AWS Black Belt Online Seminar

AWS SAW

セルフサービスなトラブルシューティングと運用の自動化 Amazon Elastic Container Service(Amazon ECS) 編

Cloud Support Engineer
古野 俊広
2023-10月

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では 2023 年 10 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://aws.amazon.com/) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、有料の AWS サポート窓口へお問い合わせください
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
  お問い合わせください (マネジメントコンソールへのログインが必要です)

本セミナーの概要

- 本セミナーの対象者
  - Amazon ECS を利用した運用を実施されている方
  - Amazon ECS のトラブルシューティングの効率化に興味のある方
- 本セミナーの Goal
  - Amazon ECS 向けに利用可能な3つの AWS Support Automation Workflows(SAW) について利用ユースケース及び概要を理解する
- 本セミナーの前提知識
  - AWS Black Belt Online Seminar Amazon Elastic Container Service
  - AWS Black Belt Online Seminar AWS SAW - セルフサービスなトラブルシューティングと運用の自動化 入門編

自己紹介

名前：古野 俊広(Furuno Toshihiro)

所属：アマゾン ウェブ サービス ジャパン

合同会社技術支援本部 クラウドサポートエンジニア

好きな AWS サービス：

Amazon Elastic Container Service
(Amazon ECS)

AWS CodeDeploy

アジェンダ

- Amazon ECS のよくあるお問い合わせと SAW の紹介
  - AWSSupport-TroubleshootECSTaskFailedToStart
  - AWSSupport-TroubleshootECSContainerInstance
  - AWSSupport-CollectECSInstanceLogs
- まとめ

Amazon ECS のよくあるお問い合わせと SAW の紹介

Amazon ECS でよくあるお問い合わせ

- How to
  - 実現したいことを達成するための方法に関するご質問
    - 例
      - 開発者と運用者で利用可能な API を分けたいが、やり方が分からない
- トラブルシューティング
  - 問題の原因調査および解消方法を知りたい
    - 例
      - タスクの起動に失敗するが原因および解消方法が分からない
      - EC2 起動タイプを利用するために EC2 インスタンスを起動したが、クラスターに登録されない
      - EC2 起動タイプのタスクで問題が発生しており、ログが収集したい

Amazon ECS でよくあるお問い合わせ

- How to
  - 実現したいことを達成するための方法に関するご質問
    - 例
      - 開発者と運用者で利用可能な API を分けたいが、やり方が分からない
- トラブルシューティング
  - 問題の原因調査および解消方法を知りたい
    - 例
      - タスクの起動に失敗するが原因および解消方法が分からない
      - EC2 起動タイプを利用するために EC2 インスタンスを起動したが、クラスターに登録されない
      - EC2 起動タイプのタスクで問題が発生しており、ログが収集したい

SAW によって解析や関連情報収集ができる範囲

Amazon ECS でよくあるお問い合わせ

- タスクの起動に失敗するが原因および解消方法が分からない
  - SAW(AWSSupport-TroubleshootECSTaskFailedToStart) を利用することで問題解析ができ、問題解消が出来る可能性がある
- EC2 起動タイプを利用するために EC2 インスタンスを起動したが、クラスターに登録されない
  - SAW(AWSSupport-TroubleshootECSContainerInstance) を利用することで問題解析ができ、問題解消が出来る可能性がある
- EC2 起動タイプのタスクで問題が発生しており、ログが収集したい
  - SAW(AWSSupport-CollectECSInstanceLogs)を利用することで調査の為に必要なログをまとめて収集出来る

Amazon ECS で利用可能な SAW(ランブック)

名称	カテゴリ	起動タイプ	概要
AWSSupport-TroubleshootECSTaskFailedToStart	トラブルシューティング	EC2, Fargate	Amazon ECS クラスター内の タスクが起動に失敗した理由のトラブルシューティングを行う
AWSSupport-TroubleshootECSContainerInstance	トラブルシューティング	EC2	Amazon ECS クラスターへの登録に失敗する EC2 インスタンスのトラブルシューティングを行う
AWSSupport-CollectECSInstanceLogs	ログ収集	EC2	Amazon ECS の一般的な問題のトラブルシューティングに役立つオペレーティングシステムと Amazon ECS 関連のログファイルを EC2 インスタンスから収集する

AWSSupport-TroubleshootECSTaskFailedToStart

AWSSupport-TroubleshootECSTaskFailedToStart

- 利用ユースケース
  - タスクの起動に失敗した場合
    - 具体例
      - CanNotPullContainerError となってコンテナイメージの Pull で問題が発生し、タスクの起動に失敗
      - ResourceInitializationError となって何らかの初期化処理で問題が発生し、タスクの起動に失敗
  - EC2 および Fargate 起動タイプいずれのタスクでも実行可能

AWSSupport-TroubleshootECSTaskFailedToStart

- 問題事象確認方法
  - マネージメントコンソール:サービスイベントもしくは直接タスク ID を選択。タスクのステータスおよび停止理由(stoppedReason)を確認

  - AWS CLI：describe-tasks コマンドの desiredStatus, lastStatus, stoppedReason で確認可能

AWSSupport-TroubleshootECSTaskFailedToStart

- SAW(ランブック)が確認するポイント
  - 設定したコンテナレジストリーへのネットワーク接続
  - タスク実行ロールに必要な IAM 権限
  - VPC エンドポイント接続
  - セキュリティグループルール設定
  - AWS Secrets Manager シークレットリファレンス
  - ログ設定

SAW(ランブック)入力パラメーター

- TaskId(必須)
  - 調査対象のタスク ID
- ClusterName(必須)
  - 調査対象タスク ID の ECS クラスター名
- CloudwatchRetentionPeriod(オプション)
  - ネットワークテストが必要な際に作成する Lambda 関数のログ保持期間。単位は「日」でデフォルトは30

https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-aws-troubleshootecstaskfailedtostart.html

SAW(ランブック)入力パラメーター

- AutomationAssumeRole(オプション)
  - Automation が各種 API を呼び出す際に利用するロール名
  - 必要な権限はドキュメント参照
  - 指定しない場合、SAW(ランブック)を実行した IAM ユーザーの権限を利用

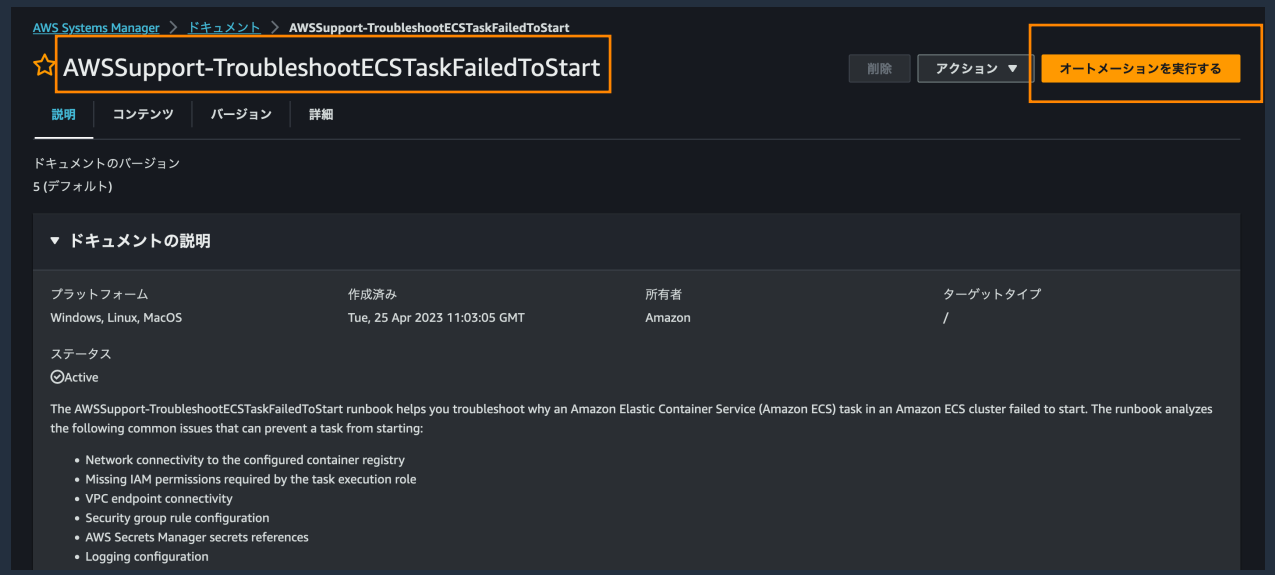
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-aws-troubleshootecstaskfailedtostart.html

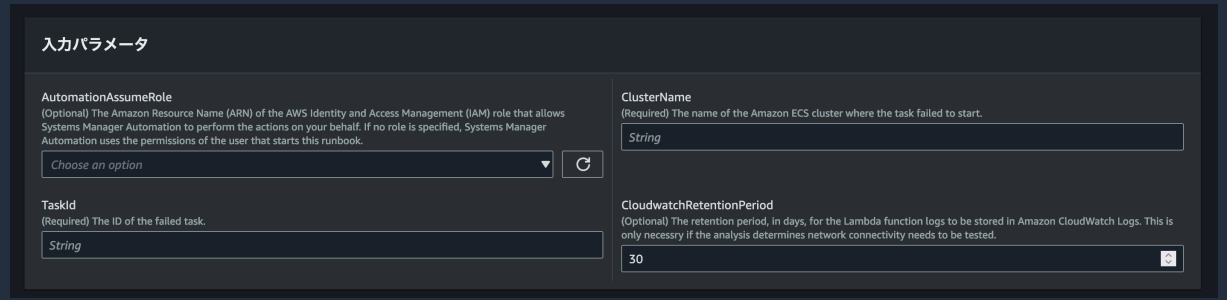
SAW(ランブック)実行例1(ネットワークの問題)

- 状況
  - Fargate 起動タイプのタスクを起動。Docker Hub からコンテナイメージを Pull するように指定
  - マネージメントコンソールもしくは AWS CLI でタスクの起動に失敗したことを確認。停止理由(stoppedReason) を見たが、ネットワークの問題であることは分かるが原因特定が出来ていない

SAW(ランブック)実行例1(ネットワークの問題)

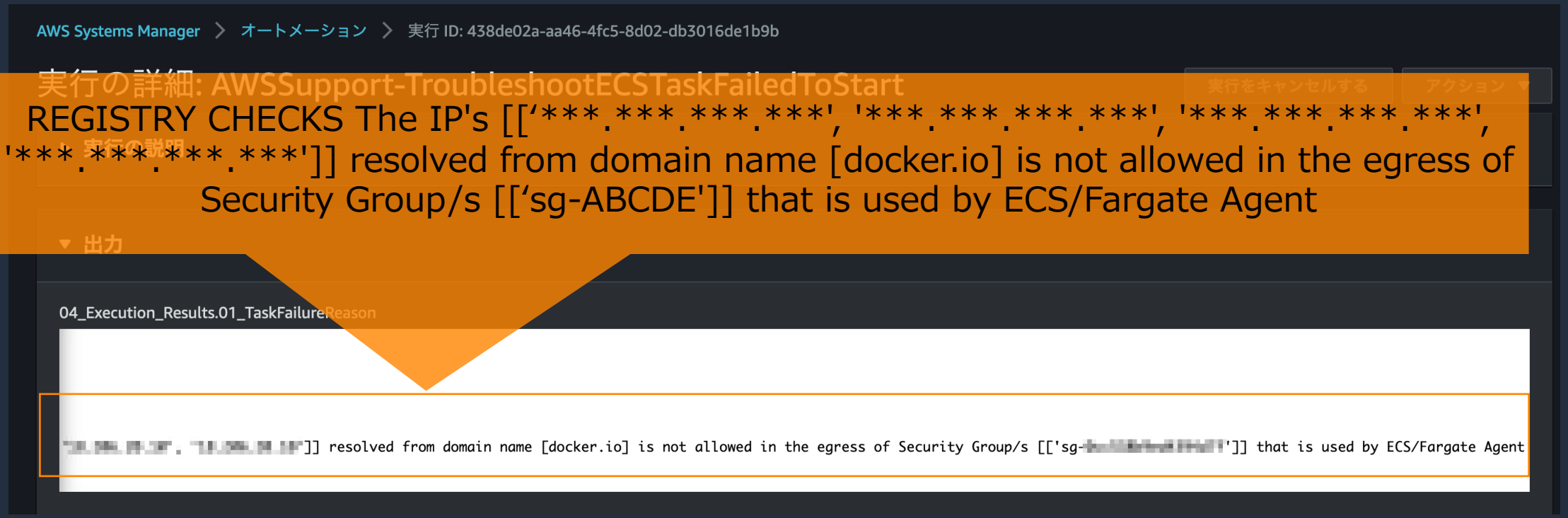
- 対象のドキュメントを検索し、「オートメーションを実行する」を選択して、入力パラメーターを指定することで実行可能。詳細は「AWS Black Belt Online Seminar AWS SAW - セルフサービスなトラブルシューティングと運用の自動化 入門編 」を参照ください。





SAW(ランブック)実行例1

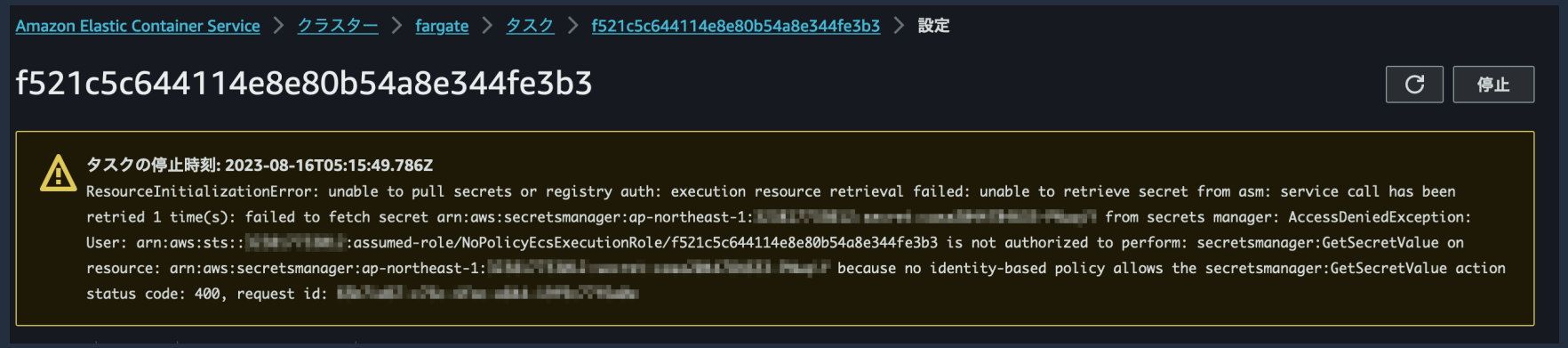
- 実行結果
  - タスクに設定されたセキュリティグループのアウトバウンド設定の問題であることが特定でき、アウトバウンドに0.0.0.0/0 を追加することで問題解消



REGISTRY CHECKS The IP's [['***.***.***.***', '***.***.***.***', '***.***.***.***', '***.***.***.***']] resolved from domain name [docker.io] is not allowed in the egress of Security Group/s [['sg-ABCDE']] that is used by ECS/Fargate Agent

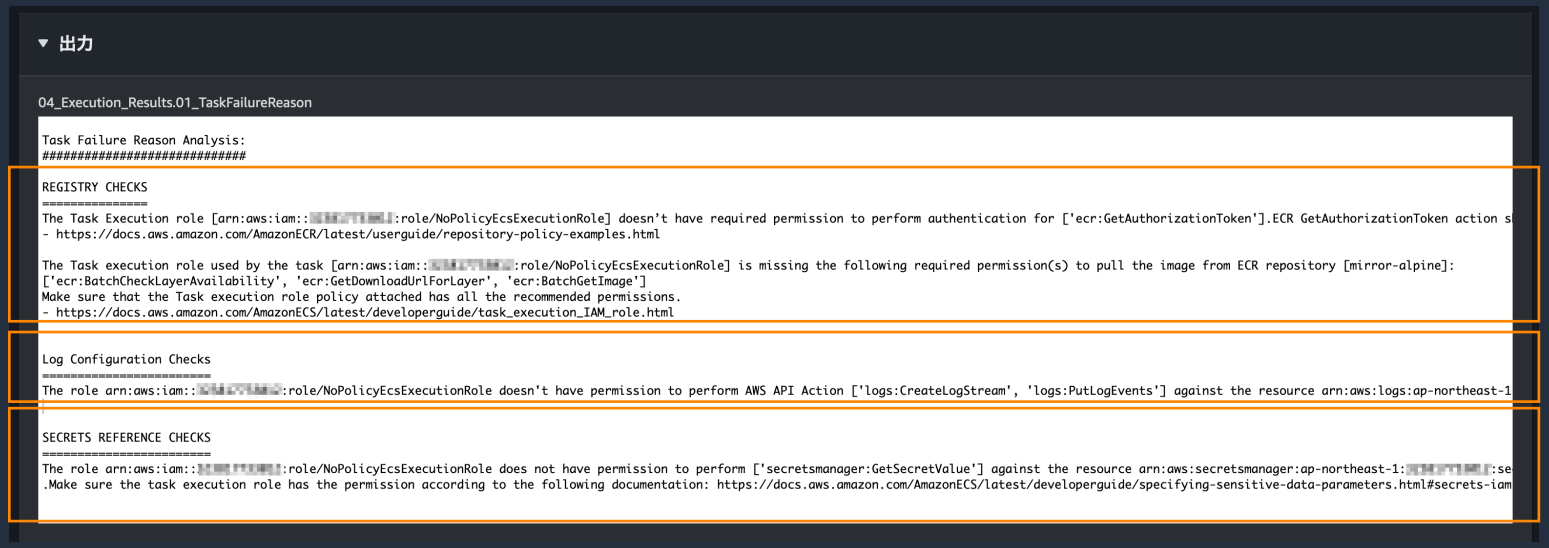
SAW(ランブック)実行例2(権限の問題)

- 状況
  - Fargate 起動タイプのタスクを起動。Secrets Manager を参照するように設定
  - マネージメントコンソールもしくは AWS CLI でタスクの起動に失敗したことを確認。停止理由(stoppedReason) を確認し、タスク実行 IAM ロールの権限が不足していることは分かったが、記載のある Secrets Manager 以外に必要な権限がないか調べたい



SAW(ランブック)実行例2(権限の問題)

- 実行結果
  - 事前に認識していた Secrets Manager だけでなく別の権限の問題点も検出し、一度で問題解決
    - ECR に関する権限の不足
    - ログ設定(CloudWatch Logs)に関する権限の不足
    - Secrets Manger に関する権限の不足



その他

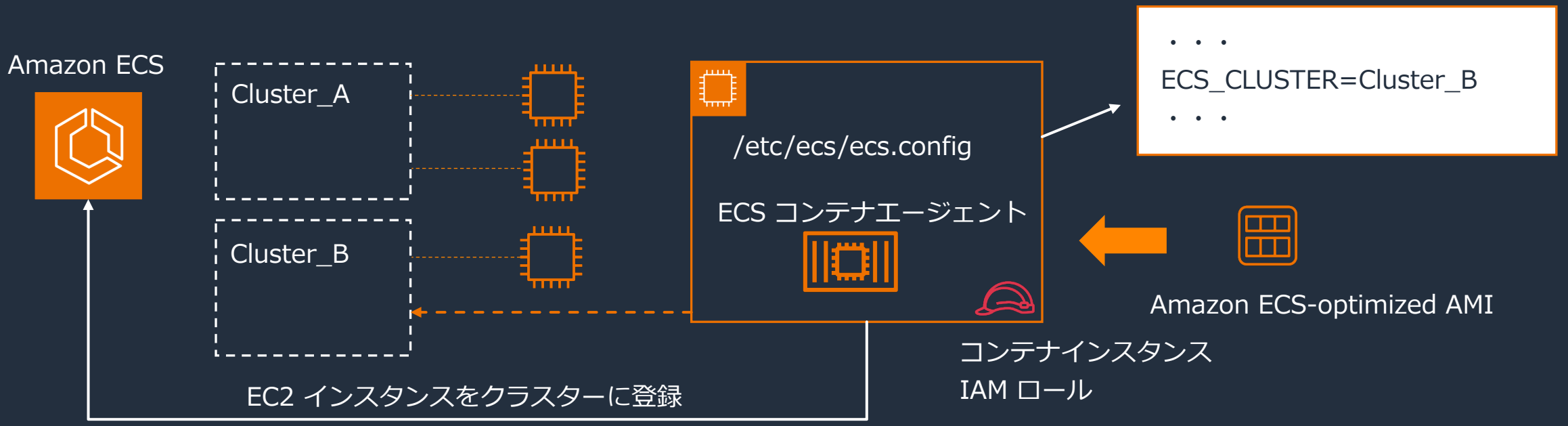
- 留意点
  - SAW(ランブック)を使用する際は、最近失敗したタスクの ID を使用する必要がある。停止した ECS タスクは停止状態になってから 1 時間以内であれば確認可能
  - 起動時のネットワークや権限の設定などに問題がある場合に解析をする。例えばコンテナイメージそのものの問題については分析しない(例: コンテナイメージに問題があり、起動後すぐに exitCode 1 で停止する場合など)
    - exitCode はマネージメントコンソールおよび AWS CLI で確認可能

AWSSupport-TroubleshootECSContainerInstance

AWSSupport-TroubleshootECSContainerInstance

- 利用ユースケース
  - ECS クラスターに登録される想定の EC2 インスタンスを起動したにも関わらず、EC2 インスタンスが対象クラスターに表示されない場合

クラスターに登録されるまでの流れ(イメージ)



AWSSupport-TroubleshootECSContainerInstance

- 問題事象確認方法
  - マネージメントコンソール:「インフラストラクチャー」タブの「コンテナインスタンス」を確認。コンテナインスタンスとして登録されている場合、こちらに表示される

  - AWS CLI：list-container-instances コマンドでクラスターに登録されているコンテナインスタンス群を確認

AWSSupport-TroubleshootECSContainerInstance

- SAW(ランブック)が確認するポイント
  - EC2 インスタンスの UserData
    - UserData を利用して ECS コンテナエージェントが利用する設定ファイルに追記を行うことで登録する ECS クラスター名の指定が可能
  - EC2 インスタンスプロファイルの権限
  - ネットワーク設定の問題
- Linux もしくは Windows EC2 インスタンスに対して実行可能
  - 基本的には OS の種類によらず、対応可能
    - Bottlerocket は UserData によるクラスター指定方法が異なっており、2023年10月時点で未サポート

AWSSupport-TroubleshootECSContainerInstance

- ECS クラスターが ACTIVE 状態、EC2 インスタンスが running 状態であること
- 調査対象インスタンス内でのコマンド実行はしない為、EC2 インスタンスで SSM Agent が動作し、Systems Manager に管理されたマネージドノードである必要はない

SAW(ランブック)入力パラメーター

- InstanceId(必須)
  - 調査対象の EC2 インスタンス ID
- ClusterName(必須)
  - 調査対象インスタンスがコンテナインスタンスとして登録される想定の ECS クラスター名
- AutomationAssumeRole(オプション)
  - 「AWSSupport-TroubleshootECSTaskFailedToStart」と同様

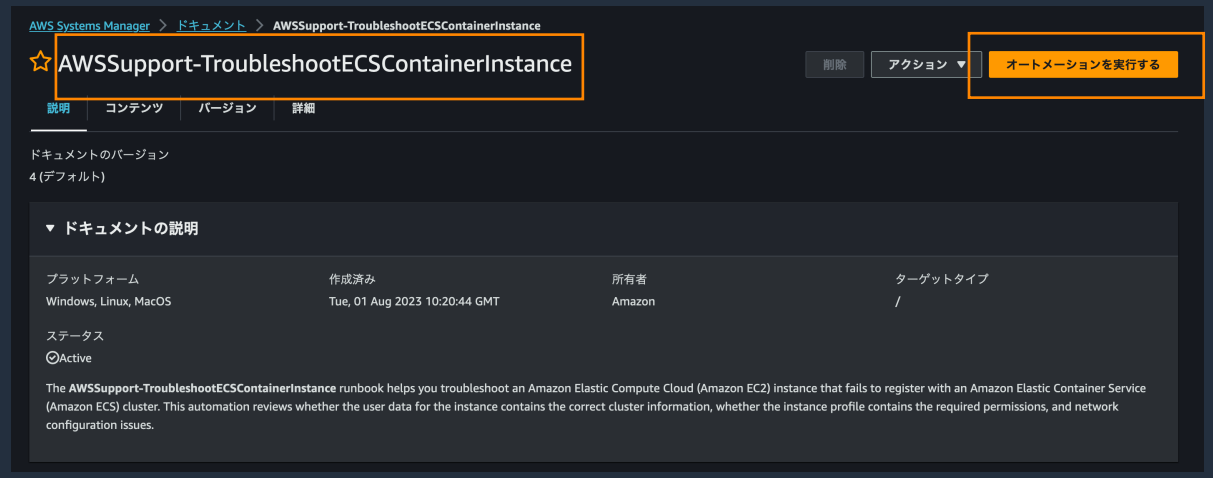
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-aws-troubleshoot-ecs-container-instance.html

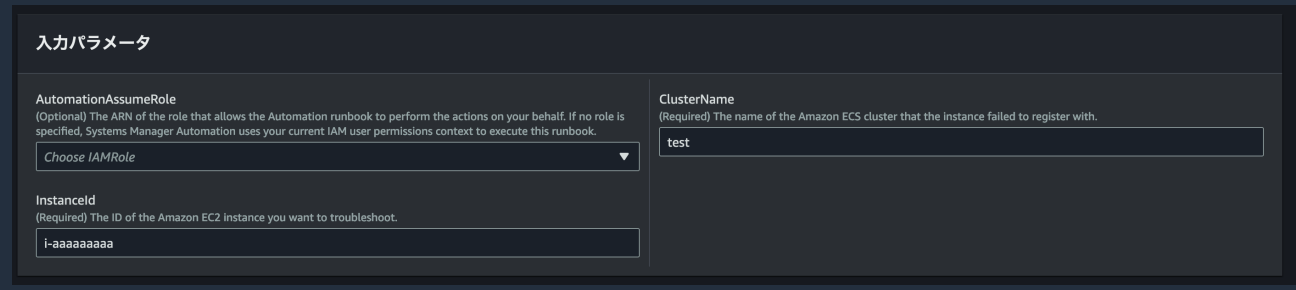
SAW(ランブック)実行例

- 状況
  - UserData を設定し、クラスターに参加させるために EC2 インスタンスを起動。EC2 インスタンスは running 状態であるが、クラスターに登録されていない
  - UserData の設定はしており、EC2 インスタンスも起動しているため、問題原因が特定出来ていない

SAW(ランブック)実行例

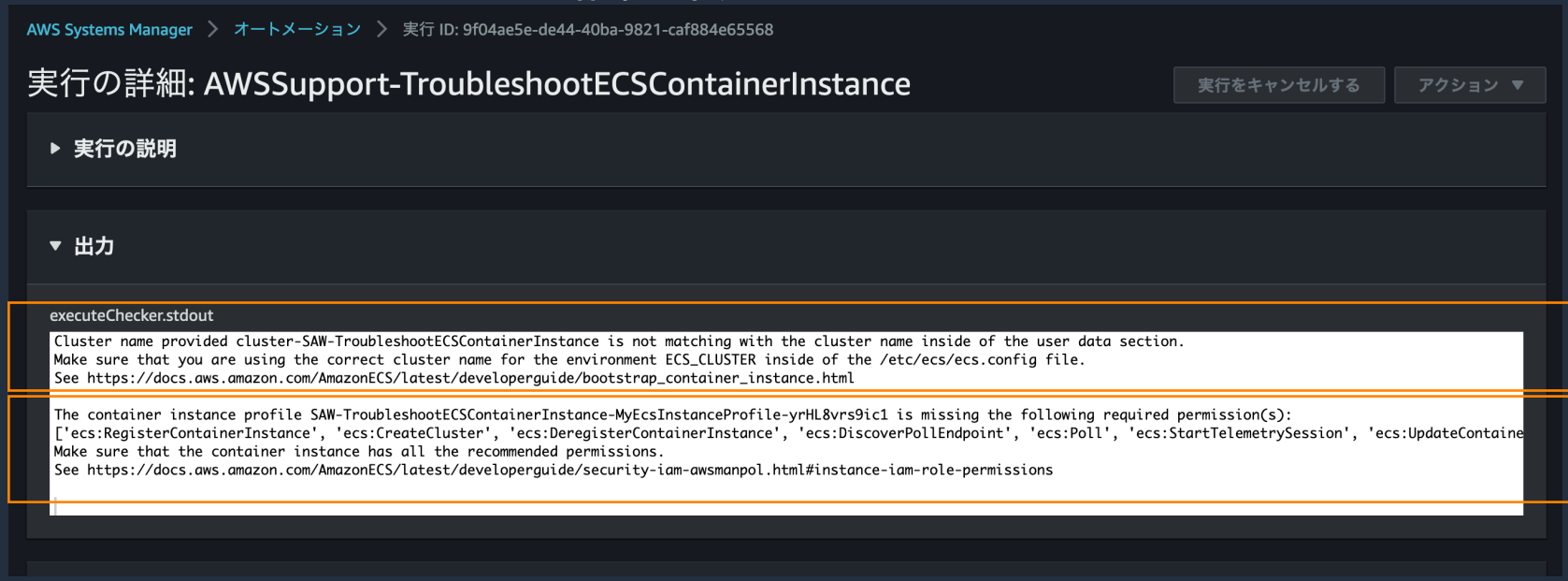
- 対象のドキュメントを検索し、「オートメーションを実行する」を選択して、入力パラメーターを指定することで実行可能。詳細は「AWS Black Belt Online Seminar AWS SAW - セルフサービスなトラブルシューティングと運用の自動化 入門編 」を参照ください。





SAW(ランブック)実行例

- 実行結果
  - 以下2点の問題点が特定でき、UserData 修正およびインスタンスプロファイルへの権限追加によって一度で問題解消
    - UserData の記述が誤っている
    - インスタンスプロファイルの権限不足



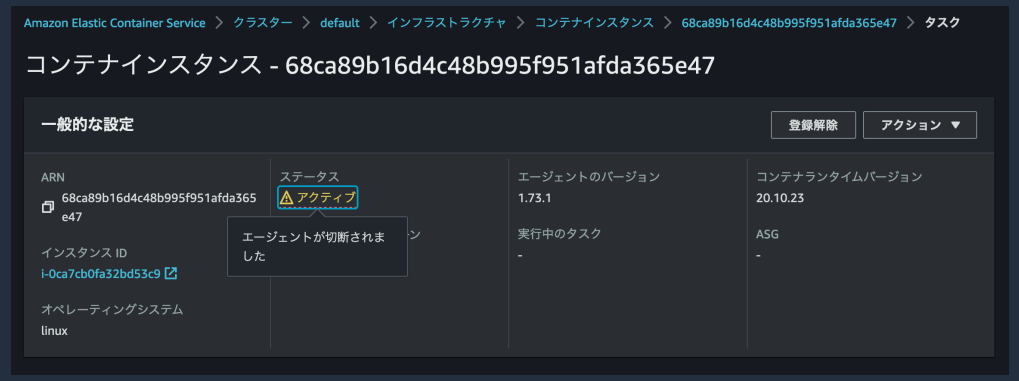
AWSSupport-CollectECSInstanceLogs

AWSSupport-CollectECSInstanceLogs

- 利用ユースケース
  - EC2 起動タイプで ECS が関連する問題があり、トラブルシューティングの際に利用する EC2 インスタンス内のログファイルを確認したい場合
    - 具体例
      - EC2 起動タイプのタスクが想定通り停止しない場合
      - EC2 インスタンス内で動作しているはずの ECS コンテナエージェントが停止していると思われる場合

AWSSupport-CollectECSInstanceLogs

- 問題事象確認方法
  - タスク状態
    - 「AWSSupport-TroubleshootECSTaskFailedToStart」で記載した方法で確認可能
  - ECS コンテナエージェント
    - マネージメントコンソール:「インフラストラクチャー」タブの「コンテナインスタンス」を確認



    - AWS CLI：describe-container-instances コマンドの agentConnected ステータスで確認可能

AWSSupport-TroubleshootECSContainerInstance

- ECS コンテナエージェントの agentConnected に関する補足事項
  - 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
    - https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/ecs_cwe_events.html
  - 一方、継続して agentConnected false となっている場合、ECS コンテナエージェントが停止している可能性も考えられる

AWSSupport-CollectECSInstanceLogs

- Linux もしくは Windows の EC2 インスタンスで利用可能
  - ECS ログコレクターの取得に対応している OS で利用可能
    - https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-logs-collector.html
    - 例えば Bottlerocket は未サポート
  - 対象 EC2 インスタンス内で SSM Agent が動作しており、Systems Manager によって管理されているマネージドノードの必要がある
  - ECS-Optimzied AMI Amazon Linux 2023, ECS-Optimzied AMI Amazon Linux 2 にて SSM Agent はインストール済み

AWSSupport-CollectECSInstanceLogs

- オプションで S3 にログを配置する場合、以下が必要
  - Linux の場合、AWS CLI、Windows の場合 AWS Tools for Windows PowerShell が EC2 インスタンスにインストールされている
    - ECS-Optimzied AMI Amazon Linux 2 には AWS CLI がインストールされていないため、事前にインストールが必要(ECS-Optimzied AMI Amazon Linux 2023 であれば AWS CLI はインストール済み)
  - EC2 インスタンスから S3 への通信が可能(インターネット接続、VPC エンドポイント)
  - インスタンスプロファイルに対象 S3 バケットへの Put 権限がある

SAW(ランブック)入力パラメーター

- ECS InstanceId(必須)
  - ログ取得対象の EC2 インスタンス ID
- LogDestination(オプション)
  - アーカイブされたログをアップロードする S3 バケット名
- AutomationAssumeRole(オプション)
  - 「AWSSupport-TroubleshootECSTaskFailedToStart」と同様

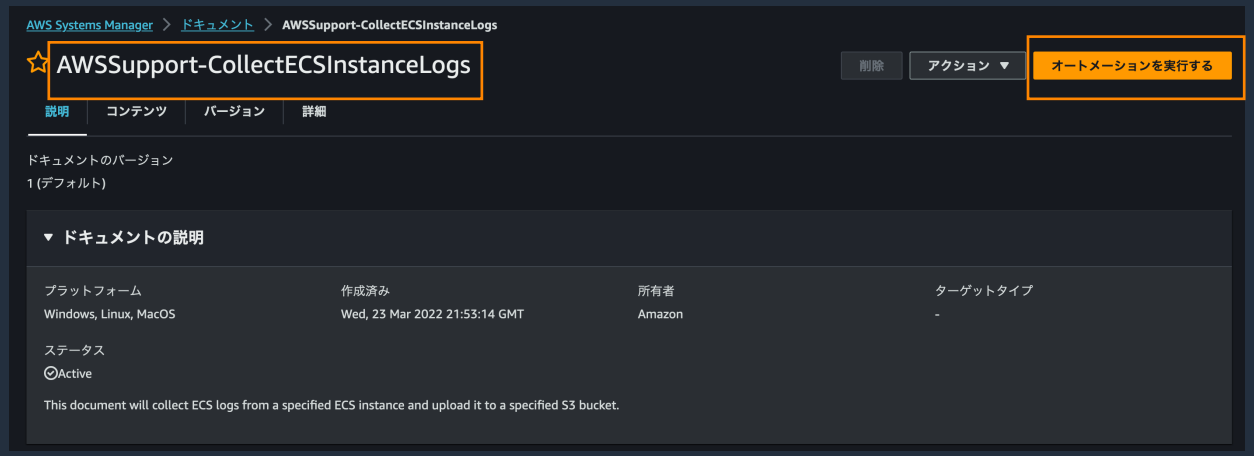
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-collectecsinstancelogs.html

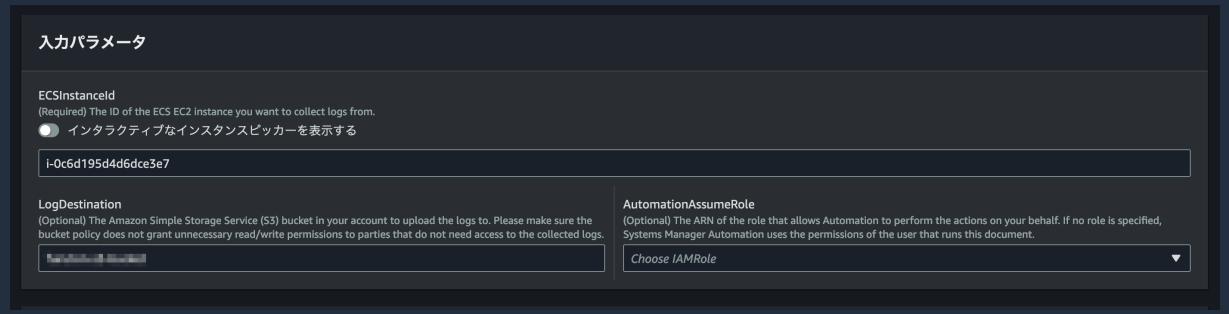
SAW(ランブック)実行例

- 問題点および状況
  - 対象 EC2 インスタンス上で動作しているタスクが停止しない
  - 原因調査のために対象インスタンス内の ECS に関する各種ログを取得したい

SAW(ランブック)実行例

- 対象のドキュメントを検索し、「オートメーションを実行する」を選択して、入力パラメーターを指定することで実行可能。詳細は「AWS Black Belt Online Seminar AWS SAW - セルフサービスなトラブルシューティングと運用の自動化 入門編 」を参照ください。





SAW(ランブック)実行例

- 実行結果
  - 成功していることを確認する

  - S3 コンソールでアップロードされたログが確認できる

その他

- 留意点
  - AWS サポートから直接お客様の S3 バケットのログは確認できないため、ケース起票の際には改めてケースへのログ添付が必要
  - SSM Agent を動作させていないなどランブックが利用できない場合、SSH などで EC2 インスタンスにログインし、手動でログを取得する方法も可能
    - https://docs.aws.amazon.com/ja_jp/AmazonECS/latest/developerguide/ecs-logs-collector.html

まとめ

まとめ

- SAW を使うことでお客様自身でトラブルシューティングを行うことができる
  - 自動化された分析によってヒューマンエラーの削減および作業の効率化
  - 問題解決までの時間を削減
- 問題解決しない場合には通常通り、サポートケースを起票いただき、AWS サポートまでお問い合わせください
- SAW を実行しても問題解決しなかった場合、実行頂いた SAW のランブック名、関連する SSM Automation の実行 ID、SAW の実行結果なども通常起票時に必要な情報と併せて記載頂けますと幸いです

Thank you!