



# 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 Kubernetes Service (Amazon EKS) 編

坂元 龍太

Cloud Support Engineer

2023/11

# 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 11 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 EKS を利用した運用を実施されている方
  - Amazon EKS のトラブルシューティングの効率化に興味のある方
- 本セミナーのゴール
  - Amazon EKS 向けに利用可能な 3 つの SAW(AWS Support Automation Workflows) について利用ユースケースおよび概要を理解する
- 本セミナーの前提知識
  - [\[AWS Black Belt Online Seminar\] Amazon Elastic Container Service for Kubernetes \(Amazon EKS\)](#)
  - [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

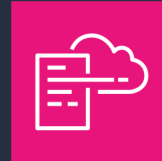
名前：坂元 龍太 (Ryota Sakamoto)

所属：技術支援本部 (AWS サポート)

好きなAWSサービス：



Amazon Elastic Kubernetes Service (Amazon EKS)



AWS CloudFormation



# アジェンダ

- Amazon EKS のよくあるお問い合わせと SAW の紹介
  - AWSPremiumSupport-TroubleshootEKSCluster
  - AWSSupport-TroubleshootEKSWorkerNode
  - AWSSupport-CollectEKSIInstanceLogs
- サポートへのお問い合わせについて
- まとめ

# Amazon EKS のよくあるお問い合わせ と SAW の紹介

# Amazon EKS の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: Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上から kubectl を実行できるようにしたい

- 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

- AWS Load Balancer Controller から Application Load Balancer が作成されない
- EC2 インスタンスを起動したが、クラスターにワーカーノードとして参加されない
- ワーカーノードで問題が発生しており、ログが収集したい



# Amazon EKS の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: Amazon Elastic Compute Cloud (Amazon EC2) インスタンス上から kubectl を実行できるようにしたい

- 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

- AWS Load Balancer Controller から Application Load Balancer が作成されない
- EC2 インスタンスを起動したが、クラスターにワーカーノードとして参加されない
- ワーカーノードで問題が発生しており、ログが収集したい

SAW によって問題の解析や解消が可能な範囲

# Amazon EKS のよくあるお問い合わせ

- AWS Load Balancer Controller から Application Load Balancer が作成されない
  - SAW(AWSPremiumSupport-TroubleshootEKSCluster)を利用することで **問題解析**ができ、**問題解消**ができる可能性がある
- EC2 インスタンスを起動したが、クラスターにワーカーノードとして参加されない
  - SAW(AWSSupport-TroubleshootEKSWorkerNode)を利用することで、**問題解析**ができ、**問題解消**ができる可能性がある
- ワーカーノードで問題が発生しており、ログが収集したい
  - SAW(AWSSupport-CollectEKSIInstanceLogs)を利用することで、調査のために必要なログを**まとめて収集**できる

# Amazon EKS で利用可能な SAW(ランブック)

名称	カテゴリ	概要
AWSPremiumSupport-TroubleshootEKSCluster	トラブルシューティング	Amazon EKS クラスタ、基盤となるインフラストラクチャに関する一般的な問題を診断し、推奨される修復手順を提供する
AWSSupport-TroubleshootEKSWorkerNode	トラブルシューティング	ワーカーノードがクラスタに参加するのを妨げる一般的な原因の特定とトラブルシューティングを行う
AWSSupport-CollectEKSInstanceLogs	ログ収集	EC2 インスタンスからオペレーティングシステムと Amazon EKS 関連のログファイルを収集

- プレフィックスが「AWSPremiumSupport」のランブックは、エンタープライズおよびビジネスサポートのお客様にご利用いただけます
- プレフィックスが「AWSSupport」のランブックは、すべてのお客様にご利用いただけます

# AWS Premium Support- Troubleshoot EKS Cluster

# AWS Premium Support-Troubleshoot EKS Cluster

- ランブックの内容
  - Amazon EKS クラスタ、基盤となるインフラストラクチャに関する一般的な問題を診断し、推奨される修復手順を提供する
- 利用ユースケース
  - 具体例
    - Pod が Pending で止まり、Pod が起動しない
    - AWS Load Balancer Controller から Application Load Balancer が作成されない場合
- ドキュメント
  - [https://docs.aws.amazon.com/ja\\_jp/systems-manager-automation-runbooks/latest/userguide/automation-awspremiumsupport-troubleshootekscluster.html](https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awspremiumsupport-troubleshootekscluster.html)
  - <https://repost.aws/ja/knowledge-center/eks-cluster-creation-errors-workflow>

# AWS Premium Support-Troubleshoot EKS Cluster

- SAW(ランブック)が確認する内容
  - クラスタセキュリティグループ
  - クラスタとノードのネットワーク関連
  - ワーカーノードの AMI
  - ワーカーノードのロールに必要なポリシーが含まれているかどうか
  - タグ関連

# AWS Premium Support-Troubleshoot EKS Cluster

- SAW(ランブック)入力パラメータ
  - ClusterName(必須)
    - EKS クラスタ名
  - S3BucketName(オプション)
    - Amazon Simple Storage Service(Amazon S3) バケット名
    - 指定した S3 バケットに SAW の実行結果が保存される
  - 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-awspremiumsupport-troubleshootekscluster.html](https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awspremiumsupport-troubleshootekscluster.html)

# SAW(ランブック)実行方法

- 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、入力パラメータ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](#)」をご参照ください

The screenshot displays the AWS Systems Manager console interface for a document titled 'AWSPremiumSupport-TroubleshootEKSCluster'. At the top, there are navigation links for 'AWS Systems Manager', 'ドキュメント', and the specific document name. The document title is accompanied by a star icon and a '削除' (Delete) button, an 'アクション' (Action) dropdown menu, and a prominent yellow 'オートメーションを実行する' (Execute Automation) button. Below the title, there are tabs for '説明' (Description), 'コンテンツ' (Content), 'バージョン' (Versions), and '詳細' (Details). The '説明' tab is active, showing the document's version (1 (デフォルト)) and a table of details. The table includes 'プラットフォーム' (Platform) as 'Windows, Linux' with a status of '作成済み' (Created) on 'Mon, 16 Aug 2021 09:04:34 GMT', and 'ステータス' (Status) as 'Active'. A brief description states: 'This document will help diagnose various issues with an EKS Cluster and underlying infrastructure and suggest re...'. To the right of the description, an '入力パラメータ' (Input Parameters) section is visible, containing three fields: 'ClusterName' (String, The name of the EKS cluster to troubleshoot.), 'S3BucketName' (String, Optional) (Optional) The name of the private S3 bucket where the generated report will be uploaded., and 'AutomationAssumeRole' (Choose IAMRole, (Optional) The ARN of the IAM role that allows the Automation to perform actions on your behalf.). Below the description, a 'ステップ 1: getEksClusterDetails' section is shown, with a table listing the step name 'getEksClusterDetails' and the action 'aws:executeAwsApi'.

プラットフォーム	作成済み
Windows, Linux	Mon, 16 Aug 2021 09:04:34 GMT

ステータス
Active

ステップ名	アクション
getEksClusterDetails	aws:executeAwsApi



# SAW(ランブック)実行例1

- シチュエーション
  - Pod のステータスが Pending となり、Pod が起動しない
- 問題の確認方法(kubectl)

## 1. Pod のステータスを確認

```
> kubectl get pods test-pod-6ddbc6dd5f-bjcrn -o wide
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED NODE	READINESS GATES
test-pod-6ddbc6dd5f-bjcrn	0/1	Pending	0	2m45s	<none>	<none>	<none>	<none>

## 2. Node のステータスを確認

```
> kubectl get node ip-172-31-95-53.ap-northeast-1.compute.internal
```

NAME	STATUS	ROLES	AGE	VERSION
ip-172-31-95-53.ap-northeast-1.compute.internal	NotReady	<none>	3m55s	v1.28.3-eks-e71965b

## 3. Amazon VPC CNI plugin for Kubernetes のステータスを確認

```
> kubectl -n kube-system get pods -o wide -l k8s-app=aws-node
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED NODE	READINESS GATES
aws-node-7dmcn	1/2	Running	3 (5s ago)	4m50s	172.31.95.53	ip-172-31-95-53.ap-northeast-1.compute.internal	<none>	<none>

# SAW(ランブック)実行例1

## • 実行結果

- EC2 インスタンスにアタッチされているロールに必要なポリシーが含まれていないことを特定
- ロールに必要なポリシーを追加することで解決

do not have the IAM policy - AmazonEKS\_CNI\_Policy. The policy must be attached to either the instance role or to a different role that is mapped to the 'aws-node' Kubernetes service account.

# SAW(ランブック)実行例2

- シチュエーション
  - AWS Load Balancer Controller から Application Load Balancer が作成されない
- 問題の確認方法
  - kubectl コマンドを実行して Ingress のステータスを確認

```
> kubectl get ingress
NAME          CLASS  HOSTS          ADDRESS  PORTS  AGE
ingress-test  alb    test.example.com    80     65s
```

ADDRESS が空であることを確認

# SAW(ランブック)実行例2

## • 実行結果

- VPC のサブネットに適切にタグが設定されていないことを特定
- サブネットへタグを追加することで問題解消

```
generateReport.Troubleshoot_EKS_Cluster_ReportUrl
generateReport.Troubleshoot_EKS_Cluster_Report
Report_Summary:
Errors
1 Error(s) were found.
- [EC2 Instance(s) Check] No instances were found in your EKS Cluster containing the tag key: 'kubernetes.io/cluster/test-cluster' and value: 'owned'. Please refer to https://docs.aws.amazon.com/eks/
Warnings
2 Warning(s) were found.
- [Load Balancer Tag Check] If you want to use internet facing Load Balancers for the subnet(s) ['subnet-***', 'subnet-***', 'subnet-***'], please add 'kuber
- [Load Balancer Tag Check] If you want to use internal Load Balancers for the subnet(s) ['
Info
1 Info notice(s)
- [Subnet Tag Check] The subnet(s) : ['
```

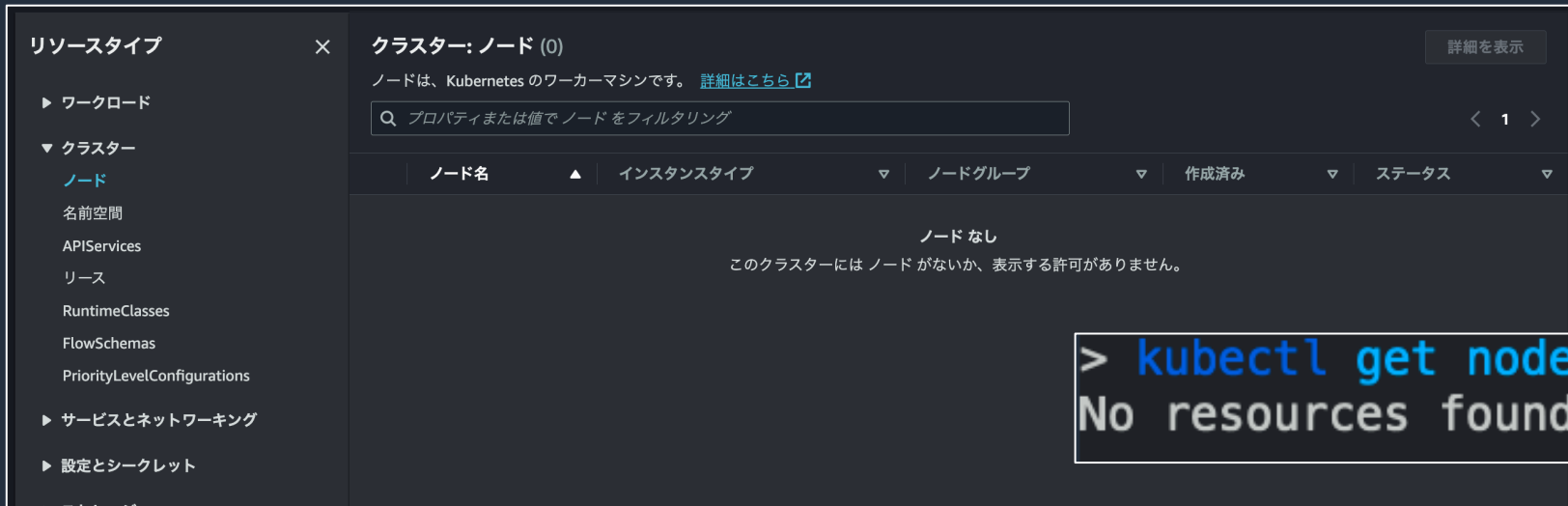
# AWS Support- Troubleshoot EKS Worker Node

# AWS Support-Troubleshoot EKS Worker Node

- ランブックの内容
  - ワーカーノードがクラスターに参加するのを妨げる一般的な原因の特定とトラブルシューティングを行う
- 利用ユースケース
  - 具体例
    - ワーカーノードを起動したがクラスターに参加しない
- ドキュメント
  - [https://docs.aws.amazon.com/ja\\_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-troubleshooteksworkernode.html](https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-troubleshooteksworkernode.html)
  - <https://repost.aws/ja/knowledge-center/resolve-eks-node-failures>

# AWS Support-Troubleshoot EKS Worker Node

- シチュエーション
  - ワーカーノードを起動したがクラスターに参加しない
- 問題の確認方法
  - マネジメントコンソールもしくは `kubectl` コマンドを実行して Node が結果に含まれているかどうか



The screenshot shows the AWS Management Console interface for an EKS cluster. The left sidebar lists various resource types, with 'ノード' (Nodes) selected under the 'クラスター' (Cluster) section. The main content area displays 'クラスター: ノード (0)' (Cluster: Nodes (0)) and indicates that no nodes are present in the cluster. A table with columns for 'ノード名' (Node Name), 'インスタンスタイプ' (Instance Type), 'ノードグループ' (Node Group), '作成済み' (Created), and 'ステータス' (Status) is shown, but it is empty. A message states: 'このクラスターには ノード がないか、表示する許可がありません。' (There are no nodes in this cluster, or you do not have permission to view them). A terminal window overlay shows the command `> kubectl get node` and the output `No resources found`.

# AWS Support-Troubleshoot EKS Worker Node

- SAW(ランブック)が確認する内容
  - クラスターレベルの解析
    - VPC
    - セキュリティグループ
    - ENI
    - クラスターロール
  - インスタンスレベルの解析
    - インスタンスタイプ
    - AMI のバージョン
    - ネットワーク関連
    - インスタンスプロファイル
    - タグ



# SAW(ランブック)入力パラメータ

- ClusterName(必須)
  - EKS クラスター名
- WorkerID(必須)
  - EC2 インスタンスの ID
- AutomationAssumeRole(オプション)
  - Automation が各種 API を呼び出す際に使用するロール名
  - 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-awssupport-troubleshooteksworkernode.html](https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-troubleshooteksworkernode.html)

# SAW(ランブック)実行方法

- 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、入力パラメータ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](#)」をご参照ください

AWSSupport-TroubleshootEKSWorkerNode

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  
11 (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
Windows, Linux, MacOS	Fri, 31 Mar 2023 05:25:24 GMT	Amazon

ステータス  
Active

### AWSSupport-TroubleshootEKSWorkerNode

The `AWSSupport-TroubleshootEKSWorkerNode` runbook is designed to help troubleshooting EKS worker node that failed to join and validates the following:

- Node tags are applied.
- Worker node Instance type is supported.
- Network communication between worker node and Cluster API server is allowed.
- Node IAM Role and Policies.
- Cluster IAM role and Policies.

### 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 an option

**WorkerID**  
(Required) The EC2 instance ID for the Worker node which failed to join the cluster  
String  
⚠ 入力が必要な期待されたパターンと一致しません: ^[a-z0-9]{8,17}\$

**ClusterName**  
(Required) The name of the EKS cluster  
String

# SAW(ランブック)実行例

## • 実行結果

- クラスターセキュリティグループにて許可されていない
- ワーカーノードにインスタンスプロファイルがアタッチされていない
- ユーザーデータが正しく記載されていない

```
▼ 出力

TroubleshootWorkerNode.Message
HERE IS A SUMMARY OF THE ITEMS THAT REQUIRE YOUR ATTENTION:

[ERROR]: The cluster Security Group sg-██████████ is not allowing traffic from the worker node.
[WARNING]: Worker node outbound IP to internet is ██████████. It is not allowed in the cluster Public CIDR ranges. Please review this URL for further details: https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html
[ERROR]: Worker node has no Instance Profile attached to it. Please review this URL for further details: https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html
[ERROR]: The UserData of the worker node must contain the bootstrap script with correct EKS cluster name. Please review this URL for further details: https://aws.amazon.com/premiumsupport/knowledge-center/eks-bootstrap-script/
[WARNING]: Worker node i-██████████ does not have the required tags. Set tag key to kubernetes.io/cluster/stella and set tag value to owned. Please review this URL for further details: https://docs.aws.amazon.com/eks/latest/userguide/worker-node-requirements.html
[WARNING]: No secondary private IP addresses are assigned to worker node i-██████████, ensure that the CNI plugin is running properly. Please review this URL for further details: https://docs.aws.amazon.com/eks/latest/userguide/worker-node-requirements.html
[WARNING]: The Outbound security group rules for worker node i-██████████ are customized and might limit outbound traffic to the EKS cluster endpoint. Please ensure that the security group outbound rules allow traffic to the EKS cluster endpoint.
[WARNING]: As SSM agent is not reachable on worker node, this document did not check the status of Containerd, Docker and Kubelet daemons. Ensure that required daemons (containerd, docker, kubelet) are installed and running.

-----
Here are the detailed steps of the document execution:

[X] Checking EKS cluster stella: EKS Cluster: stella is in Active state.

1. Checking if the cluster Security Group is allowing traffic from the worker node:
   [ERROR]: The cluster Security Group sg-██████████ is not allowing traffic from the worker node.

2. Checking DHCP options of the cluster VPC:
   Passed: AmazonProvidedDNS is enabled

3. Checking cluster IAM role arn:aws:iam::██████████:role/AmazonEKSClusterRole for the required permissions:
   Passed: IAM role for cluster stella has the required IAM policies attached.
   Passed: The cluster IAM role arn:aws:iam::██████████:role/AmazonEKSClusterRole has the required trust relationship for the EKS service.

4. Checking control plane Elastic Network Interfaces(ENIs) in the cluster VPC:
   Passed: The cluster Elastic Network Interfaces(ENIs) exist.

5. Cluster Endpoint Private access is disabled for your cluster, checking if the Public CIDR ranges include worker node i-██████████ outbound IP:
   [WARNING]: Worker node outbound IP to internet is ██████████. It is not allowed in the cluster Public CIDR ranges. Please review this URL for further details: https://docs.aws.amazon.com/eks/latest/userguide/create-node-role.html

6. Checking cluster VPC for required DNS attributes:
   Passed: Cluster VPC arn:aws:vpc:██████████:region:vpc-██████████ has the required DNS attributes correctly set.
```

複数項目のチェックが行われる

# AWS Support- Collect EKS Instance Logs

# AWSSupport-CollectEKSIInstanceLogs

- SAW(ランブック)の内容
  - ワーカーノードとして起動している EC2 インスタンスに関連する問題があり、EC2 インスタンス内のログを確認したい場合
- 利用ユースケース
  - 具体例
    - VPC CNI で何らかの問題が発生している場合
    - kubelet や containerd 等のログを確認したい場合
- ドキュメント
  - [https://docs.aws.amazon.com/ja\\_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-collecteksinstancelogs.html](https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-collecteksinstancelogs.html)
  - <https://repost.aws/ja/knowledge-center/eks-instances-log-bundles>

# AWSsupport-CollectEKSIInstanceLogs

- シチュエーション
  - Pod が ContainerCreating で止まり、正常に Pod が起動しない場合
- 問題の確認方法
  - kubectl get pods や kubectl describe pods コマンドを実行

```
> kubectl get pods test-pod-74b67d4858-78z4z -o wide
NAME                READY   STATUS             RESTARTS   AGE   IP        NODE                                                                 NOMINATED NODE   READINESS GATES
test-pod-74b67d4858-78z4z   0/1    ContainerCreating   0          37s   <none>    ip-172-31-240-75.ap-northeast-1.compute.internal             <none>            <none>
```

```
> kubectl describe pods test-pod-74b67d4858-78z4z | grep Events: -A5
Events:
  Type     Reason              Age             From              Message
  ----     -
  Normal   Scheduled           93s            default-scheduler Successfully assigned default/test-pod-74b67d4858-78z4z to ip-172-31-240-75.ap-northeast-1.compute.internal
  Warning  FailedCreatePodSandBox 86s            kubelet           Failed to create pod sandbox: rpc error: code = Unknown desc = failed to set up sandbox container "2dba9b24ae63957eae7f1903a8889f76934f758bc0ff84dc2e8534a825e058c3" network for pod "test-pod-74b67d4858-78z4z": networkPlugin cni failed to set up pod "test-pod-74b67d4858-78z4z_default" network: add cmd: failed to assign an IP address to container
  Warning  FailedCreatePodSandBox 79s            kubelet           Failed to create pod sandbox: rpc error: code = Unknown desc = failed to set up sandbox container "373463ca44c2686c46aa3cc838451076e7b2a90a8bd743fa2a83a28e4920c8be" network for pod "test-pod-74b67d4858-78z4z": networkPlugin cni failed to set up pod "test-pod-74b67d4858-78z4z_default" network: add cmd: failed to assign an IP address to container
```

IP アドレスのアサインに失敗していることを Pod のイベントから確認

# SAW(ランブック)入力パラメータ

- EKSIInstanceId(必須)
  - EC2 インスタンスの ID
  - 指定した EC2 インスタンス内にログが出力される
- LogDestination(オプション)
  - S3 バケット名
  - 指定した S3 バケットに収集したログがアップロードされる
- 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-awssupport-collecteksinstancelogs.html](https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-collecteksinstancelogs.html)



# SAW(ランブック)実行方法

- 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、入力パラメータ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](#)」をご参照ください

The screenshot shows the AWS Systems Manager console interface for the document 'AWSSupport-CollectEKSInstanceLogs'. The document is in an 'Active' state. The 'AutomationAssumeRole' dropdown menu is open, showing 'Choose IAM Role' as the selected option. The 'Input Parameters' section is also visible, with fields for 'EKSIInstanceID' and 'LogDestination'.

Document Name: AWSSupport-CollectEKSInstanceLogs

Platform: Windows, Linux, MacOS

Status: Active

AutomationAssumeRole: Choose IAM Role

Input Parameters:

- EKSIInstanceID: String
- LogDestination: String



# SAW(ランブック)実行例

- 実行結果

1. 成功していることを確認する

- 2-1. S3 コンソールでアップロードされたログが確認できる

The screenshot shows the AWS Systems Manager console. The breadcrumb navigation is 'AWS Systems Manager > オートメーション > 実行 ID: dc165ee0-24fd-48d8-adc0-e0154e4c77ea'. The main heading is '実行の詳細: AWSSupport-CollectEKSInstanceLogs'. There are buttons for '実行をキャンセルする' and 'アクション'. Under '実行の説明', there is a section for '出力' which states 'この実行には出力がありません'. Below that is the '実行ステータス' section with a table:

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	4	4
# 失敗	# キャンセル済み	# TimedOut
0	0	0

The screenshot shows the AWS S3 console 'オブジェクト' view. The breadcrumb navigation is '情報 > オブジェクト'. The main heading is 'オブジェクト (1)'. Below the heading is a table with columns: '名前', 'タイプ', '最終更新日時', 'サイズ', and 'ストレージクラス'. One object is listed:

名前	タイプ	最終更新日時	サイズ	ストレージクラス
eks_i- -9405-4db9-a0b1- 97844ff7f03a.tar.gz	gz	2023/11/15 11:37:04 AM JST	189.6 KB	スタンダード

- 2-2. EC2 インスタンス内から確認可能

```
sh-4.2$ ls /var/log/ | grep eks  
eks_i-  
_fc2c721f-9405-4db9-a0b1-97844ff7f03a.tar.gz
```

# SAW(ランブック)実行例

- 実行結果

- 3. ログを確認することで原因の解析が可能

```
sh-4.2$ grep "Insufficient" var_log/aws-routed-eni/ipamd.log
{"level":"error","ts":"2023-11-15T02:35:35.061Z","caller":"ipamd/ipamd.go:911","msg":"Failed to allocate a private IP/Prefix addresses on ENI eni-██████████: InsufficientFreeAddressesInSubnet: The specified subnet does not have enough free addresses to satisfy the request.\n\tstatus code: 400, request id: ██████████"}
{"level":"warn","ts":"2023-11-15T02:35:35.061Z","caller":"ipamd/ipamd.go:859","msg":"Failed to allocate 5 IP addresses on an ENI: InsufficientFreeAddressesInSubnet: The specified subnet does not have enough free addresses to satisfy the request.\n\tstatus code: 400, request id: ██████████"}
{"level":"debug","ts":"2023-11-15T02:35:35.061Z","caller":"ipamd/ipamd.go:916","msg":"Insufficient IP Addresses due to: InsufficientFreeAddressesInSubnet\n"}
{"level":"debug","ts":"2023-11-15T02:35:35.061Z","caller":"ipamd/ipamd.go:694","msg":"Error trying to allocate ENI: InsufficientFreeAddressesInSubnet: The specified subnet does not have enough free addresses to satisfy the request.\n\tstatus code: 400, request id: ██████████"}

```

サブネットの IP アドレスが  
枯渇していることがログから確認できる

# 収集するログについて(抜粋)

- OS 関連のログ
  - var\_log/messages, cloud-init.log
  - system/services.txt
  - kernel/dmesg.human.current
- EKS 関連のログ
  - var\_log/aws-routed-eni/ipamd.log
  - ipamd/enis.json
  - kubelet/kubelet.log

# 留意点

- EC2 インスタンスに SSM エージェントがインストールされている必要がある
- Windows や Fargate ノードには対応していません
- オプションで S3 バケット名を指定する場合、以下が必要
  - AWS CLI がインストールされている必要がある
    - Amazon EKS 最適化 AMI には、デフォルトでインストール済み
  - 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

# 補足

- ログの取得方法について
  - SAW(ランブック)を実行する
  - [EKS Log Collector](#) を実行する
    - EC2 インスタンス上で直接実行する
    - SSM ドキュメント経由で実行する
    - Amazon EKS 最適化 AMI にインストールされているスクリプトを使用

```
sh-4.2$ sudo bash /etc/eks/log-collector-script/eks-log-collector.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           %         %         Dload  Upload   Total   Spent    Left   Speed
100    56    100    56     0     0  41025      0  --:--:--  --:--:--  --:--:--  56000

This is version 0.7.6. New versions can be found at https://github.com/aws-labs/amazon-eks-ami/blob/master/log-collector-script/

Trying to collect common operating system logs...
Trying to collect kernel logs...
Trying to collect modinfo... Trying to collect mount points and volume information...
Trying to collect SELinux status...
Trying to collect iptables information...
Trying to collect installed packages...
Trying to collect active system services...
Trying to Collect Containerd daemon information...
Trying to Collect Containerd running information...
Trying to Collect Docker daemon information...

Warning: The Docker daemon is not running.
```

# サポートへのお問い合わせについて

# サポートへのお問い合わせについて

- SAW で全てのパターンの問題が解決するわけではないので、必要に応じて、サポートにケース起票をお願いします
- SAW を実行している場合、SAW の実行結果をご共有いただければと、原因絞り込みの過程で非常に有用です
- ケース起票の際は、下記の情報を記載いただければ幸いです
  - SAW(ランブック)名
  - SSM Automation の実行 ID
  - SAW(ランブック)の実行結果

# まとめ



# まとめ

- Amazon EKS の SAW を 3 つ紹介いたしました
- 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ます
  - 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
- 問題が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いただけますと幸いです



Thank you!