



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おります。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

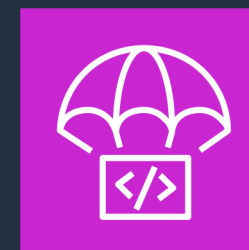
合同会社技術支援本部 クラウドサポートエンジニア



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 |

AWS Support- Troubleshoot EC2 Task Failed To Start

AWS Support-Troubleshoot ECSTaskFailedToStart

- 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

AWS Support-Troubleshoot ECSTaskFailedToStart

- 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

Amazon Elastic Container Service > クラスター > cluster-SAW-TroubleshootECSTaskFailedToStart > サービス > SAW-TroubleshootECSTaskFailedToStart-MyFargateService-bfqNwghsTkP2 > イベント

SAW-TroubleshootECSTaskFailedToStart-MyFargateService-bfqNwghsTkP2 情報

サービスを更新 サービスを削除

正常性とメトリクス タスク ログ デプロイ イベント 設定 ネットワーキング タグ

イベント (100)

値でイベントをフィルター

| 開始時刻 | メッセージ | イベント ID |
|-----------------------------|---|--------------------------------------|
| 2023年8月16日 07:33 (UTC+9:00) | service SAW-TroubleshootECSTaskFailedToStart-MyFargateService-bfqNwghsTkP2 has started 1 tasks: task 5ae92503166b43289cd9cc24d9396e6b. | 52e562f6-68fc-4b12-b3a-b97c1c41c1c6 |
| 2023年8月16日 07:20 (UTC+9:00) | service SAW-TroubleshootECSTaskFailedToStart-MyFargateService-bfqNwghsTkP2 is unable to consistently start tasks successfully. For more information, see the Troubleshooting section of the Amazon ECS Developer Guide. | 626ae6d3-21e9-4393-b4d3-9fca7062d067 |
| 2023年8月16日 07:06 (UTC+9:00) | service SAW-TroubleshootECSTaskFailedToStart-MyFargateService-bfqNwghsTkP2 has started 1 tasks: task a2df6a3d5024415aa0dccc8bb9a07f63. | 6bb3aeb6-28ea-4023-98e620060fc676 |

Amazon Elastic Container Service > クラスター > cluster-SAW-TroubleshootECSTaskFailedToStart > タスク > 5ae92503166b43289cd9cc24d9396e6b > 設定

5ae92503166b43289cd9cc24d9396e6b 設定 停止

タスクの停止時刻: 2023-08-15T22:37:18.794Z
CannotPullContainerError: pull image manifest has been retried 5 time(s): failed to resolve ref docker.io/library/amazonlinux:latest: failed to do request: Head "https://registry-1.docker.io/v2/library/amazonlinux/manifests/latest": dial tcp 3.216.34.172:443: i/o timeout

設定 ログ ネットワーキング タグ

タスクの概要

| | | | |
|---|------------------|------------------|--------------------------------------|
| ARN 5ae92503166b43289cd9cc24d9396e6b | 前回のステータス 停止済み | 必要なステータス 停止済み | 開始/作成時刻: 2023-08-15T22:33:13.310Z |
|---|------------------|------------------|--------------------------------------|

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

AWS Support-Troubleshoot EC2 Task Failed To Start

- 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

Amazon Elastic Container Service > クラスター > cluster-SAW-TroubleshootECSTaskFailedToStart > タスク > 5ae92503166b43289cd9cc24d9396e6b > 設定

5ae92503166b43289cd9cc24d9396e6b 🔄 停止

タスクの停止時刻: 2023-08-15T22:37:18.794Z
CannotPullContainerError: pull image manifest has been retried 5 time(s): failed to resolve ref docker.io/library/amazonlinux:latest: failed to do request: Head "https://registry-1.docker.io/v2/library/amazonlinux/manifests/latest": dial tcp 3.216.34.172:443: i/o timeout

設定 ログ ネットワーキング タグ

タスクの概要

| | | | |
|----------------------------------|----------|----------|-------------------------------|
| ARN | 前回のステータス | 必要なステータス | 開始/作成時刻: |
| 5ae92503166b43289cd9cc24d9396e6b | ⊖ 停止済み | ⊖ 停止済み | - 2023-08-15T22:33:13.310Z |

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。

AWS Systems Manager > ドキュメント > AWSSupport-TroubleshootECSTaskFailedToStart

☆ AWSSupport-TroubleshootECSTaskFailedToStart

説明 コンテンツ バージョン 詳細

ドキュメントのバージョン
5 (デフォルト)

▼ ドキュメントの説明

| プラットフォーム | 作成済み | 所有者 | ターゲットタイプ |
|-----------------------|-------------------------------|--------|----------|
| Windows, Linux, MacOS | Tue, 25 Apr 2023 11:03:05 GMT | Amazon | / |

ステータス
🟢 Active

The AWSSupport-TroubleshootECSTaskFailedToStart runbook helps you troubleshoot why an Amazon Elastic Container Service (Amazon ECS) task in an Amazon ECS cluster failed to start. The runbook analyzes the following common issues that can prevent a task from starting:

- Network connectivity to the configured container registry
- Missing IAM permissions required by the task execution role
- VPC endpoint connectivity
- Security group rule configuration
- AWS Secrets Manager secrets references
- Logging configuration

入力パラメータ

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.
Choose an option

ClusterName
(Required) The name of the Amazon ECS cluster where the task failed to start.
String

TaskId
(Required) The ID of the failed task.
String

CloudwatchRetentionPeriod
(Optional) The retention period, in days, for the Lambda function logs to be stored in Amazon CloudWatch Logs. This is only necessary if the analysis determines network connectivity needs to be tested.
30

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

AWS Systems Manager > オートメーション > 実行 ID: 438de02a-aa46-4fc5-8d02-db3016de1b9b

実行の詳細: AWSSupport-TroubleshootECSTaskFailedToStart

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

▼ 出力

04_Execution_Results.01_TaskFailureReason

["***.***.***.***", "***.***.***.***"] resolved from domain name [docker.io] is not allowed in the egress of Security Group/s [['sg-*****']] 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

```
Amazon Elastic Container Service > クラスタ > fargate > タスク > f521c5c644114e8e80b54a8e344fe3b3 > 設定
```

f521c5c644114e8e80b54a8e344fe3b3 🔄 停止

 **タスクの停止時刻: 2023-08-16T05:15:49.786Z**

ResourceInitializationError: unable to pull secrets or registry auth: execution resource retrieval failed: unable to retrieve secret from asm: service call has been retried 1 time(s): failed to fetch secret arn:aws:secretsmanager:ap-northeast-1:123456789012:secret:example-secret-123456789012 from secrets manager: AccessDeniedException: User: arn:aws:sts::123456789012:assumed-role/NoPolicyEcsExecutionRole/f521c5c644114e8e80b54a8e344fe3b3 is not authorized to perform: secretsmanager:GetSecretValue on resource: arn:aws:secretsmanager:ap-northeast-1:123456789012:secret:example-secret-123456789012 because no identity-based policy allows the secretsmanager:GetSecretValue action status code: 400, request id: 12345678901234567890123456789012

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

```
▼ 出力

04_Execution_Results.01_TaskFailureReason

Task Failure Reason Analysis:
#####

REGISTRY CHECKS
=====
The Task Execution role [arn:aws:iam::[REDACTED]:role/NoPolicyEcsExecutionRole] doesn't have required permission to perform authentication for ['ecr:GetAuthorizationToken'].ECR GetAuthorizationToken action s
- https://docs.aws.amazon.com/AmazonECR/latest/userguide/repository-policy-examples.html

The Task execution role used by the task [arn:aws:iam::[REDACTED]:role/NoPolicyEcsExecutionRole] is missing the following required permission(s) to pull the image from ECR repository [mirror-alpine]:
['ecr:BatchCheckLayerAvailability', 'ecr:GetDownloadUrlForLayer', 'ecr:BatchGetImage']
Make sure that the Task execution role policy attached has all the recommended permissions.
- https://docs.aws.amazon.com/AmazonECS/latest/developerguide/task_execution_IAM_role.html

Log Configuration Checks
=====
The role arn:aws:iam::[REDACTED]:role/NoPolicyEcsExecutionRole doesn't have permission to perform AWS API Action ['logs:CreateLogStream', 'logs:PutLogEvents'] against the resource arn:aws:logs:ap-northeast-1:

SECRETS REFERENCE CHECKS
=====
The role arn:aws:iam::[REDACTED]:role/NoPolicyEcsExecutionRole does not have permission to perform ['secretsmanager:GetSecretValue'] against the resource arn:aws:secretsmanager:ap-northeast-1:[REDACTED]:se
.Make sure the task execution role has the permission according to the following documentation: https://docs.aws.amazon.com/AmazonECS/latest/developerguide/specifying-sensitive-data-parameters.html#secrets-iam
```

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

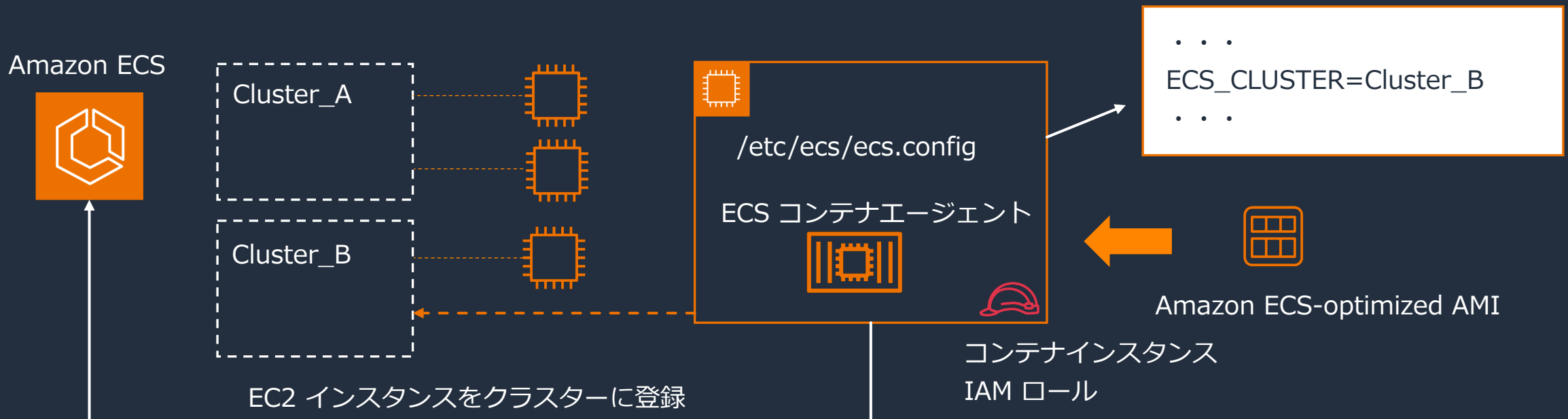
AWS Support- Troubleshoot ECS Container Instance

AWS Support-Troubleshoot ECS Container Instance

- 利用ユースケース

- ECS クラスタに登録される想定 of 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に表示されない場合

クラスタに登録されるまでの流れ(イメージ)



AWS Support-Troubleshoot ECS Container Instance

- 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

AWS Support-Troubleshoot ECS Container Instance

- 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

AWS Support-Troubleshoot ECS Container Instance

- 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エCS 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。

AWS Systems Manager > ドキュメント > AWSSupport-TroubleshootECSContainerInstance

☆ AWSSupport-TroubleshootECSContainerInstance

説明 コンテンツ バージョン 詳細

ドキュメントのバージョン
4 (デフォルト)

▼ ドキュメントの説明

| プラットフォーム | 作成済み | 所有者 | ターゲットタイプ |
|-----------------------|-------------------------------|--------|----------|
| Windows, Linux, MacOS | Tue, 01 Aug 2023 10:20:44 GMT | Amazon | / |

ステータス
⊙ Active

The AWSSupport-TroubleshootECSContainerInstance runbook helps you troubleshoot an Amazon Elastic Compute Cloud (Amazon EC2) instance that fails to register with an Amazon Elastic Container Service (Amazon ECS) cluster. This automation reviews whether the user data for the instance contains the correct cluster information, whether the instance profile contains the required permissions, and network configuration issues.

入力パラメータ

AutomationAssumeRole
(Optional) The ARN of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.
Choose IAMRole

ClusterName
(Required) The name of the Amazon ECS cluster that the instance failed to register with.
test

InstancedId
(Required) The ID of the Amazon EC2 instance you want to troubleshoot.
i-aaaaaaaa

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

```
AWS Systems Manager > オートメーション > 実行 ID: 9f04ae5e-de44-40ba-9821-caf884e65568  
実行の詳細: AWSSupport-TroubleshootECSContainerInstance [実行をキャンセルする] [アクション ▼]  
▶ 実行の説明  
▼ 出力  
executeChecker.stdout  
Cluster name provided cluster-SAW-TroubleshootECSContainerInstance is not matching with the cluster name inside of the user data section.  
Make sure that you are using the correct cluster name for the environment ECS_CLUSTER inside of the /etc/ecs/ecs.config file.  
See https://docs.aws.amazon.com/AmazonECS/latest/developerguide/bootstrap\_container\_instance.html  
The container instance profile SAW-TroubleshootECSContainerInstance-MyEcsInstanceProfile-yrHL8vrs9ic1 is missing the following required permission(s):  
['ecs:RegisterContainerInstance', 'ecs:CreateCluster', 'ecs:DeregisterContainerInstance', 'ecs:DiscoverPollEndpoint', 'ecs:Poll', 'ecs:StartTelemetrySession', 'ecs:UpdateContainerInstance']  
Make sure that the container instance has all the recommended permissions.  
See https://docs.aws.amazon.com/AmazonECS/latest/developerguide/security-iam-awsmanpol.html#instance-iam-role-permissions
```


AWS Support- Collect ECS Instance Logs

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使用する 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

AWS Support-CollectECSInstanceLogs

- 問題事象確認方法
 - タスク状態
 - 「AWS Support-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

AWS Support-Troubleshoot ECS Container Instance

- 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-Optimized AMI Amazon Linux 2023, ECS-Optimized 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-Optimized 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-Optimized 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

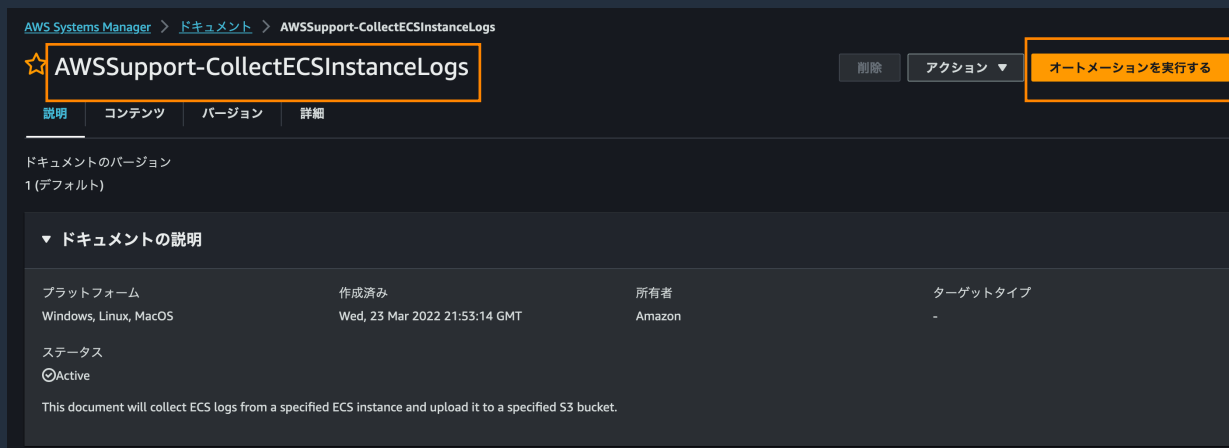


SAW(ランブック)実行例

- 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。



AWS Systems Manager > ドキュメント > AWSSupport-CollectECSInstanceLogs

☆ AWSSupport-CollectECSInstanceLogs

説明 コンテンツ バージョン 詳細

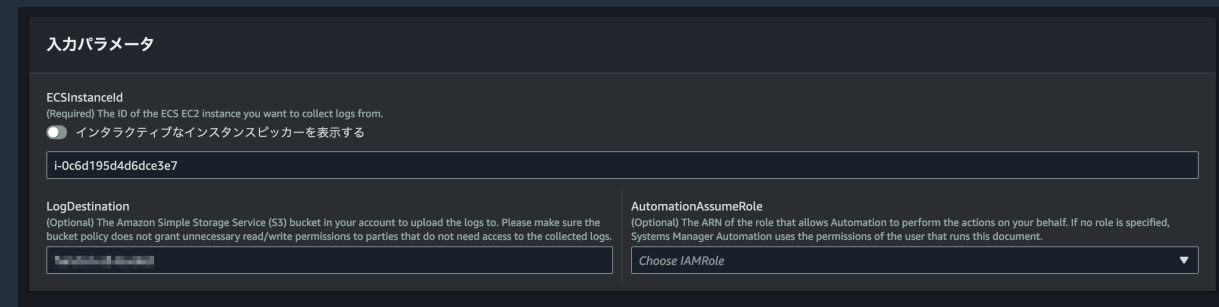
ドキュメントのバージョン
1 (デフォルト)

▼ ドキュメントの説明

| プラットフォーム | 作成済み | 所有者 | ターゲットタイプ |
|-----------------------|-------------------------------|--------|----------|
| Windows, Linux, MacOS | Wed, 23 Mar 2022 21:53:14 GMT | Amazon | - |

ステータス
● Active

This document will collect ECS logs from a specified ECS instance and upload it to a specified S3 bucket.



入力パラメータ

ECSInstanceID
(Required) The ID of the ECS EC2 instance you want to collect logs from.
 インタラクティブなインスタンスピッカーを表示する

i-0c6d195d4d6dce3e7

LogDestination
(Optional) The Amazon Simple Storage Service (S3) bucket in your account to upload the logs to. Please make sure the bucket policy does not grant unnecessary read/write permissions to parties that do not need access to the collected logs.

AutomationAssumeRole
(Optional) The ARN of the role that allows Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that runs this document.

Choose IAMRole

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

AWS Systems Manager > オートメーション > 実行 ID: 1042f910-7df1-454b-9402-87359975736b

実行の詳細: AWSSupport-CollectECSInstanceLogs

実行の説明

出力

この実行には出力がありません

実行ステータス

| | | |
|-----------|---------------|------------|
| 全体的なステータス | 実行されたすべてのステップ | # 成功 |
| 成功 | 7 | 7 |
| # 失敗 | # キャンセル済み | # TimedOut |
| 0 | 0 | 0 |

- S3 コンソールでアップロードされたログが確認できる

Amazon S3 > バケット > saw-collectecsinstance-log-s3-s3bucket-lv1ktsa0dkmf

saw-collectecsinstance-log-s3-s3bucket-lv1ktsa0dkmf 情報

オブジェクト プロパティ アクセス許可 メトリクス 管理 アクセスポイント

オブジェクト (4)

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。Amazon S3 インベントリを使用して、バケット内のすべてのオブジェクトのリストを取得できます。他のユーザーが自分のオブジェクトにアクセスできるようにするには、明示的にアクセス権限を付与する必要があります。詳細はこちら

オブジェクトの検索

| 名前 | タイプ | 最終更新日時 | サイズ | ストレージクラス |
|---|-----|----------------------------|---------|----------|
| ecs_i-0288fb28dc37c774e_5382520a-338b-4db1-baf1-101948c7688ftgz | tgz | 2023/09/08 12:31:57 PM JST | 63.5 KB | スタンダード |

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!