGID, CAP_SETUID, CAP_SETPCAP, CAP_NET_BIND_SERVICE,
CAP_NET_RAW, CAP_SYS_CHROOT, CAP_MKNOD, CAP_AUDIT_WRITE,
CAP_SETFCAP
```

コンテナが上記の Docker カーネル機能のすべてを必要としない場合は、それらをコンテナから削除することを検討してください。各 Docker カーネル機能の詳細については、「KernelCapabilities」を参照してください。次の操作を実行することで、どの機能が使われているかを確認できます。

- OS パッケージ libcap-ng をインストールし、`pscap` ユーティリティを実行して各プロセスが使用している機能を一覧表示します。
- capsh を使用して、プロセスが使用している機能を解読することもできます。

カスタマーマネージドキー (CMK) を使用して Amazon ECR にプッシュされるイメージを暗号化する

Amazon ECR にプッシュされるイメージの暗号化には、カスタマーマネージドキー (CMK) を使用してください。Amazon ECR にプッシュされたイメージは、保存時に AWS Key Management Service (AWS KMS) 管理キーで自動的に暗号化されます。独自のキーを使用したい場合は、Amazon ECR ではカスタマーマネージドキー (CMK) による AWS KMS 暗号化がサポートされています。CMK によるサーバー側の暗号化を有効にする前に、「保管データ暗号化」に関するドキュメントに記載されている考慮事項を確認してください。

Amazon ECS のチュートリアル

以下のチュートリアルでは、Amazon ECS の使用時に一般的なタスクを実行する方法を示します。

Amazon ECS の開始方法については、以下のチュートリアルのいずれかを参照してください。

チュートリアルの概要	詳細はこちら
Fargate での Amazon ECS の開始方法	Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する方法について説明します。
Fargate で Windows コンテナの使用を開始する。	Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。
EC2 起動タイプの Windows コンテナの使用を開始する。	EC2 起動タイプ用の Amazon ECS Windows タスクを作成する方法について説明します。

以下のチュートリアルのいずれかを使用すると、AWS CLI を使用して Amazon ECS にタスクをデプロイできます。

チュートリアルの概要	詳細はこちら
Fargate 起動タイプでのタスクの作成	AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する
Fargate 起動タイプでの Windows タスクの作成	AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する

チュートリアルの概要	詳細はこちら	
EC2 起動タイプでの Linux タスクの作成	AWS CLI を使用して、EC2 起動タイプ用の Amazon ECS タスクを作成する	

以下のチュートリアルのいずれかを使用すると、モニタリングとログ記録の詳細を確認できます。

チュートリアルの概要	詳細はこちら	
タスクイベントをリッスンし、CloudWatch Logs ログストリームに書き込むシンプルな Lambda 関数を設定します。	CloudWatch Events イベントをリッスンするように Amazon ECS を設定する	
重要なコンテナのいずれかが終了したことにより、タスクの実行が停止したタスクイベントのみをキャプチャする Amazon EventBridge イベントルールを設定します。	Amazon ECS タスク停止イベントに関する Amazon Simple Notification Service アラートの送信	
もともと 1 つのコンテキストに属していたが、複数のレコードまたはログ行に分割されたログメッセージを連結します。	複数行またはスタックトレースの Amazon ECS ログメッセージの連結	
Amazon ECS で実行されている Windows インスタンスに Fluent Bit コンテナをデプロイし、Windows タスクによって生成されたログを Amazon CloudWatch にストリーミン	Amazon ECS Windows コンテナに Fluent Bit をデプロイする	

チュートリアルの概要	詳細はこちら	
グして集中型ロギングを実行します。		

Amazon ECS のグループ管理サービスアカウントで Active Directory 認証を使用する方法の詳細については、以下のチュートリアルのいずれかを参照してください。

チュートリアルの概要	詳細はこちら	
EC2 上の Linux コンテナで、グループ管理サービスアカウントを使用します。	Amazon EC2 の Linux コンテナで gMSA を使用する	
EC2 上の Windows コンテナで、グループ管理サービスアカウントを使用します。	Amazon ECS の EC2 Windows コンテナで gMSA を使用する方法について説明します。	
Fargate 上の Linux コンテナで、グループ管理サービスアカウントを使用します。	Fargate で Linux コンテナに gMSA を使用する	
ドメインレスグループの Managed Service Account を使用して、Active Directory にアクセスするための認証情報を持つ Windows コンテナを実行するタスクを作成します。	AWS CLI を使用するドメインレス gMSA で Amazon ECS Windows コンテナを使用する	

AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Linux タスクを作成する

次のステップでは、AWS CLI を使って Amazon ECS でクラスターのセットアップ、タスク定義の登録、Linux タスクの実行、その他の一般的なシナリオを実行するために役立ちます。AWS CLI の最

新バージョンを使用する。最新のバージョンにアップグレードする方法については、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

トピック

前提条件

このチュートリアルでは、以下の前提条件をすでに満たしているものとします。

- AWS CLI の最新バージョンがインストールされ、設定されていること。AWS CLI のインストールまたはアップグレードについては、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。
- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- VPC およびセキュリティグループが使用できるように作成されていること。このチュートリアルは、Amazon ECR パブリックにホストされているコンテナ画像を使用するため、タスクではインターネットアクセスが必要になります。タスクでインターネットへのルートを設定するには、以下のいずれかのオプションを使用します。
  - Elastic IP アドレスが割り当てられた NAT ゲートウェイでプライベートサブネットを使用する。
  - パブリックサブネットを使用してタスクにパブリック IP アドレスを割り当てる。

  詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。

セキュリティグループとルールの詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC のデフォルト セキュリティ グループ」および「ルールの例」を参照してください。

- プライベートサブネットを使用してこのチュートリアルを実行すると、Amazon ECS Exec を使用してコンテナを直接操作し、デプロイをテストできます。ECS Exec を使用するには、タスク IAM ロールを作成する必要があります。タスク IAM ロールおよびその他の前提条件の詳細については、「ECS Exec を使用して Amazon ECS コンテナをモニタリングする」を参照してください。
- (任意) AWS CloudShell は、お客様が独自の EC2 インスタンスを作成する必要なく、コマンドラインを提供するツールです。詳細については、『AWS CloudShell ユーザーガイド』の「What is AWS CloudShell? (とは ?)」 を参照してください。

ステップ 1: クラスターを作成する

デフォルトでは、アカウントは `default` クラスターを受け取ります。

> **Note**
>
> お客様に提供される `default` クラスターを使用する利点は、後続のコマンドで `--cluster` *`cluster_name`* オプションを指定する必要がないことです。デフォルト以外の独自のクラスターを作成する場合は、そのクラスターで使用する予定のコマンドごとに `--cluster` *`cluster_name`* を指定する必要があります。

以下のコマンドを使用して、一意の名前を付けた独自のクラスターを作成します。

```
aws ecs create-cluster --cluster-name fargate-cluster
```

出力:

```
{
    "cluster": {
        "status": "ACTIVE",
        "defaultCapacityProviderStrategy": [],
        "statistics": [],
        "capacityProviders": [],
        "tags": [],
        "clusterName": "fargate-cluster",
        "settings": [
            {
```

```
                "name": "containerInsights",
                "value": "disabled"
            }
        ],
        "registeredContainerInstancesCount": 0,
        "pendingTasksCount": 0,
        "runningTasksCount": 0,
        "activeServicesCount": 0,
        "clusterArn": "arn:aws:ecs:region:aws_account_id:cluster/fargate-cluster"
    }
}
```

ステップ 2: Linux タスク定義を登録

ECS クラスターでタスクを実行する前に、タスク定義を登録する必要があります。タスク定義とは、1 つにグループ化されたコンテナのリストです。以下の例は、Docker Hub でホストされている httpd コンテナイメージを使用して PHP ウェブアプリケーションを作成するシンプルなタスク定義です。使用できるタスク定義パラメータの詳細については、「Amazon ECSの タスク定義」を参照してください。このチュートリアルでは、プライベート サブネットにタスクをデプロイし、そのデプロイメントをテストする場合にのみ taskRoleArn が必要になります。taskRoleArn を、前提条件 で説明した ECS Exec を使用するために作成した IAM タスク ロールに置き換えます。

```
{
       "family": "sample-fargate",
       "networkMode": "awsvpc",
       "taskRoleArn": "arn:aws:iam::aws_account_id:role/execCommandRole",
       "containerDefinitions": [
           {
               "name": "fargate-app",
               "image": "public.ecr.aws/docker/library/httpd:latest",
               "portMappings": [
                   {
                       "containerPort": 80,
                       "hostPort": 80,
                       "protocol": "tcp"
                   }
               ],
               "essential": true,
               "entryPoint": [
                   "sh",
                   "-c"
               ],
```

```
                "command": [
                    "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample
 App</title> <style>body {margin-top: 40px; background-color: #333;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</h1>
 <h2>Congratulations!</h2> <p>Your application is now running on a container in Amazon
 ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html && httpd-
foreground\""
                ]
            }
        ],
        "requiresCompatibilities": [
            "FARGATE"
        ],
        "cpu": "256",
        "memory": "512"
}
```

タスク定義の JSON をファイルとして保存し、`--cli-input-json file://path_to_file.json` オプションで渡します。

コンテナの定義に JSON ファイルを使用するには。

```
aws ecs register-task-definition --cli-input-json file://$HOME/tasks/fargate-task.json
```

register-task-definition コマンドによって、タスク定義の登録が完了した後、その定義の説明が返されます。

ステップ 3: タスク定義をリスト表示する

list-task-definitions コマンドを使用して、いつでもアカウントのタスク定義をリスト表示できます。このコマンドの出力は、run-task または start-task をコールするときに一緒に使用する、`family` 値および `revision` 値を表示します。

```
aws ecs list-task-definitions
```

出力:

```
{
    "taskDefinitionArns": [
        "arn:aws:ecs:region:aws_account_id:task-definition/sample-fargate:1"
    ]
```

```
}
```

ステップ 4: サービスを作成する

アカウントのタスクを登録したら、クラスターに登録されたタスク用のサービスを作成することができます。この例では、sample-fargate:1 タスク定義の 1 つのインスタンスを使用して、クラスターで実行されるサービスを作成します。このタスクにはインターネットへのルートが必要であり、そのために 2 つの方法のいずれかを使用します。1 つの方法は、パブリックサブネットに Elastic IP アドレスを持つ NAT ゲートウェイで構成されたプライベートサブネットを使用することです。もう 1 つの方法は、パブリックサブネットを使用してパブリック IP アドレスをタスクに割り当てることです。両方の例を以下に示します。

プライベートサブネットを使用した例。Amazon ECS Exec を使用するには　enable-execute-command　オプションが必要です。

```
aws ecs create-service --cluster fargate-cluster --service-name fargate-service --
task-definition sample-fargate:1 --desired-count 1 --launch-type "FARGATE" --network-
configuration "awsvpcConfiguration={subnets=[subnet-abcd1234],securityGroups=[sg-
abcd1234]}" --enable-execute-command
```

パブリックサブネットを使用した例。

```
aws ecs create-service --cluster fargate-cluster --service-name fargate-service --
task-definition sample-fargate:1 --desired-count 1 --launch-type "FARGATE" --network-
configuration "awsvpcConfiguration={subnets=[subnet-abcd1234],securityGroups=[sg-
abcd1234],assignPublicIp=ENABLED}"
```

create-service コマンドによって、タスク定義の登録が完了した後、その定義の説明が返されます。

ステップ 5: サービスをリスト表示する

クラスターのサービスをリスト表示します。前のセクションで作成したサービスが表示されます。このコマンドでサービス名または完全 ARN を取得できます。これを後で説明するサービスに使用します。

```
aws ecs list-services --cluster fargate-cluster
```

出力:

```
{
```

```
    "serviceArns": [
        "arn:aws:ecs:region:aws_account_id:service/fargate-cluster/fargate-service"
    ]
}
```

ステップ 6: 実行中のサービスを記述する

先に取得したサービス名を使用してタスクを記述し、サービスに関する詳細情報を取得します。

```
aws ecs describe-services --cluster fargate-cluster --services fargate-service
```

このコマンドが正常に実行されると、サービスの障害とサービスの説明が返されます。例えば、services セクションでは、タスクの実行中または保留中のステータスなど、デプロイに関する情報が見つかります。また、タスク定義、ネットワーク設定、タイムスタンプ付きのイベントに関する情報も見つかります。障害セクションでは、呼び出しに関連する障害がある場合にその情報が見つかります。トラブルシューティングについては、「サービスイベントメッセージ」を参照してください。サービスの説明取得の詳細については、「サービスの説明取得」を参照してください。

```
{
    "services": [
        {
            "networkConfiguration": {
                "awsvpcConfiguration": {
                    "subnets": [
                        "subnet-abcd1234"
                    ],
                    "securityGroups": [
                        "sg-abcd1234"
                    ],
                    "assignPublicIp": "ENABLED"
                }
            },
            "launchType": "FARGATE",
            "enableECSManagedTags": false,
            "loadBalancers": [],
            "deploymentController": {
                "type": "ECS"
            },
            "desiredCount": 1,
            "clusterArn": "arn:aws:ecs:region:aws_account_id:cluster/fargate-cluster",
            "serviceArn": "arn:aws:ecs:region:aws_account_id:service/fargate-service",
            "deploymentConfiguration": {
```

```
                "maximumPercent": 200,
                "minimumHealthyPercent": 100
            },
            "createdAt": 1692283199.771,
            "schedulingStrategy": "REPLICA",
            "placementConstraints": [],
            "deployments": [
                {
                    "status": "PRIMARY",
                    "networkConfiguration": {
                        "awsvpcConfiguration": {
                            "subnets": [
                                "subnet-abcd1234"
                            ],
                            "securityGroups": [
                                "sg-abcd1234"
                            ],
                            "assignPublicIp": "ENABLED"
                        }
                    },
                    "pendingCount": 0,
                    "launchType": "FARGATE",
                    "createdAt": 1692283199.771,
                    "desiredCount": 1,
                    "taskDefinition": "arn:aws:ecs:region:aws_account_id:task-
definition/sample-fargate:1",
                    "updatedAt": 1692283199.771,
                    "platformVersion": "1.4.0",
                    "id": "ecs-svc/9223370526043414679",
                    "runningCount": 0
                }
            ],
            "serviceName": "fargate-service",
            "events": [
                {
                    "message": "(service fargate-service) has started 2 tasks: (task
 53c0de40-ea3b-489f-a352-623bf1235f08) (task d0aec985-901b-488f-9fb4-61b991b332a3).",
                    "id": "92b8443e-67fb-4886-880c-07e73383ea83",
                    "createdAt": 1510811841.408
                },
                {
                    "message": "(service fargate-service) has started 2 tasks: (task
 b4911bee-7203-4113-99d4-e89ba457c626) (task cc5853e3-6e2d-4678-8312-74f8a7d76474).",
                    "id": "d85c6ec6-a693-43b3-904a-a997e1fc844d",
```

```
                    "createdAt": 1510811601.938
                },
                {
                    "message": "(service fargate-service) has started 2 tasks: (task
 cba86182-52bf-42d7-9df8-b744699e6cfc) (task f4c1ad74-a5c6-4620-90cf-2aff118df5fc).",
                    "id": "095703e1-0ca3-4379-a7c8-c0f1b8b95ace",
                    "createdAt": 1510811364.691
                }
            ],
            "runningCount": 0,
            "status": "ACTIVE",
            "serviceRegistries": [],
            "pendingCount": 0,
            "createdBy": "arn:aws:iam::aws_account_id:user/user_name",
            "platformVersion": "LATEST",
            "placementStrategy": [],
            "propagateTags": "NONE",
            "roleArn": "arn:aws:iam::aws_account_id:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
            "taskDefinition": "arn:aws:ecs:region:aws_account_id:task-definition/
sample-fargate:1"
        }
    ],
    "failures": []
}
```

ステップ 7: テスト

パブリックサブネットを使用してデプロイされたタスクのテスト

タスクの Elastic Network Interface (ENI) を取得できるようにサービス内のタスクを記述します。

まず、タスク ARN を取得します。

```
aws ecs list-tasks --cluster fargate-cluster --service fargate-service
```

出力にはタスク ARN が含まれます。

```
{
    "taskArns": [
        "arn:aws:ecs:us-east-1:123456789012:task/fargate-service/EXAMPLE
    ]
```

```
}
```

タスクを記述して ENI ID を見つけます。tasks パラメータにはタスク ARN を使用します。

```
aws ecs describe-tasks --cluster fargate-cluster --tasks arn:aws:ecs:us-
east-1:123456789012:task/service/EXAMPLE
```

添付情報は出力にリストされます。

```
{
    "tasks": [
        {
            "attachments": [
                {
                    "id": "d9e7735a-16aa-4128-bc7a-b2d5115029e9",
                    "type": "ElasticNetworkInterface",
                    "status": "ATTACHED",
                    "details": [
                        {
                            "name": "subnetId",
                            "value": "subnetabcd1234"
                        },
                        {
                            "name": "networkInterfaceId",
                            "value": "eni-0fa40520aeEXAMPLE"
                        },
                    ]
                }
…
}
```

パブリック IP アドレスを取得するには ENI を記述します。

```
aws ec2 describe-network-interfaces --network-interface-id  eni-0fa40520aeEXAMPLE
```

パブリック IP アドレスが出力に表示されます。

```
{
    "NetworkInterfaces": [
        {
            "Association": {
```

```
                "IpOwnerId": "amazon",
                "PublicDnsName": "ec2-34-229-42-222.compute-1.amazonaws.com",
                "PublicIp": "198.51.100.2"
            },
…
}
```

ウェブブラウザにパブリック IP アドレスを入力すると、Amazon ECS のサンプルアプリケーションを表示するウェブページが確認できます。

プライベートサブネットを使用してデプロイされたタスクのテスト

タスクを説明し、managedAgents を見つけて、ExecuteCommandAgent が実行されていることを確認します。後で使用するために privateIPv4Address をメモしておきます。

```
aws ecs describe-tasks --cluster fargate-cluster --tasks arn:aws:ecs:us-
east-1:123456789012:task/fargate-service/EXAMPLE
```

マネージドエージェントの情報が出力にリストされます。

```
{
    "tasks": [
        {
            "attachments": [
                {
                    "id": "d9e7735a-16aa-4128-bc7a-b2d5115029e9",
                    "type": "ElasticNetworkInterface",
                    "status": "ATTACHED",
                    "details": [
                        {
                            "name": "subnetId",
                            "value": "subnetabcd1234"
                        },
                        {
                            "name": "networkInterfaceId",
                            "value": "eni-0fa40520aeEXAMPLE"
                        },
                        {
                            "name": "privateIPv4Address",
                            "value": "10.0.143.156"
                        }
                    ]
```

```
                }
            ],
    ...
    "containers": [
        {
        ...
       "managedAgents": [
                        {
                            "lastStartedAt": "2023-08-01T16:10:13.002000+00:00",
                            "name": "ExecuteCommandAgent",
                            "lastStatus": "RUNNING"
                        }
                ],
        ...
   }
```

ExecuteCommandAgent が実行されていることを確認した後、次のコマンドを実行して、タスク内のコンテナ上で対話的なシェルを実行できます。

```
aws ecs execute-command --cluster fargate-cluster \
    --task  arn:aws:ecs:us-east-1:123456789012:task/fargate-service/EXAMPLE  \
    --container  fargate-app \
    --interactive \
    --command "/bin/sh"
```

対話的なシェルの実行後、次のコマンドを実行して cURL をインストールします。

```
apt update
```

```
apt install curl
```

cURL をインストール後、先ほど取得したプライベート IP アドレスを使用して次のコマンドを実行します。

```
curl 10.0.143.156
```

Amazon ECS サンプルアプリケーションの Web ページと同等の HTML が表示されます。

```
<html>
    <head>
```

```
     <title>Amazon ECS Sample App</title>
     <style>body {margin-top: 40px; background-color: #333;} </style>
    </head>
      <body>
      <div style=color:white;text-align:center>
      <h1>Amazon ECS Sample App</h1>
      <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p>
      </div>
      </body>
</html>
```

ステップ 8: クリーンアップ

このチュートリアルが終了したら、未使用のリソースに対する料金が発生しないように、それに関連付けられたリソースをクリーンアップする必要があります。

サービスを削除します。

```
aws ecs delete-service --cluster fargate-cluster --service fargate-service --force
```

クラスターを削除します。

```
aws ecs delete-cluster --cluster fargate-cluster
```

AWS CLI を使用して、Fargate 起動タイプ用の Amazon ECS Windows タスクを作成する

次のステップでは、AWS CLI を使って Amazon ECS でクラスターのセットアップ、タスク定義の登録、Windows タスクの実行、その他の一般的なシナリオを実行するために役立ちます。最新バージョンの AWS CLI を使用していることを確認してください。最新のバージョンにアップグレードする方法については、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

トピック

前提条件

このチュートリアルでは、以下の前提条件をすでに満たしているものとします。

- AWS CLI の最新バージョンがインストールされ、設定されていること。AWS CLI のインストールまたはアップグレードについては、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。
- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- VPC およびセキュリティグループが使用できるように作成されていること。このチュートリアルでは、Docker Hub でホストされているコンテナイメージを使用するため、タスクではインターネットにアクセスできる必要があります。タスクでインターネットへのルートを設定するには、以下のいずれかのオプションを使用します。
  - Elastic IP アドレスが割り当てられた NAT ゲートウェイでプライベートサブネットを使用する。
  - パブリックサブネットを使用してタスクにパブリック IP アドレスを割り当てる。

  詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。

  セキュリティグループとルールの詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「VPC のデフォルト セキュリティ グループ」および「ルールの例」を参照してください。
- (任意) AWS CloudShell は、お客様が独自の EC2 インスタンスを作成する必要なく、コマンドラインを提供するツールです。詳細については、『AWS CloudShell ユーザーガイド』の「What is AWS CloudShell? (とは ?)」 を参照してください。

ステップ 1: クラスターを作成する

デフォルトでは、アカウントは `default` クラスターを受け取ります。

> **Note**
>
> お客様に提供される default クラスターを使用する利点は、後続のコマンドで --cluster *cluster_name* オプションを指定する必要がないことです。デフォルト以外の独自のクラスターを作成する場合は、そのクラスターで使用する予定のコマンドごとに --cluster *cluster_name* を指定する必要があります。

以下のコマンドを使用して、一意の名前を付けた独自のクラスターを作成します。

```
aws ecs create-cluster --cluster-name fargate-cluster
```

出力:

```
{
    "cluster": {
        "status": "ACTIVE",
        "statistics": [],
        "clusterName": "fargate-cluster",
        "registeredContainerInstancesCount": 0,
        "pendingTasksCount": 0,
        "runningTasksCount": 0,
        "activeServicesCount": 0,
        "clusterArn": "arn:aws:ecs:region:aws_account_id:cluster/fargate-cluster"
    }
}
```

ステップ 2: Windows タスク定義を登録する

Amazon ECS クラスターに Windows タスクを実行する前に、タスク定義を登録する必要があります。タスク定義とは、1 つにグループ化されたコンテナのリストです。次の例では、ウェブアプリを作成する単純なタスク定義です。使用できるタスク定義パラメータの詳細については、「Amazon ECSの タスク定義」を参照してください。

```
{
    "containerDefinitions": [
        {
            "command": ["New-Item -Path C:\\inetpub\\wwwroot\\index.html -Type file
 -Value '<html> <head> <title>Amazon ECS Sample App</title> <style>body {margin-top:
```

```
 40px; background-color: #333;} </style> </head><body> <div style=color:white;text-
align:center> <h1>Amazon ECS Sample App</h1> <h2>Congratulations!</h2> <p>Your
 application is now running on a container in Amazon ECS.</p>'; C:\\ServiceMonitor.exe
 w3svc"],
            "entryPoint": [
                "powershell",
                "-Command"
            ],
            "essential": true,
            "cpu": 2048,
            "memory": 4096,
            "image": "mcr.microsoft.com/windows/servercore/iis:windowsservercore-
ltsc2019",
            "name": "sample_windows_app",
            "portMappings": [
                {
                    "hostPort": 80,
                    "containerPort": 80,
                    "protocol": "tcp"
                }
            ]
        }
    ],
    "memory": "4096",
    "cpu": "2048",
    "networkMode": "awsvpc",
    "family": "windows-simple-iis-2019-core",
    "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
    "runtimePlatform": {"operatingSystemFamily": "WINDOWS_SERVER_2019_CORE"},
    "requiresCompatibilities": ["FARGATE"]
}
```

上の JSON 例は次の 2 通りの方法で AWS CLI に渡すことができます。1 番目はタスク定義 JSON をファイルとして保存し、`--cli-input-json file://path_to_file.json` オプションで渡すことができます。

コンテナの定義に JSON ファイルを使用するには。

```
aws ecs register-task-definition --cli-input-json file://$HOME/tasks/fargate-task.json
```

register-task-definition コマンドによって、タスク定義の登録が完了した後、その定義の説明が返されます。

ステップ 3: タスク定義をリスト表示する

list-task-definitions コマンドを使用して、いつでもアカウントのタスク定義をリスト表示できます。このコマンドの出力は、run-task または start-task をコールするときに一緒に使用する、`family` 値および `revision` 値を表示します。

```
aws ecs list-task-definitions
```

出力:

```
{
    "taskDefinitionArns": [
        "arn:aws:ecs:region:aws_account_id:task-definition/sample-fargate-windows:1"
    ]
}
```

ステップ 4: サービスを作成する

アカウントのタスクを登録したら、クラスターに登録されたタスク用のサービスを作成することができます。この例では、`sample-fargate:1` タスク定義の 1 つのインスタンスを使用して、クラスターで実行されるサービスを作成します。このタスクにはインターネットへのルートが必要であり、そのために 2 つの方法のいずれかを使用します。1 つの方法は、パブリックサブネットに Elastic IP アドレスを持つ NAT ゲートウェイで構成されたプライベートサブネットを使用することです。もう 1 つの方法は、パブリックサブネットを使用してパブリック IP アドレスをタスクに割り当てることです。両方の例を以下に示します。

プライベートサブネットを使用した例。

```
aws ecs create-service --cluster fargate-cluster --service-name fargate-service
 --task-definition sample-fargate-windows:1 --desired-count 1 --launch-type
 "FARGATE" --network-configuration "awsvpcConfiguration={subnets=[subnet-
abcd1234],securityGroups=[sg-abcd1234]}"
```

パブリックサブネットを使用した例。

```
aws ecs create-service --cluster fargate-cluster --service-name fargate-service
 --task-definition sample-fargate-windows:1 --desired-count 1 --launch-type
 "FARGATE" --network-configuration "awsvpcConfiguration={subnets=[subnet-
abcd1234],securityGroups=[sg-abcd1234],assignPublicIp=ENABLED}"
```

create-service コマンドによって、タスク定義の登録が完了した後、その定義の説明が返されます。

ステップ 5: サービスをリスト表示する

クラスターのサービスをリスト表示します。前のセクションで作成したサービスが表示されます。このコマンドでサービス名または完全 ARN を取得できます。これを後で説明するサービスに使用します。

```
aws ecs list-services --cluster fargate-cluster
```

出力:

```
{
    "serviceArns": [
        "arn:aws:ecs:region:aws_account_id:service/fargate-service"
    ]
}
```

ステップ 6: 実行中のサービスを記述する

先に取得したサービス名を使用してタスクを記述し、サービスに関する詳細情報を取得します。

```
aws ecs describe-services --cluster fargate-cluster --services fargate-service
```

このコマンドが正常に実行されると、サービスの障害とサービスの説明が返されます。例えば、サービスセクションでは、タスクの実行中または保留中のステータスなど、デプロイに関する情報が見つかります。また、タスク定義、ネットワーク設定、タイムスタンプ付きのイベントに関する情報も見つかります。障害セクションでは、呼び出しに関連する障害がある場合にその情報が見つかります。トラブルシューティングについては、「サービスイベントメッセージ」を参照してください。サービスの説明取得の詳細については、「サービスの説明取得」を参照してください。

```
{
    "services": [
        {
            "status": "ACTIVE",
            "taskDefinition": "arn:aws:ecs:region:aws_account_id:task-definition/
sample-fargate-windows:1",
            "pendingCount": 2,
            "launchType": "FARGATE",
            "loadBalancers": [],
```

```
            "roleArn": "arn:aws:iam::aws_account_id:role/aws-service-role/
ecs.amazonaws.com/AWSServiceRoleForECS",
            "placementConstraints": [],
            "createdAt": 1510811361.128,
            "desiredCount": 2,
            "networkConfiguration": {
                "awsvpcConfiguration": {
                    "subnets": [
                        "subnet-abcd1234"
                    ],
                    "securityGroups": [
                        "sg-abcd1234"
                    ],
                    "assignPublicIp": "DISABLED"
                }
            },
            "platformVersion": "LATEST",
            "serviceName": "fargate-service",
            "clusterArn": "arn:aws:ecs:region:aws_account_id:cluster/fargate-cluster",
            "serviceArn": "arn:aws:ecs:region:aws_account_id:service/fargate-service",
            "deploymentConfiguration": {
                "maximumPercent": 200,
                "minimumHealthyPercent": 100
            },
            "deployments": [
                {
                    "status": "PRIMARY",
                    "networkConfiguration": {
                        "awsvpcConfiguration": {
                            "subnets": [
                                "subnet-abcd1234"
                            ],
                            "securityGroups": [
                                "sg-abcd1234"
                            ],
                            "assignPublicIp": "DISABLED"
                        }
                    },
                    "pendingCount": 2,
                    "launchType": "FARGATE",
                    "createdAt": 1510811361.128,
                    "desiredCount": 2,
                    "taskDefinition": "arn:aws:ecs:region:aws_account_id:task-
definition/sample-fargate-windows:1",
```

```
                    "updatedAt": 1510811361.128,
                    "platformVersion": "0.0.1",
                    "id": "ecs-svc/9223370526043414679",
                    "runningCount": 0
                }
            ],
            "events": [
                {
                    "message": "(service fargate-service) has started 2 tasks: (task
 53c0de40-ea3b-489f-a352-623bf1235f08) (task d0aec985-901b-488f-9fb4-61b991b332a3).",
                    "id": "92b8443e-67fb-4886-880c-07e73383ea83",
                    "createdAt": 1510811841.408
                },
                {
                    "message": "(service fargate-service) has started 2 tasks: (task
 b4911bee-7203-4113-99d4-e89ba457c626) (task cc5853e3-6e2d-4678-8312-74f8a7d76474).",
                    "id": "d85c6ec6-a693-43b3-904a-a997e1fc844d",
                    "createdAt": 1510811601.938
                },
                {
                    "message": "(service fargate-service) has started 2 tasks: (task
 cba86182-52bf-42d7-9df8-b744699e6cfc) (task f4c1ad74-a5c6-4620-90cf-2aff118df5fc).",
                    "id": "095703e1-0ca3-4379-a7c8-c0f1b8b95ace",
                    "createdAt": 1510811364.691
                }
            ],
            "runningCount": 0,
            "placementStrategy": []
        }
    ],
    "failures": []
}
```

ステップ 7: クリーンアップする

このチュートリアルが終了したら、未使用のリソースに対する料金が発生しないように、それに関連付けられたリソースをクリーンアップする必要があります。

サービスを削除します。

```
aws ecs delete-service --cluster fargate-cluster --service fargate-service --force
```

クラスターを削除します。

```
aws ecs delete-cluster --cluster fargate-cluster
```

AWS CLI を使用して、EC2 起動タイプ用の Amazon ECS タスクを作成する

次のステップでは、AWS CLI を使って Amazon ECS でクラスターのセットアップ、タスク定義の登録、タスクの実行、その他の一般的なシナリオを実行するために役立ちます。AWS CLI の最新バージョンを使用する。最新のバージョンにアップグレードする方法については、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

トピック

前提条件

このチュートリアルでは、以下の前提条件が完了済みであることを前提としています。

- AWS CLI の最新バージョンがインストールされ、設定されていること。AWS CLI のインストールまたはアップグレードについては、「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。
- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。

- VPC およびセキュリティグループが使用できるように作成されていること。詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。
- (任意) AWS CloudShell は、お客様が独自の EC2 インスタンスを作成する必要なく、コマンドラインを提供するツールです。詳細については、『AWS CloudShell ユーザーガイド』の「What is AWS CloudShell? (とは ?)」 を参照してください。

ステップ 1: クラスターを作成する

デフォルトでは、初めてコンテナインスタンスを起動すると、アカウントが `default` クラスターを受け取ります。

> **Note**
>
> お客様に提供される `default` クラスターを使用する利点は、後続のコマンドで `--cluster` *`cluster_name`* オプションを指定する必要がないことです。デフォルト以外の独自のクラスターを作成する場合は、そのクラスターで使用する予定のコマンドごとに `--cluster` *`cluster_name`* を指定する必要があります。

以下のコマンドを使用して、一意の名前を付けた独自のクラスターを作成します。

```
aws ecs create-cluster --cluster-name MyCluster
```

出力:

```
{
    "cluster": {
        "clusterName": "MyCluster",
        "status": "ACTIVE",
        "clusterArn": "arn:aws:ecs:region:aws_account_id:cluster/MyCluster"
    }
}
```

ステップ 2: Amazon ECS AMI を使用してインスタンスの起動

タスクを実行する前に、クラスターに Amazon ECS コンテナインスタンスがあることが必要です。クラスターにコンテナインスタンスがない場合は、Amazon ECS Linux コンテナインスタンスの起動で詳細を参照してください。

ステップ 3: コンテナインスタンスを一覧表示する

コンテナインスタンスを起動してから数分以内に、Amazon ECS エージェントがインスタンスをデフォルトクラスターで登録します。次のコマンドを実行して、クラスターのコンテナインスタンスをリスト表示できます。

```
aws ecs list-container-instances --cluster default
```

出力:

```
{
    "containerInstanceArns": [
        "arn:aws:ecs:us-east-1:aws_account_id:container-instance/container_instance_ID"
    ]
}
```

ステップ 4: コンテナインスタンスを定義する

コンテナインスタンスの ARN または ID を取得した後、describe-container-instances コマンドを使用して、登録済みおよび残りの CPU やメモリリソースなど、インスタンスの変数情報を取得できます。

```
aws ecs describe-container-instances --cluster default --container-
instances container_instance_ID
```

出力:

```
{
    "failures": [],
    "containerInstances": [
        {
            "status": "ACTIVE",
            "registeredResources": [
                {
                    "integerValue": 1024,
                    "longValue": 0,
                    "type": "INTEGER",
                    "name": "CPU",
                    "doubleValue": 0.0
                },
                {
```

```
                    "integerValue": 995,
                    "longValue": 0,
                    "type": "INTEGER",
                    "name": "MEMORY",
                    "doubleValue": 0.0
                },
                {
                    "name": "PORTS",
                    "longValue": 0,
                    "doubleValue": 0.0,
                    "stringSetValue": [
                        "22",
                        "2376",
                        "2375",
                        "51678"
                    ],
                    "type": "STRINGSET",
                    "integerValue": 0
                },
                {
                    "name": "PORTS_UDP",
                    "longValue": 0,
                    "doubleValue": 0.0,
                    "stringSetValue": [],
                    "type": "STRINGSET",
                    "integerValue": 0
                }
            ],
            "ec2InstanceId": "instance_id",
            "agentConnected": true,
            "containerInstanceArn": "arn:aws:ecs:us-west-2:aws_account_id:container-
instance/container_instance_ID",
            "pendingTasksCount": 0,
            "remainingResources": [
                {
                    "integerValue": 1024,
                    "longValue": 0,
                    "type": "INTEGER",
                    "name": "CPU",
                    "doubleValue": 0.0
                },
                {
                    "integerValue": 995,
                    "longValue": 0,
```

```
                "type": "INTEGER",
                "name": "MEMORY",
                "doubleValue": 0.0
            },
            {
                "name": "PORTS",
                "longValue": 0,
                "doubleValue": 0.0,
                "stringSetValue": [
                    "22",
                    "2376",
                    "2375",
                    "51678"
                ],
                "type": "STRINGSET",
                "integerValue": 0
            },
            {
                "name": "PORTS_UDP",
                "longValue": 0,
                "doubleValue": 0.0,
                "stringSetValue": [],
                "type": "STRINGSET",
                "integerValue": 0
            }
        ],
        "runningTasksCount": 0,
        "attributes": [
            {
                "name": "com.amazonaws.ecs.capability.privileged-container"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.17"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.18"
            },
            {
                "name": "com.amazonaws.ecs.capability.docker-remote-api.1.19"
            },
            {
                "name": "com.amazonaws.ecs.capability.logging-driver.json-file"
            },
            {
```

```
                    "name": "com.amazonaws.ecs.capability.logging-driver.syslog"
                }
            ],
            "versionInfo": {
                "agentVersion": "1.5.0",
                "agentHash": "b197edd",
                "dockerVersion": "DockerVersion: 1.7.1"
            }
        }
    ]
}
```

Amazon EC2 コンソールまたは aws ec2 describe-instances --instance-id ***instance_id*** コマンドを使用して、インスタンスのモニタリングに使用できる Amazon EC2 インスタンス ID も検索することもできます。

ステップ 5: タスク定義を登録する

ECS クラスターでタスクを実行する前に、タスク定義を登録する必要があります。タスク定義とは、1 つにグループ化されたコンテナのリストです。次の例は、Docker Hub から取得した busybox イメージを使用し、360 秒間スリープ状態になるシンプルなタスク定義です。使用できるタスク定義パラメータの詳細については、「Amazon ECSの タスク定義」を参照してください。

```
{
    "containerDefinitions": [
        {
            "name": "sleep",
            "image": "busybox",
            "cpu": 10,
            "command": [
                "sleep",
                "360"
            ],
            "memory": 10,
            "essential": true
        }
    ],
    "family": "sleep360"
}
```

上の JSON 例は次の 2 通りの方法で AWS CLI に渡すことができます。1 番目はタスク定義 JSON をファイルとして保存し、`--cli-input-json file://`***path_to_file.json*** オプションで渡す

ことができます。2 番目は、以下の例のように、JSON の引用符をエスケープして JSON コンテナの定義をコマンドラインで渡すことができます。コマンドラインにコンテナ定義を渡す方法を選択した場合、追加で複数のバージョンのタスクを相互に関連付けたままにする `--family` パラメータが必要です。

コンテナの定義に JSON ファイルを使用するには。

```
aws ecs register-task-definition --cli-input-json file://$HOME/tasks/sleep360.json
```

コンテナの定義に JSON 文字列を使用するには。

```
aws ecs register-task-definition --family sleep360 --container-definitions "[{\"name
\":\"sleep\",\"image\":\"busybox\",\"cpu\":10,\"command\":[\"sleep\",\"360\"],\"memory
\":10,\"essential\":true}]"
```

register-task-definition は登録を完了させた後、タスク定義の記述を返します。

```
{
    "taskDefinition": {
        "volumes": [],
        "taskDefinitionArn": "arn:aws:ec2:us-east-1:aws_account_id:task-definition/
sleep360:1",
        "containerDefinitions": [
            {
                "environment": [],
                "name": "sleep",
                "mountPoints": [],
                "image": "busybox",
                "cpu": 10,
                "portMappings": [],
                "command": [
                    "sleep",
                    "360"
                ],
                "memory": 10,
                "essential": true,
                "volumesFrom": []
            }
        ],
        "family": "sleep360",
        "revision": 1
```

```
    }
}
```

ステップ 6: タスク定義をリスト表示する

list-task-definitions コマンドを使用して、いつでもアカウントのタスク定義をリスト表示できます。このコマンドの出力は、run-task または start-task をコールするときに一緒に使用する、`family` 値および `revision` 値を表示します。

```
aws ecs list-task-definitions
```

出力:

```
{
    "taskDefinitionArns": [
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/sleep300:1",
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/sleep300:2",
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/sleep360:1",
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/wordpress:3",
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/wordpress:4",
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/wordpress:5",
        "arn:aws:ec2:us-east-1:aws_account_id:task-definition/wordpress:6"
    ]
}
```

ステップ 7: タスクを実行する

アカウントのタスクを登録して、クラスターに登録されたコンテナインスタンスを起動すると、クラスターの登録済みタスクを実行できます。この例では、デフォルトのクラスターに `sleep360:1` タスク定義の単独インスタンスを配置します。

```
aws ecs run-task --cluster default --task-definition sleep360:1 --count 1
```

出力:

```
{
    "tasks": [
        {
            "taskArn": "arn:aws:ecs:us-east-1:aws_account_id:task/task_ID",
```

```
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "sleep"
                    }
                ]
            },
            "lastStatus": "PENDING",
            "containerInstanceArn": "arn:aws:ecs:us-east-1:aws_account_id:container-
instance/container_instance_ID",
            "clusterArn": "arn:aws:ecs:us-east-1:aws_account_id:cluster/default",
            "desiredStatus": "RUNNING",
            "taskDefinitionArn": "arn:aws:ecs:us-east-1:aws_account_id:task-definition/
sleep360:1",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-
east-1:aws_account_id:container/container_ID",
                    "taskArn": "arn:aws:ecs:us-east-1:aws_account_id:task/task_ID",
                    "lastStatus": "PENDING",
                    "name": "sleep"
                }
            ]
        }
    ]
}
```

ステップ 8: タスクのリスト表示

クラスターのタスクをリスト表示します。前のセクションで実行したタスクが表示されます。このコマンドでタスク ID または完全 ARN を取得できます。これを後で説明するタスクに使用します。

```
aws ecs list-tasks --cluster default
```

出力:

```
{
    "taskArns": [
        "arn:aws:ecs:us-east-1:aws_account_id:task/task_ID"
    ]
}
```

ステップ 9: 実行中のタスクを定義する

先ほど取得したタスク ID を使用してタスクを定義し、タスクに関する詳細情報を取得します。

```
aws ecs describe-tasks --cluster default --task task_ID
```

出力:

```
{
    "failures": [],
    "tasks": [
        {
            "taskArn": "arn:aws:ecs:us-east-1:aws_account_id:task/task_ID",
            "overrides": {
                "containerOverrides": [
                    {
                        "name": "sleep"
                    }
                ]
            },
            "lastStatus": "RUNNING",
            "containerInstanceArn": "arn:aws:ecs:us-east-1:aws_account_id:container-
instance/container_instance_ID",
            "clusterArn": "arn:aws:ecs:us-east-1:aws_account_id:cluster/default",
            "desiredStatus": "RUNNING",
            "taskDefinitionArn": "arn:aws:ecs:us-east-1:aws_account_id:task-definition/
sleep360:1",
            "containers": [
                {
                    "containerArn": "arn:aws:ecs:us-
east-1:aws_account_id:container/container_ID",
                    "taskArn": "arn:aws:ecs:us-east-1:aws_account_id:task/task_ID",
                    "lastStatus": "RUNNING",
                    "name": "sleep",
                    "networkBindings": []
                }
            ]
        }
    ]
}
```

CloudWatch Events イベントをリッスンするように Amazon ECS を設定する

タスクイベントをリッスンし、それを CloudWatch Logs ログストリームに書き込むシンプルな Lambda 関数を設定する方法について説明します。

前提条件: テストクラスターを設定する

イベントをキャプチャする実行中のクラスターがなければ、the section called “Fargate 起動タイプ用のクラスターの作成” のステップに従ってクラスターを作成します。このチュートリアルの最後に、このクラスターでタスクを実行して Lambda 関数が正しく設定されていることをテストします。

ステップ 1: Lambda 関数を作成する

この手順では、Amazon ECS イベントストリームメッセージのターゲットとなるシンプルな Lambda 関数を作成します。

1. AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ を開いてください。
2. [関数の作成] を選択します。
3. [Author from scratch] 画面で、次の操作を行います。
   a. [名前] に値を入力します。
   b. [Runtime] (ランタイム) で、Python のバージョン (Python 3.9 など) を選択します。
   c. [Role] で、[Create a new role with basic Lambda permissions] を選択します。
4. [関数の作成] を選択します。
5. [Function code] (関数コード) セクションで、以下の例に一致するようにサンプルコードを編集します。

```
import json

def lambda_handler(event, context):
    if event["source"] != "aws.ecs":
       raise ValueError("Function only supports input from events with a source
 type of: aws.ecs")

    print('Here is the event:')
```

```
    print(json.dumps(event))
```

これは、Amazon ECS から送信されたイベントを出力するシンプルな Python 3.9 関数です。すべてが正しく設定されると、このチュートリアルの最後に、この Lambda 関数に関連付けられている CloudWatch Logs ログストリームにイベントの詳細が表示されます。

6. [Save] を選択します。

ステップ 2: イベントルールを登録する

次に、Amazon ECS クラスターから送信されるタスクイベントをキャプチャする CloudWatch Events イベントルールを作成します。このルールでは、それが定義されているアカウント内のすべてのクラスターから送信されるすべてのイベントがキャプチャされます。タスクメッセージ自体内に、イベントソースに関する情報 (イベントソースがあるクラスターの情報など) が含まれており、この情報を使用してプログラムでイベントをフィルタしてソートできます。

> **Note**
>
> AWS Management Console を使用してイベントルールを作成すると、コンソールが CloudWatch Eventsに Lambda 関数を呼び出す権限を付与するために必要な IAM 権限を自動的に追加します。AWS CLI を使用してイベントルールを作成する場合は、この権限を明示的に付与する必要があります。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge イベント」と「Amazon EventBridge のイベントパターン」を参照してください。

Lambda 関数にイベントをルートするには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Events]、[Rules]、[Create rule] の順に選択します。
3. [Event Source] で、イベントソースとして [ECS] を選択します。デフォルトでは、ルールはすべての Amazon ECS グループのすべての Amazon ECS イベントに適用されます。または、特定のイベントや特定の Amazon ECS グループを選択することもできます。
4. [Targets] (ターゲット) に [Add target] (ターゲットの追加) を選択し、[Target type] (ターゲットの種類) に [Lambda function] (Lambda 関数) を選択したら、Lambda 関数を選択します。
5. [詳細の設定] を選択します。
6. [Rule definition] で、ルールの名前と説明を入力し、[Create rule] を選択します。

ステップ 3: タスク定義を作成する

タスク定義を作成します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、[タスク定義] を選択します。
3. [Create new Task Definition] (新しいタスク定義の作成)、[Create new revision with JSON] (JSON で新しいリビジョンを作成) の順に選択します。
4. 以下のタスク定義の例をコピーしてボックスに貼り付け、[Save (保存)] を選択します。

```
{
   "containerDefinitions": [
      {
         "command": [
            "/bin/sh -c \"echo '<html> <head> <title>Amazon ECS Sample App</
title> <style>body {margin-top: 40px; background-color: #333;} </style> </
head><body> <div style=color:white;text-align:center> <h1>Amazon ECS Sample App</
h1> <h2>Congratulations!</h2> <p>Your application is now running on a container in
 Amazon ECS.</p> </div></body></html>' >  /usr/local/apache2/htdocs/index.html &&
 httpd-foreground\""
         ],
         "entryPoint": [
            "sh",
            "-c"
         ],
         "essential": true,
         "image": "public.ecr.aws/docker/library/httpd:2.4",
         "logConfiguration": {
            "logDriver": "awslogs",
            "options": {
               "awslogs-group" : "/ecs/fargate-task-definition",
               "awslogs-region": "us-east-1",
               "awslogs-stream-prefix": "ecs"
            }
         },
         "name": "sample-fargate-app",
         "portMappings": [
            {
               "containerPort": 80,
               "hostPort": 80,
               "protocol": "tcp"
            }
```

```
            ]
        }
    ],
    "cpu": "256",
    "executionRoleArn": "arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
    "family": "fargate-task-definition",
    "memory": "512",
    "networkMode": "awsvpc",
    "runtimePlatform": {
         "operatingSystemFamily": "LINUX"
     },
    "requiresCompatibilities": [
        "FARGATE"
     ]
}
```

5. [Create] (作成) を選択します。

ステップ 4: ルールをテストする

最後に、Amazon ECS クラスターから送信されるタスクイベントをキャプチャする CloudWatch Events イベントルールを作成します。このルールでは、それが定義されているアカウント内のすべてのクラスターから送信されるすべてのイベントがキャプチャされます。タスクメッセージ自体内に、イベントソースに関する情報 (イベントソースがあるクラスターの情報など) が含まれており、この情報を使用してプログラムでイベントをフィルタしてソートできます。

ルールをテストするには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [Task definitions] (タスク定義) を選択します。
3. [console-sample-app-static] を選択し、[Deploy] (デプロイ)、[Run new task] (新しいタスクの実行) の順に選択します。
4. [Cluster] (クラスター) で [default] (デフォルト) を選択し、[Deploy] (デプロイ) を選択します。
5. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
6. ナビゲーションペインで、ログ を選択して Lambda 関数 (例えば、/aws/lambda/*my-function ##*)] のロググループを選択します。
7. イベントデータを表示するログストリームを選択します。

Amazon ECS タスク停止イベントに関する Amazon Simple Notification Service アラートの送信

重要なコンテナのいずれかが終了したことにより、タスクの実行が停止したタスクイベントのみをキャプチャする Amazon EventBridge イベントルールを設定します。イベントは、特定の `stoppedReason` プロパティを持つタスクイベントのみが、指定された Amazon SNS トピックに送信します。

前提条件: テストクラスターを設定する

イベントをキャプチャする実行中のクラスターがなければ、「AWS Fargate の Linux コンテナによるコンソールの使用開始」のステップに従ってクラスターを作成します。このチュートリアルの最後に、このクラスターでタスクを実行し、 Amazon SNS トピックと EventBridge ルールが正しく設定されていることをテストします。

前提条件: Amazon SNS 用のアクセス許可の設定

EventBridge による Amazon SNS トピックへの公開を許可するには、aws sns get-topic-attributes コマンドと aws sns set-topic-attributes コマンドを使用します。

アクセス許可を追加する方法については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS のアクセス許可」を参照してください。

以下のアクセス許可を追加します。

```
{
  "Sid": "PublishEventsToMyTopic",
  "Effect": "Allow",
  "Principal": {
     "Service": "events.amazonaws.com"
  },
  "Action": "sns: Publish",
  "Resource": "arn:aws:sns:region:account-id:TaskStoppedAlert",
}
```

ステップ 1: Amazon SNS トピックを作成してサブスクライブする

このチュートリアルでは、新しいイベントルールのイベントターゲットとして使用する Amazon SNS トピックを設定します。

Amazon SNS トピックの作成とサブスクライブの方法については、「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS の開始方法」を参照し、さらに、次の表から選択するオプションを決定します。

オプション	値
タイプ	標準
名前	TaskStoppedAlert
プロトコル	E メール
エンドポイント	現在アクセスできる E メールアドレス

ステップ 2: イベントルールを登録する

次に、コンテナが停止されたタスクについてのみ、タスク停止時のイベントをキャプチャするイベントルールを登録します。

Amazon SNS トピックを作成してサブスクライブする方法については、Amazon EventBridge デベロッパーガイドの「Amazon EventBridge でルールを作成する」を参照し、次の表を使用して、選択するオプションを決定します。

オプション	値
ルールタイプ	イベントパターンを持つルール
イベントソース	AWS イベントまたは EventBridge パートナーイベント
イベントパターン	カスタムパターン (JSON エディター)

イベントパターン	<pre>{
	"source":[
	"aws.ecs"</pre>

オプション	値

	<pre>],
	"detail-type":[
	"ECS Task State Change"
	],
	"detail":{
	"lastStatus":[
	"STOPPED"
	],
	"stoppedReason":[
	"Essential container in task exited"
	]
	}
	}</pre>

対象タイプ	AWS サービス
Target	SNS トピック
トピック	TaskStoppedAlert (ステップ 1 で作成したトピック)

ステップ 3: ルールをテストする

開始直後に終了するタスクを実行して、ルールが機能していることを確認します。イベントルールが正しく設定されていれば、数分以内にイベントテキストが記載されたメールメッセージが届きます。ルールの要件を満たす既存のタスク定義がある場合は、それを使用してタスクを実行します。そうでない場合は、次の手順に従って Fargate タスク定義を登録し、その定義を使用してタスクを実行します。

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. ナビゲーションペインで、タスクの定義 を選択します。
3. [Create new task definition] (新しいタスク定義の作成)、[Create new task definition with JSON] (JSON で新しいタスク定義を作成) の順に選択します。
4. JSON エディタボックスで、JSON ファイルを編集し、以下をエディタにコピーします。

```
{
   "containerDefinitions":[
      {
         "command":[
            "sh",
            "-c",
            "sleep 5"
         ],
         "essential":true,
         "image":"public.ecr.aws/amazonlinux/amazonlinux:latest",
         "name":"test-sleep"
      }
   ],
   "cpu":"256",
   "executionRoleArn":"arn:aws:iam::012345678910:role/ecsTaskExecutionRole",
   "family":"fargate-task-definition",
   "memory":"512",
   "networkMode":"awsvpc",
   "requiresCompatibilities":[
      "FARGATE"
   ]
}
```

5. [Create] (作成) を選択します。

コンソールからタスクを実行するには

1. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
2. [クラスター] ページで、前提条件の下で作成したクラスターを選択します。
3. Tasksタブで、Run new taskを選択します。
4. Application type(アプリケーションの種類)で、Task(タスク)を選択します。
5. [タスク定義] で、[fargate-task-definition] を選択します。
6. [Desired tasks] (必要なタスク) で、起動するタスクの数を入力します。
7. [Create] (作成) を選択します。

複数行またはスタックトレースの Amazon ECS ログメッセージの連結

Fluent Bit バージョン 2.22.0 以降の AWS では、複数行フィルターが含まれています。複数行フィルターは、もともと 1 つのコンテキストに属していても、複数のレコードまたはログ行に分割されたログメッセージを連結するのに役立ちます。複数行フィルターの詳細については、「Fluent Bit documentation」(Fluent Bit ドキュメント) を参照してください。

以下は、分割されたログメッセージの一般的な例です。

- スタックトレース
- 複数の行にログを出力するアプリケーション。
- 指定されたランタイムの最大バッファサイズを超過した場合に、ログメッセージが分割されます GitHub の例、「FireLens Example: Concatenate Partial/Split Container Logs」(FireLens の例:部分/分割コンテナログの連結) に従い、コンテナランタイムによって分割されたログメッセージを連結することができます。

必要な IAM 許可

コンテナエージェントが Amazon ECR からコンテナイメージをプルし、コンテナがログを CloudWatch Logs にルーティングするために必要なIAM 許可を持っていることを確認する必要があります。

これらの許可には、次のロールが必要です。

- タスク IAM ロール
- タスク実行 IAM ロールです。

JSON ポリシーエディタでポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左側のナビゲーションペインで、[ポリシー] を選択します。

   初めて [ポリシー] を選択する場合には、[管理ポリシーにようこそ] ページが表示されます。[今すぐ始める] を選択します。
3. ページの上部で、[ポリシーを作成] を選択します。

4. [ポリシーエディタ] セクションで、[JSON] オプションを選択します。
5. 次の JSON ポリシードキュメントを入力します。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "logs:CreateLogStream",
   "logs:CreateLogGroup",
   "logs:PutLogEvents"
  ],
  "Resource": "*"
 }]
}
```

6. [次へ] をクリックします。

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

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

複数行ログの設定を使用する場合を決定する

CloudWatch Logs コンソールで、デフォルトのログ設定で表示されるログスニペットの例を次に示します。log で始まる行を見て、複数行フィルタが必要かどうかを判断できます。コンテキストが同じ場合は、複数行ログ設定を使用できます。この例の場合、コンテキストは「com.myproject.model.MyProject」です。

```
2022-09-20T15:47:56:595-05-00                                {"container_id":
 "82ba37cada1d44d389b03e78caf74faa-EXAMPLE", "container_name": "example-
```

```
app", "source=": "stdout", "log": ": "     at com.myproject.modele.
(MyProject.badMethod.java:22)",
    {
      "container_id":  "82ba37cada1d44d389b03e78caf74faa-EXAMPLE",
      "container_name: ": "example-app",
      "source": "stdout",
      "log": ": "     at com.myproject.model.MyProject.badMethod(MyProject.java:22)",
      "ecs_cluster": "default",
      "ecs_task_arn": "arn:aws:region:123456789012:task/default/
b23c940d29ed4714971cba72cEXAMPLE",
      "ecs_task_definition": "firelense-example-multiline:3"
     }
```

```
2022-09-20T15:47:56:595-05-00                              {"container_id":
 "82ba37cada1d44d389b03e78caf74faa-EXAMPLE", "container_name": "example-app", "stdout",
 "log": ": "     at com.myproject.modele.(MyProject.oneMoreMethod.java:18)",
    {
      "container_id":  "82ba37cada1d44d389b03e78caf74faa-EXAMPLE",
      "container_name: ": "example-app",
      "source": "stdout",
      "log": ": "     at
 com.myproject.model.MyProject.oneMoreMethod(MyProject.java:18)",
      "ecs_cluster": "default",
      "ecs_task_arn": "arn:aws:region:123456789012:task/default/
b23c940d29ed4714971cba72cEXAMPLE,
      "ecs_task_definition": "firelense-example-multiline:3"
     }
```

複数行のログ設定を使用すると、出力は次の例のようになります。

```
2022-09-20T15:47:56:595-05-00                              {"container_id":
 "82ba37cada1d44d389b03e78caf74faa-EXAMPLE", "container_name": "example-app",
 "stdout",...
    {
      "container_id":  "82ba37cada1d44d389b03e78caf74faa-EXAMPLE",
      "container_name: ": "example-app",
      "source": "stdout",
      "log:    "September 20, 2022 06:41:48 Exception in thread \"main\"
 java.lang.RuntimeException: Something has gone wrong, aborting!\n
    at com.myproject.module.MyProject.badMethod(MyProject.java:22)\n    at
```

```
    at com.myproject.model.MyProject.oneMoreMethod(MyProject.java:18)
 com.myproject.module.MyProject.main(MyProject.java:6)",
      "ecs_cluster": "default",
      "ecs_task_arn": "arn:aws:region:123456789012:task/default/
b23c940d29ed4714971cba72cEXAMPLE",
      "ecs_task_definition": "firelense-example-multiline:2"
     }
```

オプションを解析して連結する

ログを解析し、改行によって分割された行を連結するには、以下の 2 つのオプションのいずれかを使用します。

- 同じメッセージに属する行を解析および連結するルールを含む独自のパーサーファイルを作成します。
- Fluent Bit 組み込みパーサーを使用します。Fluent Bit 組み込みパーサーでサポートされている言語のリストについては、「Fluent Bit ドキュメント」を参照してください。

次のチュートリアルでは、各ユースケースの手順を説明します。この手順では、複数行を連結し、ログを Amazon CloudWatch に送信する方法について説明します。ログに別の宛先を指定できます。

例:作成したパーサーを使用する

このチュートリアルでは、次の手順を実行します。

1. Fluent Bit コンテナのイメージをビルドしてアップロードします。
2. 実行され、失敗し、複数行スタックトレースを生成するデモ複数行アプリケーションのイメージをビルドしてアップロードします。
3. タスク定義を作成して、タスクを起動する
4. ログを表示して、複数の行にまたがるメッセージが連結されて表示されることを確認します。

Fluent Bit コンテナのイメージをビルドしてアップロードします。

このイメージには、正規表現を指定するパーサーファイルと、パーサーファイルを参照する設定ファイルが含まれます。

1. `FluentBitDockerImage` という名前のフォルダを作成します。

2. フォルダ内で、ログを解析し、同じメッセージに属する行を連結するためのルールを含むパーサーファイルを作成します。

   a. パーサーファイルに次のコンテンツを貼り付けます。

```
[MULTILINE_PARSER]
    name          multiline-regex-test
    type          regex
    flush_timeout 1000
    #
    # Regex rules for multiline parsing
    # ---------------------------------
    #
    # configuration hints:
    #
    #  - first state always has the name: start_state
    #  - every field in the rule must be inside double quotes
    #
    # rules |   state name  | regex pattern                  | next state
    # ------|---------------|--------------------------------------------
    rule      "start_state"   "/(Dec \d+ \d+\:\d+\:\d+)(.*)/"  "cont"
    rule      "cont"          "/^\s+at.*/"                     "cont"
```

   正規表現パターンをカスタマイズするときは、正規表現エディタを使用して式をテストすることをお勧めします。

   b. `parsers_multiline.conf` という名前でファイルを保存します。

3. `FluentBitDockerImage` フォルダで、前のステップで作成したパーサーファイルを参照するカスタム設定ファイルを作成します。

   カスタム設定ファイルの詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「カスタム設定ファイルの指定」を参照してください。

   a. ファイルに次のコンテンツを貼り付けます。

```
[SERVICE]
    flush                1
    log_level            info
    parsers_file         /parsers_multiline.conf

[FILTER]
    name                 multiline
```

```
    match                 *
    multiline.key_content log
    multiline.parser      multiline-regex-test
```

> **Note**
>
> パーサーの絶対パスを使用する必要があります。

b. `extra.conf` という名前でファイルを保存します。

4. `FluentBitDockerImage` フォルダで、Fluent Bit イメージと、作成したパーサーファイルと設定ファイルを使用して Dockerfile を作成します。

a. ファイルに次のコンテンツを貼り付けます。

```
FROM public.ecr.aws/aws-observability/aws-for-fluent-bit:latest

ADD parsers_multiline.conf /parsers_multiline.conf
ADD extra.conf /extra.conf
```

b. `Dockerfile` という名前でファイルを保存します。

5. Dockerfile を使用して、パーサーとカスタム設定ファイルが含まれたカスタム Fluent Bit イメージをビルドします。

> **Note**
>
> このファイルパスが FireLens によって使用される `/fluent-bit/etc/fluent-bit.conf` の場合を除いて、Dockerイメージの任意の場所にパーサーファイルと構成ファイルを配置できます。

a. イメージを構築します: `docker build -t fluent-bit-multiline-image .`

どこ: `fluent-bit-multiline-image` この例のイメージの名前です。

b. 次を実行して、イメージが正しく作成されたことを確認します: `docker images –filter reference=fluent-bit-multiline-image`

成功すると、出力にイメージと `latest` タグが表示されます。

6. カスタムの Fluent Bit イメージを Amazon Elastic Container Registry にアップロードします。

a. イメージを保存する Amazon ECR リポジトリを作成します: `aws ecr create-repository --repository-name fluent-bit-multiline-repo --region us-east-1`

   どこ: `fluent-bit-multiline-repo` は、リポジトリの名前です。`us-east-1` はこの例のリージョンです。

   出力には、新しいリポジトリの詳細が表示されます。

b. 前のステップの `docker tag` *`fluent-bit-multiline-image repositoryUri`* の値で `repositoryUri` イメージにタグを付けます。

   例 : `docker tag fluent-bit-multiline-image xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/fluent-bit-multiline-repo`

c. Docker イメージを実行して、正しく実行されたことを確認します: `docker images –filter reference=`*`repositoryUri`*

   出力では、リポジトリ名が fluent-bit-multiline-repo から `repositoryUri` に変わります。

d. `aws ecr get-login-password` コマンドを実行し、認証先のレジストリ ID を指定して Amazon ECR を認証します: `aws ecr get-login-password | docker login --username AWS --password-stdin` *`registry ID`*`.dkr.ecr.`*`region`*`.amazonaws.com`

   例 : `ecr get-login-password | docker login --username AWS --password-stdin xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com`

   正常にログインメッセージが表示されます。

e. Amazon ECR にイメージをプッシュします: `docker push` *`registry ID`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`repository name`*

   例 : `docker push xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/fluent-bit-multiline-repo`

デモ複数行アプリケーションのイメージをビルドしてアップロードする

このイメージには、アプリケーションを実行する Python スクリプトファイルと、サンプルログファイルが含まれます。

タスクを実行すると、アプリケーションは実行をシミュレートし、失敗してスタックトレースを作成します。

1. multiline-app という名前のフォルダを作成します: mkdir multiline-app
2. Python スクリプトファイルを作成します。
   a. multiline-app フォルダで、ファイルを作成して、main.py という名前を付けます。
   b. ファイルに次のコンテンツを貼り付けます。

```
import os
import time
file1 = open('/test.log', 'r')
Lines = file1.readlines()

count = 0

for i in range(10):
    print("app running normally...")
    time.sleep(1)

# Strips the newline character
for line in Lines:
    count += 1
    print(line.rstrip())
print(count)
print("app terminated.")
```

   c. main.py ファイルを保存します。
3. サンプルのログファイルを作成します。
   a. multiline-app フォルダで、ファイルを作成して、test.log という名前を付けます。
   b. ファイルに次のコンテンツを貼り付けます。

```
single line...
Dec 14 06:41:08 Exception in thread "main" java.lang.RuntimeException:
 Something has gone wrong, aborting!
    at com.myproject.module.MyProject.badMethod(MyProject.java:22)
    at com.myproject.module.MyProject.oneMoreMethod(MyProject.java:18)
    at com.myproject.module.MyProject.anotherMethod(MyProject.java:14)
    at com.myproject.module.MyProject.someMethod(MyProject.java:10)
```

```
    at com.myproject.module.MyProject.main(MyProject.java:6)
another line...
```

c. test.log ファイルを保存します。

4. multiline-app フォルダで Dockerfile を作成します。

a. ファイルに次のコンテンツを貼り付けます。

```
FROM public.ecr.aws/amazonlinux/amazonlinux:latest
ADD test.log /test.log

RUN yum upgrade -y && yum install -y python3

WORKDIR /usr/local/bin

COPY main.py .

CMD ["python3", "main.py"]
```

b. Dockerfile ファイルを保存します。

5. Dockerfile を使用して、イメージをビルドします。

a. イメージを構築します: docker build -t multiline-app-image .

どこ: multiline-app-image この例のイメージの名前です。

b. 次を実行して、イメージが正しく作成されたことを確認します: docker images –filter reference=multiline-app-image

成功すると、出力にイメージと latest タグが表示されます。

6. イメージを Amazon Elastic コンテナレジストリにアップロードします。

a. イメージを保存する Amazon ECR リポジトリを作成します: aws ecr create-repository --repository-name multiline-app-repo --region us-east-1

どこ: multiline-app-repo は、リポジトリの名前です。us-east-1 はこの例のリージョンです。

出力には、新しいリポジトリの詳細が表示されます。次のステップで必要になるため、repositoryUri の値を書きとめておきます。

b. 前のステップの docker tag *multiline-app-image repositoryUri* の値で repositoryUri イメージにタグを付けます。

例 : docker tag multiline-app-image xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/multiline-app-repo

c. Docker イメージを実行して、正しく実行されたことを確認します: docker images –filter reference=*repositoryUri*

出力では、リポジトリ名が multiline-app-repo から repositoryUri に変更されます。

d. Amazon ECR にイメージをプッシュします: docker push *aws_account_id*.dkr.ecr.*region*.amazonaws.com/*repository name*

例 : docker push *xxxxxxxxxxxx*.dkr.ecr.*us-east-1*.amazonaws.com/multiline-app-repo

タスク定義を作成して、タスクを実行する

1. ファイル名 multiline-task-definition.json でタスク定義ファイルを作成します。
2. multiline-task-definition.json ファイルに次のコンテンツを貼り付けます。

```
{
    "family": "firelens-example-multiline",
    "taskRoleArn": "task role ARN,
    "executionRoleArn": "execution role ARN",
    "containerDefinitions": [
        {
            "essential": true,
            "image": "aws_account_id.dkr.ecr.us-east-1.amazonaws.com/fluent-bit-
multiline-image:latest",
            "name": "log_router",
            "firelensConfiguration": {
                "type": "fluentbit",
                "options": {
                    "config-file-type": "file",
                    "config-file-value": "/extra.conf"
                }
            },
            "memoryReservation": 50
        },
```

```
        {
            "essential": true,
            "image": "aws_account_id.dkr.ecr.us-east-1.amazonaws.com/multiline-app-
image:latest",
            "name": "app",
            "logConfiguration": {
                "logDriver": "awsfirelens",
                "options": {
                    "Name": "cloudwatch_logs",
                    "region": "us-east-1",
                    "log_group_name": "multiline-test/application",
                    "auto_create_group": "true",
                    "log_stream_prefix": "multiline-"
                }
            },
            "memoryReservation": 100
        }
    ],
    "requiresCompatibilities": ["FARGATE"],
    "networkMode": "awsvpc",
    "cpu": "256",
    "memory": "512"
}
```

multiline-task-definition.json タスク定義で以下を置き換えます:

a. *task role ARN*

タスクロールの ARN を検索するには、IAM コンソールに移動します。ロールを選択し、作成した ecs-task-role-for-firelens タスクロールを検索します。ロールを選択し、概要セクションに表示される ARN をコピーします。

b. *execution role ARN*

実行ロールの ARN を検索するには、IAM コンソールに移動します。ロールを選択し、ecsTaskExecutionRole ロールを検索します。ロールを選択し、概要セクションに表示される ARN をコピーします。

c. *aws_account_id*

aws_account_id を検索するには、AWS Management Console にログインします。右上のユーザー名を選択し、アカウント ID をコピーします。

d. *us-east-1*

必要に応じてリージョンを置換します。

3. タスク定義ファイルを登録します: `aws ecs register-task-definition --cli-input-json file://multiline-task-definition.json --region region`
4. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
5. ナビゲーションペインで、[タスク定義] を選択し、上記のタスク定義の最初の行でタスク定義をこのファミリに登録したため、`firelens-example-multiline` ファミリを選択します。
6. 最新バージョンを選択します。
7. [デプロイ]、[タスクを実行] を選択します。
8. [タスクを実行] ページの [クラスター] でクラスターを選択し、[ネットワーク] の [サブネット] で、タスクに使用できるサブネットを選択します。
9. [Create] (作成) を選択します。

Amazon CloudWatch の複数行のログメッセージが連結されて表示されることを確認する

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Logs (ログ)] を展開して、[Log groups (ロググループ)] を選択します。
3. `multiline-test/applicatio` ロググループを選択します。
4. ログを選択します。メッセージを表示します。パーサーファイル内のルールに一致する行は連結され、1 つのメッセージとして表示されます。

   次のログスニペットは、単一の Java スタックトレースイベントで連結された行を示しています。

```
{
    "container_id": "xxxxxx",
    "container_name": "app",
    "source": "stdout",
    "log": "Dec 14 06:41:08 Exception in thread \"main\"
 java.lang.RuntimeException: Something has gone wrong, aborting!\n
 at com.myproject.module.MyProject.badMethod(MyProject.java:22)\n    at
 com.myproject.module.MyProject.oneMoreMethod(MyProject.java:18)\n
 at com.myproject.module.MyProject.anotherMethod(MyProject.java:14)\n
 at com.myproject.module.MyProject.someMethod(MyProject.java:10)\n    at
 com.myproject.module.MyProject.main(MyProject.java:6)",
    "ecs_cluster": "default",
```

```
    "ecs_task_arn": "arn:aws:ecs:us-east-1:xxxxxxxxxxxx:task/default/xxxxxx",
    "ecs_task_definition": "firelens-example-multiline:2"
}
```

次のログスニペットは、複数行のログメッセージを連結するように設定されていない Amazon ECS コンテナを実行する場合に、同じメッセージが 1 行でどのように表示されるかを示しています。

```
{
    "log": "Dec 14 06:41:08 Exception in thread \"main\"
 java.lang.RuntimeException: Something has gone wrong, aborting!",
    "container_id": "xxxxxx-xxxxxx",
    "container_name": "app",
    "source": "stdout",
    "ecs_cluster": "default",
    "ecs_task_arn": "arn:aws:ecs:us-east-1:xxxxxxxxxxxx:task/default/xxxxxx",
    "ecs_task_definition": "firelens-example-multiline:3"
}
```

例: Fluent Bit 組み込みパーサーを使用します。

このチュートリアルでは、次の手順を実行します。

1. Fluent Bit コンテナのイメージをビルドしてアップロードします。
2. 実行され、失敗し、複数行スタックトレースを生成するデモ複数行アプリケーションのイメージをビルドしてアップロードします。
3. タスク定義を作成して、タスクを起動する
4. ログを表示して、複数の行にまたがるメッセージが連結されて表示されることを確認します。

Fluent Bit コンテナのイメージをビルドしてアップロードします。

このイメージには、Fluent Bit パーサーを参照する設定ファイルが含まれています。

1. `FluentBitDockerImage` という名前のフォルダを作成します。
2. `FluentBitDockerImage` フォルダで、Fluent Bit 組み込みパーサーファイルを参照するカスタム設定ファイルを作成します。

カスタム設定ファイルの詳細については、「Amazon Elastic Container Service デベロッパーガイド」の「カスタム設定ファイルの指定」を参照してください。

a. ファイルに次のコンテンツを貼り付けます。

```
[FILTER]
    name                  multiline
    match                 *
    multiline.key_content log
    multiline.parser      go
```

b. `extra.conf` という名前でファイルを保存します。

3. `FluentBitDockerImage` フォルダで、Fluent Bit イメージと、作成したパーサーファイルと設定ファイルを使用して Dockerfile を作成します。

a. ファイルに次のコンテンツを貼り付けます。

```
FROM public.ecr.aws/aws-observability/aws-for-fluent-bit:latest
ADD extra.conf /extra.conf
```

b. `Dockerfile` という名前でファイルを保存します。

4. Dockerfile を使用して、カスタム設定ファイルを含めてカスタム Fluent Bit イメージをビルドします。

> **Note**
>
> このファイルパスが FireLens によって使用される `/fluent-bit/etc/fluent-bit.conf` の場合を除いて、Docker イメージの任意の場所に設定ファイルを配置できます。

a. イメージを構築します: `docker build -t fluent-bit-multiline-image .`

どこ: `fluent-bit-multiline-image` この例のイメージの名前です。

b. 次を実行して、イメージが正しく作成されたことを確認します: `docker images –filter reference=fluent-bit-multiline-image`

成功すると、出力にイメージと `latest` タグが表示されます。

5. カスタムの Fluent Bit イメージを Amazon Elastic Container Registry にアップロードします。

   a. イメージを保存する Amazon ECR リポジトリを作成します: `aws ecr create-repository --repository-name fluent-bit-multiline-repo --region us-east-1`

      どこ: `fluent-bit-multiline-repo` は、リポジトリの名前です。`us-east-1` はこの例のリージョンです。

      出力には、新しいリポジトリの詳細が表示されます。

   b. 前のステップの `docker tag *fluent-bit-multiline-image repositoryUri*` の値で `repositoryUri` イメージにタグを付けます。

      例 : `docker tag fluent-bit-multiline-image xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/fluent-bit-multiline-repo`

   c. Docker イメージを実行して、正しく実行されたことを確認します: `docker images –filter reference=*repositoryUri*`

      出力では、リポジトリ名が fluent-bit-multiline-repo から `repositoryUri` に変わります。

   d. `aws ecr get-login-password` コマンドを実行し、認証先のレジストリ ID を指定して Amazon ECR を認証します: `aws ecr get-login-password | docker login --username AWS --password-stdin *registry ID*.dkr.ecr.*region*.amazonaws.com`

      例 : `ecr get-login-password | docker login --username AWS --password-stdin xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com`

      正常にログインメッセージが表示されます。

   e. Amazon ECR にイメージをプッシュします: `docker push *registry ID*.dkr.ecr.*region*.amazonaws.com/*repository name*`

      例 : `docker push xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/fluent-bit-multiline-repo`

デモ複数行アプリケーションのイメージをビルドしてアップロードする

このイメージには、アプリケーションを実行する Python スクリプトファイルと、サンプルログファイルが含まれます。

1. multiline-app という名前のフォルダを作成します: mkdir multiline-app
2. Python スクリプトファイルを作成します。
   a. multiline-app フォルダで、ファイルを作成して、main.py という名前を付けます。
   b. ファイルに次のコンテンツを貼り付けます。

```
import os
import time
file1 = open('/test.log', 'r')
Lines = file1.readlines()

count = 0

for i in range(10):
    print("app running normally...")
    time.sleep(1)

# Strips the newline character
for line in Lines:
    count += 1
    print(line.rstrip())
print(count)
print("app terminated.")
```

   c. main.py ファイルを保存します。
3. サンプルのログファイルを作成します。
   a. multiline-app フォルダで、ファイルを作成して、test.log という名前を付けます。
   b. ファイルに次のコンテンツを貼り付けます。

```
panic: my panic

goroutine 4 [running]:
panic(0x45cb40, 0x47ad70)
  /usr/local/go/src/runtime/panic.go:542 +0x46c fp=0xc42003f7b8 sp=0xc42003f710
 pc=0x422f7c
main.main.func1(0xc420024120)
  foo.go:6 +0x39 fp=0xc42003f7d8 sp=0xc42003f7b8 pc=0x451339
runtime.goexit()
```

```
  /usr/local/go/src/runtime/asm_amd64.s:2337 +0x1 fp=0xc42003f7e0
 sp=0xc42003f7d8 pc=0x44b4d1
created by main.main
  foo.go:5 +0x58

goroutine 1 [chan receive]:
runtime.gopark(0x4739b8, 0xc420024178, 0x46fcd7, 0xc, 0xc420028e17, 0x3)
  /usr/local/go/src/runtime/proc.go:280 +0x12c fp=0xc420053e30 sp=0xc420053e00
 pc=0x42503c
runtime.goparkunlock(0xc420024178, 0x46fcd7, 0xc, 0x1000f010040c217, 0x3)
  /usr/local/go/src/runtime/proc.go:286 +0x5e fp=0xc420053e70 sp=0xc420053e30
 pc=0x42512e
runtime.chanrecv(0xc420024120, 0x0, 0xc420053f01, 0x4512d8)
  /usr/local/go/src/runtime/chan.go:506 +0x304 fp=0xc420053f20 sp=0xc420053e70
 pc=0x4046b4
runtime.chanrecv1(0xc420024120, 0x0)
  /usr/local/go/src/runtime/chan.go:388 +0x2b fp=0xc420053f50 sp=0xc420053f20
 pc=0x40439b
main.main()
  foo.go:9 +0x6f fp=0xc420053f80 sp=0xc420053f50 pc=0x4512ef
runtime.main()
  /usr/local/go/src/runtime/proc.go:185 +0x20d fp=0xc420053fe0 sp=0xc420053f80
 pc=0x424bad
runtime.goexit()
  /usr/local/go/src/runtime/asm_amd64.s:2337 +0x1 fp=0xc420053fe8
 sp=0xc420053fe0 pc=0x44b4d1

goroutine 2 [force gc (idle)]:
runtime.gopark(0x4739b8, 0x4ad720, 0x47001e, 0xf, 0x14, 0x1)
  /usr/local/go/src/runtime/proc.go:280 +0x12c fp=0xc42003e768 sp=0xc42003e738
 pc=0x42503c
runtime.goparkunlock(0x4ad720, 0x47001e, 0xf, 0xc420000114, 0x1)
  /usr/local/go/src/runtime/proc.go:286 +0x5e fp=0xc42003e7a8 sp=0xc42003e768
 pc=0x42512e
runtime.forcegchelper()
  /usr/local/go/src/runtime/proc.go:238 +0xcc fp=0xc42003e7e0 sp=0xc42003e7a8
 pc=0x424e5c
runtime.goexit()
  /usr/local/go/src/runtime/asm_amd64.s:2337 +0x1 fp=0xc42003e7e8
 sp=0xc42003e7e0 pc=0x44b4d1
created by runtime.init.4
  /usr/local/go/src/runtime/proc.go:227 +0x35

goroutine 3 [GC sweep wait]:
```

```
runtime.gopark(0x4739b8, 0x4ad7e0, 0x46fdd2, 0xd, 0x419914, 0x1)
  /usr/local/go/src/runtime/proc.go:280 +0x12c fp=0xc42003ef60 sp=0xc42003ef30
 pc=0x42503c
runtime.goparkunlock(0x4ad7e0, 0x46fdd2, 0xd, 0x14, 0x1)
  /usr/local/go/src/runtime/proc.go:286 +0x5e fp=0xc42003efa0 sp=0xc42003ef60
 pc=0x42512e
runtime.bgsweep(0xc42001e150)
  /usr/local/go/src/runtime/mgcsweep.go:52 +0xa3 fp=0xc42003efd8
 sp=0xc42003efa0 pc=0x419973
runtime.goexit()
  /usr/local/go/src/runtime/asm_amd64.s:2337 +0x1 fp=0xc42003efe0
 sp=0xc42003efd8 pc=0x44b4d1
created by runtime.gcenable
  /usr/local/go/src/runtime/mgc.go:216 +0x58
one more line, no multiline
```

c. test.log ファイルを保存します。

4. multiline-app フォルダで Dockerfile を作成します。

a. ファイルに次のコンテンツを貼り付けます。

```
FROM public.ecr.aws/amazonlinux/amazonlinux:latest
ADD test.log /test.log

RUN yum upgrade -y && yum install -y python3

WORKDIR /usr/local/bin

COPY main.py .

CMD ["python3", "main.py"]
```

b. Dockerfile ファイルを保存します。

5. Dockerfile を使用して、イメージをビルドします。

a. イメージを構築します: docker build -t multiline-app-image .

どこ: multiline-app-image この例のイメージの名前です。

b. 次を実行して、イメージが正しく作成されたことを確認します: docker images –filter reference=multiline-app-image

成功すると、出力にイメージと latest タグが表示されます。

6. イメージを Amazon Elastic コンテナレジストリにアップロードします。

   a. イメージを保存する Amazon ECR リポジトリを作成します: `aws ecr create-repository --repository-name multiline-app-repo --region us-east-1`

      どこ: `multiline-app-repo` は、リポジトリの名前です。`us-east-1` はこの例のリージョンです。

      出力には、新しいリポジトリの詳細が表示されます。次のステップで必要になるため、`repositoryUri` の値を書きとめておきます。

   b. 前のステップの `docker tag` *`multiline-app-image repositoryUri`* の値で `repositoryUri` イメージにタグを付けます。

      例 : `docker tag multiline-app-image xxxxxxxxxxxx.dkr.ecr.us-east-1.amazonaws.com/multiline-app-repo`

   c. Docker イメージを実行して、正しく実行されたことを確認します: `docker images –filter reference=`*`repositoryUri`*

      出力では、リポジトリ名が `multiline-app-repo` から `repositoryUri` に変更されます。

   d. Amazon ECR にイメージをプッシュします: `docker push` *`aws_account_id`*`.dkr.ecr.`*`region`*`.amazonaws.com/`*`repository name`*

      例 : `docker push` *`xxxxxxxxxxxx`*`.dkr.ecr.`*`us-east-1`*`.amazonaws.com/multiline-app-repo`

タスク定義を作成して、タスクを実行する

1. ファイル名 `multiline-task-definition.json` でタスク定義ファイルを作成します。
2. `multiline-task-definition.json` ファイルに次のコンテンツを貼り付けます。

```
{
    "family": "firelens-example-multiline",
    "taskRoleArn": "task role ARN,
    "executionRoleArn": "execution role ARN",
    "containerDefinitions": [
        {
            "essential": true,
```

```
            "image": "aws_account_id.dkr.ecr.us-east-1.amazonaws.com/fluent-bit-
multiline-image:latest",
            "name": "log_router",
            "firelensConfiguration": {
                "type": "fluentbit",
                "options": {
                    "config-file-type": "file",
                    "config-file-value": "/extra.conf"
                }
            },
            "memoryReservation": 50
        },
        {
            "essential": true,
            "image": "aws_account_id.dkr.ecr.us-east-1.amazonaws.com/multiline-app-
image:latest",
            "name": "app",
            "logConfiguration": {
                "logDriver": "awsfirelens",
                "options": {
                    "Name": "cloudwatch_logs",
                    "region": "us-east-1",
                    "log_group_name": "multiline-test/application",
                    "auto_create_group": "true",
                    "log_stream_prefix": "multiline-"
                }
            },
            "memoryReservation": 100
        }
    ],
    "requiresCompatibilities": ["FARGATE"],
    "networkMode": "awsvpc",
    "cpu": "256",
    "memory": "512"
}
```

multiline-task-definition.json タスク定義で以下を置き換えます:

a. *task role ARN*

タスクロールの ARN を検索するには、IAM コンソールに移動します。ロールを選択し、作成した ecs-task-role-for-firelens タスクロールを検索します。ロールを選択し、概要セクションに表示される ARN をコピーします。

b. *execution role ARN*

実行ロールの ARN を検索するには、IAM コンソールに移動します。ロールを選択し、ecsTaskExecutionRole ロールを検索します。ロールを選択し、概要セクションに表示される ARN をコピーします。

c. *aws_account_id*

aws_account_id を検索するには、AWS Management Console にログインします。右上のユーザー名を選択し、アカウント ID をコピーします。

d. *us-east-1*

必要に応じてリージョンを置換します。

3. タスク定義ファイルを登録します: `aws ecs register-task-definition --cli-input-json file://multiline-task-definition.json --region us-east-1`
4. コンソール (https://console.aws.amazon.com/ecs/v2) を開きます。
5. ナビゲーションペインで、[タスク定義] を選択し、上記のタスク定義の最初の行でタスク定義をこのファミリに登録したため、firelens-example-multiline ファミリを選択します。
6. 最新バージョンを選択します。
7. [デプロイ]、[タスクを実行] を選択します。
8. [タスクを実行] ページの [クラスター] でクラスターを選択し、[ネットワーク] の [サブネット] で、タスクに使用できるサブネットを選択します。
9. [Create] (作成) を選択します。

Amazon CloudWatch の複数行のログメッセージが連結されて表示されることを確認する

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Logs (ログ)] を展開して、[Log groups (ロググループ)] を選択します。
3. multiline-test/applicatio ロググループを選択します。
4. ログを選択し、メッセージを表示します。パーサーファイル内のルールに一致する行は連結され、1 つのメッセージとして表示されます。

次のログスニペットは、単一の Go スタックトレースイベントで連結された行を示しています。

```
{
```

```
    "log": "panic: my panic\n\ngoroutine 4 [running]:\npanic(0x45cb40,
 0x47ad70)\n  /usr/local/go/src/runtime/panic.go:542 +0x46c fp=0xc42003f7b8
 sp=0xc42003f710 pc=0x422f7c\nmain.main.func1(0xc420024120)\n  foo.go:6
 +0x39 fp=0xc42003f7d8 sp=0xc42003f7b8 pc=0x451339\nruntime.goexit()\n  /usr/
local/go/src/runtime/asm_amd64.s:2337 +0x1 fp=0xc42003f7e0 sp=0xc42003f7d8
 pc=0x44b4d1\ncreated by main.main\n  foo.go:5 +0x58\n\ngoroutine 1 [chan receive]:
\nruntime.gopark(0x4739b8, 0xc420024178, 0x46fcd7, 0xc, 0xc420028e17, 0x3)\n  /usr/
local/go/src/runtime/proc.go:280 +0x12c fp=0xc420053e30 sp=0xc420053e00 pc=0x42503c
\nruntime.goparkunlock(0xc420024178, 0x46fcd7, 0xc, 0x1000f010040c217, 0x3)\n
  /usr/local/go/src/runtime/proc.go:286 +0x5e fp=0xc420053e70 sp=0xc420053e30
 pc=0x42512e\nruntime.chanrecv(0xc420024120, 0x0, 0xc420053f01, 0x4512d8)\n
  /usr/local/go/src/runtime/chan.go:506 +0x304 fp=0xc420053f20 sp=0xc420053e70
 pc=0x4046b4\nruntime.chanrecv1(0xc420024120, 0x0)\n  /usr/local/go/src/runtime/
chan.go:388 +0x2b fp=0xc420053f50 sp=0xc420053f20 pc=0x40439b\nmain.main()\n
 foo.go:9 +0x6f fp=0xc420053f80 sp=0xc420053f50 pc=0x4512ef\nruntime.main()\n
  /usr/local/go/src/runtime/proc.go:185 +0x20d fp=0xc420053fe0 sp=0xc420053f80
 pc=0x424bad\nruntime.goexit()\n  /usr/local/go/src/runtime/asm_amd64.s:2337
 +0x1 fp=0xc420053fe8 sp=0xc420053fe0 pc=0x44b4d1\n\ngoroutine 2 [force gc
 (idle)]:\nruntime.gopark(0x4739b8, 0x4ad720, 0x47001e, 0xf, 0x14, 0x1)\n  /
usr/local/go/src/runtime/proc.go:280 +0x12c fp=0xc42003e768 sp=0xc42003e738
 pc=0x42503c\nruntime.goparkunlock(0x4ad720, 0x47001e, 0xf, 0xc420000114, 0x1)\n
  /usr/local/go/src/runtime/proc.go:286 +0x5e fp=0xc42003e7a8 sp=0xc42003e768
 pc=0x42512e\nruntime.forcegchelper()\n  /usr/local/go/src/runtime/proc.go:238
 +0xcc fp=0xc42003e7e0 sp=0xc42003e7a8 pc=0x424e5c\nruntime.goexit()\n  /usr/
local/go/src/runtime/asm_amd64.s:2337 +0x1 fp=0xc42003e7e8 sp=0xc42003e7e0
 pc=0x44b4d1\ncreated by runtime.init.4\n  /usr/local/go/src/runtime/proc.go:227
 +0x35\n\ngoroutine 3 [GC sweep wait]:\nruntime.gopark(0x4739b8, 0x4ad7e0,
 0x46fdd2, 0xd, 0x419914, 0x1)\n  /usr/local/go/src/runtime/proc.go:280 +0x12c
 fp=0xc42003ef60 sp=0xc42003ef30 pc=0x42503c\nruntime.goparkunlock(0x4ad7e0,
 0x46fdd2, 0xd, 0x14, 0x1)\n  /usr/local/go/src/runtime/proc.go:286 +0x5e
 fp=0xc42003efa0 sp=0xc42003ef60 pc=0x42512e\nruntime.bgsweep(0xc42001e150)\n
  /usr/local/go/src/runtime/mgcsweep.go:52 +0xa3 fp=0xc42003efd8 sp=0xc42003efa0
 pc=0x419973\nruntime.goexit()\n  /usr/local/go/src/runtime/asm_amd64.s:2337 +0x1
 fp=0xc42003efe0 sp=0xc42003efd8 pc=0x44b4d1\ncreated by runtime.gcenable\n  /usr/
local/go/src/runtime/mgc.go:216 +0x58",
    "container_id": "xxxxxx-xxxxxx",
    "container_name": "app",
    "source": "stdout",
    "ecs_cluster": "default",
    "ecs_task_arn": "arn:aws:ecs:us-east-1:xxxxxxxxxxxx:task/default/xxxxxx",
    "ecs_task_definition": "firelens-example-multiline:2"
}
```

次のログスニペットは、複数行のログメッセージを連結するように設定されていない ECS コンテナを実行する場合に、同じイベントがどのように表示されるかを示しています。ログフィールドには 1 行が含まれます。

```
{
    "log": "panic: my panic",
    "container_id": "xxxxxx-xxxxxx",
    "container_name": "app",
    "source": "stdout",
    "ecs_cluster": "default",
    "ecs_task_arn": "arn:aws:ecs:us-east-1:xxxxxxxxxxxx:task/default/xxxxxx",
    "ecs_task_definition": "firelens-example-multiline:3"
```

> **Note**
>
> ログが標準出力ではなくログファイルに移動する場合は、フィルターではなく Tail 入力プラグインで `multiline.parser` および `multiline.key_content` 構成パラメーターを指定することをお勧めします。

Amazon ECS Windows コンテナに Fluent Bit をデプロイする

Fluent Bit とは、さまざまなオペレーティングシステムでサポートされている高速で柔軟なログプロセッサおよびルーターです。Amazon CloudWatch Logs、Firehose Amazon S3、Amazon OpenSearch Service など、さまざまな AWS の宛先にログをルーティングするために使用できます。Fluent Bit は、Datadog、Splunk、カスタム HTTP サーバーなどの一般的なパートナーソリューションをサポートしています。Fluent Bit の詳細については、Fluent Bit のウェブサイトを参照してください。

AWS for Fluent Bit イメージは、高可用性を実現するためにほとんどのリージョンの Amazon ECR Public Gallery と Amazon ECR リポジトリの両方の Amazon ECR で利用できます。この詳細については、GitHub ウェブサイトの「aws-for-fluent-bit」を参照してください。

このチュートリアルでは、Amazon ECS で実行されている Windows インスタンスに Fluent Bit コンテナをデプロイし、Windows タスクによって生成されたログを Amazon CloudWatch にストリーミングして集中型ロギングを実現する方法について説明します。

このチュートリアルでは、次のようなアプローチを使用します。

- Fluent Bit は、デーモンスケジューリングストラテジーを備えたサービスとして実行されます。この戦略により、Fluent Bit の 1 つのインスタンスが常にクラスター内のコンテナインスタンス上で実行されるようになります。
  - 転送入力プラグインを使用して、ポート 24224 でリッスンします。
  - Docker ランタイムがこの公開ポートを使用して Fluent Bit にログを送信できるように、ポート 24224 をホストに公開します。
  - Fluent Bit がログレコードを指定された宛先に送信できるようにする設定があります。
- fluentd ロギングドライバーを使用して、その他すべての Amazon ECS タスクコンテナを起動します。詳細については、Docker ドキュメントのウェブサイトの「Fluentd ロギングドライバー」を参照してください。
  - Docker は、ホスト名前空間内のローカルホスト上の TCP ソケット 24224 に接続します。
  - Amazon ECS エージェントは、クラスター名、タスク定義ファミリー名、タスク定義リビジョン番号、タスク ARN、およびコンテナ名を含むラベルをコンテナに追加します。fluentd docker ロギングドライバーの labels オプションを使用して、同じ情報がログレコードに追加されます。詳細については、Docker ドキュメントのウェブサイトの「ラベル、labels-regex、env、env、env-regex」を参照してください。
  - fluentd ロギングドライバーの `async` オプションは `true` に設定されているため、Fluent Bit コンテナを再起動すると、docker は Fluent Bit コンテナが再起動されるまでログをバッファー処理します。fluentd-buffer-limit オプションを設定することで、バッファー制限を増やすことができます。詳細については、Docker ドキュメントのウェブサイトの「fluentd-buffer-limit」を参照してください。

ワークフローは次のとおりです。

- Fluent Bit コンテナは、ホストに公開されているポート 24224 で起動してリッスンします。
- Fluent Bit では、タスク定義で指定されたタスク IAM ロール認証情報を使用します。
- 同じインスタンスで起動された他のタスクは、fluentd docker ロギングドライバーを使用してポート 24224 にある Fluent Bit コンテナに接続します。
- アプリケーションコンテナがログを生成すると、docker ランタイムはそれらのレコードにタグを付け、ラベルに指定されたメタデータを追加して、ホスト名前空間のポート 24224 に転送します。
- Fluent Bit はホスト名前空間に公開されているため、ポート 24224 でログレコードを受信します。
- Fluent Bit は内部処理を実行し、指定されたとおりにログをルーティングします。

このチュートリアルでは、以下を行うデフォルトの CloudWatch Fluent Bit 設定を使用します。

- 各クラスターとタスク定義ファミリーごとに新しいロググループを作成します。
- 新しいタスクが開始されるたびに、上記で生成されたロググループのタスクコンテナごとに新しいログストリームを作成します。各ストリームは、コンテナが属しているタスク ID でマークされます。
- クラスター名、タスク ARN、タスクコンテナ名、タスク定義ファミリー、タスク定義リビジョン番号などのを含むメタデータを各ログエントリに追加します。

  例えば、`container_1` と `container_2` のある `task_1` および `container_3` のある task_2 の場合、CloudWatch ログストリームは次のようになります。

  - `/aws/ecs/windows.ecs_task_1`

    `task-out.`*`TASK_ID`*`.container_1`

    `task-out.`*`TASK_ID`*`.container_2`
  - `/aws/ecs/windows.ecs_task_2`

    `task-out.`*`TASK_ID`*`.container_3`

ステップ

- 前提条件
- ステップ 1: IAM アクセスロールを作成する
- ステップ 2: Amazon ECS Windows コンテナインスタンスを作成する
- ステップ 3: Fluent Bit の設定
- ステップ 4: ログを CloudWatch にルーティングする Windows Fluent Bit タスク定義を登録する
- ステップ 5: デーモンスケジューリング戦略を使用して ecs-windows-fluent-bit タスク定義を Amazon ECS サービスとして実行する
- ステップ 6: ログを生成する Windows タスク定義を登録する
- ステップ 7: windows-app-task タスク定義を実行する
- ステップ 8: CloudWatch でログを確認する
- ステップ 9: クリーンアップする。

前提条件

このチュートリアルでは、以下の前提条件が完了済みであることを前提としています。

- AWS CLI の最新バージョンがインストールされ、設定されていること。詳細については、「AWS CLIの最新バージョンをインストールまたは更新」を参照してください。
- `aws-for-fluent-bit` コンテナイメージは、次の Windows オペレーティングシステムで使用できます。
  - Windows Server 2019 Core
  - Windows Server 2019 Full
  - Windows Server 2022 Core
  - Windows Server 2022 Full
- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- クラスターがあります。このチュートリアルでは、クラスター名は [FluentBit-Cluster] です。
- EC2 インスタンスを起動するパブリックサブネットを持つ VPC があります。デフォルトの VPC を使用できます。Amazon CloudWatch エンドポイントがサブネットに到達できるようにするプライベートサブネットを使用することもできます。Amazon CloudWatch エンドポイントの詳細については、「AWS 全般のリファレンス」の「Amazon CloudWatch のエンドポイントとクォータ」を参照してください。Amazon VPC ウィザードを使用して VPC を作成する方法の詳細については、「the section called “仮想プライベートクラウドを作成する”」を参照してください。

ステップ 1: IAM アクセスロールを作成する

Amazon ECS の IAM ロールを作成します。

1. 「ecsInstanceRole」という名前の Amazon ECS コンテナインスタンスロールを作成します。詳細については、「Amazon ECS コンテナインスタンス IAM ロール」を参照してください。
2. `fluentTaskRole` と名付けられた Fluent Bit タスク用の IAM ロールを作成します。詳細については、「the section called “タスク IAM ロール”」を参照してください。

   この IAM ロールで付与される IAM 許可は、タスクコンテナによって引き受けられます。Fluent Bit が CloudWatch にログを送信できるようにするには、タスク IAM ロールに次の権限をアタッチする必要があります。

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

```
    "Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "logs:CreateLogStream",
            "logs:CreateLogGroup",
            "logs:DescribeLogStreams",
            "logs:PutLogEvents"
        ],
        "Resource": "*"
    }
    ]
}
```

3. ロールへのポリシーの付与

    a. 上記の内容を、`fluent-bit-policy.json` という名前のファイルに保存します。

    b. `fluentTaskRole` IAM ロールにインラインポリシーをアタッチするには、次のコマンドを実行します。

```
aws iam put-role-policy --role-name fluentTaskRole --policy-name
 fluentTaskPolicy --policy-document file://fluent-bit-policy.json
```

ステップ 2: Amazon ECS Windows コンテナインスタンスを作成する

Amazon ECS Windows コンテナインスタンスを作成します。

Amazon ECS インスタンスを作成するには

1. `aws ssm get-parameters` コマンドを使用して、VPC をホストするリージョン用の AMI ID を取得します。詳細については、「Amazon ECS に最適化された AMI メタデータを取得する」を参照してください。
2. Amazon EC2 コンソールを使用して、インスタンスを起動します。

    a. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。

    b. ナビゲーションバーから、使用するリージョンを選択します。

    c. EC2 ダッシュボードから、[Launch Instance] を選択します。

    d. [Name (名前)] に一意の名前を入力します。

e. [Application and OS Images (Amazon Machine Image)] (アプリケーションおよび OS イメージ (Amazon マシンイメージ)) で、最初の手順で取得した AMI を選択します。

f. [Instance type (インスタンスタイプ)] として [t3.xlarge] を選択します。

g. [Key pair (login)] (キーペア (ログイン)) には、キーペアを選択します。

h. [Network settings] (ネットワーク設定) にある [Security group] (セキュリティグループ) には、既存のセキュリティグループを選択することも、新しいセキュリティグループを作成することもできます。

i. [Network settings] (ネットワーク設定) の [Auto-assign Public IP] (パブリック IP の自動割り当て) で、[Enable] (有効にする) を選択します。

j. [Advanced details] (高度な詳細) で、[IAM instance profile] (IAM インスタンスプロファイル) として [ecsInstanceRole] を選択します。

k. 次のユーザーデータを使用して、Amazon ECS コンテナインスタンスを設定します。[Advanced Details] (詳細情報) にある [User data] (ユーザーデータ) フィールドに以下のスクリプトを貼り付け、*cluster_name* をクラスターの名前に置き換えます。

```
<powershell>
Import-Module ECSTools
Initialize-ECSAgent -Cluster cluster-name -EnableTaskENI -EnableTaskIAMRole -
LoggingDrivers '["awslogs","fluentd"]'
</powershell>
```

l. 準備ができたら、確認フィールドを選択してから、[Launch Instances] を選択します。

m. 確認ページは、インスタンスが起動中であることを通知します。[View Instances] (インスタンスを表示) を選択して確認ページを閉じ、コンソールに戻ります。

ステップ 3: Fluent Bit の設定

AWS に用意されている次のデフォルト設定を使用すると、すぐに開始できます。

- Amazon CloudWatch。「Fluent Bit 公式マニュアル」にある Amazon CloudWatch 用 Fluent Bit プラグインをベースにしています。

または、AWS で提供されている他のデフォルト設定を使用することもできます。詳細については、aws-for-fluent-bit Github ウェブサイトの「Windows イメージのエントリポイントのオーバーライド」を参照してください。

デフォルトの Amazon CloudWatch Fluent Bit 設定を以下に示します。

以下の変数を置き換えます。

- *region* を、Amazon CloudWatch ログを送信したいリージョンで置き換えます。

```
[SERVICE]
    Flush               5
    Log_Level           info
    Daemon              off

[INPUT]
    Name                forward
    Listen              0.0.0.0
    Port                24224
    Buffer_Chunk_Size   1M
    Buffer_Max_Size     6M
    Tag_Prefix          ecs.

# Amazon ECS agent adds the following log keys as labels to the docker container.
# We would use fluentd logging driver to add these to log record while sending it to
 Fluent Bit.
[FILTER]
    Name                modify
    Match               ecs.*
    Rename              com.amazonaws.ecs.cluster ecs_cluster
    Rename              com.amazonaws.ecs.container-name ecs_container_name
    Rename              com.amazonaws.ecs.task-arn ecs_task_arn
    Rename              com.amazonaws.ecs.task-definition-family
 ecs_task_definition_family
    Rename              com.amazonaws.ecs.task-definition-version
 ecs_task_definition_version

[FILTER]
    Name                rewrite_tag
    Match               ecs.*
    Rule                $ecs_task_arn ^([a-z-:0-9]+)/([a-zA-Z0-9-_]+)/([a-z0-9]+)$
 out.$3.$ecs_container_name false
    Emitter_Name        re_emitted

[OUTPUT]
    Name                cloudwatch_logs
    Match               out.*
```

```
    region              region
    log_group_name      fallback-group
    log_group_template  /aws/ecs/$ecs_cluster.$ecs_task_definition_family
    log_stream_prefix   task-
    auto_create_group   On
```

Fluent Bit に入るすべてのログには、ユーザーが指定したタグが付いているか、指定しない場合は自動的に生成されます。タグを使用して、さまざまなログをさまざまな宛先にルーティングできます。追加情報については、「Fluent Bit 公式マニュアル」の「タグ」を参照してください。

前述の Fluent Bit 設定には次のプロパティがあります。

- 転送入力プラグインは TCP ポート 24224 で受信トラフィックをリッスンします。
- ポートで受信した各ログエントリにはタグがあり、転送入力プラグインはこれを変更してレコードのプレフィックスに `ecs.` 文字列を付けます。
- Fluent Bit の内部パイプラインは、Match regex を使用してログエントリをルーティングし、フィルターを変更します。このフィルターは、ログレコード JSON のキーを Fluent Bit が使用できる形式に置き換えます。
- 変更されたログエントリは、その後 rewrite_tag フィルターによって使用されます。このフィルターは、ログレコードのタグを out.*TASK_ID*。*CONTAINER_NAME* 形式に変更します。
- 新しいタグは、CloudWatch 出力プラグインの `log_group_template` オプションおよび `log_stream_prefix` オプションを使用して前述のようにロググループとストリームを作成する出力 cloudwatch_logs プラグインにルーティングされます。追加情報については、「Fluent Bit 公式マニュアル」の「設定パラメータ」を参照してください。

ステップ 4: ログを CloudWatch にルーティングする Windows Fluent Bit タスク定義を登録する

ログを CloudWatch にルーティングする Windows Fluent Bit タスク定義を登録します。

> **Note**
>
> このタスク定義では、Fluent Bit コンテナポート 24224 をホストポート 24224 に公開します。外部からのアクセスを防ぐため、EC2 インスタンスのセキュリティグループでこのポートが開いていないことを確認してください。

タスク定義を登録するには

1. 次の内容で、fluent-bit.json という名前のファイルを作成します。

   以下の変数を置き換えます。

   - *task-iam-role*。タスク IAM ロールの Amazon リソースネーム (ARN) に置き換えます。
   - *region*。タスクが実行されるリージョンに置き換えます。

```
{
  "family": "ecs-windows-fluent-bit",
  "taskRoleArn": "task-iam-role",
  "containerDefinitions": [
    {
      "name": "fluent-bit",
      "image": "public.ecr.aws/aws-observability/aws-for-fluent-
bit:windowsservercore-latest",
      "cpu": 512,
      "portMappings": [
        {
          "hostPort": 24224,
          "containerPort": 24224,
          "protocol": "tcp"
        }
      ],
      "entryPoint": [
        "Powershell",
        "-Command"
      ],
      "command": [
        "C:\\entrypoint.ps1 -ConfigFile C:\\ecs_windows_forward_daemon\
\cloudwatch.conf"
      ],
      "environment": [
        {
          "name": "AWS_REGION",
          "value": "region"
        }
      ],
      "memory": 512,
      "essential": true,
      "logConfiguration": {
```

```
        "logDriver": "awslogs",
        "options": {
          "awslogs-group": "/ecs/fluent-bit-logs",
          "awslogs-region": "region",
          "awslogs-stream-prefix": "flb",
          "awslogs-create-group": "true"
        }
      }
    }
  ],
  "memory": "512",
  "cpu": "512"
}
```

2. 次のコマンドを実行して、タスク定義を登録します。

```
aws ecs register-task-definition --cli-input-json file://fluent-bit.json --
region region
```

list-task-definitions コマンドを実行して、アカウントのタスク定義をリスト表示できます。出力には、run-task または start-task と一緒に使用できるファミリーとリビジョンの値が表示されます。

ステップ 5: デーモンスケジューリング戦略を使用して **ecs-windows-fluent-bit** タスク定義を Amazon ECS サービスとして実行する

アカウントのタスク定義を登録したら、クラスターでタスクを実行できます。このチュートリアルでは、FluentBit-cluster クラスターで ecs-windows-fluent-bit:1 タスク定義のインスタンスを 1 つ実行します。デーモンスケジューリング戦略を使用するサービスでタスクを実行することにより、Fluent Bit の単一インスタンスが常に各コンテナインスタンスで実行されます。

タスクを実行するには

1. 以下のコマンドを実行して、ecs-windows-fluent-bit:1 タスク定義 (前のステップで登録済み) をサービスとして起動します。

> **Note**
>
> このタスク定義は awslogs ロギングドライバーを使用するため、コンテナインスタンスには必要な権限が必要です。

以下の変数を置き換えます。

- *region*。サービスが実行されるリージョンに置き換えます。

```
aws ecs create-service \
    --cluster FluentBit-cluster \
    --service-name FluentBitForwardDaemonService \
    --task-definition ecs-windows-fluent-bit:1 \
    --launch-type EC2 \
    --scheduling-strategy DAEMON \
    --region region
```

2. 次のコマンドを実行して、タスクを一覧表示します。

以下の変数を置き換えます。

- *region*。サービスタスクが実行されるリージョンに置き換えます。

```
aws ecs list-tasks --cluster FluentBit-cluster --region region
```

ステップ 6: ログを生成する Windows タスク定義を登録する

ログを生成するタスク定義を登録します。このタスク定義では、1 秒ごとに増分数を stdout に書き込む Windows コンテナイメージをデプロイします。

タスク定義では、Fluent Bit プラグインがリッスンするポート 24224 に接続する fluentd ロギングドライバーを使用します。Amazon ECS エージェントは、クラスター名、タスク ARN、タスク定義ファミリー名、タスク定義リビジョン番号、タスクコンテナ名などを含むタグのある各 Amazon ECS コンテナにラベルを付けます。これらのキー値ラベルは Fluent Bit に渡されます。

> **Note**
>
> このタスクは、default ネットワークモードを使用します。ただし、タスクで awsvpc ネットワークモードを使用することもできます。

タスク定義を登録するには

1. 次の内容で、windows-app-task.json という名前のファイルを作成します。

```
{
  "family": "windows-app-task",
  "containerDefinitions": [
    {
      "name": "sample-container",
      "image": "mcr.microsoft.com/windows/servercore:ltsc2019",
      "cpu": 512,
      "memory": 512,
      "essential": true,
      "entryPoint": [
        "Powershell",
        "-Command"
      ],
      "command": [
        "$count=1;while(1) { Write-Host $count; sleep 1; $count=$count+1;}"
      ],
      "logConfiguration": {
        "logDriver": "fluentd",
        "options": {
          "fluentd-address": "localhost:24224",
          "tag": "{{ index .ContainerLabels \"com.amazonaws.ecs.task-definition-
family\" }}",
          "fluentd-async": "true",
          "labels": "com.amazonaws.ecs.cluster,com.amazonaws.ecs.container-
name,com.amazonaws.ecs.task-arn,com.amazonaws.ecs.task-definition-
family,com.amazonaws.ecs.task-definition-version"
        }
      }
    }
  ],
  "memory": "512",
  "cpu": "512"
```

```
}
```

2. 次のコマンドを実行して、タスク定義を登録します。

   以下の変数を置き換えます。

   - *region*。タスクが実行されるリージョンに置き換えます。

   ```
   aws ecs register-task-definition --cli-input-json file://windows-app-task.json --
   region region
   ```

   list-task-definitions コマンドを実行して、アカウントのタスク定義をリスト表示できます。出力には、run-task または start-task と一緒に使用できるファミリーとリビジョンの値が表示されます。

ステップ 7: windows-app-task タスク定義を実行する

windows-app-task タスク定義を登録したら、FluentBit-cluster クラスターで実行します。

タスクを実行するには

1. 前の手順で登録した windows-app-task:1 タスク定義を実行します。

   以下の変数を置き換えます。

   - *region*。タスクが実行されるリージョンに置き換えます。

   ```
   aws ecs run-task --cluster FluentBit-cluster --task-definition windows-app-task:1
    --count 2 --region region
   ```

2. 次のコマンドを実行して、タスクを一覧表示します。

   ```
   aws ecs list-tasks --cluster FluentBit-cluster
   ```

ステップ 8: CloudWatch でログを確認する

Fluent Bit の設定を確認するには、CloudWatch コンソールで次のロググループを確認します。

- /ecs/fluent-bit-logs - これは、コンテナインスタンスで実行されている Fluent Bit デーモンコンテナに対応するロググループです。
- /aws/ecs/FluentBit-cluster.windows-app-task - これは、FluentBit-cluster クラスター内の windows-app-task タスク定義ファミリーで起動されたすべてのタスクに対応するロググループです。

  task-out.*FIRST_TASK_ID*.sample-container - このログストリームには、sample-container タスクコンテナ内のタスクの最初のインスタンスによって生成されたすべてのログが含まれます。

  task-out.*SECOND_TASK_ID*.sample-container - このログストリームには、sample-container タスクコンテナ内のタスクの 2 番目のインスタンスによって生成されたすべてのログが含まれます。

task-out.*TASK_ID*.sample-container ログストリームには次のようなフィールドがあります。

```
{
    "source": "stdout",
    "ecs_task_arn": "arn:aws:ecs:region:0123456789012:task/FluentBit-
cluster/13EXAMPLE",
    "container_name": "/ecs-windows-app-task-1-sample-container-cEXAMPLE",
    "ecs_cluster": "FluentBit-cluster",
    "ecs_container_name": "sample-container",
    "ecs_task_definition_version": "1",
    "container_id": "61f5e6EXAMPLE",
    "log": "10",
    "ecs_task_definition_family": "windows-app-task"
}
```

Fluent Bit 設定を検証するには

1. CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。
2. ナビゲーションペインで、[Log groups] (ロググループ) を選択します。Fluent Bit をコンテナにデプロイしたリージョンにいることを確認してください。

   AWS リージョンのロググループのリストは、以下のように表示されます。

   - /ecs/fluent-bit-logs
   - /aws/ecs/FluentBit-cluster.windows-app-task

これらのロググループが表示される場合、Fluent Bit のセットアップは検証済みです。

ステップ 9: クリーンアップする。

このチュートリアルが終了したら、使用していないリソースに対する料金が発生しないように、チュートリアルに関連付けられたリソースをクリーンアップします。

チュートリアルリソースをクリーンアップするには

1. `windows-simple-task` タスクおよび `ecs-fluent-bit` タスクを停止します。詳細については、「the section called “タスクの停止”」を参照してください。
2. 次のコマンドを実行して、`/ecs/fluent-bit-logs` ロググループを削除します。ロググループの削除に関する詳細については、「AWS Command Line Interface リファレンス」の「delete-log-group」を参照してください。

```
aws logs delete-log-group --log-group-name /ecs/fluent-bit-logs
aws logs delete-log-group --log-group-name /aws/ecs/FluentBit-cluster.windows-app-task
```

3. 次のコマンドを実行して、インスタンスを停止します。

```
aws ec2 terminate-instances --instance-ids instance-id
```

4. 次のコマンドを実行して、IAM ロールを削除します。

```
aws iam delete-role --role-name ecsInstanceRole
aws iam delete-role --role-name fluentTaskRole
```

5. 次のコマンドを実行して、Amazon ECS クラスターを削除します。

```
aws ecs delete-cluster --cluster FluentBit-cluster
```

Amazon EC2 の Linux コンテナで gMSA を使用する

Amazon ECS は、グループ管理サービスアカウント (gMSA) と呼ばれる特殊なサービスアカウントを使用して、EC2 上の Linux コンテナの Active Directory 認証をサポートします。

Linux Core アプリケーションなどの .NET ベースのネットワークアプリケーションは、Active Directory を使用して、ユーザーとサービス間の認証と認可の管理を円滑化することができます。この機能は、Active Directory と統合され、ドメインに参加しているサーバー上で実行されるアプリケーションを設計することで利用できます。しかし、Linux コンテナはドメインに参加できないため、gMSA を使用して実行する Linux コンテナを設定する必要があります。

gMSA で実行される Linux コンテナは、コンテナのホスト Amazon EC2 インスタンスで実行される `credentials-fetcher` デーモンに依存します。つまり、デーモンは Active Directory ドメインコントローラーからも認証情報を取得し、これらの gMSA 認証情報をコンテナインスタンスに転送します。サービスアカウントの詳細については、Microsoft Learn Web サイトの「Windows コンテナ向け gMSAs の作成」を参照してください。

考慮事項

Linux コンテナ向け gMSA を使用する前に、次の点を考慮してください。

- コンテナが EC2 で実行されている場合は、Windows コンテナおよびLinux コンテナ向け gMSA を使用できます。Fargate で Linux コンテナに gMSA を使用する方法については、Fargate で Linux コンテナに gMSA を使用する を参照してください。
- 前提条件を完全に満たすには、ドメインに参加している Windows コンピュータが必要になる場合があります。例えば、PowerShell を使用して Active Directory で gMSA を作成するには、ドメインに参加している Windows コンピュータが必要になる場合があります。RSAT Active Director PowerShell ツールは Windows でのみ使用できます。詳細については、「Active Directory 管理ツールのインストール」を参照してください。
- ドメインレス gMSAか各インスタンスを単一のドメインに結合するを選択しました。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

  次に、CredSpec のデータ ストレージを選択し、必要に応じて、ドメインレス gMSA の Active Directory ユーザー認証情報を選択します。

  Amazon ECS は Active Directory の認証情報仕様ファイル (CredSpec) を使用します。このファイルは、gMSA アカウントコンテキストをコンテナに伝達するために使用される gMSA メタデータを含む認証情報仕様ファイルを使用します。CredSpec ファイルを生成し、コンテナインスタンスのオペレーティングシステムに応じて、次の表にある CredSpec ストレージオプションのいずれかに保存します。ドメインレス方式を使用するには、CredSpec ファイル内のオプションのセクショ

ンで、コンテナインスタンスのオペレーティングシステムに固有の、次の表の domainless user credentials ストレージオプションのいずれかの認証情報を指定できます。

ストレージの場所	リナックス	Windows
Amazon Simple Storage Service	CredSpec	CredSpec
AWS Secrets Manager	ドメインレスユーザー認証情報	ドメインレスユーザー認証情報
Amazon EC2 Systems Manager Parameter Store	CredSpec	CredSpec、ドメインレスユーザー認証情報
ローカルファイル	該当なし	CredSpec

前提条件

gMSA を使用する前に、Amazon ECS の Linux コンテナ機能のために必ず以下を完了してください。

- コンテナがアクセスするリソースを含む Active Directory ドメインを設定します。Amazon ECS は以下の設定をサポートしています。
  - AWS Directory Service Active Directory。AWS Directory Service は、Amazon EC2 でホストされる AWS マネージド Active Directory です。詳細については、「AWS Directory Service 管理ガイド」の「AWS Managed Microsoft AD の開始方法」を参照してください。
  - オンプレミスの Active Directory。Amazon ECS Linux コンテナインスタンスがドメインに参加できることを確認する必要があります。詳細については、「AWS Direct Connect」を参照してください。
- Active Directory に既存の gMSA アカウントがあります。詳細については、「Amazon EC2 の Linux コンテナで gMSA を使用する」を参照してください。
- Amazon ECS Linux コンテナインスタンスに `credentials-fetcher` デーモンをインストールして実行しています。また、Active Directory で認証するための初期資格情報セットを `credentials-fetcher` デーモンに追加しました。

> **Note**
>
> `credentials-fetcher` デーモンは、Amazon Linux 2023 および Fedora 37 以降でのみ使用できます。デーモン は Amazon Linux 2 では使用できません。詳細については、GitHub の「aws/credentials-fetcher」を参照してください。

- Active Directory で認証するための `credentials-fetcher` デーモンの認定情報を設定します。認証情報は、gMSA アカウントにアクセスできる Active Directory セキュリティグループのメンバーである必要があります。インスタンスをドメインに参加させるか、ドメインレス gMSA を使用するかを決定します。 には複数のオプションがあります。
- 必須の IAM アクセス権限を追加しました。必要な権限は、初期認証情報と認証情報の仕様の保存に選択した方法によって異なります。
  - 初期認証情報にドメインレス gMSA を使用する場合は、タスク実行ロールに AWS Secrets Manager の IAM アクセス許可が必要です。
  - 認証情報の仕様を SSM Parameter Store に保存する場合は、タスク実行ロールで Amazon EC2 Systems Manager Parameter Store に対する IAM 許可が必要です。
  - 認証情報の仕様を Amazon S3 で保存する場合は、タスク実行ロールで Amazon Simple Storage Service の IAM 許可が必要です。

Amazon ECS での gMSA 対応の Linux コンテナの設定

インフラストラクチャを準備する

次のステップは、考慮事項と 1 回実行される設定です。これらのステップを完了したら、コンテナインスタンスの作成を自動化して、この設定を再利用できます。

初期認証情報の提供方法を決定し、再利用可能な EC2 起動テンプレートで EC2 ユーザーデータを設定して、`credentials-fetcher` デーモンをインストールします。

1. インスタンスをドメインに参加させるか、ドメインレス gMSA を使用するかを決定します。
   - EC2 インスタンスを Active Directory ドメインに参加させる

- ユーザーデータを使用してインスタンスを参加させる

  Active Directory ドメインを EC2 起動テンプレートの EC2 ユーザーデータに参加させるステップを追加します。複数の Amazon EC2 Auto Scaling グループが同じ起動テンプレートを使用できます。

  Fedora ドキュメントの「Active Directory または FreeIPA ドメインへの参加」のこれらのステップを使用できます。

- ドメインレス gMSA 用に Active Directory ユーザーを作成する

`credentials-fetcher` デーモンには、ドメインレス gMSA と呼ばれる機能があります。この機能にはドメインが必要ですが、EC2 インスタンスをドメインに参加させる必要はありません。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。代わりに、CredSpec ファイルの AWS Secrets Manager にシークレットの名前を指定します。シークレットには、ユーザー名、パスワード、ログイン先のドメインが含まれている必要があります。

この機能はサポートされており、Linux および Windows コンテナで使用できます。

この機能は gMSA support for non-domain-joined container hosts 機能に似ています。Windows の機能の詳細については、Microsoft Learn ウェブサイトの「gMSA アーキテクチャと改善」を参照してください。

a. Active Directory ドメインでユーザーを作成します。Active Directory のユーザーは、タスクで使用する gMSA サービスアカウントにアクセスするための許可を持っている必要があります。

b. Active Directory でユーザーを作成した後、AWS Secrets Manager でシークレットを作成します。詳細については、「AWS Secrets Manager シークレットを作成する」を参照してください。

c. ユーザーのユーザー名、パスワード、ドメインを、それぞれ `username`、`password`、`domainName` と呼ばれる JSON キーと値のペアに入力します。

```
{"username":"username","password":"passw0rd", "domainName":"example.com"}
```

d. サービスアカウントの CredSpec ファイルに構成を追加します。追加の `HostAccountConfig` には、Secrets Manager のシークレットの Amazon リソースネーム (ARN) が含まれています。

Windows では、`PluginGUID` は次のスニペットの例の GUID と一致する必要があります。Linux では、`PluginGUID` は無視されます。`MySecret` の例を、シークレットの Amazon リソースネーム (ARN) に置き換えます。

```
    "ActiveDirectoryConfig": {
        "HostAccountConfig": {
            "PortableCcgVersion": "1",
            "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
            "PluginInput": {
                "CredentialArn": "arn:aws:secretsmanager:aws-
region:111122223333:secret:MySecret"
            }
        }
```

e. ドメインレス gMSA 機能には、タスク実行ロールの追加のアクセス許可が必要です。ステップ (オプション) ドメインレス gMSA シークレット に従います。

2. インスタンスを設定し、**credentials-fetcher** デーモンをインストールする

EC2 起動テンプレートでユーザーデータスクリプトを使用して `credentials-fetcher` デーモンをインストールできます。次の例は、2 種類のユーザーデータ (`cloud-config` YAML または bash スクリプト) を示しています。これらの例は、Amazon Linux 2023 (AL2023) についてのものです。`MyCluster` を、これらのインスタンスが参加する Amazon ECS クラスターの名前に置き換えます。

- **cloud-config** YAML

```
Content-Type: text/cloud-config
package_reboot_if_required: true
packages:
  # prerequisites
  - dotnet
  - realmd
  - oddjob
  - oddjob-mkhomedir
  - sssd
  - adcli
  - krb5-workstation
```

```
  - samba-common-tools
  # https://github.com/aws/credentials-fetcher gMSA credentials management for
 containers
  - credentials-fetcher
write_files:
# configure the ECS Agent to join your cluster.
# replace MyCluster with the name of your cluster.
- path: /etc/ecs/ecs.config
  owner: root:root
  permissions: '0644'
  content: |
    ECS_CLUSTER=MyCluster
    ECS_GMSA_SUPPORTED=true
runcmd:
# start the credentials-fetcher daemon and if it succeeded, make it start after
 every reboot
- "systemctl start credentials-fetcher"
- "systemctl is-active credentials-fetcher && systemctl enable credentials-
fetcher"
```

- bash スクリプト

  bash スクリプトに慣れていて、/etc/ecs/ecs.config に書き込む変数が複数ある場合は、次の heredoc 形式を使用します。この形式は cat で始まる行と EOF の間のすべてを設定ファイルに書き込みます。

```
#!/usr/bin/env bash
set -euxo pipefail

# prerequisites
timeout 30 dnf install -y dotnet realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation samba-common-tools
# install https://github.com/aws/credentials-fetcher gMSA credentials
 management for containers
timeout 30 dnf install -y credentials-fetcher

# start credentials-fetcher
systemctl start credentials-fetcher
systemctl is-active credentials-fetcher && systemctl enable credentials-fetcher

cat <<'EOF' >> /etc/ecs/ecs.config
ECS_CLUSTER=MyCluster
```

```
ECS_GMSA_SUPPORTED=true
EOF
```

/etc/ecs/ecs.config で設定できる credentials-fetcher デーモンのオプションの設定変数があります。YAML ブロック内のユーザーデータに変数を設定するか、heredoc前の例と同様に変数を設定することをお勧めします。これにより、1 つのファイルを複数回編集した場合に発生する、部分的な構成に関する問題を回避できます。ECS エージェントの設定の詳細については、GitHub の「Amazon ECS コンテナエージェント」を参照してください。

- オプションで、credentials-fetcher デーモン設定を変更してソケットを別の場所に移動する場合は、この変数 CREDENTIALS_FETCHER_HOST を使用できます。

許可とシークレットの設定

各アプリケーションおよび各タスク定義のために、次のステップを 1 回実行します。最小特権を認めるというベストプラクティスに従い、ポリシーで使用されるアクセス許可を絞り込むことをお勧めします。これにより、各タスクは必要なシークレットのみを読み取れます。

1. (オプション) ドメインレス gMSA シークレット

   インスタンスがドメインに参加していないドメインレス方式を使用する場合は、次のステップに従います。

   次の権限をインラインポリシーとしてタスク実行 IAM ロールに追加する必要があります。これにより、credentials-fetcher デーモンが Secrets Manager シークレットにアクセスできるようになります。MySecret の例を、Resource リスト内のシークレットの Amazon リソースネーム (ARN) に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": [
                "arn:aws:ssm:aws-region:111122223333:secret:MySecret"
            ]
        }
```

```
    ]
}
```

> **Note**
>
> 独自の KMS キーを使用してシークレットを暗号化する場合は、必要な許可をこのロールに追加し、このロールを AWS KMS キーポリシーに追加する必要があります。

2. SSM Parameter Store または S3 を使用して CredSpec を保存するかどうかを決定する

   Amazon ECS では、タスク定義の `credentialSpecs` フィールドでファイルパスを参照する次の方法がサポートされています。

   インスタンスを単一のドメインに参加させる場合は、文字列内の ARN の先頭にプレフィックス `credentialspec:` を使用します。ドメインレス gMSA を使用する場合は、次に `credentialspecdomainless:` を使用します。

   CredSpec の詳細については、「認証情報仕様ファイル」を参照してください。

   - Amazon S3 バケット

     認証情報の仕様を Amazon S3 バケットに追加します。次に、タスク定義の `credentialSpecs` フィールドで Amazon S3 バケットの Amazon リソースネーム (ARN) を参照します。

     ```
     {
         "family": "",
         "executionRoleArn": "",
         "containerDefinitions": [
             {
                 "name": "",
                 ...
                 "credentialSpecs": [
                     "credentialspecdomainless:arn:aws:s3:::${BucketName}/${ObjectName}"
                 ],
                 ...
             }
         ],
         ...
     }
     ```

タスクに S3 バケットへのアクセスを許可するには、次のアクセス許可をインラインポリシーとして Amazon ECS タスク実行 IAM ロールに追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/{object}"
            ]
        }
    ]
}
```

- SSM パラメータストアパラメータ

  SSM Parameter Store パラメータに認証情報仕様を追加します。タスク定義の `credentialSpecs` フィールドで SSM パラメータストアパラメータの Amazon リソースネーム (ARN) を参照します。

```
{
    "family": "",
    "executionRoleArn": "",
    "containerDefinitions": [
        {
            "name": "",
            ...
            "credentialSpecs": [
                "credentialspecdomainless:arn:aws:ssm:aws-
region:111122223333:parameter/parameter_name"
            ],
            ...
        }
    ],
    ...
```

```
}
```

タスクに SSM Parameter Store パラメータへのアクセスを許可するには、次のアクセス許可をインラインポリシーとして Amazon ECS タスク実行 IAM ロールに追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameters"
            ],
            "Resource": [
                "arn:aws:ssm:aws-region:111122223333:parameter/parameter_name"
            ]
        }
    ]
}
```

認証情報仕様ファイル

Amazon ECS は Active Directory の認証情報仕様ファイル (CredSpec) を使用します。このファイルには、gMSA アカウントコンテキストを Linux コンテナに伝達するために使用される gMSA メタデータが含まれています。CredSpec を生成し、タスク定義の `credentialSpecs` フィールドで参照します。CredSpec ファイルにはシークレットは含まれていません。

次は、CredSpec ファイルの例です。

```
{
    "CmsPlugins": [
        "ActiveDirectory"
    ],
    "DomainJoinConfig": {
        "Sid": "S-1-5-21-2554468230-2647958158-2204241789",
        "MachineAccountName": "WebApp01",
        "Guid": "8665abd4-e947-4dd0-9a51-f8254943c90b",
        "DnsTreeName": "example.com",
        "DnsName": "example.com",
        "NetBiosName": "example"
    },
```

```
    "ActiveDirectoryConfig": {
        "GroupManagedServiceAccounts": [
            {
                "Name": "WebApp01",
                "Scope": "example.com"
            }
        ],
        "HostAccountConfig": {
            "PortableCcgVersion": "1",
            "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
            "PluginInput": {
                "CredentialArn": "arn:aws:secretsmanager:aws-
region:111122223333:secret:MySecret"
            }
        }
    }
}
```

「CredSpec」の作成

CredSpec を作成するには、ドメインに参加している Windows コンピューター上の CredSpec PowerShell モジュールを使用します。Microsoft Learn Web サイトの「認証情報の仕様を作成する」のステップに従います。

Fargate で Linux コンテナに gMSA を使用する

Amazon ECS は、グループ管理サービスアカウント (gMSA) と呼ばれる特殊なサービスアカウントを使用して、Fargate 上の Linux コンテナの Active Directory 認証をサポートします。

Linux Core アプリケーションなどの .NET ベースのネットワークアプリケーションは、Active Directory を使用して、ユーザーとサービス間の認証と認可の管理を円滑化することができます。この機能は、Active Directory と統合され、ドメインに参加しているサーバー上で実行されるアプリケーションを設計することで利用できます。しかし、Linux コンテナはドメインに参加できないため、gMSA を使用して実行する Linux コンテナを設定する必要があります。

考慮事項

Fargate で Linux コンテナ向けに gMSA を使用する前に、次の点を考慮してください。

- プラットフォームバージョン 1.4 以降を実行している必要があります。

- 前提条件を完全に満たすには、ドメインに参加している Windows コンピュータが必要になる場合があります。例えば、PowerShell を使用して Active Directory で gMSA を作成するには、ドメインに参加している Windows コンピュータが必要になる場合があります。RSAT Active Director PowerShell ツールは Windows でのみ使用できます。詳細については、「Active Directory 管理ツールのインストール」を参照してください。
- ドメインレス gMSA を使用する必要があります。

  Amazon ECS は Active Directory の認証情報仕様ファイル (CredSpec) を使用します。このファイルは、gMSA アカウントコンテキストをコンテナに伝達するために使用される gMSA メタデータを含む認証情報仕様ファイルを使用します。CredSpec ファイルを生成し、Amazon S3 バケットに保存します。
- 1 つのタスクでサポートできるアクティブディレクトリは 1 つだけです。

前提条件

gMSA を使用する前に、Amazon ECS の Linux コンテナ機能のために必ず以下を完了してください。

- コンテナがアクセスするリソースを含む Active Directory ドメインを設定します。Amazon ECS は以下の設定をサポートしています。
  - AWS Directory Service Active Directory。AWS Directory Service は、Amazon EC2 でホストされる AWS マネージド Active Directory です。詳細については、「AWS Directory Service 管理ガイド」の「AWS Managed Microsoft AD の開始方法」を参照してください。
  - オンプレミスの Active Directory。Amazon ECS Linux コンテナインスタンスがドメインに参加できることを確認する必要があります。詳細については、「AWS Direct Connect」を参照してください。
- Active Directory に既存の gMSA アカウントがあり、その gMSA サービスアカウントにアクセスする権限を持つユーザーがいます。詳細については、「ドメインレス gMSA 用に Active Directory ユーザーを作成する」を参照してください。
- Amazon S3 バケットがある。詳細については、「Amazon S3 ユーザーガイド」の「バケットの作成」を参照してください。

Amazon ECS での gMSA 対応の Linux コンテナの設定

インフラストラクチャを準備する

次のステップは、考慮事項と 1 回実行される設定です。

- ドメインレス gMSA 用に Active Directory ユーザーを作成する

  ドメインレス gMSAを使用する場合、コンテナはドメインに接続されません。コンテナ上で実行される他のアプリケーションは、Active Directory の認証情報を使用してドメインにアクセスすることはできません。別のドメインを使用するタスクも同じコンテナ上で実行できます。CredSpec ファイルの AWS Secrets Manager にシークレットの名前を指定します。シークレットには、ユーザー名、パスワード、ログイン先のドメインが含まれている必要があります。

  この機能は gMSA support for non-domain-joined container hosts 機能に似ています。Windows の機能の詳細については、Microsoft Learn ウェブサイトの「gMSA アーキテクチャと改善」を参照してください。

  a. Active Directory ドメインでユーザーを設定します。Active Directory のユーザーは、タスクで使用する gMSA サービスアカウントにアクセスするための許可を持っている必要があります。

  b. Active Directory ドメイン名を解決できる VPC とサブネットがあります。DHCP オプションを使用して、Active Directory サービス名を指すドメイン名で VPC を設定します。VPC 向け DHCP オプション設定の詳細については、「Amazon Virtual Private Cloud ユーザーガイド」の「DHCP オプションセットの使用」を参照してください。

  c. AWS Secrets Manager にシークレットを作成します。

  d. 認証情報仕様ファイルを作成します。

許可とシークレットの設定

各アプリケーションおよび各タスク定義ごとに、次のステップを 1 回ずつ実行します。最小特権を認めるというベストプラクティスに従い、ポリシーで使用されるアクセス許可を絞り込むことをお勧めします。これにより、各タスクは必要なシークレットのみを読み取れます。

1. Active Directory ドメインでユーザーを作成します。Active Directory のユーザーは、タスクで使用する gMSA サービスアカウントにアクセスするための許可を持っている必要があります。
2. Active Directory ユーザーを作成した後、AWS Secrets Manager でシークレットを作成します。詳細については、「AWS Secrets Manager シークレットを作成する」を参照してください。
3. ユーザーのユーザー名、パスワード、ドメインを、それぞれ `username`、`password`、`domainName` と呼ばれる JSON キーと値のペアに入力します。

```
{"username":"username","password":"passw0rd", "domainName":"example.com"}
```

4. 次の権限をインラインポリシーとしてタスク実行 IAM ロールに追加する必要があります。これにより、credentials-fetcher デーモンが Secrets Manager シークレットにアクセスできるようになります。MySecret の例を、Resource リスト内のシークレットの Amazon リソースネーム (ARN) に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": [
        "arn:aws:secretsmanager:aws-region:111122223333:secret:MySecret"
      ]
    }
  ]
}
```

> **Note**
>
> 独自の KMS キーを使用してシークレットを暗号化する場合は、必要な許可をこのロールに追加し、このロールを AWS KMS キーポリシーに追加する必要があります。

5. 認証情報の仕様を Amazon S3 バケットに追加します。次に、タスク定義の credentialSpecs フィールドで Amazon S3 バケットの Amazon リソースネーム (ARN) を参照します。

```
{
    "family": "",
    "executionRoleArn": "",
    "containerDefinitions": [
        {
            "name": "",
            ...
            "credentialSpecs": [
                "credentialspecdomainless:arn:aws:s3:::${BucketName}/${ObjectName}"
```

```
            ],
            ...
        }
    ],
    ...
}
```

タスクに S3 バケットへのアクセスを許可するには、次のアクセス許可をインラインポリシーとして Amazon ECS タスク実行 IAM ロールに追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListObject"
            ],
            "Resource": [
                "arn:aws:s3:::{bucket_name}",
                "arn:aws:s3:::{bucket_name}/{object}"
            ]
        }
    ]
}
```

認証情報仕様ファイル

Amazon ECS は Active Directory の認証情報仕様ファイル (CredSpec) を使用します。このファイルには、gMSA アカウントコンテキストを Linux コンテナに伝達するために使用される gMSA メタデータが含まれています。CredSpec を生成し、タスク定義の `credentialSpecs` フィールドで参照します。CredSpec ファイルにはシークレットは含まれていません。

次は、CredSpec ファイルの例です。

```
{
    "CmsPlugins": [
        "ActiveDirectory"
    ],
```

```
    "DomainJoinConfig": {
        "Sid": "S-1-5-21-2554468230-2647958158-2204241789",
        "MachineAccountName": "WebApp01",
        "Guid": "8665abd4-e947-4dd0-9a51-f8254943c90b",
        "DnsTreeName": "example.com",
        "DnsName": "example.com",
        "NetBiosName": "example"
    },
    "ActiveDirectoryConfig": {
        "GroupManagedServiceAccounts": [
            {
                "Name": "WebApp01",
                "Scope": "example.com"
            }
        ],
        "HostAccountConfig": {
            "PortableCcgVersion": "1",
            "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
            "PluginInput": {
                "CredentialArn": "arn:aws:secretsmanager:aws-
region:111122223333:secret:MySecret"
            }
        }
    }
}
```

CredSpec を作成して Amazon S3 にアップロードする

CredSpec を作成するには、ドメインに参加している Windows コンピューター上の CredSpec PowerShell モジュールを使用します。Microsoft Learn Web サイトの「認証情報の仕様を作成する」のステップに従います。

認証情報仕様ファイルを作成したら、Amazon S3 バケットにアップロードします。AWS CLI コマンドを実行しているコンピューターまたは環境に CredSpec ファイルをコピーします。

次の AWS CLI コマンドを実行し、Amazon S3 に CredSpec をアップロードします。*amzn-s3-demo-bucket* をお使いの Amazon S3 バケットの名前に置き換えます。ファイルは任意のバケットと場所にオブジェクトとして保存できますが、タスク実行ロールにアタッチするポリシーでそのバケットと場所へのアクセスを許可する必要があります。

PowerShell については、次のコマンドを実行します。

```
$ Write-S3Object -BucketName "amzn-s3-demo-bucket" -Key "ecs-domainless-gmsa-credspec"
 -File "gmsa-cred-spec.json"
```

次の AWS CLI コマンドでは、sh および互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。

```
$ aws s3 cp gmsa-cred-spec.json \
s3://amzn-s3-demo-bucket/ecs-domainless-gmsa-credspec
```

AWS CLI を使用するドメインレス gMSA で Amazon ECS Windows コンテナを使用する

次のチュートリアルでは、AWS CLI を使用して Active Directory にアクセスするための認証情報を持つ Windows コンテナを実行する Amazon ECS タスクを作成する方法を示します。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

トピック

- ステップ 13: コンテナに gMSA 認証情報があることを検証する
- ステップ 14: クリーンアップする
- Windows コンテナ用 Amazon ECS ドメインレス gMSA のデバッグ

前提条件

このチュートリアルでは、以下の前提条件が完了済みであることを前提としています。

- 「Amazon ECS を使用するようにセットアップする」のステップを完了していること。
- AWS ユーザーに AmazonECS_FullAccess IAMポリシー例で指定されている必要なアクセス権限があること。
- AWS CLI の最新バージョンがインストールされ、設定されていること。AWS CLI のインストールまたはアップグレードの詳細については、「AWS Command Line Interface のインストール」を参照してください。
- コンテナがアクセスするリソースを含む Active Directory ドメインを設定します。Amazon ECS は以下の設定をサポートしています。
  - AWS Directory Service Active Directory。AWS Directory Service は、Amazon EC2 でホストされる AWS マネージド Active Directory です。詳細については、「AWS Directory Service 管理ガイド」の「AWS Managed Microsoft AD の開始方法」を参照してください。
  - オンプレミスの Active Directory。Amazon ECS Linux コンテナインスタンスがドメインに参加できることを確認する必要があります。詳細については、「AWS Direct Connect」を参照してください。
- Active Directory ドメイン名を解決できる VPC とサブネットがあります。
- ドメインレス gMSAか各インスタンスを単一のドメインに結合するを選択しました。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

  次に、CredSpec のデータ ストレージを選択し、必要に応じて、ドメインレス gMSA の Active Directory ユーザー認証情報を選択します。

  Amazon ECS は Active Directory の認証情報仕様ファイル (CredSpec) を使用します。このファイルは、gMSA アカウントコンテキストをコンテナに伝達するために使用される gMSA メタデータを含む認証情報仕様ファイルを使用します。CredSpec ファイルを生成し、コンテナインスタンスのオペレーティングシステムに応じて、次の表にある CredSpec ストレージオプションのいずれか

に保存します。ドメインレス方式を使用するには、CredSpec ファイル内のオプションのセクションで、コンテナインスタンスのオペレーティングシステムに固有の、次の表の domainless user credentials ストレージオプションのいずれかの認証情報を指定できます。

ストレージの場所	リナックス	Windows
Amazon Simple Storage Service	CredSpec	CredSpec
AWS Secrets Manager	ドメインレスユーザー認証情報	ドメインレスユーザー認証情報
Amazon EC2 Systems Manager Parameter Store	CredSpec	CredSpec、ドメインレスユーザー認証情報
ローカルファイル	該当なし	CredSpec

- (任意) AWS CloudShell は、お客様が独自の EC2 インスタンスを作成する必要なく、コマンドラインを提供するツールです。詳細については、『AWS CloudShell ユーザーガイド』の「What is AWS CloudShell? (とは ?)」 を参照してください。

ステップ 1: Active Directory ドメイン サービス (AD DS) で gMSA アカウントを作成して設定する

Active Directory ドメインの gMSA アカウントを作成して設定します。

1. Key Distribution Service のルートキーを生成する

> **Note**
>
> AWS Directory Service を使用している場合は、このステップを省略できます。

KDS ルートキーと gMSA アクセス許可は、AWS マネージド Microsoft AD で構成されます。

ドメインに 1 つの gMSA Service Account をまだ作成していない場合は、まず Key Distribution Service (KDS) ルートキーを生成する必要があります。KDS は、gMSA パスワードの作成、ロー

テーション、承認されたホストへのパスワードのリリースを担います。ccg.exe が gMSA 認証情報を取得する必要がある場合は、KDS に連絡して現在のパスワードを取得します。

KDS ルート キーが既に作成されているかどうかを確認するには、ActiveDirectory PowerShell モジュールを使用して、ドメインコントローラー上でドメイン管理者権限で次の PowerShell コマンドレットを実行します。モジュールの詳細については、Microsoft Learn Web サイトの「ActiveDirectory モジュール」を参照してください。

```
PS C:\> Get-KdsRootKey
```

コマンドがキー ID を返す場合は、このステップの残りをスキップできます。それ以外の場合は、次のコマンドを実行して KDS ルートキーを作成します。

```
PS C:\> Add-KdsRootKey -EffectiveImmediately
```

コマンドへの引数 EffectiveImmediately は、キーがすぐに有効になることを暗示していますが、KDS ルートキーが複製され、すべてのドメインコントローラーで使用できるようになるまで 10 時間待つ必要があります。

2. gMSA アカウントを作成するには

gMSA アカウントを作成して ccg.exe が gMSA パスワードを取得できるようにするには、ドメインにアクセスできる Windows サーバーまたはクライアントから次の PowerShell コマンドを実行します。ExampleAccount を gMSA アカウントに使用する名前に置き換えます。

a.
```
PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
```

b.
```
PS C:\> New-ADGroup -Name "ExampleAccount Authorized Hosts" -SamAccountName
 "ExampleAccountHosts" -GroupScope DomainLocal
```

c.
```
PS C:\> New-ADServiceAccount -Name "ExampleAccount" -DnsHostName
 "contoso" -ServicePrincipalNames "host/ExampleAccount", "host/contoso" -
PrincipalsAllowedToRetrieveManagedPassword "ExampleAccountHosts"
```

d. 有効期限のない永続的なパスワードでユーザーを作成します。これらの認証情報は AWS Secrets Manager に保存され、各タスクがドメインに参加するために使用されます。

```
PS C:\> New-ADUser -Name "ExampleAccount" -AccountPassword (ConvertTo-
SecureString -AsPlainText "Test123" -Force) -Enabled 1 -PasswordNeverExpires 1
```

e.
```
PS C:\> Add-ADGroupMember -Identity "ExampleAccountHosts" -Members
 "ExampleAccount"
```

f. Active Directory に CredSpec オブジェクトを作成するための PowerShell モジュールをインストールし、CredSpec JSON を出力します。

```
PS C:\> Install-PackageProvider -Name NuGet -Force
```

```
PS C:\> Install-Module CredentialSpec
```

g.
```
PS C:\> New-CredentialSpec -AccountName ExampleAccount
```

3. 前のコマンドの JSON 出力を、`gmsa-cred-spec.json` と呼ばれるファイルにコピーします。これは、CredSpec ファイルです。ステップ 3 の ステップ 3: CredSpec JSON を変更してドメインレス gMSA 情報を含める で使用されます。

ステップ 2: Secrets Manager に認証情報をアップロードする

Active Directory 認証情報を安全な認証情報ストレージシステムにコピーして、各タスクがそれを取得できるようにします。これはドメインレス gMSA メソッドです。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

- AWS CLI コマンドを実行し、ユーザー名、パスワード、ドメイン名を環境に合わせて置き換えます。シークレットの ARN を保管して次のステップ ステップ 3: CredSpec JSON を変更してドメインレス gMSA 情報を含める で使用します。

  次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

```
$ aws secretsmanager create-secret \
--name gmsa-plugin-input \
--description "Amazon ECS - gMSA Portable Identity." \
```

```
--secret-string "{\"username\":\"ExampleAccount\",\"password\":\"Test123\",
\"domainName\":\"contoso.com\"}"
```

ステップ 3: CredSpec JSON を変更してドメインレス gMSA 情報を含める

CredSpec をいずれかのストレージオプションにアップロードする前に、前の手順で Secrets Manager のシークレットの ARN を含む情報を CredSpec に追加します。詳細については、Microsoft Learn Web サイトの「ドメイン結合されていないコンテナホストのユースケース向けの追加の認証情報仕様設定」を参照してください。

1. `ActiveDirectoryConfig` 内部の CredSpec ファイルに以下の情報を追加します。ARN を、前の手順の Secrets Manager のシークレットに置き換えます。

   `PluginGUID` 値は次のサンプルのスニペットの GUID と一致する必要があり、必須であることに注意してください。

   ```
   "HostAccountConfig": {
         "PortableCcgVersion": "1",
         "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
         "PluginInput": "{\"credentialArn\": \"arn:aws:secretsmanager:aws-
   region:111122223333:secret:gmsa-plugin-input\"}"
       }
   ```

   また、この形式 `\"arn:aws:ssm:aws-region:111122223333:parameter/gmsa-plugin-input\"` の ARN を使用して SSM Parameter Store でシークレットを使用できます。

2. CredSpec ファイルを修正すると、次の例のようになります。

   ```
   {
     "CmsPlugins": [
       "ActiveDirectory"
     ],
     "DomainJoinConfig": {
       "Sid": "S-1-5-21-4066351383-705263209-1606769140",
       "MachineAccountName": "ExampleAccount",
       "Guid": "ac822f13-583e-49f7-aa7b-284f9a8c97b6",
       "DnsTreeName": "contoso",
       "DnsName": "contoso",
       "NetBiosName": "contoso"
     },
     "ActiveDirectoryConfig": {
   ```

```
    "GroupManagedServiceAccounts": [
      {
        "Name": "ExampleAccount",
        "Scope": "contoso"
      },
      {
        "Name": "ExampleAccount",
        "Scope": "contoso"
      }
    ],
    "HostAccountConfig": {
      "PortableCcgVersion": "1",
      "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
      "PluginInput": "{\"credentialArn\": \"arn:aws:secretsmanager:aws-
region:111122223333:secret:gmsa-plugin-input\"}"
    }
  }
}
```

ステップ 4： Amazon S3 に CredSpec をアップロードする

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

1. AWS CLI コマンドを実行しているコンピューターまたは環境に CredSpec ファイルをコピーします。
2. 次の AWS CLI コマンドを実行し、Amazon S3 に CredSpec をアップロードします。MyBucket をお使いの Amazon S3 バケットの名前に置き換えます。ファイルは任意のバケットと場所にオブジェクトとして保存できますが、タスク実行ロールにアタッチするポリシーでそのバケットと場所へのアクセスを許可する必要があります。

   次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

   ```
   $ aws s3 cp gmsa-cred-spec.json \
   s3://MyBucket/ecs-domainless-gmsa-credspec
   ```

ステップ 5: (オプション) Amazon ECS クラスターを作成する

デフォルトでは、アカウントには `default` という名前の Amazon ECS クラスターがあります。このクラスターは、AWS CLI、SDK、AWS CloudFormation でデフォルトで使用されます。追加のクラスターを使用してタスクとインフラストラクチャをグループ化および整理し、一部の構成にデフォルトを割り当てることができます。

クラスターは、AWS Management Console、AWS CLI、SDK、または AWS CloudFormation のいずれかを使用して作成できます。クラスター内の設定と構成は gMSA に影響しません。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである `bash` で実行できます。

```
$ aws ecs create-cluster --cluster-name windows-domainless-gmsa-cluster
```

> **Important**
>
> 独自のクラスターを作成することを選択する場合は、そのクラスターで使用する予定のコマンドごとに `--cluster clusterName` を指定する必要があります。

ステップ 6: コンテナインスタンスの IAM ロールを作成する

コンテナインスタンスは、Amazon EC2 インスタンスなどの ECS タスクでコンテナを実行するホストコンピュータです。各コンテナインスタンスは Amazon ECS クラスターに登録されます。Amazon EC2 インスタンスを起動してクラスターに登録する前に、使用するコンテナインスタンス用の IAM ロールを作成する必要があります。

コンテナインスタンスロールを作成するには、「Amazon ECS コンテナインスタンスの IAM ロール」を参照してください。デフォルトの`ecsInstanceRole` は、このチュートリアルを完了するための十分なアクセス許可を持っています。

ステップ 7: カスタムのタスク実行ロールを作成する

Amazon ECS では、各タスクの開始に必要なアクセス権限として、コンテナインスタンスロールの代わりに別の IAM ロールを使用できます。このロールは実行ロールです。ECS がタスクを実行するために必要なアクセス許可 (最小特権アクセス許可とも呼ばれる) のみを持つタスク実行ロールを作

成することをお勧めします。最小特権の原則の詳細については、AWS Well-Architected Flamework の「SEC03-BP02 最小特権アクセスの付与」を参照してください。

1. タスク実行ロールを作成するには、「タスク実行 ロールの作成」を参照してください。デフォルトの権限では、コンテナインスタンスは Amazon Elastic Container Registry、`stdout` および `stderr` からコンテナイメージを取得でき、アプリケーションから Amazon CloudWatch Logs に記録されます。

   このチュートリアルではロールにカスタム権限が必要なため、ロールには `ecsTaskExecutionRole` とは異なる名前を付けられます。このチュートリアルでは、以降の手順で `ecsTaskExecutionRole` を使用します。
2. このロールにのみ存在するインラインポリシー、または再利用可能なポリシーのいずれかのカスタムポリシーを作成して、次の権限を追加します。最初のステートメントの `Resource` の ARN を Amazon S3 バケットと場所に置き換え、2 番目の `Resource` を Secrets Manager のシークレットの ARN に置き換えます。

   Secrets Manager でカスタムキーを使用してシークレットを暗号化する場合は、そのキーの `kms:Decrypt` も許可する必要があります。

   Secrets Manager の代わりに SSM Parameter Store を使用する場合は、`secretsmanager:GetSecretValue` の代わりにパラメータの `ssm:GetParameter` を許可する必要があります。

```
{
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::MyBucket/ecs-domainless-gmsa-credspec/gmsa-cred-spec.json"
    },
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:aws-region:111122223333:secret:gmsa-plugin-input"
```

```
    }
  ]
}
```

ステップ 8: Amazon ECS Exec のタスクロールを作成する

このチュートリアルでは、Amazon ECS Exec を使用して、実行中のタスク内でコマンドを実行して機能を検証します。ECS Exec を使用するには、サービスまたはタスクが ECS Exec を有効にし、タスク ロール (タスク実行ロールではない) に ssmmessages アクセス許可が必要です。必要な IAM ポリシーについては、「ECS Exec のアクセス許可」を参照してください。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

AWS CLI を使用してタスクロールを作成するには、次の手順に従ってください。

1. ecs-tasks-trust-policy.json というファイルを次の内容で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ecs-tasks.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. IAM ロールを作成します。名前 ecs-exec-demo-task-role は置き替えられますが、次の手順のために名前を保持しておいてください。

   次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

```
$ aws iam create-role --role-name ecs-exec-demo-task-role \
--assume-role-policy-document file://ecs-tasks-trust-policy.json
```

ecs-tasks-trust-policy.json ファイルを削除できます。

3. ecs-exec-demo-task-role-policy.json というファイルを次の内容で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
                "ssmmessages:OpenDataChannel"
            ],
            "Resource": "*"
        }
    ]
}
```

4. IAM ポリシーを作成し、前述のロールにアタッチします。

次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

```
$ aws iam put-role-policy \
    --role-name ecs-exec-demo-task-role \
    --policy-name ecs-exec-demo-task-role-policy \
    --policy-document file://ecs-exec-demo-task-role-policy.json
```

ecs-exec-demo-task-role-policy.json ファイルを削除できます。

ステップ 9: ドメインレス gMSA を使用するタスク定義を登録する

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

1. windows-gmsa-domainless-task-def.json というファイルを次の内容で作成します。

```
{
  "family": "windows-gmsa-domainless-task",
  "containerDefinitions": [
    {
      "name": "windows_sample_app",
      "image": "mcr.microsoft.com/windows/servercore/iis",
      "cpu": 1024,
      "memory": 1024,
      "essential": true,
      "credentialSpecs": [
                "credentialspecdomainless:arn:aws:s3:::ecs-domainless-gmsa-
credspec/gmsa-cred-spec.json"
      ],
      "entryPoint": [
        "powershell",
        "-Command"
      ],
      "command": [
        "New-Item -Path C:\\inetpub\\wwwroot\\index.html -ItemType file -Value
 '<html> <head> <title>Amazon ECS Sample App</title> <style>body {margin-top:
 40px; background-color: #333;} </style> </head><body> <div style=color:white;text-
align:center> <h1>Amazon ECS Sample App</h1> <h2>Congratulations!</h2> <p>Your
 application is now running on a container in Amazon ECS.</p>' -Force ; C:\
\ServiceMonitor.exe w3svc"
      ],
      "portMappings": [
        {
          "protocol": "tcp",
          "containerPort": 80,
          "hostPort": 8080
        }
      ]
    }
  ],
  "taskRoleArn": "arn:aws:iam::111122223333:role/ecs-exec-demo-task-role",
  "executionRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole"
}
```

2. 次のコマンドを実行して、タスク定義を登録します。

次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

```
$ aws ecs register-task-definition \
--cli-input-json file://windows-gmsa-domainless-task-def.json
```

ステップ 10: Windows コンテナインスタンスをクラスターに登録する

Amazon EC2 Windows インスタンスを起動し、ECS コンテナエージェントを実行して、それをコンテナインスタンスとしてクラスターに登録します。ECS は、タスクが開始されたクラスターに登録されているコンテナインスタンスでタスクを実行します。

1. AWS Management Console で Amazon ECS 用に設定された Amazon EC2 Windows インスタンスを起動するには、「Amazon ECS Windows コンテナインスタンスの起動」を参照してください。ユーザーデータのステップで停止します。
2. gMSA には、ECS コンテナエージェントを開始する前に、ユーザーデータで環境変数 ECS_GMSA_SUPPORTED を設定する必要があります。

   ECS Exec の場合、エージェントは引数 -EnableTaskIAMRole で始まる必要があります。

   タスクが EC2 IMDS Web サービスに到達してロール認証情報を取得できないようにしてインスタンス IAM ロールを保護するには、引数 -AwsvpcBlockIMDS を追加します。これは、awsvpc ネットワークモードを使用するタスクにのみ適用されます。

   ```
   <powershell>
   [Environment]::SetEnvironmentVariable("ECS_GMSA_SUPPORTED", $TRUE, "Machine")
   Import-Module ECSTools
   Initialize-ECSAgent -Cluster windows-domainless-gmsa-cluster -EnableTaskIAMRole -
   AwsvpcBlockIMDS
   </powershell>
   ```

3. Summary (概要) パネルでインスタンス設定の要約を確認します。準備が完了したら、[Launch instance] (インスタンスを起動) を選択してください。

ステップ 11: コンテナインスタンスを検証する

AWS Management Console を使用して、クラスター内にコンテナインスタンスがあることを確認できます。ただし、gMSA は属性として示される追加の機能が必要です。これらの属性は AWS Management Console では表示されないため、このチュートリアルでは AWS CLI を使用します。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

1. クラスター内のコンテナインスタンスをリストします。コンテナインスタンスの ID は EC2 インスタンスの ID とは異なります。

   ```
   $ aws ecs list-container-instances
   ```

   出力:

   ```
   {
       "containerInstanceArns": [
           "arn:aws:ecs:aws-region:111122223333:container-
   instance/default/MyContainerInstanceID"
       ]
   }
   ```

   例えば、526bd5d0ced448a788768334e79010fd は有効なコンテナインスタンス ID です。
2. 前のステップのコンテナインスタンス ID を使用して、コンテナインスタンスの詳細を取得します。MyContainerInstanceID を ID に置き換えます。

   次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

   ```
   $ aws ecs describe-container-instances \
        ----container-instances MyContainerInstanceID
   ```

   出力が非常に長いことに注意してください。
3. attributes リストに、name というキーと値 ecs.capability.gmsa-domainless を持つオブジェクトがあることを確認します。以下は、オブジェクトの例です。

   出力:

```
{
    "name": "ecs.capability.gmsa-domainless"
}
```

ステップ 12: Windows タスクを実行する

Amazon ECS タスクを実行します。クラスターにコンテナインスタンスが 1 つしかない場合は、run-task を使用できます。さまざまなコンテナインスタンスが多数ある場合は、タスク定義に配置制約を追加して、このタスクを実行するコンテナインスタンスの種類を制御するよりも、タスクを実行するには start-task を使用してコンテナインスタンス ID を指定する方が簡単な場合があります。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

1. 次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

   ```
   aws ecs run-task --task-definition windows-gmsa-domainless-task \
       --enable-execute-command --cluster windows-domainless-gmsa-cluster
   ```

   コマンドによって返されるタスク ID をメモします。
2. 次のコマンドを実行して、タスクが開始されたことを確認します。このコマンドは、タスクが開始されるまで待機し、シェルプロンプトを返しません。MyTaskID を前のステップのタスク ID に置き換えます。

   ```
   $ aws ecs wait tasks-running --task MyTaskID
   ```

ステップ 13: コンテナに gMSA 認証情報があることを検証する

タスク内のコンテナに Kerberos トークン gMSA があることを確認します。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

1.
次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

```
$ aws ecs execute-command \
--task MyTaskID \
--container windows_sample_app \
--interactive \
--command powershell.exe
```

出力は PowerShell プロンプトになります。

2. コンテナ内の PowerShell ターミナルで次のコマンドを実行します。

```
PS C:\> klist get ExampleAccount$
```

出力では、Principal は以前に作成したものであることに注意してください。

ステップ 14: クリーンアップする

このチュートリアルが終了したら、未使用のリソースに対する料金が発生しないように、それに関連付けられたリソースをクリーンアップする必要があります。

このステップでは、AWS CLI を使用します。AWS CloudShell のこれらのコマンドは、デフォルトのシェルである bash で実行できます。

1. タスクを停止します。MyTaskID をステップ 12 のタスク ID ステップ 12: Windows タスクを実行する に置き換えます。

```
$ aws ecs stop-task --task MyTaskID
```

2. Amazon EC2 インスタンスを停止します。その後、クラスター内のコンテナインスタンスは 1 時間後に自動で削除されます。

Amazon EC2 コンソールを使用し、インスタンスを検索して終了できます。または、以下のコマンドを実行できます。コマンドを実行するには、ステップ 1、ステップ 11: コンテナインスタンスを検証する の aws ecs describe-container-instances コマンドの出力で EC2 インスタンス ID を見つけます。i-10a64379 は EC2 インスタンス ID の例です。

```
$ aws ec2 terminate-instances --instance-ids MyInstanceID
```

3. Amazon S3 の CredSpec ファイルを削除します。MyBucket をお使いの Amazon S3 バケットの名前に置き換えます。

```
$ aws s3api delete-object --bucket MyBucket --key ecs-domainless-gmsa-credspec/
gmsa-cred-spec.json
```

4. シークレットを Secrets Manager から削除するには 代わりに SSM Parameter Store を使用した場合は、パラメータを削除してください。

   次のコマンドでは、sh と互換性のあるシェルで使用されるバックスラッシュ継続文字を使用します。このコマンドは PowerShell と互換性がありません。PowerShell で使用するには、コマンドを変更する必要があります。

```
$ aws secretsmanager delete-secret --secret-id gmsa-plugin-input \
    --force-delete-without-recovery
```

5. タスク定義を登録解除して削除します。タスク定義を登録解除すると、そのタスク定義を非アクティブとしてマークするため、新しいタスクを開始するのに使用できなくなります。その後、タスク定義を削除できます。

   a. バージョンを指定してタスク定義の登録を解除します。ECS は、1 から始まる番号の付いたタスク定義のバージョンを自動的に作成します。:1 などのコンテナイメージのラベルと同じ形式のバージョンを参照します。

```
$ aws ecs deregister-task-definition --task-definition windows-gmsa-domainless-
task:1
```

   b. タスク定義を削除します。

```
$ aws ecs delete-task-definitions --task-definition windows-gmsa-domainless-
task:1
```

6. (オプション) クラスターを作成した場合は、ECS クラスターを削除します。

```
$ aws ecs delete-cluster --cluster windows-domainless-gmsa-cluster
```

Windows コンテナ用 Amazon ECS ドメインレス gMSA のデバッグ

Amazon ECS タスクの状態

ECS はタスクを 1 回のみ開始しようとします。問題のあるタスクはすべて停止され、STOPPED 状態に設定されます。タスクに関する一般的な問題には 2 つのタイプがあります。最初に、開始できなかったタスクです。2 つ目は、アプリケーションがいずれかのコンテナ内で停止したタスクです。AWS Management Console で、タスクが停止された理由については、タスクの [停止理由] フィールドを確認してください。AWS CLI に、タスクを説明して stoppedReason を見ます。AWS Management Console および AWS CLI での手順については、「Amazon ECS の停止したタスクのエラーを表示する」を参照してください。

Windows イベント

コンテナ内の gMSA 用 Windows イベントは Microsoft-Windows-Containers-CCG ログファイルに記録され、Logs\Microsoft\Windows\Containers-CCG\Admin にある「アプリケーションとサービス」セクションのイベント ビューアに表示されます。デバッグのヒントの詳細については、Microsoft Learn Web サイトの「Windows コンテナの gMSA のトラブルシューティング」を参照してください。

ECS エージェント gMSA プラグイン

Windows コンテナインスタンス上の ECS エージェントの gMSA プラグインのログは、次のディレクトリ C:/ProgramData/Amazon/gmsa-plugin/ にあります。このログを調べて、ドメインレスユーザーの認証情報がSecrets Manager などのストレージ場所からダウンロードされたかどうか、および認証情報の形式が正しく読み取られたかどうかを確認してください。

Amazon ECS の EC2 Windows コンテナで gMSA を使用する方法について説明します。

Amazon ECS は、グループマネージドサービスアカウント (gMSA) と呼ばれる特殊なサービスアカウントを使用して、Windows コンテナの Active Directory 認証をサポートします。

.NET アプリケーションなどの Windows ベースのネットワークアプリケーションは、多くの場合、Active Directory を使用して、ユーザーとサービス間の認証と認可の管理を容易にします。開発者は、通常、Active Directory と統合し、この目的のためにドメインに参加しているサーバーで実行するようにアプリケーションを設計します。Windows コンテナはドメインに結合できないため、gMSA で実行するように Windows コンテナを設定する必要があります。

gMSA で実行されている Windows コンテナは、ホスト Amazon EC2 インスタンスに依存して、Active Directory ドメインコントローラから gMSA 資格情報を取得し、コンテナインスタンスに提供します。詳細については、「Windows コンテナでの gMSA の使用」を参照してください。

> **Note**
>
> この機能は、Fargate の Windows コンテナではサポートされていません。

トピック

考慮事項

Windows コンテナに gMSAs を使用する場合は、次の点を考慮する必要があります。

- コンテナインスタンスに Amazon ECSに最適化されたWindows Server 2016 Full AMI を使用する場合、コンテナのホスト名は、認証情報仕様ファイルで定義されている gMSA アカウント名と同じである必要があります。コンテナのホスト名を指定するには、`hostname` コンテナ定義パラメータを使用します。詳細については、「ネットワーク設定」を参照してください。
- ドメインレス gMSAか各インスタンスを単一のドメインに結合するを選択しました。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

  次に、CredSpec のデータ ストレージを選択し、必要に応じて、ドメインレス gMSA の Active Directory ユーザー認証情報を選択します。

  Amazon ECS は Active Directory の認証情報仕様ファイル (CredSpec) を使用します。このファイルは、gMSA アカウントコンテキストをコンテナに伝達するために使用される gMSA メタデータを含む認証情報仕様ファイルを使用します。CredSpec ファイルを生成し、コンテナインスタンスのオペレーティングシステムに応じて、次の表にある CredSpec ストレージオプションのいずれかに保存します。ドメインレス方式を使用するには、CredSpec ファイル内のオプションのセクションで、コンテナインスタンスのオペレーティングシステムに固有の、次の表の domainless user credentials ストレージオプションのいずれかの認証情報を指定できます。

ストレージの場所	リナックス	Windows
Amazon Simple Storage Service	CredSpec	CredSpec
AWS Secrets Manager	ドメインレスユーザー認証情報	ドメインレスユーザー認証情報
Amazon EC2 Systems Manager Parameter Store	CredSpec	CredSpec、ドメインレスユーザー認証情報
ローカルファイル	該当なし	CredSpec

前提条件

Amazon ECS で Windows コンテナ向け gMSA 機能を使用する前に、必ず次の作業を完了してください。

- コンテナがアクセスするリソースを含む Active Directory ドメインを設定します。Amazon ECS は以下の設定をサポートしています。
  - AWS Directory Service Active Directory。AWS Directory Service は、Amazon EC2 でホストされる AWS マネージド Active Directory です。詳細については、「AWS Directory Service 管理ガイド」の「AWS Managed Microsoft AD の開始方法」を参照してください。
  - オンプレミスの Active Directory。Amazon ECS Linux コンテナインスタンスがドメインに参加できることを確認する必要があります。詳細については、「AWS Direct Connect」を参照してください。
- Active Directory に既存の gMSA アカウントがあります。詳細については、「Windows コンテナでの gMSA の使用」を参照してください。
- ドメインレス gMSA を使用することを選択した場合、または Amazon ECS タスクをホストする Amazon ECS Windows コンテナインスタンスは、Active Directory にドメイン参加しており、gMSA アカウントにアクセスできる Active Directory セキュリティグループのメンバーである必要があります。

  ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

- 必須の IAM アクセス権限を追加しました。必要な権限は、初期認証情報と認証情報の仕様の保存に選択した方法によって異なります。
  - 初期認証情報にドメインレス gMSA を使用する場合は、Amazon EC2 インスタンスロールに AWS Secrets Manager の IAM アクセス許可が必要です。
  - 認証情報の仕様を SSM Parameter Store に保存する場合は、タスク実行ロールで Amazon EC2 Systems Manager Parameter Store に対する IAM 許可が必要です。
  - 認証情報の仕様を Amazon S3 で保存する場合は、タスク実行ロールで Amazon Simple Storage Service の IAM 許可が必要です。

Amazon ECS での Windows コンテナ向け gMSA の設定

前提条件 AWS CLI を使用するドメインレス gMSA で Amazon ECS Windows コンテナを使用する の設定を含む完全なチュートリアルに従い、Windows コンテナ向け gMSA を Amazon ECS 上で設定できます。

次のセクションでは、CredSpec の構成について詳しく説明します。

トピック

- CredSpec の例
- ドメインレス gMSA 設定
- タスク定義での認証情報仕様ファイルの参照

CredSpec の例

Amazon ECS は、gMSA アカウントコンテキストを Windows コンテナに伝達するために使用される gMSA メタデータを含む認証情報仕様ファイルを使用します。認証情報仕様ファイルを生成し、タスク定義の `credentialSpec` フィールドで参照できます。認証情報仕様ファイルにはシークレットが含まれていません。

認証情報仕様ファイルの例を次に示します。

```
{
    "CmsPlugins": [
        "ActiveDirectory"
    ],
    "DomainJoinConfig": {
        "Sid": "S-1-5-21-2554468230-2647958158-2204241789",
```

```
        "MachineAccountName": "WebApp01",
        "Guid": "8665abd4-e947-4dd0-9a51-f8254943c90b",
        "DnsTreeName": "contoso.com",
        "DnsName": "contoso.com",
        "NetBiosName": "contoso"
    },
    "ActiveDirectoryConfig": {
        "GroupManagedServiceAccounts": [
            {
                "Name": "WebApp01",
                "Scope": "contoso.com"
            }
        ]
    }
}
```

ドメインレス gMSA 設定

コンテナインスタンスを単一のドメインに参加させるのではなく、ドメインレス gMSA をお勧めします。ドメインレス gMSA を使用すると、コンテナインスタンスはドメインに参加せず、インスタンス上の他のアプリケーションは認証情報を使用してドメインにアクセスできなくなり、異なるドメインに参加するタスクを同じインスタンス上で実行できます。

1. CredSpec をいずれかのストレージオプションにアップロードする前に、Secrets Manager または SSM Parameter Store のシークレットの ARN を含む情報を CredSpec に追加します。詳細については、Microsoft Learn Web サイトの「ドメイン結合されていないコンテナホストのユースケース向けの追加の認証情報仕様設定」を参照してください。

   ドメインレス gMSA 認証情報の形式

   以下は、Active Directory のドメインレス gMSA 認証情報の JSON 形式です。認証情報を Secrets Manager または SSM Parameter Store に保存します。

   ```
   {
       "username":"WebApp01",
       "password":"Test123!",
       "domainName":"contoso.com"
   }
   ```

2. `ActiveDirectoryConfig` 内部の CredSpec ファイルに以下の情報を追加します。ARN を Secrets Manager または SSM Parameter Store のシークレットに置き換えます。

PluginGUID 値は次のサンプルのスニペットの GUID と一致する必要があり、必須であることに注意してください。

```
    "HostAccountConfig": {
        "PortableCcgVersion": "1",
        "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
        "PluginInput": "{\"credentialArn\": \"arn:aws:secretsmanager:aws-region:111122223333:secret:gmsa-plugin-input\"}"
    }
```

また、この形式 \"arn:aws:ssm:*aws-region*:111122223333:parameter/*gmsa-plugin-input*\" の ARN を使用して SSM Parameter Store でシークレットを使用できます。

3. CredSpec ファイルを修正すると、次の例のようになります。

```
{
  "CmsPlugins": [
    "ActiveDirectory"
  ],
  "DomainJoinConfig": {
    "Sid": "S-1-5-21-4066351383-705263209-1606769140",
    "MachineAccountName": "WebApp01",
    "Guid": "ac822f13-583e-49f7-aa7b-284f9a8c97b6",
    "DnsTreeName": "contoso",
    "DnsName": "contoso",
    "NetBiosName": "contoso"
  },
  "ActiveDirectoryConfig": {
    "GroupManagedServiceAccounts": [
      {
        "Name": "WebApp01",
        "Scope": "contoso"
      },
      {
        "Name": "WebApp01",
        "Scope": "contoso"
      }
    ],
    "HostAccountConfig": {
      "PortableCcgVersion": "1",
      "PluginGUID": "{859E1386-BDB4-49E8-85C7-3070B13920E1}",
```

```
      "PluginInput": "{\"credentialArn\": \"arn:aws:secretsmanager:aws-
region:111122223333:secret:gmsa-plugin-input\"}"
    }
  }
}
```

タスク定義での認証情報仕様ファイルの参照

Amazon ECS では、タスク定義の `credentialSpecs` フィールドでファイルパスを参照する次の方法がサポートされています。これらの各オプションでは、コンテナインスタンスを単一のドメインに参加させるかドメインレス gMSA を使用するかに応じて、`credentialspec:` または `domainlesscredentialspec:` を指定できます。

Amazon S3 バケット

認証情報仕様を Amazon S3 バケットに追加し、タスク定義の `credentialSpecs` フィールドで Amazon S3 バケットの Amazon リソースネーム (ARN) を参照します。

```
{
    "family": "",
    "executionRoleArn": "",
    "containerDefinitions": [
        {
            "name": "",
            ...
            "credentialSpecs": [
                "credentialspecdomainless:arn:aws:s3:::${BucketName}/${ObjectName}"
            ],
            ...
        }
    ],
    ...
}
```

また、次のアクセス権限をインラインポリシーとして Amazon ECS タスク実行 IAM ロール に追加して、タスクに Amazon S3 バケットへのアクセスを付与する必要があります。

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

```
            "Sid": "VisualEditor",
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*"
            ],
            "Resource": [
                "arn:aws:s3:::{bucket_name}",
                "arn:aws:s3:::{bucket_name}/{object}"
            ]
        }
    ]
}
```

SSM パラメータストアパラメータ

認証情報仕様を SSM パラメータストアパラメータに追加し、タスク定義の `credentialSpecs` フィールドで SSM パラメータストアパラメータの Amazon リソースネーム (ARN) を参照します。

```
{
    "family": "",
    "executionRoleArn": "",
    "containerDefinitions": [
        {
            "name": "",
            ...
            "credentialSpecs": [

 "credentialspecdomainless:arn:aws:ssm:region:111122223333:parameter/parameter_name"
            ],
            ...
        }
    ],
    ...
}
```

また、次のアクセス権限をインラインポリシーとして Amazon ECS タスク実行 IAM ロール に追加して、タスクに SSM パラメータストアパラメータへのアクセス権を付与する必要があります。

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

```
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameters"
            ],
            "Resource": [
                "arn:aws:ssm:region:111122223333:parameter/parameter_name"
            ]
        }
    ]
}
```

ローカルファイル

ローカルファイルの認証情報仕様の詳細を使用して、タスク定義の credentialSpecs フィールドでファイルパスを参照します。参照されるファイルパスは C:\ProgramData\Docker\CredentialSpecs ディレクトリからの相対パスで、ファイルパスの区切り文字にはバックスラッシュ ('\') を使用する必要があります。

```
{
    "family": "",
    "executionRoleArn": "",
    "containerDefinitions": [
        {
            "name": "",
            ...
            "credentialSpecs": [
                "credentialspec:file://CredentialSpecDir\CredentialSpecFile.json"
            ],
            ...
        }
    ],
    ...
}
```

EC2 Image Builder を使用して、Amazon ECS に最適化されたカスタム AMI を構築する

AWS では、コンテナ ワークロードを実行するための要件および推奨事項であらかじめ設定されている、Amazon ECS に最適化された AMI の使用をお勧めしています。ソフトウェアの追加には AMI のカスタマイズが必要になる場合があります。EC2 Image Builder は、サーバーイメージの作成、管

理、デプロイに使用できます。アカウントで作成されるカスタムイメージの所有権は、お客様に保持されます。EC2 Image Builder パイプラインを使用してイメージの更新やシステムパッチを自動化したり、スタンドアロンコマンドを使用して定義済みの設定リソースでイメージを作成することができます。

イメージのレシピを作成します。レシピには親画像とその他の追加コンポーネントが含まれます。さらに、カスタマイズした AMI を配信するパイプラインを作成します。

イメージのレシピを作成します。Image Builder イメージレシピは、ベースイメージとベースイメージに適用するコンポーネントを定義し、必要な構成の出力イメージを生成するためのドキュメントです。さらに、カスタマイズした AMI を配信するパイプラインを作成します。詳細については、「EC2 Image Builder ユーザーガイド」の「EC2 Image Builder の仕組み」を参照してください。

EC2 Image Builder の「親イメージ」として、次の Amazon ECS に最適化された AMI のいずれかの使用をお勧めします。

- リナックス
  - Amazon ECS 最適化 AL2023 x86
  - Amazon ECS 最適化 Amazon Linux 2023 (arm64) AMI
  - Amazon ECS 最適化 Amazon Linux 2 カーネル 5 AMI
  - Amazon ECS 最適化 Amazon Linux 2 x86 AMI
- Windows
  - Amazon ECS 最適化 Windows 2022 Full x86
  - Amazon ECS 最適化 Windows 2022 Core x86
  - Amazon ECS 最適化 Windows 2019 Full x86
  - Amazon ECS 最適化 Windows 2019 Core x86
  - Amazon ECS 最適化 Windows 2016 Full x86

利用可能な最新バージョンを使用することをお勧めします。パイプラインでは親イメージにセマンティックバージョニングを使用します。これにより、自動スケジューリングされたジョブの依存関係の更新を検出しやすくなります。詳細については、「EC2 Image Builder ユーザーガイド」の「セマンティックバージョニング」を参照してください。

AWS は、Amazon ECS に最適化された AMI イメージを、セキュリティパッチと新しいコンテナエージェントバージョンで定期的に更新しています。AMI ID をイメージレシピの親イメージとして使用する場合、親イメージの更新がないかを定期的に確認する必要があります。更新がある場合は、

更新した AMI を使用して新しいバージョンのレシピを作成する必要があります。これにより、カスタムイメージに最新バージョンの親イメージが組み込まれます。新しく作成した AMI を使用して Amazon ECS クラスターの EC2 インスタンスを自動的に更新するワークフローを作成する方法については、「AMI 強化パイプラインを作成して ECS インスタンスフリートの更新を自動化する方法」を参照してください。

マネージド EC2 Image Builder パイプラインを通じて公開された親イメージの Amazon リソースネーム (ARN) を指定することもできます。Amazon は、マネージドパイプラインを通じて、Amazon ECS 最適化 AMI イメージを定期的に公開します。これらのイメージはパブリックアクセス可能です。イメージにアクセスするには、適切なアクセス許可が必要です。Image Builder レシピで AMI の代わりにイメージ ARN を使用すると、パイプラインは実行のたびに最新バージョンの親イメージを自動的に使用します。この方法により、更新のたびに新しいレシピバージョンを手動で作成する必要がなくなります。

イメージ ARN と Infrastructure as Code (IaC) の使用

EC2 Image Builder コンソール、Infrastructure as Code (例: AWS CloudFormation)、または AWS SDK を使用してレシピを設定できます。レシピで親イメージを指定する場合、EC2 AMI ID、Image Builder イメージ ARN、AWS Marketplace プロダクト ID、またはコンテナイメージを指定できます。AWS は、Amazon ECS 最適化 AMI の AMI ID と Image Builder イメージ ARN の両方を公開します。イメージの ARN 形式は以下の通りです。

```
arn:${Partition}:imagebuilder:${Region}:${Account}:image/${ImageName}/${ImageVersion}
```

`ImageVersion` の形式は以下のようになっています。*`[####]`*、*`[####]`*、*`[###]`*を最新の値に置き換えます。

```
<major>.<minor>.<patch>
```

`major`、`minor`、`patch` を特定の値に置き換えたり、イメージのバージョンレス ARN を使用することができます。これにより、パイプラインは常に親イメージの最新バージョンに更新された状態に保たれます。バージョンレス ARN では、ワイルドカード形式「x.x.x」でイメージバージョンを表現します。この方法により、Image Builder サービスは最新バージョンのイメージに自動的に解決されます。バージョンレス ARN を使用すると、参照先は常に利用可能な最新のイメージを示すため、デプロイ内のイメージを最新の状態に維持するプロセスが効率化されます。コンソールでレシピを作成すると、EC2 Image Builder は親イメージの ARN を自動的に識別します。IaC を使用してレシピを作成する場合、ARN を特定して目的のイメージバージョンを選択するか、バージョンレス ARN を使用して使用可能な最新のイメージを示す必要があります。フィルタリングにより条件に合致す

るイメージのみを表示する自動スクリプトを作成することをお勧めします。次の Python スクリプトは、Amazon ECS 最適化 AMI のリストを取得する方法を示しています。

このスクリプトは、owner と platform の 2 つのオプション引数を受け付けます。デフォルト値はそれぞれ「Amazon」と「Windows」です。owner 引数の有効値は、Self、Shared、Amazon、ThirdParty です。プラットフォーム引数の有効値は、Windows と Linux です。たとえば、owner 引数を Amazon に設定し、platform を Linux に設定してスクリプトを実行すると、スクリプトは Amazon ECS 最適化イメージを含む、Amazon によって公開されたイメージのリストを生成します。

```
import boto3
import argparse

def list_images(owner, platform):
    # Create a Boto3 session
    session = boto3.Session()

    # Create an EC2 Image Builder client
    client = session.client('imagebuilder')

    # Define the initial request parameters
    request_params = {
        'owner': owner,
        'filters': [
            {
                'name': 'platform',
                'values': [platform]
            }
        ]
    }

    # Initialize the results list
    all_images = []

    # Get the initial response with the first page of results
    response = client.list_images(**request_params)

    # Extract images from the response
    all_images.extend(response['imageVersionList'])

    # While 'nextToken' is present, continue paginating
    while 'nextToken' in response and response['nextToken']:
        # Update the token for the next request
```

```
        request_params['nextToken'] = response['nextToken']

        # Get the next page of results
        response = client.list_images(**request_params)

        # Extract images from the response
        all_images.extend(response['imageVersionList'])

    return all_images

def main():
    # Initialize the parser
    parser = argparse.ArgumentParser(description="List AWS images based on owner and
 platform")

    # Add the parameters/arguments
    parser.add_argument("--owner", default="Amazon", help="The owner of the images.
 Default is 'Amazon'.")
    parser.add_argument("--platform", default="Windows", help="The platform type of the
 images. Default is 'Windows'.")

    # Parse the arguments
    args = parser.parse_args()

    # Retrieve all images based on the provided owner and platform
    images = list_images(args.owner, args.platform)

    # Print the details of the images
    for image in images:
        print(f"Name: {image['name']}, Version: {image['version']}, ARN:
 {image['arn']}")

if __name__ == "__main__":
    main()
```

AWS CloudFormation でのイメージ ARN の使用

Image Builder のイメージレシピは、出力イメージの意図した構成を実現するために必要な親イメージとコンポーネントを指定するブループリントです。AWS::ImageBuilder::ImageRecipe リソースを使用します。ParentImage 値をイメージ ARN に設定します。パイプラインが常に最新バージョンのイメージを使用するように、目的のイメージのバージョンレス ARN を使用してください。例えば、arn:aws:imagebuilder:us-east-1:aws:image/amazon-linux-2023-ecs-

optimized-x86/x.x.x と指定します。以下の AWS::ImageBuilder::ImageRecipe リソースの定義は、Amazon マネージドイメージ ARN を使用しています。

```
ECSRecipe:
    Type: AWS::ImageBuilder::ImageRecipe
    Properties:
      Name: MyRecipe
      Version: '1.0.0'
      Components:
        - ComponentArn: [<The component arns of the image recipe>]
      ParentImage: "arn:aws:imagebuilder:us-east-1:aws:image/amazon-linux-2023-ecs-
optimized-x86/x.x.x"
```

これらの AWS::ImageBuilder::ImageRecipe リソースの詳細については、「AWS CloudFormation ユーザーガイド」を参照してください。

AWS::ImageBuilder::ImagePipeline リソースの Schedule プロパティを設定することで、パイプラインでの新しいイメージの作成を自動化できます。スケジュールには開始条件と cron 式が含まれています。詳細については、AWS CloudFormation ユーザーガイドの AWS::ImageBuilder::ImagePipelineを参照してください。

AWS::ImageBuilder::ImagePipeline次の例では、パイプラインで毎日協定世界時 (UTC) の午前 10 時にビルドを実行しています。以下の Schedule 値を設定します。

- PipelineExecutionStartCondition を EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE に設定します。ビルドは、セマンティックバージョンでワイルドカード「x」を使用する親イメージやコンポーネントなどの依存リソースが更新された場合にのみ開始されます。これにより、ビルドにはそれらのリソースの最新の更新が確実に組み込まれます。
- ScheduleExpression を cron 式 (`0 10 * * ? *`) に設定します。

```
ECSPipeline:
    Type: AWS::ImageBuilder::ImagePipeline
    Properties:
      Name: my-pipeline
      ImageRecipeArn: <arn of the recipe you created in previous step>
      InfrastructureConfigurationArn: <ARN of the infrastructure configuration
 associated with this image pipeline>
      Schedule:
```

```
        PipelineExecutionStartCondition:
EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE
        ScheduleExpression: 'cron(0 10 * * ? *)'
```

Terraform でのイメージ ARN の使用

Terraform でパイプラインの親イメージとスケジュールを指定する方法は、AWS CloudFormation での方法と同様です。`aws_imagebuilder_image_recipe` リソースを使用します。`parent_image` 値をイメージ ARN に設定します。目的のイメージのバージョンレス ARN を使用して、パイプラインが常に最新バージョンのイメージを使用するようにします。詳細については、Terraform ドキュメントの `aws_imagebuilder_image_recipe` を参照してください。

`aws_imagebuilder_image_pipeline resource` のスケジュール設定ブロックで、`schedule_expression` 引数の値を任意の cron 式に設定してパイプラインの実行頻度を指定し、`pipeline_execution_start_condition` を `EXPRESSION_MATCH_AND_DEPENDENCY_UPDATES_AVAILABLE` に設定します。詳細については、Terraform ドキュメントの `aws_imagebuilder_image_pipeline` を参照してください。

Amazon ECS で AWS 深層学習コンテナを使用する

AWSDeep Learning Containersは、 Amazon ECS の TensorFlow と Apache MXNet(インキュベーション)のモデルをトレーニングして提供するためのDockerイメージのセットを提供します。Deep Learning Containersは、TensorFlow、NVIDIA CUDA(GPUインスタンス用)、Intel MKL(CPUインスタンス用)のライブラリを使用し、最適化された環境を実現します。Deep Learning Containers のコンテナイメージは、Amazon ECR で利用でき、Amazon ECS タスク定義で参照できます。Deep Learning Containers と Amazon Elastic Inference を併用することで、推論コストを削減できます。

Elastic Inference を使用せずに Deep Learning Containers の使用を開始するには、「AWS Deep Learning AMIs デベロッパーガイド」の「Amazon ECS setup」を参照してください。

Amazon ECS の Service Quotas

次の表は、AWS アカウント の Amazon ECS に対するデフォルトのサービスクォータ (制限とも呼ばれます) を示します。Elastic Load Balancing や Auto Scaling など、Amazon ECS で使用できるその他の AWS のサービス のサービスクォータの詳細については、「Amazon Web Services 全般のリファレンス」の「AWS サービスクォータ」を参照してください。Amazon ECS API での API スロットリングの詳細については、「Request throttling for the Amazon ECS API」(Amazon ECS API のスロットリングをリクエストする) を参照してください。

Amazon ECS のサービスクォータ

Amazon ECS の Service Quotasは以下のとおりです。

新規 AWS アカウントの初期の低いクォータは、経時的に引き上げられる可能性があります。Amazon ECS は、各リージョン内のアカウント使用率を常に監視し、使用率に基づいてクォータを自動的に引き上げます。調整可能として表示される値のクォータの引き上げをリクエストすることもできます。「Service Quotas ユーザーガイド」でクォータ引き上げのリクエストの方法をご確認ください。

名前	デフォルト	引き上げ可能	説明
クラスターあたりのキャパシティープロバイダー	サポートされている各リージョン: 20	いいえ	クラスターに関連付けることができるキャパシティープロバイダーの最大数。
サービスあたりの Classic Load Balancer	サポートされている各リージョン: 1	[いいえ]	サービスあたりの Classic Load Balancer の最大数。

名前	デフォルト	引き上げ可能	説明
アカウントあたりのクラスター	サポートされている各リージョン: 10,000	あり	アカウントあたりのクラスターの数
クラスターあたりのコンテナインスタンスの数	サポートされている各リージョン: 5,000	いいえ	クラスターあたりのコンテナインスタンスの数
start-task あたりのコンテナインスタンス	サポートされている各リージョン: 10	いいえ	StartTask API アクションで指定されたコンテナインスタンスの最大数。
タスク定義あたりのコンテナ数	サポートされている各リージョン: 10	いいえ	タスク定義内のコンテナ定義の最大数
ECS Exec セッション	サポートされている各リージョン: 1,000	いいえ	各コンテナの ECS Exec セッションの最大数。
AWS Fargate 上のサービスによって起動されたタスクの割合	サポートされている各リージョン: 500	いいえ	Amazon ECS サービススケジューラによって、1 分あたりのサービスごとに Fargate でプロビジョニングできるタスクの最大数。

名前	デフォルト	引き上げ可能	説明
Amazon EC2 または外部インスタンスのサービスによって起動されるタスク	サポートされている各リージョン: 500	いいえ	Amazon ECS サービススケジューラによって、1 分あたりのサービスごとに Amazon EC2 または外部インスタンスでプロビジョニングできるタスクの最大数です。
タスク定義ファミリーあたりのリビジョンの数	サポートされている各リージョン: 1,000,000	いいえ	タスク定義ファミリーあたりのリビジョンの最大数 タスク定義リビジョンを登録解除または削除しても、この制限から除外することはできません。
awsvpcConfiguration あたりのセキュリティグループ	サポートされている各リージョン : 5	いいえ	awsvpcConfiguration 内で指定されるセキュリティグループの最大数
クラスターあたりのサービスの数	サポートされている各リージョン: 5,000	いいえ	クラスターあたりのサービスの最大数。
名前空間あたりのサービス	サポートされている各リージョン: 100	可能	名前空間で実行できるサービスの最大数。
awsvpcConfiguration あたりのサブネット	サポートされている各リージョン: 16	いいえ	awsvpcConfiguration 内で指定されるサブネットの最大数

名前	デフォルト	引き上げ可能	説明
リソースあたりのタグ	サポートされている各リージョン: 50	いいえ	リソースあたりのタグの最大数 これは、タスク定義、クラスター、タスク、サービスに適用されます。
サービスあたりのターゲットグループ	サポートされている各リージョン : 5	いいえ	Application Load Balancer または Network Load Balancer を使用している場合、サービスごとのターゲットグループの最大数。
タスク定義サイズ	サポートされている各リージョン: 64 キロバイト	いいえ	タスク定義の最大サイズ (KiB 単位)
クラスタごとのプロビジョニング状態のタスク	サポートされている各リージョン: 500	いいえ	クラスターごとにある PROVISIONING 状態で待機しているタスクの最大数。このクォータは、EC2 Auto Scaling グループキャパシティープロバイダーを使用して起動されたタスクにのみ適用されます。
run-task 当たりの起動されるタスク	サポートされている各リージョン: 10	いいえ	RunTask API アクションあたりの起動できるタスクの最大数。

名前	デフォルト	引き上げ可能	説明
サービスあたりのタスク	サポートされている各リージョン: 5,000	いいえ	サービスあたりのタスクの最大数 (必要な数)

> **Note**
>
> デフォルト値は、AWS によって設定された初期クォータです。この値は、実際に適用されたクォータ値および適用可能な最大サービスクォータとは異なります。詳細については、「Service Quotas ユーザーガイド」の「Service Quotas の用語」を参照してください。

> **Note**
>
> Amazon ECS サービス検出を使用するように設定されたサービスには、サービスごとに 1,000 タスクに制限があります。これは、サービスあたりのインスタンス数に対する AWS Cloud Map の Service Quotasによるものです。詳細については、「Amazon Web Services 全般のリファレンス」の「AWS Cloud Map の Service Quotas」を参照してください。

> **Note**
>
> 実際には、タスク起動レートは、ダウンロードおよび圧縮されていないコンテナイメージ、ヘルスチェックやロードバランサーへのタスクの登録などの有効なその他の統合といった考慮事項にも依存します。ここに表示されているクォータと比較すると、タスク起動レートにばらつきが見られる場合があります。これらのばらつきは、サービスに使用する機能によって生じます。詳細については、「Amazon ECS サービスパラメータのベストプラクティス」を参照してください。

> **Note**
>
> Amazon ECS Service Connect を使用するように設定されたサービスには、サービスごとに 1,000 タスクの制限があります。これは、サービスあたりのインスタンス数に対する AWS Cloud Map の Service Quotasによるものです。詳細については、「Amazon Web Services 全般のリファレンス」の「AWS Cloud Map の Service Quotas」を参照してください。

AWS Fargate Service Quotas

AWS Fargate サービスクォータの Amazon ECS を次に示します。これは、Service Quotas コンソールの [AWS Fargate] サービスの下に一覧表示されます。

新規 AWS アカウントの初期の低いクォータは、経時的に引き上げられる可能性があります。Fargate は、各リージョン内のアカウント使用率を常に監視し、使用率に基づいてクォータを自動的に引き上げます。調整可能として表示される値のクォータの引き上げをリクエストすることもできます。「Service Quotas ユーザーガイド」でクォータ引き上げのリクエストの方法をご確認ください。

名前	デフォルト	引き上げ可能	説明
Fargate オンデマンドバースト起動レート	サポートされている各リージョン: 100	可能	現在のリージョンでの、このアカウントで 1 回のバーストで起動されるオンデマンド Amazon ECS タスクまたは Amazon EKS ポッドの最大数 (バースト率)。
Fargate オンデマンド持続起動レート	サポートされている各リージョン: 20	可能	現在のリージョンでの、このアカウントで 1 秒あたりに起動されるオン

名前	デフォルト	引き上げ可能	説明
			デマンド Amazon ECS タスクまたは Amazon EKS ポッドの最大数 (持続率)。
Fargate オンデマンド vCPU リソース数	サポートされている各リージョン: 6	あり	現在のリージョンのこのアカウントで Fargate On-Demand として同時に実行される Fargate vCPU の数。
Fargate スポットバースト起動レート	サポートされている各リージョン: 100	可能	現在のリージョンでの、このアカウントで 1 回のバーストで起動されるスポット Amazon ECS タスクの最大数 (バースト率)。
Fargate スポットの持続起動レート	サポートされている各リージョン: 20	可能	現在のリージョンでの、このアカウントで 1 秒あたりに起動されるスポット Amazon ECS タスクの最大数 (持続率)。
Fargate Spot vCPU リソース数	サポートされている各リージョン: 6	あり	現在のリージョンのこのアカウントの Fargate Spot として同時に実行されている Fargate vCPU の数。

> **Note**
>
> デフォルト値は、AWS によって設定された初期クォータです。この値は、実際に適用されたクォータ値および適用可能な最大サービスクォータとは異なります。詳細については、「Service Quotas ユーザーガイド」の「Service Quotas の用語」を参照してください。

> **Note**
>
> Fargate は、Amazon ECS タスクと Amazon EKS ポッドの起動レート制限をさらに強制します。詳細については、「AWS Fargate スロットリングのクォータ」を参照してください。

AWS Management Console での Amazon ECS とAWS FargateService Quotasの管理

Amazon ECS は、Service Quotas と統合されています。Service Quotas は、クォータを一元的な場所から表示および管理できる AWS サービスです。詳細については、「Service Quotas ユーザーガイド」の「Service Quotas とは」を参照してください。

Service Quotas を使用すると、Amazon ECS Service Quotasの値を簡単に調べることができます。

AWS Management Console

AWS Management Console を使用して Amazon ECS Service QuotasおよびFargate Service Quotasを表示するには

1. https://console.aws.amazon.com/servicequotas/ で Service Quotasのコンソールを開きます。
2. ナビゲーションペインで、[AWS のサービス] を選択します。
3. [AWS services] リストから、[Amazon Elastic Container Service (Amazon ECS)] または [AWS Fargate] を選択します。

   Service quotas (Service Quotas)の一覧には、Service Quotas名、適用された値 (使用可能な場合)、AWS デフォルトのクォータ、クォータ値が調整可能かどうかが表示されます。
4. 説明など、Service Quotas に関する追加情報を表示するには、クォータ名を選択します。

5. (オプション) クォータの引き上げをリクエストするには、引き上げるクォータを選択し、[クォータ引き上げリクエスト] を選択します。必要な情報を入力または選択して、[リクエスト] を選択します。

AWS Management Console を使用してさらにService Quotasの操作を行うには、Service Quotas ユーザーガイドを参照してください。クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。

AWS CLI

AWS CLI を使用して Amazon ECS Service Quotasおよび Fargate Service Quotasを表示するには

次のコマンドを実行して、デフォルトの Amazon ECS クォータを表示します。

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code ecs \
    --output table
```

次のコマンドを実行して、デフォルトの Fargate クォータを表示します。

```
aws service-quotas list-aws-default-service-quotas \
    --query 'Quotas[*].
{Adjustable:Adjustable,Name:QuotaName,Value:Value,Code:QuotaCode}' \
    --service-code fargate \
    --output table
```

次のコマンドを実行して、適用された Fargate クォータを表示します。

```
aws service-quotas list-service-quotas \
    --service-code fargate
```

> **Note**
>
> Amazon ECS は、適用されたクォータをサポートしていません。

AWS CLI を使用して Service Quotas を操作する方法の詳細については、「AWS CLI コマンドリファレンス Service Quotas」を参照してください。クォータの引き上げをリクエストするには、「AWS CLI コマンド リファレンス」で `request-service-quota-increase` コマンドを参照してください。

Amazon ECS Service Quotas と API スロットリング制限を処理する

Amazon ECS は、Elastic Load Balancing、AWS Cloud Map、Amazon EC2 など、いくつかの AWS のサービス と統合されています。この緊密な統合により、Amazon ECS ではサービスの負荷分散、Service Connect、タスクネットワーク、クラスターの自動スケーリングなどのいくつかの機能を利用できます。Amazon ECS および、統合されているその他の AWS のサービス はすべて、一貫したパフォーマンスと利用率を確保するために、サービスクォータと API レート制限を維持します。また、これらのサービスクォータは、必要以上のリソースを誤ってプロビジョニングすることを防ぎ、請求額を増やす可能性のある悪意のある行為からも保護します。

サービスクォータと AWS API のレート制限をよく理解しておけば、予期しないパフォーマンスの低下を心配することなく、ワークロードのスケーリングを計画できます。詳細については、「Amazon ECS API のリクエストのスロットリング」を参照してください。

Amazon ECS でワークロードをスケーリングする場合は、次のサービスクォータを検討することをお勧めします。

- AWS Fargate には、各 AWS リージョン のタスクで同時に実行できるタスクの数を制限するクォータがあります。Amazon ECS では、オンデマンドタスクと Fargate Spot タスクの両方にクォータが設定されています。各サービスクォータには、Fargate で実行するすべての Amazon EKS ポッドも含まれます。
- Amazon EC2 インスタンスで実行されるタスクの場合、各クラスターに登録できる Amazon EC2 インスタンスの最大数は 5,000 です。Auto Scaling グループの容量プロバイダーで Amazon ECS クラスターの自動スケーリングを使用する場合、またはクラスターの Amazon EC2 インスタンスを自分で管理する場合、このクォータがデプロイのボトルネックになる可能性があります。さらに容量が必要な場合は、クラスターをさらに作成するか、サービスクォータの引き上げをリクエストすることができます。
- Auto Scaling グループのキャパシティプロバイダーで Amazon ECS クラスターの自動スケーリングを使用する場合は、サービスをスケーリングする際に `Tasks in the PROVISIONING state per cluster` クォータを考慮してください。このクォータは、キャパシティプロバイダーがキャ

パシティを増やすことができる各クラスターの PROVISIONING 状態にあるタスクの最大数です。多数のタスクを同時に起動すると、すぐにこのクォータに達してしまいます。たとえば、それぞれ数百のタスクを含む数十のサービスを同時にデプロイする場合です。この場合、クラスターのキャパシティが不足すると、キャパシティープロバイダーは新しいコンテナインスタンスを起動してタスクを配置する必要があります。キャパシティープロバイダーが追加の Amazon EC2 インスタンスを起動している間、Amazon ECS サービススケジューラーは引き続きタスクを並行して起動する可能性があります。ただし、クラスターのキャパシティが不十分なため、このアクティビティが抑制される可能性があります。Amazon ECS サービススケジューラは、新しいコンテナインスタンスが起動したときにタスク配置を再試行するためのバックオフおよびエクスポネンシャルスロットリング戦略を実装しています。その結果、デプロイやスケールアウトに時間がかかる可能性があります。このような状況を回避するには、以下のいずれかの方法でサービスのデプロイを計画してください。クラスター容量を増やす必要がないように多数のタスクをデプロイするか、新しいタスクの起動に備えて予備のクラスター容量を確保しておくかのどちらかです。

ワークロードをスケーリングする際には Amazon ECS サービスクォータを考慮することに加えて、Amazon ECS と統合されている他の AWS のサービス 用のサービスクォータも考慮してください。

エラスティックロードバランシング

Fargate の Amazon ECS サービスは、Elastic Load Balancing を使用してタスク間でトラフィックを均等に分散するように設定できます。ロードバランサーの選択方法の詳細と推奨ベストプラクティスについては、ロードバランサーを使用して Amazon ECS サービストラフィックを分散する を参照してください。

Elastic Load Balancing のサービスクォータ

ワークロードをスケーリングするときは、以下の Elastic Load Balancing のサービスクォータを考慮してください。Elastic Load Balancing のサービスクォータのうち、ほとんどは調整可能で、Service Quotas コンソールでリクエストできます。

Application Load Balancer

Application Load Balancer を使用する際、ユースケースによっては、以下のクォータ増加をリクエストする必要がある場合があります。

- Application Load Balancer の背後にあるターゲットの数である `Targets per Application Load Balancer` クォータ。

- ターゲットグループの背後にあるターゲットの数である `Targets per Target Group per Region` クォータ。

詳細については、Application Load Balancer ユーザーガイドの「Application Load Balancer のクォータ」を参照してください。

Network Load Balancer

Network Load Balancer に登録できるターゲットの数には、より厳しい制限があります。Network Load Balancer を使用する場合、クロスゾーンサポートを有効にする必要があることがよくあります。これには、各 Network Load Balancer のアベイラビリティーゾーンあたりの `Targets per Availability Zone Per Network Load Balancer` 最大ターゲット数に対する追加のスケーリング制限が伴います。詳細については、Network Load Balancers ユーザーガイドの「Network Load Balancer のクォータ」を参照してください。

Elastic Load Balancing API のスロットリング

ロードバランサーを使用するように Amazon ECS サービスを設定する場合、サービスが正常であると見なされるには、ターゲットグループのヘルスチェックに合格する必要があります。これらのヘルスチェックを実行するために、Amazon ECS はユーザーに代わって Elastic Load Balancing API 操作を呼び出します。アカウントにロードバランサーが設定されたサービスが多数ある場合、特に `RegisterTarget`、`DeregisterTarget`、`DescribeTargetHealth` Elastic Load Balancing API 操作のスロットリングが発生する可能性があるため、サービスのデプロイが遅くなる可能性があります。スロットリングが発生すると、Amazon ECS サービスのイベントメッセージにスロットリングエラーが発生します。

AWS Cloud Map API でスロットリングが発生した場合は、AWS Cloud Map API のスロットリング制限を引き上げる方法について サポート までお問い合わせください。これらのスロットリングエラーの監視とトラブルシューティングの詳細については、「Amazon ECS のスロットリングに関する問題を処理する」を参照してください。

Elastic Network Interface

タスクが `awsvpc` ネットワークモードを使用する場合、Amazon ECS はタスクごとに独自の Elastic Network Interface (ENI) をプロビジョニングします。Amazon ECS サービスが Elastic Load Balancing ロードバランサーを使用する場合、これらのネットワークインターフェイスは、サービスで定義された適切なターゲットグループのターゲットとしても登録されます。

Elastic Network Interface のサービスクォータ

awsvpc ネットワークモードを使用するタスクを実行すると、固有の エラスティックネットワークインターフェイスが各タスクにアタッチされます。インターネット経由でこれらのタスクにアクセスする必要がある場合は、タスクの エラスティックネットワークインターフェイスにパブリック IP アドレスを割り当てます。Amazon ECS ワークロードをスケーリングするときは、次の 2 つの重要なクォータを考慮してください。

- アカウントの AWS リージョン におけるネットワークインターフェイスの最大数である `Network interfaces per Region` クォータ。
- AWS リージョン に含まれる Elastic IP アドレスの最大数である `Elastic IP addresses per Region` クォータ。

これらのサービスクォータは両方とも調整可能で、Service Quotas コンソールから増加をリクエストできます。詳細については、Amazon Virtual Private Cloud ユーザーガイドの「Amazon VPC サービスクォータ」を参照してください。

Amazon EC2 インスタンスでホストされている Amazon ECS ワークロードの場合、awsvpc ネットワークモードを使用するタスクを実行するときは、各 Amazon EC2 インスタンスの最大ネットワークインスタンスの数である `Maximum network interfaces` サービスクォータを考慮してください。このクォータは、1 つのインスタンスに配置できるタスクの数を制限します。クォータを調整することはできず、Service Quotas コンソールでは使用できません。詳細については、Amazon EC2 ユーザーガイドの「各インスタンスタイプのネットワークインターフェイスごとの IP アドレス」を参照してください。

Amazon EC2 インスタンスにアタッチできるネットワークインターフェイスの数は変更できませんが、エラスティックネットワークインターフェイスのトランキング機能を使用して利用可能なネットワークインターフェイスの数を増やすことができます。たとえば `c5.large` インスタンスにはデフォルトでネットワークインターフェイスを最大 3 つアタッチできます。このインスタンスのプライマリネットワークインターフェイスも、1 個としてカウントされます。そのため、このインスタンスに追加で 2 個のネットワークインターフェイスをアタッチできます。awsvpc ネットワークモードを使用する各タスクにはネットワークインターフェイスが必要なため、通常このインスタンスタイプでは、これらのタスクを 2 つのみ実行できます。これにより、クラスターの容量が十分に活用されない可能性があります。エラスティックネットワークインターフェイスでトランキングを有効にすると、ネットワークインターフェイスの密度を上げて、各インスタンスにより多くのタスクを配置できます。トランキングをオンにすると、1 つの `c5.large` インスタンスに最大 12 のネットワークインターフェースを設定できます。インスタンスはプライマリネットワークインターフェイスを持

ち、Amazon ECS は「トランク」ネットワークインターフェイスを作成し、アタッチします。その結果、この構成では、デフォルトの 2 つのタスクではなく、10 のタスクをインスタンスで実行できます。詳細については、「Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす」を参照してください。

エラスティックネットワークインターフェイス API のスロットリング

awsvpc ネットワークモードを使用するタスクを実行する場合、Amazon ECS は次の Amazon EC2 API に依存します。これらの API にはそれぞれ異なる API スロットリングがあります。詳細については、Amazon EC2 API リファレンスの「Amazon EC2 API におけるリクエストのスロットリング」を参照してください。

- CreateNetworkInterface
- AttachNetworkInterface
- DetachNetworkInterface
- DeleteNetworkInterface
- DescribeNetworkInterfaces
- DescribeVpcs
- DescribeSubnets
- DescribeSecurityGroups
- DescribeInstances

エラスティックネットワークインターフェイスのプロビジョニングワークフロー中に Amazon EC2 API コールがスロットリングされた場合、Amazon ECS サービススケジューラは自動的にエクスポネンシャルバックオフを行って再試行します。これらの自動廃止により、タスクの起動が遅れ、デプロイ速度が遅くなることがあります。API スロットリングが発生すると、サービスイベントメッセージにメッセージ `Operations are being throttled. Will try again later.` が表示されます。Amazon EC2 API でスロットリングが継続的に発生する場合は、API のスロットリング制限を引き上げる方法について サポート までお問い合わせください。スロットリングエラーの監視とトラブルシューティングの詳細については、「スロットリング問題の処理」を参照してください。

AWS Cloud Map

Amazon ECS サービス検出と Service Connect では、AWS Cloud Map API を使用して Amazon ECS サービスの名前空間を管理します。サービスに多数のタスクがある場合は、以下の推奨事項を考慮してください。

AWS Cloud Map Service Quotas

Amazon ECS サービスがサービス検出または Service Connect を使用するように設定されている場合、サービスの最大タスク数である `Tasks per service` クォータは、そのサービスの最大インスタンス数である AWS Cloud Map `Instances per service` サービスクォータの影響を受けます。特に、AWS Cloud Map サービスクォータにより、実行できるインスタンスの数は、サービスあたり最大 1,0000 インスタンスに減少します。AWS Cloud Map のクォータは変更できません。詳細については、「AWS Cloud Map のサービスクォータ」を参照してください。

AWS Cloud Map API スロットリング

Amazon ECS はユーザーに代わってListInstances、GetInstancesHealthStatus、RegisterInstance、および DeregisterInstance AWS Cloud Map API を呼び出します。これらはサービス検出を支援し、タスクを起動するとヘルスチェックを実行します。多数のタスクを伴うサービス検出を使用する複数のサービスを同時にデプロイすると、AWS Cloud Map API のスロットリング制限を超える可能性があります。この場合、Amazon ECS サービスのイベントメッセージに次のようなメッセージが表示される場合があります: Amazon ECS サービスイベントで `Operations are being throttled. Will try again later` が発生しました。デプロイとタスクの起動速度が遅くなっています。AWS Cloud Map には、これらの API のスロットリング制限は記録されていません。これらのスロットリングが発生した場合は、API のスロットリング制限を引き上げる方法について サポート までお問い合わせください。これらのスロットリングエラーの監視とトラブルシューティングに関する推奨事項については、「Amazon ECS のスロットリングに関する問題を処理する」を参照してください。

Amazon ECS API リファレンス

AWS Management Console と AWS Command Line Interface (AWS CLI) の他に、Amazon ECS には API も用意されています。API を使用して、Amazon ECS リソースを管理するタスクを自動化できます。

- Amazon ECS リソースごとの API オペレーションのリストについては、「Amazon ECS リソースごとのアクション」を参照してください。
- API オペレーションのアルファベット順リストについては、「アクション」を参照してください。
- データ型のアルファベット順リストについては、「データ型」を参照してください。
- 共通クエリパラメータのリストについては、「共通パラメータ」を参照してください。
- エラーコードの説明については、「共通エラー」を参照してください。

AWS CLI の詳細については、「Amazon ECS の AWS Command Line Interface リファレンス」を参照してください。

ドキュメント履歴

以下の表は、Amazon Elastic Container Service デベロッパーガイドの主な更新や新機能を示しています。また、お客様からいただいたフィードバックに対応するために、ドキュメントを頻繁に更新しています。

変更	説明	日付
短い ARN 形式から長い ARN 形式へのサービス移行をサポート。	短い ARN 形式のサービスを長い ARN 形式のパケットに移行できるようになりました。詳細については、「Migrate an Amazon ECS short service ARN to a long ARN」を参照してください。	2025 年 2 月 13 日
Amazon ECS と Fargate での 3 種類のフォールトインジェクションをサポート。	Amazon ECS と Fargate で、ネットワークブラックホールポート、ネットワークレイテンシー、ネットワークパケット損失フォールトインジェクションが利用可能になりました。詳細については、「Use AWS Fault Injection Service to test your Amazon ECS workloads」を参照してください。	2024 年 12 月 19 日
オブザーバビリティが強化された CloudWatch Container Insights のサポート。	オブザーバビリティが強化された CloudWatch Container Insights を使用できます。詳細については、「Container Insights を使用して Amazon ECS コンテナをモニタリングする」を参照してください。	2024 年 12 月 2 日
予測スケーリングのサポート。	予測スケーリングを使用すると、将来のニーズを予測し、必要に応じてサービスのタスクをプロアクティブに増やすことができます。詳細については、「履歴パターンを使用して予測スケーリングで CloudWatch サービスをスケールする」を参照してください。	2024 年 11 月 21 日
サービスの再調整のサポート。	Amazon ECS で、サービスタスクのバランスをアベイラビリティーゾーン間で自動調整できるようになりました。詳細については、「アベイラビリティーゾーン間での Amazon ECS サービスの調整」を参照してください。	2024 年 11 月 19 日

変更	説明	日付
コンテナイメージタグをイメージダイジェストに解決する設定のサポート。	サービスの一部であるタスクで、コンテナごとにコンテナイメージタグをダイジェストに解決する設定が可能になりました。詳細については、コンテナイメージの解決および`versionConsistency`を参照してください。	2024 年 11 月 19 日
新しい `AmazonECSInfrastructureRolePolicyForVpcLattice` IAM ポリシーの追加	`AmazonECSInfrastructureRolePolicyForVpcLattice` ポリシーは、ユーザーに代わって Amazon ECS ワークロードの VPC Lattice 機能を管理するために必要な他の AWS サービスリソースへのアクセスを提供します。	2024 年 11 月 18 日
VPC Lattice が Amazon ECS サービスで利用できるようになりました。	VPC Lattice を使用して、サービス間の接続、セキュリティ、およびオブザーバビリティを標準化できるようになりました。詳細については、「Amazon VPC Lattice を使用して Amazon ECS サービスを接続、監視、保護する」を参照してください。	2024 年 11 月 18 日
サービスデプロイとサービスリビジョンを使用するサービス履歴のサポート。	サービスデプロイとサービスリビジョンを使用してデプロイ履歴を表示できます。詳細については、「Amazon ECS サービスデプロイを使用してサービス履歴を表示する」と「Amazon ECS サービスリビジョン」を参照してください。	2024 年 10 月 30 日
Windows オペレーティングシステムを使用する EC2 起動タイプの Amazon EBS ボリュームのサポート。	Amazon ECS は、Windows の EC2 インスタンスで実行されているタスクにアタッチされた Amazon EBS ボリュームをサポートします。詳細については、「Amazon ECS での Amazon EBS ボリュームの使用」を参照してください。	2024 年 10 月 24 日

変更	説明	日付
AmazonECSInfrastructureRolePolicyForVolumes へのアクセス許可を追加する。	AmazonECSInfrastructureRolePolicyForVolumes ポリシーが更新され、お客様がスナップショットから Amazon EBS ボリュームを作成できるようになりました。詳細については、「AmazonECSInfrastructureRolePolicyForVolumes」を参照してください。	2024 年 10 月 10 日
Fargate Spot が Linux ARM で利用可能。	Linux ARM での Fargate Spot のサポートが Amazon ECS に追加されました。	2024 年 9 月 6 日
Amazon ECS タスク内の個々のコンテナのコンテナ再起動ポリシー。	タスク定義で定義されている重要なコンテナと重要でないコンテナの再起動ポリシーを有効にして、一時的な障害を迅速に克服し、タスクの可用性を維持できます。詳細については、「コンテナ再起動ポリシーを使用して Amazon ECS タスク内の個々のコンテナを再起動する」を参照してください。	2024 年 8 月 15 日
アクセス許可を the section called “AmazonECS_FullAccess” に追加しました。	AmazonECS_FullAccess ポリシーが更新され、ecsInfrastructureRole という名前のロールの IAM ロールの iam:PassRole アクセス許可が追加されました。これは、AWS Management Console によって作成されたデフォルトの IAM ロールで、Amazon ECS が ECS タスクにアタッチされた Amazon EBS ボリュームを管理できる ECS インフラストラクチャロールとして使用されることを目的としています。	2024 年 8 月 13 日
Amazon Linux 2023、CentOS Stream 9、Fedora 40、Ubuntu 24 のサポートが ECS Anywhere に追加されました	Amazon Linux 2023、CentOS Stream 9、Fedora 40、Ubuntu 24 オペレーティングシステムのサポートが ECS Anywhere に追加されました。詳細については、「サポートされるオペレーティングシステムとシステムアーキテクチャ」を参照してください。	2024 年 7 月 23 日

変更	説明	日付
ローリングアップデート (ECS) デプロイタイプを使用するサービスのコンテナイメージ解決。	ローリングアップデートデプロイコントローラーを使用するサービス内のすべてのタスクで同じコンテナイメージが使用されるように、Amazon ECS はタスク定義で指定されたコンテナイメージ名とイメージタグをコンテナイメージダイジェストに解決します。詳細については、「コンテナイメージの解決」を参照してください。	2024 年 7 月 10 日
Debian 11 と Debian 12 のサポートが ECS Anywhere に追加されました	Debian 11 と Debian 12 オペレーティングシステムのサポートが ECS Anywhere に追加されました。詳細については、「サポートされるオペレーティングシステムとシステムアーキテクチャ」を参照してください。	2024 年 3 月 28 日
Fargate サポートの Linux コンテナ用 gMSA	Amazon ECS は、グループマネージドサービスアカウント (gMSA) と呼ばれる特殊なサービスアカウントを使用して、Fargate 上の Linux コンテナの Active Directory 認証をサポートします。詳細については、「Fargate の Linux コンテナに gMSA を使用する」を参照してください。	2024 年 3 月 5 日
タスクにアタッチされた Amazon EBS ボリュームに CloudWatch メトリクスが追加されました	Amazon ECS は、Amazon EBS ボリュームがアタッチされているタスクの、Amazon EBS ストレージの使用状況に関する CloudWatch メトリクスを発行できるようになりました。詳細については、「Amazon ECS CloudWatch メトリクス」を参照してください。	2024 年 2 月 8 日
Service Connect TLS	Service Connect で TLS を使用できるようになりました。	2024 年 1 月 22 日
Service Connect TLS マネージドポリシー	新しく、AmazonECSInfrastructureRolePolicyForServiceConnectTransportLayerSecurity ポリシーを追加しました。	2024 年 1 月 22 日

変更	説明	日付
Service Connect タイムアウト設定の更新	Service Connect のタイムアウト設定を更新できるようになりました。これには、2 つのオプションパラメータ `idleTimeout` 、`perRequestTimeout` が含まれます。	2024 年 1 月 22 日
Amazon ECS マネージドインスタンスドレイニング	Amazon ECS マネージドインスタンスドレイニングを使用すると、Amazon ECS インスタンスの正常な終了が容易になります。	2024 年 1 月 19 日
ECS Anywhere に Ubuntu 22 サポートが追加されました	Ubuntu 22 オペレーティングシステムのサポートが ECS Anywhere に追加されました。詳細については、「サポートされるオペレーティングシステムとシステムアーキテクチャ」を参照してください。	2024 年 1 月 16 日
`AmazonECSInfrastructureRolePolicyForVolumes` IAM ポリシーを追加する	`AmazonECSInfrastructureolePolicyForVolumes` が追加されました。このポリシーにより、Amazon ECS が AWS API コールを行い、Amazon ECS ワークロードに関連付けられた Amazon EBS ボリュームを管理するために必要な権限が付与されます。	2024 年 1 月 11 日
Amazon ECS タスク用の Amazon EBS データボリューム	スタンドアロンの Amazon ECS タスク、またはタスクのデプロイ時に ECS サービスによって管理されるタスクにアタッチするために、タスクごとに 1 つの Amazon EBS データボリュームを設定できます。デプロイ時にボリュームを設定すると、特定のボリュームタイプや設定に限定されず、再利用可能なタスク定義を作成できます。Amazon EBS ボリュームは、データ集約型のコンテナ化されたワークロード向けに、可用性に優れ、費用対効果が高く、耐久性があり、高性能なブロックストレージを提供します。	2024 年 1 月 11 日
Amazon ECS 従来型コンソールのサポートが終了しました	Amazon ECS コンソールのサポートが終了しました	2023 年 12 月 4 日

変更	説明	日付
ポリシーの更新	AmazonECSServiceRolePolicy マネージド IAM ポリシーでは、新しい events アクセス許可が更新され、autoscaling 、および autoscaling-plans アクセス許可が追加、更新されました。	2023 年 12 月 4 日
Runtime Monitoring サポート	Runtime Monitoring を使用すると、Amazon ECS ワークロードを監視して、悪意のある動作や不正な動作を識別できます。詳細については、「Runtime Monitoring」を参照してください。	2023 年 11 月 26 日
ポリシーの更新	AmazonECSServiceRolePolicy マネージド IAM ポリシーが AWS Cloud Map DiscoverInstancesRevision API へのアクセスを許可するように更新されました。	2023 年 10 月 4 日
AWS Fargate タスクの廃止設定	Fargate タスクが廃止されるまでの待機時間を設定できます。詳細については、「AWS Fargate タスクのメンテナンス」を参照してください。	2023 年 9 月 5 日
AWS Fargate での追加のタスク定義パラメータ	AWS Fargate は、Linux プラットフォームバージョン 1.4.0 で pidMode および systemControls のサポートを追加します。詳細については、「タスク定義」を参照してください。	2023 年 8 月 9 日
Amazon ECS コンソールのタスク定義ページの再設計	Amazon ECS コンソールのタスク定義ページが再設計され、オプションが追加されました。詳細については、「コンソールを使用したタスク定義の作成」を参照してください。	2023 年 7 月 26 日

変更	説明	日付
Fargate は Seekable OCI インデックスによる遅延読み込みをサポートしています	AWS Fargate は Seekable OCI (SOCI) インデックスを導入しています。SOCI では、コンテナは起動前にイメージプルに数秒しかかからないため、イメージがバックグラウンドでダウンロードされている間、環境のセットアップとアプリケーションのインスタンス化に時間を割けます。詳細については、「Lazy loading container images using Seekable OCI (SOCI)」を参照してください。	2023 年 7 月 17 日
Linux と Windows での gMSA のサポートが改善されました	タスク定義には、Linux および Windows 用の gMSA 用の新しい `credentialSpecs` フィールドがあります。Windows 上のドメインレス gMSA の新しい完全なチュートリアルが追加されました。「チュートリアル: AWS CLI を使用したドメインレス gMSA での Windows コンテナの使用」を参照してください。詳細については、「Linux コンテナ向け gMSAs を使用する」と「Windows コンテナ向けの gMSAs の使用」を参照してください。	2023 年 7 月 14 日
ECS エージェントバージョンのドキュメントが改善されました	Amazon ECS エージェントバージョンのドキュメントが更新されました。Amazon ECS コンテナエージェントの最新バージョンでは、Docker の `v20.10.13` バージョン以降を使用することをお勧めします。リリースされたバージョンとエージェントの変更は GitHub で確認できます。詳細については、「Amazon ECS Linux コンテナエージェントのバージョン」を参照してください。	2023 年 6 月 20 日
Fargate ARM64 サポートの利用可能なリージョンを更新	Fargate ARM64 サポートの利用可能なリージョンを更新しました。詳細については、「考慮事項」を参照してください。	2023 年 6 月 19 日

変更	説明	日付
クラスターの自動スケーリングに関するドキュメントの改善	Amazon EC2 Auto Scaling の Amazon ECS スケーリングに関するドキュメントでは、精度と読みやすさが大幅に向上しています。詳細については、「Amazon ECS のクラスター自動スケーリング」を参照してください。	2023 年 5 月 4 日
リソース作成のタグ付け認可。	ユーザーには、リソースを作成するアクションの許可が必要です (`ecsCreateCluster` など)。リソースを作成し、そのリソースのタグを指定すると、AWS は、追加の認可を実行して、タグを作成するための許可があることを検証します。詳細については、「タグ付け権限」と「作成時にリソースにタグを付ける権限の付与」を参照してください。	2023 年 4 月 18 日
EC2 での Linux コンテナの gMSA のサポート	gMSA を使用して、EC2 での Linux コンテナ用に、Active Directory に対して認証できます。詳細については、「Linux コンテナに gMSA を使用する」を参照してください。	2023 年 4 月 14 日
AWS Fargate での Windows コンテナのエフェメラルストレージのサポート	AWS Fargate での Windows コンテナにエフェメラルストレージを使用できます。詳細については、「Fargate タスクストレージ」を参照してください。	2023 年 4 月 14 日
タスクレベルの CUR データの AWS Cost Management サポート	コストと使用状況レポートで、タスクレベルのコストとリソースの使用状況をオンにできます。これにより、AWS Fargate と EC2 で実行されるタスクについてのコスト配分データの分割が追加されます。詳細については、「タスクレベルのコストと使用状況レポート」を参照してください。	2023 年 4 月 12 日
Amazon Linux 2023 Amazon ECS 最適化 AMI	ワークロードを Amazon Linux 2023 Amazon ECS 最適化 AMI にデプロイできます。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2023 年 4 月 10 日

変更	説明	日付
AWS Fargate 連邦情報処理標準 (FIPS) 140	連邦情報処理標準 (FIPS) 140 に準拠した態様で、AWS Fargate での Amazon ECS でワークロードをデプロイできます。詳細については、「AWS Fargate 連邦情報処理標準 (FIPS-140)」を参照してください。	2023 年 4 月 10 日
タスク定義の削除	タスク定義は、Amazon ECS コンソール、SDK、および AWS CLI を使用して削除できます。詳細については、「コンソールを使用したタスク定義リビジョンの削除」および「タスク定義」を参照してください。	2023 年 2 月 24 日
Compute Optimizer 内の AWS Fargate サービスについての推奨事項	AWS Compute Optimizer は、AWS Fargate の Amazon ECS サービスで実行中のタスクの使用率に基づいて、タスクとコンテナサイズに関する推奨事項を生成します。詳細については、「Fargate の Amazon ECS サービスに関する推奨事項の表示」を参照してください。	2023 年 1 月 27 日
Amazon ECS コンソール	新しい Amazon ECS コンソールが、デフォルトのコンソールになりました。詳細については、「新しい Amazon Elastic Container Service コンソール」を参照してください。	2023 年 1 月 19 日
`AmazonECS_FullAccess` IAM ポリシーが更新されました	`AmazonECS_FullAccess` IAM ポリシーが更新され、作成時にロードバランサーにタグを追加する権限が含まれるようになりました。詳細については、「AmazonECS_FullAccess」を参照してください。	2023 年 1 月 4 日
CloudWatch アラームを使用して Amazon ECS サービスのデプロイ障害を検出する	指定された CloudWatch アラームが ALARM 状態になったことを検出したとき、デプロイが失敗に設定されるように Amazon ECS を設定できます。詳細については、「the section called “ローリング更新デプロイ”」を参照してください。	2022 年 12 月 19 日

変更	説明	日付
コンテナポートマッピングのサポート	動的にマッピングされたホストポート範囲にバインドされるコンテナポートの番号範囲を設定できます。詳細については、「the section called “ポートマッピング”」を参照してください。	2022 年 12 月 15 日
Amazon ECS Service Connect の一般提供	この機能により、Amazon ECS サービスデプロイによって制御されるサービス検出とサービスメッシュが追加されます。詳細については、「the section called “Service Connect”」を参照してください。	2022 年 11 月 27 日
新しい Amazon ECS コンソールエクスペリエンスでは、タスク定義の操作が更新されました。	新しい Amazon ECS コンソールエクスペリエンスでは、タスク定義に JSON エディタが使用できるようになりました。詳細については、「the section called “コンソールを使用したタスク定義の作成”」を参照してください。	2022 年 10 月 27 日
新しい Amazon ECS コンソールエクスペリエンスでは、タスク定義の操作が更新されました。	新しい Amazon ECS コンソールエクスペリエンスでは、タスク定義に JSON エディタが使用できるようになりました。詳細については、「the section called “コンソールを使用したタスク定義の作成”」を参照してください。	2022 年 10 月 27 日
新しい Amazon ECS コンソールのエクスペリエンスが更新されました	新しい Amazon ECS コンソールエクスペリエンスでは、サービスとタスクのパラメータが追加され、更新されています。詳細については、the section called “サービスの作成”およびthe section called “タスクとしてのアプリケーションの実行”を参照してください。	2022 年 10 月 7 日
タスクメタデータエンドポイントバージョン 4 の新しい情報	タスクメタデータのエンドポイントバージョン 4 には、VPC ID とサービス名が含まれるようになりました。詳細については、「the section called “タスクメタデータエンドポイントバージョン 4”」を参照してください。	2022 年 10 月 7 日

変更	説明	日付
新しいタスク定義サイズ	Fargate の Amazon ECS は 8 個の vCPU と 16 個の vCPU タスクサイズをサポートするようになりました。詳細については、「the section called “タスクサイズ”」を参照してください。	2022 年 9 月 16 日
ECS CLI ページがアーカイブされました	ECS CLI のドキュメントがアーカイブされました。コマンドラインツールのニーズに合わせて AWS Copilot を使用することをお勧めします。詳細については、「AWS Copilot コマンドラインインターフェイスを使用した Amazon ECS リソースの作成」を参照してください。	2022 年 9 月 15 日
Fargate クォータ	Fargate は、タスク数ベースのクォータから vCPU ベースのクォータに移行しています。詳細については、「the section called “AWS Fargate Service Quotas”」を参照してください。	2022 年 9 月 8 日
Amazon EC2 Auto Scaling でのウォームプールのサポート	Amazon EC2 Auto Scaling のウォームプールを使用して、アプリケーションのスケールアウトを高速化し、コストを削減できるようになりました。詳細については、「Amazon ECS Auto Scaling グループ用に事前初期化されたインスタンスを設定する」を参照してください。	2022 年 3 月 23 日
ECS Anywhere での Windows インスタンスのサポート。	ECS Anywhere は Windows インスタンスをサポートするようになりました。詳細については、「外部起動タイプ用の Amazon ECS クラスター」を参照してください。	2022 年 3 月 3 日
外部インスタンスに対する ECS Exec サポートを追加	外部インスタンスに対して ECS Exec が対応するようになりました。詳細については、「ECS Exec を使用して Amazon ECS コンテナをモニタリングする」を参照してください。	2022 年 1 月 24 日

変更	説明	日付
新しい Amazon ECS コンソールのエクスペリエンスが更新されました	新しい Amazon ECS コンソールエクスペリエンスでは、クラスターの作成と削除、タスク定義の更新、およびタスク定義の登録解除がサポートされています。詳細については、「Fargate 起動タイプ用の Amazon ECS クラスターを作成する」、「Amazon ECS クラスターを削除する」、「コンソールを使用した Amazon ECS タスク定義の更新」、および「新しいコンソールを使用した Amazon ECS タスク定義リビジョンの登録解除」を参照してください。	2021 年 12 月 8 日
新しい Amazon ECS コンソールのエクスペリエンスが更新されました	新しい Amazon ECS コンソールエクスペリエンスでは、タスク定義の作成がサポートされています。詳細については、「コンソールを使用した Amazon ECS タスク定義の作成」を参照してください。	2021 年 11 月 23 日
Amazon ECS は、Linux 用の 64 ビット ARM アーキテクチャをサポートしています。	Amazon ECS は、Linux オペレーティングシステム 64 ビット ARM CPU アーキテクチャをサポートしています。詳細については、「the section called “64 ビット ARM ワークロードでのタスク定義”」を参照してください。	2021 年 11 月 23 日
fluentd log-driver-buffer-limit オプションに対する Amazon ECS のサポート	Amazon ECS は、fluentd `log-driver-buffer-limit` オプションをサポートしています。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。	2021 年 11 月 22 日
Amazon ECS 最適化 Linux AMI のビルドスクリプト	Amazon ECS は、Amazon ECS に最適化された AMI の Linux バリアントの構築に使用するビルドスクリプトをオープンソース化しました。詳細については、「Amazon ECS 最適化 Linux AMI のビルドスクリプト」を参照してください。	2021 年 11 月 19 日
コンテナインスタンスのヘルス	Amazon ECS は、コンテナインスタンスのヘルスモニタリングのサポートを追加します。詳細については、「Amazon ECS コンテナインスタンスの正常性をモニタリングする」を参照してください。	2021 年 11 月 10 日

変更	説明	日付
Windows Amazon ECS Exec のサポート	Amazon ECS Exec は、Windows をサポートしています。詳細については、「ECS Exec を使用して Amazon ECS コンテナをモニタリングする」を参照してください。	2021 年 11 月 1 日
Fargate での Windows コンテナのサポート。	Amazon ECS は、Fargate で Windows コンテナをサポートします。詳細については、「Fargate Windows プラットフォームバージョンの変更ログ」を参照してください。	2021 年 10 月 28 日
Amazon ECS Anywhere での外部インスタンスの GPU サポート	Amazon ECS は、外部インスタンスで実行するタスクのタスク定義で GPU 要件の指定をサポートしています。詳細については、GPU ワークロード向けの Amazon ECS タスク定義およびAmazon ECS クラスターに外部インスタンスを登録するを参照してください。	2021 年 10 月 8 日
Windows のawsvpcネットワークモードのサポート	Amazon ECS が Windows で awsvpc ネットワークモードをサポートします。詳細については、「Amazon ECS タスクにネットワークインターフェイスを割り当てる」を参照してください。	2021 年 7 月 15 日
Bottlerocket の一般提供	Amazon ECS は、Bottlerocket オペレーティングシステムの Amazon ECS に最適化された AMI バリアントを AMI として提供します。詳細については、「Amazon ECS 最適化 Bottlerocket AMI」を参照してください。	2021 年 6 月 30 日
Amazon ECS のスケジュールされたタスクの更新	Amazon EventBridge は、Amazon ECS のスケジュールされたタスクをトリガーするルールを作成するときに、追加のパラメータのサポートを追加しました。	2021 年 6 月 25 日
Amazon ECS の AWS 管理ポリシー	Amazon ECS は、サービスにリンクされたロールのAWS 管理ポリシーのドキュメントを追加しました。詳細については、「Amazon Elastic Container Service に関する AWS 管理ポリシー」を参照してください。	2021 年 6 月 8 日

変更	説明	日付
AWS CDK の開始方法	Amazon ECS でAWS CDKを使用するための入門ガイドを追加しました 詳細については、「AWS CDK を使用した Amazon ECS リソースの作成」を参照してください。	2021 年 5 月 27 日
Amazon ECS Anywhere	Amazon ECS は、オンプレミスのサーバーまたは仮想マシン (VM) をクラスターに登録するためのサポートを追加しました。詳細については、「外部起動タイプ用の Amazon ECS クラスター」を参照してください。	2021 年 5 月 25 日
Amazon ECS に最適化された Windows Server 20H2 Core AMI	Amazon ECS では、Windows サーバー 20H2 コア用の新しい Windows Amazon ECS 最適化 AMI バリアントのサポートが追加されました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2021 年 4 月 19 日
Amazon ECS Exec	Amazon ECS は、ECS Exec という新しいデバッグツールをリリースしました。詳細については、「ECS Exec を使用して Amazon ECS コンテナをモニタリングする」を参照してください。	2021 年 3 月 15 日
VPC エンドポイントポリシーのサポート	Amazon ECS は Amazon VPC エンドポイントポリシーをサポートするようになりました。詳細については、「Amazon ECS 用の VPC エンドポイントポリシーの作成」を参照してください。	2021 年 1 月 11 日
新しいコンソールエクスペリエンス	Amazon ECSは、サービスの作成もしくは更新、またはスタンドアロンタスクの実行をサポートする新しいコンソールエクスペリエンスをリリースしました。詳細については、コンソールを使用した Amazon ECS サービスの作成およびAmazon ECS タスクとしてのアプリケーションの実行を参照してください。	2020 年 12 月 28 日

変更	説明	日付
キャパシティープロバイダーの更新	Amazon ECS は既存の Auto Scaling グループキャパシティープロバイダーの更新をサポートするようになりました。	2020 年 11 月 23 日
ECS は、Windows タスク用の Amazon FSx for Windows File Server をサポートするようになりました。	Amazon ECS は Windows タスク定義で Amazon FSx for Windows File Server ボリュームを指定するサポートを追加しました。詳細については、「Amazon ECS での FSx for Windows File Server ボリュームの使用」を参照してください。	2020 年 11 月 11 日
VPC デュアルスタックモードのサポートを追加	Amazon ECS は、IPv6 アドレスのサポートを提供する awsvpc ネットワークモードを使用するタスクで VPC をデュアルスタックモードで使用するためのサポートを追加しました。詳細については、「デュアルスタックモードでの VPC の使用」を参照してください。	2020 年 11 月 5 日
タスクメタデータエンドポイント v4 更新	Amazon ECS はタスクメタデータエンドポイント v4 出力にメタデータを追加しました。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。	2020 年 11 月 5 日
Local Zones と Wavelength Zone のサポート	Amazon ECS では、Local Zones と Wavelength Zone のワークロードのサポートが追加されました。詳細については、「共有サブネット、Local Zones、および Wavelength Zones の Amazon ECS アプリケーション」を参照してください。	2020 年 9 月 4 日
Bottlerocket AMI の Amazon ECS バリアント	Bottlerocket は Linux ベースのオープンソースのオペレーティングシステムで、コンテナを実行するために AWS によって専用に構築されています。Amazon ECS コンテナインスタンスを起動するときに使用できる AMI として、Bottlerocket オペレーティングシステムの Amazon ECS 最適化された AMI バリアントが用意されています。詳細については、「Amazon ECS 最適化 Bottlerocket AMI」を参照してください。	2020 年 8 月 31 日

変更	説明	日付
ネットワークレートの統計情報用に更新されたタスクメタデータエンドポイントバージョン 4	タスクメタデータエンドポイントバージョン 4 が更新され、コンテナエージェントのバージョン `1.43.0` 以上を実行している Amazon EC2 インスタンスでホストされる `awsvpc` または `bridge` ネットワークモードを使用する Amazon ECS タスクのネットワークレート統計が提供されました。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。	2020 年 8 月 10 日
Fargate 使用状況メトリクス	AWS Fargate は、Fargate·と·Fargate·Spot リソースのアカウント使用状況を可視化する CloudWatch 使用状況メトリクスを提供します。詳細については、「使用状況メトリクス」を参照してください。	2020 年 8 月 3 日
AWS Copilot バージョン 0.1.0	ローカル開発環境からAmazon ECS のコンテナ化されたアプリケーションのモデル化、作成、リリース、管理を簡素化するハイレベルのコマンドを提供する新しいAWSコパイロット CLI が公開されました。詳細については、「AWS Copilot コマンドラインインターフェイスを使用した Amazon ECS リソースの作成」を参照してください。	2020 年 7 月 9 日
AWS Fargate プラットフォームバージョンの廃止スケジュール	Fargateプラットフォームバージョンの廃止スケジュールが追加されました。詳細については、「AWS Fargate Linux プラットフォームバージョンの廃止」を参照してください。	2020 年 7 月 8 日
AWS Fargateリージョンの拡大	Amazon ECS onAWS Fargate が欧州 (ミラノ) リージョンに拡大しました。	2020 年 6 月 25 日
Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI がリリースされました	Amazon ECS は、Inferentia ワークロード用に Amazon ECS 最適化 Amazon Linux 2 (Neuron) AMI をリリースしました。 詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2020 年 6 月 24 日

変更	説明	日付
キャパシティープロバイダーの削除に関するサポートを追加	Auto Scaling グループキャパシティープロバイダーの削除に関するサポートを Amazon ECS に追加しました。	2020 年 6 月 11 日
AWS Fargateプラットフォームバージョン 1.4.0 の更新	2020 年 5 月 28 日以降、プラットフォームバージョン 1.4.0 を使用して起動されるすべての新しいFargateタスクには、AWS Fargateマネージド 暗号化キーを使用し AES-256 暗号化アルゴリズムで暗号化された 20 GB のエフェメラルストレージが搭載されます。詳細については、「Amazon ECS 向けの Fargate タスクエフェメラルストレージ」を参照してください。	2020 年 5 月 28 日
環境変数ファイルのサポート	タスク定義で環境変数ファイルを指定するためのサポートが追加されました。これにより、環境変数をコンテナに一括追加できます。詳細については、「個々の環境変数を Amazon ECS コンテナに渡す」を参照してください。	2020 年 5 月 18 日
AWS Fargateリージョンの拡大	AWS Fargate with Amazon ECS がアフリカ (ケープタウン) リージョンに拡大しました。	2020 年 5 月 11 日
サービスクォータが更新されました	次のサービスクォータが更新されました。 • アカウントあたりのクラスターが 2,000 から 10,000 に引き上げられました。 詳細については、「Amazon ECS の Service Quotas」を参照してください。	2020 年 4 月 17 日

変更	説明	日付
AWS Fargate プラットフォームバージョン 1.4.0	AWS Fargate プラットフォームバージョン 1.4.0 がリリースされました。このバージョンには、次の機能が含まれます: • 永続的なタスクストレージとしてAmazon EFS ファイルシステムボリュームを使用するサポートを追加しました。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。 • エフェメラルタスクストレージを 20 GB に増加しました。詳細については、「Amazon ECS 向けの Fargate タスクエフェメラルストレージ」を参照してください。 • タスクとの間のネットワークトラフィック動作を更新しました。プラットフォームバージョン 1.4 以降、すべての Fargate タスクは単一の Elastic Network Interface (タスク ENI と呼ばれる) を受け取り、すべてのネットワークトラフィックは VPC 内でこの ENI を通過し、VPC フローログを通じて表示されます。詳細については、「Fargate 起動タイプの Amazon ECS タスクのネットワークオプション」を参照してください。 • タスク ENI は、ジャンボフレームのサポートを追加しています。ネットワークインターフェイスは、最大転送単位 (MTU) で設定されます。MTU は、1 つのフレームに収まるペイロードの最大サイズです。MTU が大きいほど、1 つのフレーム内に収まるアプリケーションのペイロードが増えるため、フレームあたりのオーバーヘッドが減少し、効率が向上します。ジャンボフレームをサポートすると、オーバーヘッドが減ります。タスクと転送先との	2020 年 4 月 8 日

変更	説明	日付
	ネットワークパスでジャンボフレームをサポートすると、VPC 内に残っているすべてのトラフィックなどのオーバーヘッドが軽減されます。 • CloudWatch Container Insights には、Fargate タスクのネットワークパフォーマンスメトリクスが含まれます。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。 • タスクメタデータエンドポイント v4 のサポートを追加しました。これにより、タスクのネットワーク統計情報や、タスクが実行されているアベイラビリティーゾーンなど、Fargate タスクに関する追加情報が提供されます。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。 • コンテナの定義に SYS_PTRACE Linux パラメータのサポートを追加しました。詳細については、「Linux パラメータ」を参照してください。 • Fargateコンテナエージェントは、Amazon ECS コンテナエージェントの使用をすべての Fargate タスクに置き換えます。この変更は、タスクの実行方法には影響しません。 • コンテナランタイムは Docker の代わりに Containerd を使用するようになりました。この変更は、タスクの実行方法には影響しません。コンテナランタイムで発生するいくつかのエラーメッセージは、より一般的な内容になり、Docker には言及されなくなります。	

変更	説明	日付
	詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。	
タスクボリュームに対するAmazon EFS ファイルシステムのサポート	Amazon EFS ファイルシステムは、Amazon ECS タスクと Fargate タスクの両方でデータボリュームとして使用できます。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。	2020 年 4 月 8 日
Amazon ECS タスクメタデータエンドポイントバージョン 4	Amazon ECS コンテナエージェントバージョン 1.39.0 および Fargate プラットフォームバージョン 1.4.0 以降、`ECS_CONTAINER_METADATA_URI_V4` という環境変数がタスク内の各コンテナに挿入されます。タスクメタデータバージョン 4 エンドポイントに対してクエリを実行すると、さまざまなタスクメタデータおよび Docker 統計情報がタスクで利用可能になります。詳細については、「Amazon ECS タスクメタデータエンドポイントバージョン 4」を参照してください。	2020 年 4 月 8 日
環境変数として挿入される特定のバージョンの Secrets Manager シークレットのサポート	特定のバージョンの Secrets Manager のシークレットを使用して機密データを指定するためのサポートが追加されました。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。	2020 年 2 月 24 日
ブルー/グリーンデプロイ用の CodeDeploy デプロイ設定オプションをさらに追加しました	CodeDeploy サービスの Amazon ECS デプロイタイプとして新しい Canary および線形デプロイ設定を追加しました。カスタムのデプロイ設定を定義する機能も使用できます。詳細については、「デプロイ前に Amazon ECS サービスの状態を検証する 」を参照してください。	2020 年 2 月 6 日

変更	説明	日付
efsVolumeConfiguration タスク定義パラメータを追加	`efsVolumeConfiguration` タスク定義パラメータはパブリックプレビューであるため、Amazon ECS タスクで Amazon EFS ファイルシステムを簡単に使用できます。詳細については、「Amazon ECS での Amazon EFS ボリュームの使用」を参照してください。	2020 年 1 月 17 日
Amazon ECS コンテナエージェントのログ記録動作を更新	Amazon ECS コンテナエージェントのログの場所とローテーション動作が更新されました。詳細については、「Amazon ECS コンテナエージェントのログ設定パラメータ」を参照してください。	2020 年 1 月 13 日
Fargate Spot	Amazon ECSでは、Fargate Spot を使用したタスクの実行のサポートが追加されました。詳細については、「Fargate 起動タイプ用の Amazon ECS クラスター」を参照してください。	2019 年 12 月 3 日
クラスターの自動スケーリング	Amazon ECS クラスターの自動スケーリング を使用すると、クラスター内のタスクをスケールする方法をより詳細に制御できます。詳細については、「クラスターの自動スケーリングで Amazon ECS キャパシティーを自動的に管理する」を参照してください。	2019 年 12 月 3 日
クラスターキャパシティープロバイダー	Amazon ECS クラスターキャパシティープロバイダーは、タスクに使用するインフラストラクチャを決定します。詳細については、「Amazon ECS クラスター」を参照してください。	2019 年 12 月 3 日
AWS Outposts でのクラスターの作成	Amazon ECS では、AWS Outposts でのクラスターの作成がサポートされるようになりました。詳細については、「the section called “AWS OutpostsのAmazon Elastic Container Service”」を参照してください。	2019 年 12 月 3 日

変更	説明	日付
サービスアクションイベント	Amazon ECS では、特定のサービスアクションが発生したときにAmazon EventBridge にイベントを送信するようになりました。詳細については、「Amazon ECS サービスアクションイベント」を参照してください。	2019 年 11 月 25 日
Amazon ECS GPU 最適化 AMI は、G4 インスタンスをサポートします。	Amazon ECS では、Amazon ECS GPU 最適化 AMI の使用時に g4 インスタンスタイプファミリーのサポートが追加されました。詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。	2019 年 10 月 8 日
FireLens for Amazon ECS	FireLens for Amazon ECS は一般提供されています。FireLens for Amazon ECS では、タスク定義パラメータを使用して、ログのストレージと分析のために AWS サービスまたはパートナーの宛先にログをルーティングできます。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。	2019 年 9 月 30 日
AWS Fargate リージョンの拡大	AWS Fargate with Amazon ECS は、欧州 (パリ)、欧州 (ストックホルム)、および中東 (バーレーン) の各リージョンに拡大しました。	2019 年 9 月 30 日
Amazon ECS で Elastic Inference を使用する Deep Learning Containers	Amazon ECS では、Amazon Elastic Inference アクセラレーターをコンテナにアタッチして、深層学習推論ワークロードをより効率的に実行できます。	2019 年 9 月 3 日
FireLens for Amazon ECS	FireLens for Amazon ECSはパブリックプレビューです。FireLens for Amazon ECS では、タスク定義パラメータを使用して、ログのストレージと分析のために AWS サービスまたはパートナーの宛先にログをルーティングできます。詳細については、「Amazon ECS ログを AWS サービスまたは AWS Partner に送信する」を参照してください。	2019 年 8 月 30 日

変更	説明	日付
CloudWatch Container Insights	CloudWatch Container Insights の一般提供が開始されました。コンテナ化されたアプリケーションとマイクロサービスのメトリクスとログを収集、集計、要約できます。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。	2019 年 8 月 30 日
コンテナレベルのスワップ設定	Amazon ECS では、Linux コンテナインスタンスのスワップメモリ空間の使用状況をコンテナレベルで制御するサポートが追加されました。コンテナごとのスワップ設定を使用すると、タスク定義内の各コンテナでスワップを有効または無効にできます。有効になっているコンテナでは、使用されるスワップ領域の最大量を制限できます。詳細については、「Amazon ECS のコンテナスワップメモリ空間の管理」を参照してください。	2019 年 8 月 16 日
AWS Fargate リージョンの拡大	AWS Fargate with Amazon ECSは、アジアパシフィック (香港) リージョンに拡大されました。	2019 年 8 月 6 日
Elastic Network Interface のトランキング	ENI トランキング機能用にサポートされている追加の Amazon EC2 インスタンスタイプが追加されました。詳細については、「Amazon ECS コンテナネットワークインターフェイスの増加でサポートされるインスタンス」を参照してください。	2019 年 8 月 1 日
サービスに複数のターゲットグループを登録する	サービス定義で複数のターゲットグループを指定するためのサポートが追加されました。詳細については、「Amazon ECS サービスに複数のターゲットグループを登録する」を参照してください。	2019 年 7 月 30 日
Secrets Manager のシークレットを使用した機密データの指定	Secrets Manager のシークレットを使用して機密データを指定するためのチュートリアルが追加されました。詳細については、「Amazon ECS の Secrets Manager シークレットを使用した機密データの指定」を参照してください。	2019 年 7 月 20 日

変更	説明	日付
CloudWatch Container Insights	Amazon ECS は、CloudWatch Container Insights のサポートを追加しました。詳細については、「オブザーバビリティが強化された Container Insights を使用し、Amazon ECS コンテナを監視する」を参照してください。	2019 年 7 月 9 日
Amazon ECS サービスとタスクセットのリソースレベルのアクセス許可	Amazon ECSは、Amazon ECSサービスとタスクのリソースレベルのアクセス許可のサポートを拡張しました。詳細については、「IAM を使用するAmazon Elastic Container Service」を参照してください。	2019 年 6 月 27 日
新しい Amazon ECS 最適化 AMI に AWS-2019-005 用のパッチが適用されました。	Amazon ECS は AWS-2019-005 で説明されている脆弱性に対応するため、Amazon ECS 最適化 AMI を更新しました。	2019 年 6 月 17 日
Elastic Network Interface のトランキング	Amazon ECS で、Elastic Network Interface (ENI) の密度が高い、サポートされている Amazon EC2 インスタンスタイプを使用したコンテナインスタンスの起動サポートが導入されました。これらのインスタンスタイプを使用し、`awsvpcTrunking` アカウント設定をオプトインすることで、新しく起動されたコンテナインスタンスの ENI の密度が高くなります。これにより、各コンテナインスタンスにより多くのタスクを配置することができます。詳細については、「Amazon ECS Linux コンテナインスタンスのネットワークインターフェイスを増やす」を参照してください。	2019 年 6 月 6 日
AWS Fargateプラットフォームバージョン 1.3.0 の更新	2019 年 5 月 1 日以降、起動されるすべての新しい Fargate タスクでは、`splunk` ログドライバーに加えて`awslogs` ログドライバーをサポートします。詳細については、「ストレージとログ記録」を参照してください。	2019 年 5 月 1 日

変更	説明	日付
AWS Fargateプラットフォームバージョン 1.3.0の更新	2019 年 5 月 1 日以降、起動される新しい Fargate タスクでは、`secretOptions` コンテナ定義パラメータを使用してコンテナのログ設定内の機密データの参照をサポートします。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。	2019 年 5 月 1 日
AWS Fargateプラットフォームバージョン 1.3.0の更新	2019 年 4 月 2 日以降、起動される新しい Fargateタスクでは、機密データをAWS Secrets Manager シークレットまたは AWS Systems Manager パラメータストアのパラメータに保存してコンテナの定義でそれらを参照することにより、コンテナへの機密データの挿入をサポートします。詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。	2019 年 4 月 2 日
AWS Fargate プラットフォームバージョン 1.3.0の更新	2019 年 3 月 27 日以降、発表された新しい Fargate タスクでは、プロキシ設定、コンテナの起動およびシャットダウンの依存関係、コンテナ別の起動および停止のタイムアウト値を定義できる、追加タスク定義パラメータを使用できます。詳細についてはプロキシ設定、コンテナの依存関係、および[コンテナのタイムアウト]を参照してください。	2019 年 3 月 27 日
Amazon ECS外部デプロイタイプの導入	この外部 デプロイタイプでは、Amazon ECS サービスのデプロイプロセスを完全に制御するために、すべてのサードパーティーのデプロイコントローラーを使用できます。詳細については、「サードパーティーのコントローラーを使用して Amazon ECS サービスをデプロイする」を参照してください。	2019 年 3 月 27 日

変更	説明	日付
Amazon ECS の AWS Deep Learning Containers	AWS Deep Learning Containers は、Amazon Elastic Container Service (Amazon ECS) の TensorFlow で、モデルをトレーニングおよび処理するための Docker イメージのセットです。Deep Learning Containers は、TensorFlow、Nvidia CUDA (GPU インスタンス用)、およびインテル MKL (CPU インスタンス用) ライブラリを使用して、最適化された環境を提供し、Amazon ECR で利用できます。詳細については、「Amazon ECS で AWS 深層学習コンテナを使用する」を参照してください。	2019 年 3 月 27 日
Amazon ECS、強化されたコンテナ依存関係管理を導入	Amazon ECS は、コンテナのスタートアップとシャットダウンの依存関係を定義したり、開始と停止のタイムアウト値をコンテナごとに定義したりできる、新たなタスク定義のパラメータを導入します。詳細については、「コンテナの依存関係」を参照してください。	2019 年 3 月 7 日
Amazon ECSでの `PutAccountSettingDefault` APIの導入	Amazon ECS では、`PutAccountSettingDefault` API を導入しました。これにより、ユーザーはアカウントのすべてのユーザーおよびロールに対して、デフォルトの ARN/ID 形式のオプトインステータスを設定できます。以前は、アカウントのデフォルトのオプトインステータスを設定するには、アカウント所有者を使用する必要がありました。 詳細については、「Amazon リソースネーム (ARN) と ID」を参照してください。	2019 年 2 月 8 日

変更	説明	日付
Amazon ECS で GPU ワークロードをサポート	Amazon ECS では、GPU 対応コンテナインスタンスを使用してクラスターを作成できるようにすることで、GPU ワークロードのサポートが導入されました。タスク定義で GPU の必要数を指定でき、ECS エージェントにより物理 GPU がコンテナに固定されます。 詳細については、「GPU ワークロード向けの Amazon ECS タスク定義」を参照してください。	2019 年 2 月 4 日
Amazon ECS のシークレットサポートの拡張	Amazon ECS では、機密データをコンテナに挿入するため、タスク定義で直接 AWS Secrets Manager シークレットを使用するためのサポートを拡大しました。 詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。	2019 年 1 月 21 日
インターフェイス VPC エンドポイント (AWS PrivateLink)	AWS PrivateLinkを搭載したインターフェイスVPCエンドポイントを設定するためのサポートが追加されました。これにより、インターネット、NAT インスタンス、VPN 接続、またはAWS Direct Connect を経由せずに、VPC とAmazon ECS とをプライベートに接続することができます。 詳細については、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。	2018 年 12 月 26 日

変更	説明	日付
AWS Fargate プラットフォームバージョン 1.3.0	以下を含む新しくリリースされたAWS Fargateプラットフォームバージョン: • AWS Systems Manager パラメータストアパラメータを使用して、コンテナに機密データを挿入する機能のサポートが追加されました。 詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。 • Fargateタスクのタスクリサイクルが追加されました。これは、Amazon ECS サービスの一部であるタスクを更新するプロセスです。 詳細については、AWS Fargate on Amazon ECS のタスクの廃止とメンテナンス」を参照してください。 詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。	2018 年 12 月 17 日
サービスの制限を更新しました	次のサービスの制限が更新されました。 • リージョンごと、アカウントごとのクラスターの数が 1000 から 2000 に引き上げられました。 • クラスターごとのコンテナインスタンスの数が 1000 から 2000 に引き上げられました。 • クラスターごとのサービスの数が 500 から 1000 に引き上げられました。 詳細については、「Amazon ECS の Service Quotas」を参照してください。	2018 年 12 月 14 日

変更	説明	日付
AWS Fargate リージョンの拡大	AWS Fargate with Amazon ECSは、アジアパシフィック (ムンバイ)、およびカナダ (中部) の各リージョンに拡大されました。 詳細については、「AWS Fargate で使用する Amazon ECS でサポートされているリージョン」を参照してください。	2018 年 12 月 7 日
Amazon ECS ブルー/グリーンデプロイ	CodeDeploy を使用した ブルー/グリーンデプロイのサポートがAmazon ECS に追加されました。このデプロイタイプでは、本番稼働用トラフィックを送信する前にサービスの新しいデプロイメントを検証することができます。 詳細については、「デプロイ前に Amazon ECS サービスの状態を検証する 」を参照してください。	2018 年 11 月 27 日
Amazon ECS 最適化 Amazon Linux 2 (arm64) AMI がリリースされました	Amazon ECS は、Amazon ECS に最適化された、arm64 アーキテクチャのための Amazon Linux 2 AMI をリリースしました。 詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2018 年 11 月 26 日
タスク定義に追加の Docker フラグのサポートが追加されました	Amazon ECS ではタスク定義に次の Docker フラグのサポートを導入しました。 • IPC モード • PID モード	2018 年 11 月 16 日

変更	説明	日付
Amazon ECS シークレットのサポート	AWS Systems Manager パラメータストアパラメータを使用して、コンテナに機密データを挿入する機能のサポートが Amazon ECS に追加されました。 詳細については、「Amazon ECS コンテナに機密データを渡す」を参照してください。	2018 年 11 月 15 日
リソースへのタグ付け	サービス、タスク定義、タスク、クラスター、コンテナインスタンスにメタデータタグを追加する機能のサポートがAmazon ECS に追加されました。 詳細については、「Amazon ECS リソースにタグ付けする」を参照してください。	2018 年 11 月 15 日
AWS Fargateリージョンの拡大	AWS Fargate with Amazon ECS は米国西部 (北カリフォルニア)、アジアパシフィック (ソウル) の各リージョンに拡張されました。 詳細については、「Amazon ECS の AWS Fargate」を参照してください。	2018 年 11 月 7 日
サービスの制限を更新しました	次のサービスの制限が更新されました。 • リージョンごとアカウントごとに、Fargate 起動タイプを使用するタスクの数が20 から50 に引き上げられました。 • Fargate 起動タイプを使用するタスクのパブリック IP アドレスの数が 20 から50 に引き上げられました。 詳細については、「Amazon ECS の Service Quotas」を参照してください。	2018 年 10 月 31 日

変更	説明	日付
AWS Fargateリージョンの拡大	AWS Fargate with Amazon ECSは欧州 (ロンドン) リージョンに拡大されました。 詳細については、「Amazon ECS の AWS Fargate」を参照してください。	2018 年 10 月 26 日
Amazon ECS に最適化された AMI 2 AMI のリリース	Amazon ECS は、2 つのバリアントでサービスに最適化された Linux AMI を提供しています。最新の推奨バージョンは、x に基づいています。Amazon ECS は Amazon Linux AMI に基づいている AMI も提供しますが、ワークロードを Amazon Linux 2 のバリアントに移行することをお勧めします。Amazon Linux AMI のサポートは 2020 年 6 月 30 日までには終了します。 詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2018 年 10 月 18 日
Amazon ECS タスクメタデータエンドポイントバージョン 3	Amazon ECS コンテナエージェントの 1.21.0 バージョン以降では、エージェントはタスクの各コンテナに、環境変数 `ECS_CONTAINER_METADATA_URI` を挿入します。タスクメタデータのバージョン 3 エンドポイントをクエリするとき、さまざまなタスクメタデータおよび Docker 統計を、Amazon ECS コンテナエージェントによって指定される HTTP エンドポイントで `awsvpc` ネットワークモードを使用するタスクで利用できます。詳細については、「Amazon ECS メタデータを使用したワークロードのモニタリング」を参照してください。	2018 年 10 月 18 日

変更	説明	日付
Amazon ECS サービスの検出リージョンの拡大	Amazon ECS サービス検出は、サポート範囲が拡張され、カナダ (中部)、南米 (サンパウロ)、アジアパシフィック (ソウル)、アジアパシフィック (ムンバイ)、および欧州 (パリ) の各リージョンで利用できます。 詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。	2018 年 9 月 27 日
コンテナ定義に追加の Docker フラグのサポートを追加する	Amazon ECS ではコンテナ定義に次の Docker フラグのサポートを導入しました。 • システムコントロール • インタラクティブ • 擬似ターミナル	2018 年 9 月 17 日
AWS Fargateタスク を使用した Amazon ECS のプライベートレジストリ認証のサポート	Amazon ECSはAWS Secrets Managerを使用したプライベートレジストリ認証を使用した Fargate タスクのサポートが導入されました。この機能では、認証情報を安全に保管してコンテナの定義で参照できるため、タスクでプライベートイメージを使用することができます。 詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。	2018 年 9 月 10 日

変更	説明	日付
Amazon ECS サービス検出リージョンの拡大	Amazon ECSサービス検出は、サポート範囲が拡張され、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、アジアパシフィック (東京)、欧州 (フランクフルト)、欧州 (ロンドン) の各リージョンで利用できます。 詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。	2018 年 8 月 30 日
Fargateタスクのサポートでスケジュールされたタスク	Amazon ECS ではFargate 起動タイプのスケジュールされたタスクのサポートが導入されました。	2018 年 8 月 28 日
AWS Secrets Managerサポートを使用したプライベートレジストリ認証	Amazon ECS では、AWS Secrets Managerを使用したプライベートレジストリ認証のサポートが導入されました。この機能では、認証情報を安全に保管してコンテナの定義で参照できるため、タスクでプライベートイメージを使用することができます。 詳細については、「Amazon ECS での AWS 以外のコンテナイメージの使用」を参照してください。	2018 年 8 月 16 日
Docker ボリュームのサポートが追加されました	Amazon ECS では、Docker ボリュームのサポートが導入されました。 詳細については、「Amazon ECS タスクのストレージオプション」を参照してください。	2018 年 8 月 9 日
AWS Fargateリージョンの拡大	AWS Amazon ECS でのFargate の使用は、欧州 (フランクフルト)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー) の各リージョンに拡張されました。 詳細については、「Amazon ECS の AWS Fargate」を参照してください。	2018 年 7 月 19 日

変更	説明	日付
Amazon ECSサービススケジューラ戦略の追加	Amazon ECSにサービススケジューラ戦略の概念を導入しました。 利用できる 2 つのサービススケジューラ戦略があります。 • REPLICA - レプリカスケジュール戦略では、クラスター全体で必要数のタスクを配置して維持します。デフォルトでは、サービススケジューラによってタスクはアベイラビリティーゾーン間に分散されます。タスク配置の戦略と制約を使用すると、タスク配置の決定をカスタマイズできます。詳細については、「レプリカ戦略」を参照してください。 • DAEMON - デーモンのスケジュール戦略では、指定したすべてのタスク配置制約を満たすクラスター内のアクティブなコンテナインスタンスごとに、1 つのタスクのみをデプロイします。この戦略を使用する場合、タスクの必要数や配置戦略、サービスの自動スケーリングポリシーを指定する必要はありません。詳細については、「デーモン戦略」を参照してください。 Note Fargate タスクは DAEMON スケジュール戦略をサポートしていません。 .	2018 年 12 月 6 日

変更	説明	日付
Amazon ECS コンテナエージェント v1.18.0	新しいバージョンの Amazon ECS コンテナエージェントがリリースされ、以下の機能が追加されました。 • `ECS_IMAGE_PULL_BEHAVIOR` パラメータを使用したコンテナエージェントイメージのプル動作のカスタマイズのサポートが追加されました。詳細については、「Amazon ECS コンテナエージェントの設定」を参照してください。 詳細については、amazon-ecs-agent github を参照してください。	2018 年 5 月 24 日
Service Discovery の設定時に `bridge` および `host` ネットワークモードのサポートが追加されました。	`bridge` または `host` ネットワークモードを指定するタスク定義を使用して Amazon ECS サービスのサービス検出を設定するためのサポートが追加されました。詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。	2018 年 5 月 22 日
Amazon ECS に最適化された AMI のその他のメタデータパラメータのサポートが追加されました	Amazon ECS に最適化された AMI の ID、イメージ名、オペレーティングシステム、コンテナエージェントバージョン、およびランタイムバージョンをプログラムで取得できるサブパラメータが追加されました。Systems Manager Parameter Store API を使用してメタデータをクエリします。詳細については、「Amazon ECS に最適化された Linux AMI メタデータを取得する」を参照してください。	2018 年 5 月 9 日
AWS Fargateリージョンの拡大	AWS Fargate with Amazon ECS は、米国東部 (オハイオ)、米国西部 (オレゴン)、欧州西部 (アイルランド) リージョンに拡大されます。 詳細については、「Amazon ECS の AWS Fargate」を参照してください。	2018 年 4 月 26 日

変更	説明	日付
Amazon ECS に最適化された AMI メタデータの取得	Systems Manager パラメータストア API を使用して、Amazon ECS に最適化された AMI メタデータをプログラムで取得する機能を追加しました。詳細については、「Amazon ECS に最適化された Linux AMI メタデータを取得する」を参照してください。	2018 年 4 月 10 日
AWS Fargate プラットフォームバージョン	以下を含む新しくリリースされたAWS Fargateプラットフォームバージョン: • Amazon ECS メタデータを使用したワークロードのモニタリング のサポートが追加されました。 • ヘルスチェック のサポートが追加されました。 • サービス検出を使用して Amazon ECS サービスを DNS 名で接続する のサポートの追加 詳細については、「Amazon ECS 向け Fargate プラットフォームバージョン」を参照してください。	2018 年 3 月 26 日
Amazon ECSサービス検出	Amazon ECS サービス検出をサポートする Route 53 との統合を追加しました。詳細については、「サービス検出を使用して Amazon ECS サービスを DNS 名で接続する」を参照してください。	2018 年 3 月 22 日
Docker shm-size および tmpfs のサポート	Amazon ECS タスク定義に Docker shm-size および tmpfs パラメータのサポートが追加されていること。 更新された ECS CLI 構文の詳細については、「Linux パラメータ」を参照してください。	2018 年 3 月 20 日
コンテナヘルスチェック	コンテナ定義に追加された Docker ヘルスチェックのサポート。詳細については、「ヘルスチェック」を参照してください。	2018 年 3 月 8 日

変更	説明	日付
AWS Fargate	AWS Fargate を使用する Amazon ECS の概要が追加されました。詳細については、「Amazon ECS の AWS Fargate」を参照してください。	2018 年 2 月 22 日
Amazon ECSタスクメタデータエンドポイント	Amazon ECSコンテナエージェントのバージョン 1.17.0 以降、Amazon ECSコンテナエージェントによって提供される HTTP エンドポイントで awsvpc ネットワークモードを使用するタスクで、さまざまなタスクメタデータおよび Docker 統計を使用できます。詳細については、「Amazon ECS メタデータを使用したワークロードのモニタリング」を参照してください。	2018 年 2 月 8 日
ターゲット追跡ポリシーを使用したAmazon ECS Service Auto Scaling	Amazon ECS コンソールにターゲット追跡ポリシーを使用した ECS Service Auto Scaling のサポートが追加されました。詳細については、「ターゲットメトリクスを使用して Amazon ECS サービスをスケールする」を参照してください。 ECS の初回実行ウィザードの前段階チュートリアルのステップスケーリングが削除されていること。これはターゲット追跡用の新しいチュートリアルに置き換えられます。	2018 年 2 月 8 日
Docker 17.09 のサポート	Docker 17.09 のサポートを追加しました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2018 年 1 月 18 日
新しいサービススケジューラの動作	起動に失敗するサービスタスクの動作に関する情報を更新しました。サービスタスクが連続して失敗する場合にトリガーされる新しいサービスイベントメッセージについて文書化しました。	2018 年 1 月 11 日
Elastic Load Balancing のヘルスチェックの初期化待機期間	ヘルスチェックの待機期間を指定する機能を追加しました。	2017 年 12 月 27 日

変更	説明	日付
タスクレベルの CPU とメモリ	タスク定義でタスクレベルの CPU とメモリを指定するためのサポートを追加しました。詳細については、「TaskDefinition」を参照してください。	2017 年 12 月 12 日
タスク実行ロール	Amazon ECSコンテナエージェントはユーザーに代わって Amazon ECS API アクションを呼び出すため、エージェントがユーザーに属していることをサービスに伝えるために、IAM ポリシーおよびロールが必要です。次のアクションがタスク実行ロールの対象になっています。 • コンテナイメージをプルするためのAmazon ECR の呼び出し • コンテナアプリケーションログを保存するための CloudWatch の呼び出し 詳細については、「Amazon ECS タスク実行IAM ロール」を参照してください。	2017 年 12 月 7 日
Windows コンテナが GA をサポート	Windows Server 2016 コンテナのサポートが追加されました。詳細については、「Amazon ECS に最適化された AMI バリアント」を参照してください。	2017 年 5 月 12 日
AWS Fargateの一般提供	Fargate 起動タイプを使用したAmazon ECS サービスの起動のサポートを追加しました。詳細については、「Amazon ECS 起動タイプ」を参照してください。	2017 年 11 月 29 日
Amazon ECS の名前の変更	Amazon Elastic Container Service の名前が変更されました (旧 Amazon EC2 Container Service)。	2017 年 11 月 21 日

変更	説明	日付
タスクネットワーク	awsvpc ネットワークモードで利用できるタスクネットワーキング機能により、Amazon EC2 インスタンスと同じネットワーキングプロパティが Amazon ECS タスクに提供されます。タスク定義で awsvpc ネットワークモードを使用すると、このタスク定義から起動されるすべてのタスクが、独自の Elastic Network Interface、プライマリプライベート IP アドレス、および内部 DNS ホスト名を取得します。タスクネットワーキング機能により、コンテナネットワークを簡素化できるだけでなく、コンテナ化されたアプリケーションの相互通信や、コンテナ化されたアプリケーションと VPC 内のその他のサービスとの通信に対する統制力を強化できます。詳細については、「EC2 起動タイプの Amazon ECS タスクネットワークオプション」を参照してください。	2017 年 11 月 14 日
Amazon ECS コンテナメタデータ	Amazon ECS コンテナが、Docker コンテナ、イメージ ID、ネットワーク設定、Amazon ARN などのメタデータにアクセスできるようになりました。詳細については、「Amazon ECS コンテナメタデータファイル」を参照してください。	2017 年 11 月 2 日
Docker 17.06 のサポート	Docker 17.06 のサポートを追加しました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2017 年 11 月 2 日
Docker フラグ device および init のサポート	`LinuxParameters` パラメータ (`devices` および `initProcessEnabled`) を使用した、タスク定義での Docker の device および init 機能のサポートを追加しました。詳細については、LinuxParameters を参照してください。	2017 年 11 月 2 日

変更	説明	日付
Docker フラグ cap-add および cap-drop のサポート	`LinuxParameters` パラメータ (`capabilities`) を使用した、タスク定義での Docker の cap-add および cap-drop 機能のサポートを追加しました。詳細については、LinuxParameters を参照してください。	2017 年 9 月 22 日
Network Load Balancer のサポート	Amazon ECS では、Amazon ECS コンソールで Network Load Balancer のサポートが追加されました。	2017 年 9 月 7 日
RunTask の上書き	タスクの実行時のタスク定義の上書きのサポートが追加されました。これにより、タスク定義の変更中に、新しいタスク定義のリビジョンを作成することなくタスクを実行できます。詳細については、「Amazon ECS タスクとしてのアプリケーションの実行」を参照してください。	2017 年 6 月 27 日
Amazon ECS のスケジュールされたタスク	cron を使用したタスクのスケジューリングのサポートを追加しました。	2017 年 6 月 7 日
Amazon ECS コンソールのスポットインスタンス	Amazon ECS コンソール内でスポットフリートコンテナインスタンスを作成するためのサポートを追加しました。詳細については、「Amazon ECS Linux コンテナインスタンスの起動」を参照してください。	2017 年 6 月 6 日
新しい Amazon ECS 最適化 AMI リリース用の Amazon SNS 通知	新しい Amazon ECS 最適化 AMI リリースに関する SNS 通知にサブスクライブする機能が追加されました。	2017 年 3 月 23 日
マイクロサービスとバッチジョブ	Amazon ECS の 2 つの一般的ユースケース (マイクロサービスおよびバッチジョブ) に関するドキュメントを追加しました。詳細については、「Amazon ECS の関連情報」を参照してください。	2017 年 2 月

変更	説明	日付
コンテナインスタンスのドレイン	コンテナインスタンスのドレインのサポートを追加しました。これにより、クラスターからコンテナインスタンスを削除するメソッドが提供されます。詳細については、「Amazon ECS コンテナインスタンスをドレインする」を参照してください。	2017 年 1 月 24 日
Docker 1.12 のサポート	Docker 1.12 のサポートを追加しました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2017 年 1 月 24 日
新しいタスク配置戦略	タスク配置戦略のサポート (属性ベースの配置、ビンパック、アベイラビリティーゾーン分散、ホストごとに 1 つ) を追加しました。詳細については、「戦略を使用して Amazon ECS タスク配置を定義する」を参照してください。	2016 年 12 月 29 日
Windows コンテナのベータ版のサポート	Windows Server 2016 コンテナ (ベータ版) のサポートが追加されました。詳細については、「Amazon ECS に最適化された AMI バリアント」を参照してください。	2016 年 12 月 20 日
Blox OSS のサポート	Blox OSS のサポートが追加されました。これにより、カスタムタスクスケジューラを使用できます。詳細については、「Amazon ECS でコンテナをスケジュールする」を参照してください。	2016 年 12 月 1 日
CloudWatch Events の Amazon ECS イベントストリーム	Amazon ECS が、コンテナインスタンスとタスクの状態の変更を CloudWatch Events に送信するようになりました。詳細については、「EventBridge を使用して Amazon ECS エラーへの対応を自動化する」を参照してください。	2016 年 11 月 21 日
CloudWatch Logs への Amazon ECS コンテナのロギング	awslogs ドライバーがコンテナログストリームを CloudWatch Logs に送信するためのサポートを追加しました。詳細については、「Amazon ECS ログを CloudWatch に送信する 」を参照してください。	2016 年 9 月 12 日

変更	説明	日付
動的ポートの Elastic Load Balancing をサポートする Amazon ECS サービス	リスナーあたり複数の instance:port の組み合わせをサポートするためのロードバランサーのサポートを追加しました。これにより、コンテナの柔軟性が高まります。Docker でコンテナのホストポートを動的に定義し、ECS スケジューラでロードバランサーを使用して instance:port を登録できます。詳細については、「ロードバランサーを使用して Amazon ECS サービストラフィックを分散する」を参照してください。	2016 年 8 月 11 日
Amazon ECS タスク用の IAM ロール	タスクへの IAM ロールの関連付けのサポートが追加されました。これにより、コンテナインスタンス全体に対して 1 つのロールを使用するのではなく、コンテナに対するより詳細なアクセス許可が提供されます。詳細については、「Amazon ECS タスクの IAM ロール」を参照してください。	2016 年 7 月 13 日
Docker 1.11 のサポート	Docker 1.11 のサポートを追加しました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2016 年 5 月 31 日
タスクの自動スケーリング	Amazon ECS で、サービスによって実行されるタスクの自動的なスケーリングのサポートが追加されました。詳細については、「Amazon ECS サービスを自動的にスケールする」を参照してください。	2016 年 5 月 18 日
タスクファミリーでのタスク定義のフィルタリング	タスク定義ファミリーに基づいてタスク定義のリストをフィルタリングするサポートが追加されました。詳細については、「ListTaskDefinitions」を参照してください。	2016 年 5 月 17 日
Docker コンテナおよび Amazon ECS エージェントのログ記録	Amazon ECS で、問題のトラブルシューティングを簡単にするため、コンテナインスタンスから ECS エージェントと Docker コンテナログを CloudWatch Logs に送信する機能が追加されました。	2016 年 5 月 5 日

変更	説明	日付
ECS 最適化 AMI が Amazon Linux 2016.03 をサポートするようになりました。	ECS 最適化 AMI では Amazon Linux 2016.03 のサポートを追加しました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2016 年 4 月 5 日
Docker 1.9 のサポート	Docker 1.9 のサポートを追加しました。詳細については、「Amazon ECS に最適化された Linux AMI」を参照してください。	2015 年 12 月 22 日
クラスターの CPU およびメモリ予約に関する CloudWatch メトリクス	Amazon ECS で、CPU およびメモリ予約に関するカスタム CloudWatch メトリクスが追加されました。	2015 年 12 月 22 日
新しい Amazon ECS の初回実行のエクスペリエンス	Amazon ECS コンソールの初回実行のエクスペリエンスで、ゼロクリックのロール作成が追加されました。	2015 年 23 月 11 日
複数のアベイラビリティーゾーンにわたるタスクの配置	Amazon ECS サービススケジューラで、複数のアベイラビリティーゾーンにわたるタスク配置のサポートが追加されました。	2015 年 10 月 8 日
Amazon ECS クラスターとサービスの CloudWatch メトリクス	Amazon ECS で、クラスターの各コンテナインスタンス、サービス、タスク定義ファミリーの CPU およびメモリ使用率に関するカスタム CloudWatch メトリクスが追加されました。これらの新しいメトリクスを使用すると、Auto Scaling グループを使用してクラスターでコンテナインスタンスをスケールするか、カスタム CloudWatch アラームを作成できます。	2015 年 8 月 17 日
UDP ポートのサポート	タスク定義で UDP ポートのサポートが追加されました。	2015 年 7 月 7 日
[環境変数の上書き]	deregisterTaskDefinition と環境変数による runTask の上書きのサポートが追加されました。	2015 年 6 月 18 日

変更	説明	日付
自動化された Amazon ECS エージェントの更新	コンテナインスタンスで実行されている ECS エージェントバージョンを表示する機能を追加しました。AWS Management Console、AWS CLI、および SDK から ECS エージェントを更新することもできます。	2015 年 6 月 11 日
Amazon ECS サービススケジューラと Elastic Load Balancing の統合	サービスを定義し、そのサービスを Elastic Load Balancing ロードバランサーに関連付ける機能を追加しました。	2015 年 4 月 9 日
Amazon ECS GA	Amazon ECS は米国東部 (バージニア北部)、米国西部 (オレゴン)、アジアパシフィック (東京)、欧州 (アイルランド) の各リージョンで一般提供されます。	2015 年 4 月 9 日