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

高橋 尚久

Senior Cloud Support Engineer
2023/10

自己紹介

名前：高橋 尚久（なおひさ）

所属：技術支援本部（AWS サポート）

経歴：メーカー、スタートアップで設計、開発、運用を経験

AWS Japan に入社し、アイルランド勤務後、日本に帰国

組織のプロセス改善、トレーニング、技術的な支援を推進

好きな AWS サービス：  Amazon S3、  Amazon Athena

本セミナーの対象者

自分の AWS 環境のトラブルシューティング経験のある方
運用、トラブルシューティングをより効率化したい方

本セミナーの目的

- AWS Support Automation Workflows(SAW) の使用方法とユースケースをご理解いただく
- 目的とするランブックを探し、実行する手順をご理解いただく

本日お話ししないこと

- AWS Systems Manager の全体的な説明
- AWS Systems Manager については全体像、各機能にフォーカスしたセッションを参照ください

セミナー概要

AWS SAW(AWS Support Automation Workflows) は、お客様の問題を解決して得たベストプラクティスをもとに AWS サポートによって作成されたセルフサービスな自動化のための仕組みをご提供しています

こちらを使用することにより、AWS リソースに関する一般的な問題のトラブルシューティング、診断、修正、運用が可能になります

AWS Systems Manager Automation を使用して実装されており、その仕組み、どのようなことができるか、どのようなシチュエーションで役立つかといった点について解説します

例として Amazon EC2 に関するランブックを 2 つご紹介します

アジェンダ

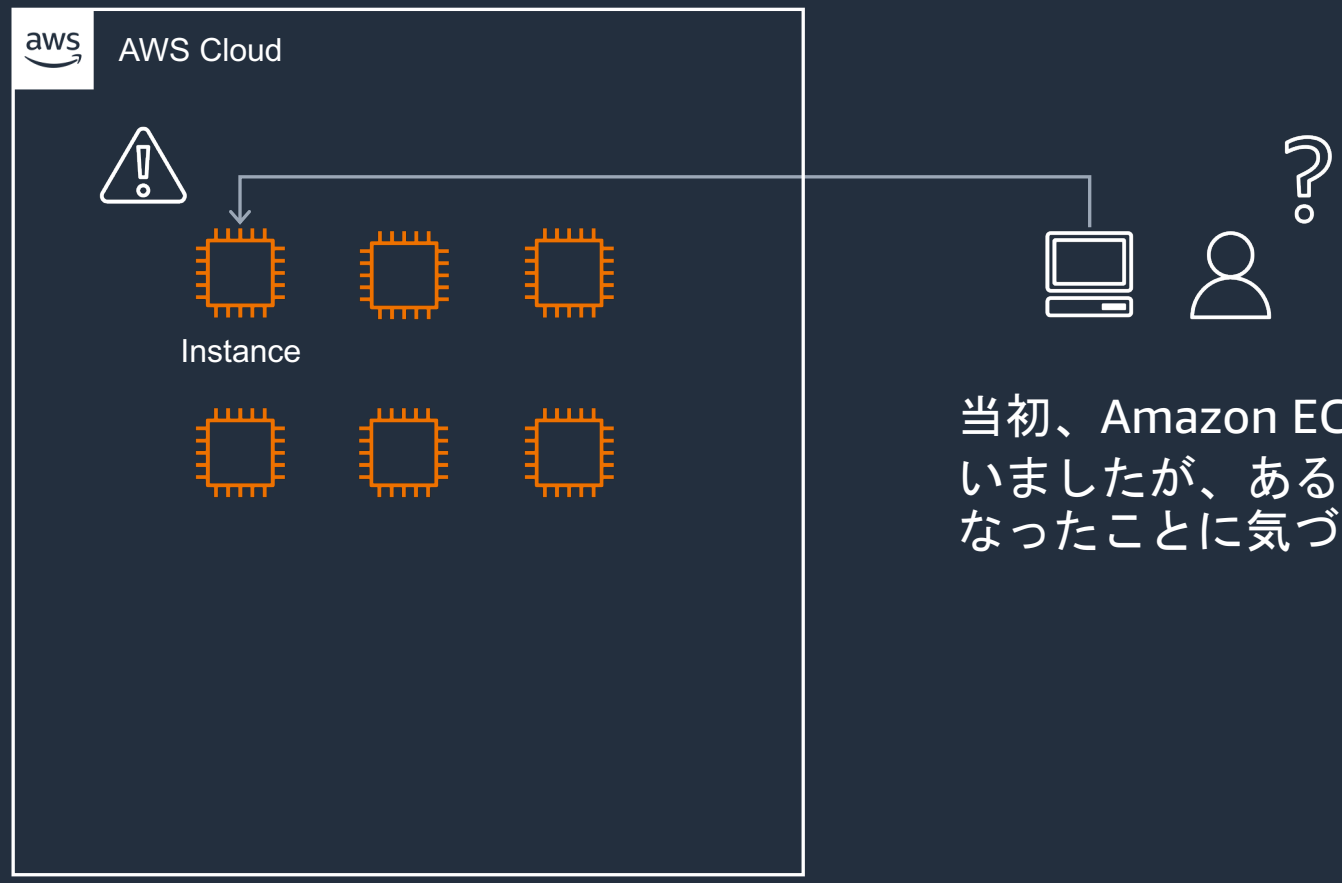
1. AWS Support Automation Workflows(SAW) が使用できるシチュエーション、具体的なシナリオの例
2. 概要と特徴
3. ランブックの使用方法
4. Amazon EC2 でよく使われるランブックの例
5. ランブックの探し方
6. 料金の説明
7. まとめ

AWS Support Automation Workflows(SAW) が使用できるシチュエーション

シチュエーションの例

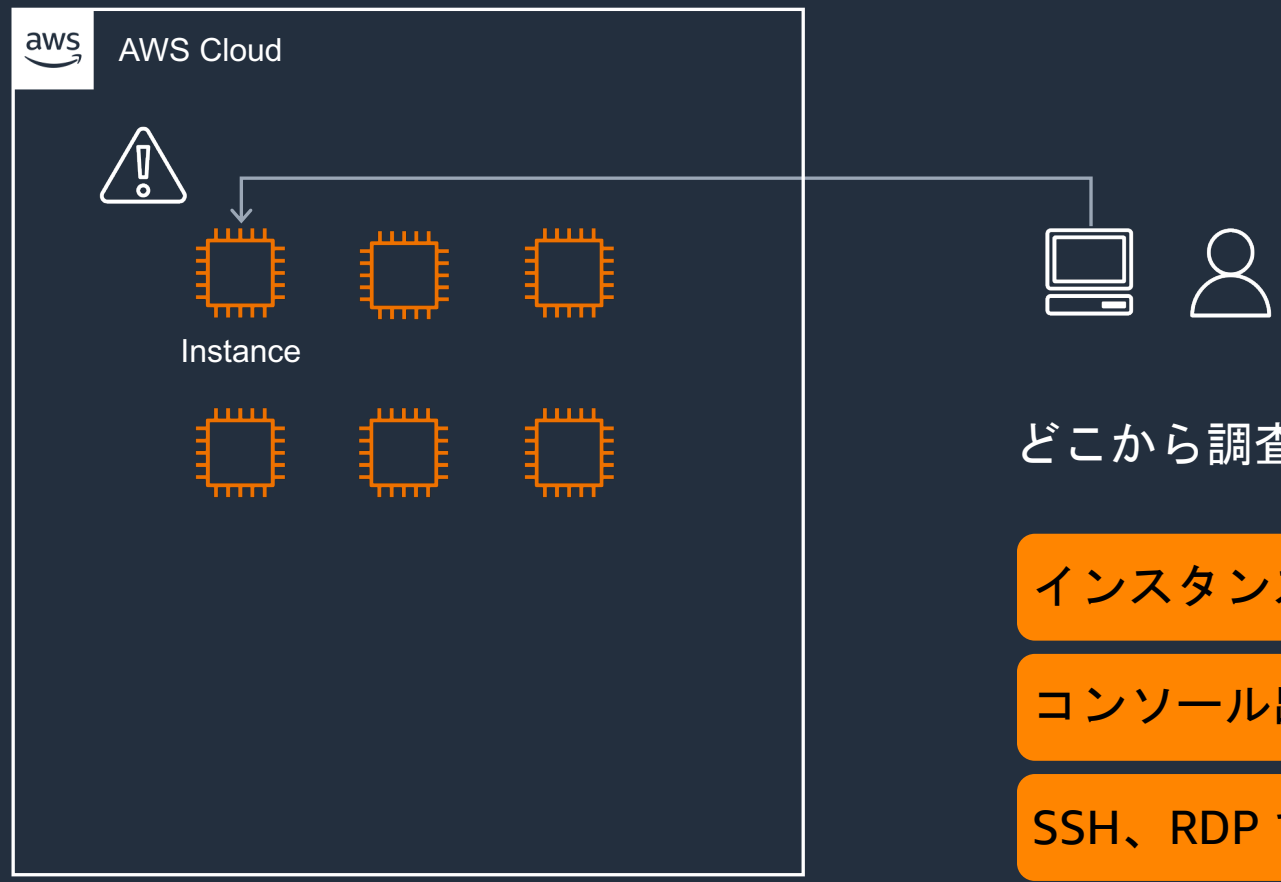
- SAW にはさまざまなトラブルシューティング、管理タスクを自動化するためのランブックが存在します
- 今回は一例として、「Amazon EC2 インスタンスにアクセスできなくなった」場合にどのような形で SAW を使用可能か解説します

運用中に問題が発生した場合



当初、Amazon EC2 インスタンスにアクセスできていましたが、あるタイミングからアクセスできなくなったことに気づきました

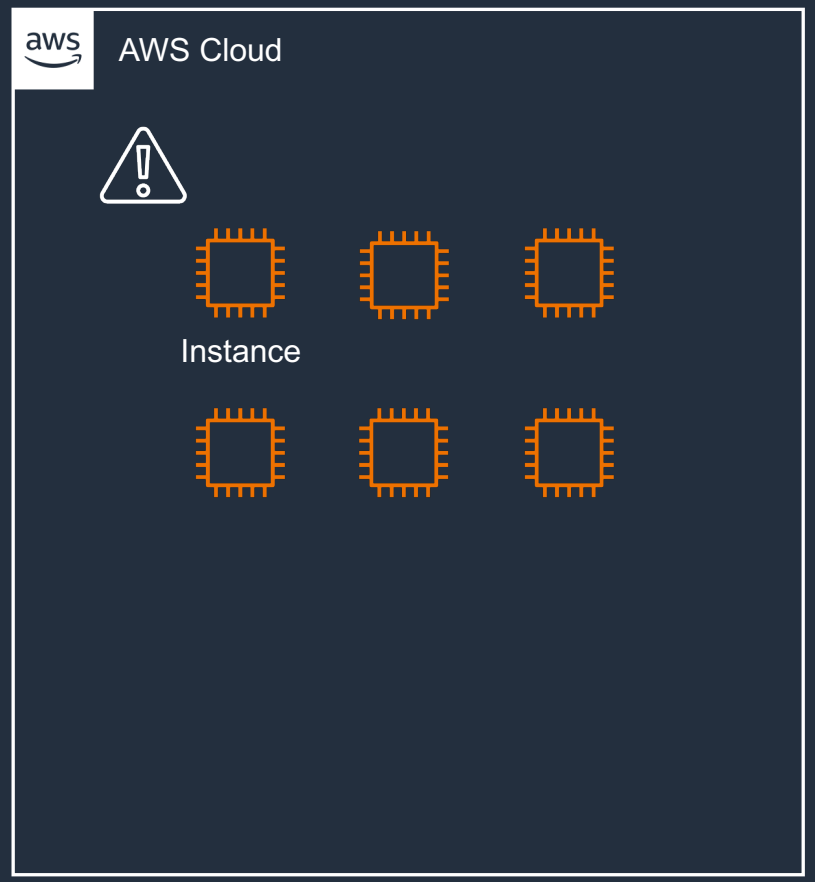
運用中に問題が発生した場合

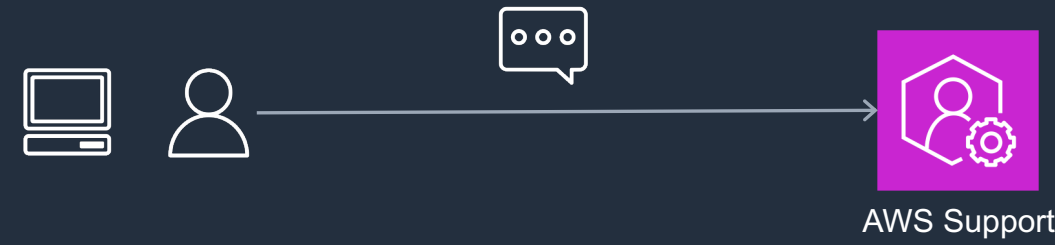


どこから調査していくべきでしょうか？

- インスタンスの再起動？停止・開始？
- コンソール出力、スクリーンショットの確認？
- SSH、RDP で接続？

運用中に問題が発生した場合

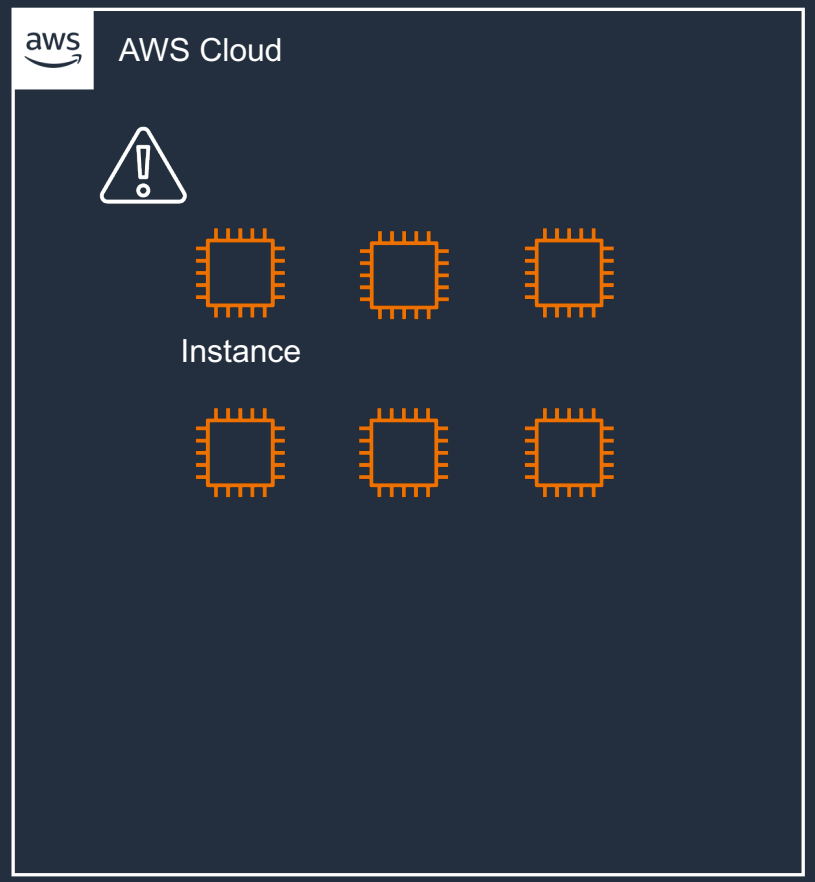




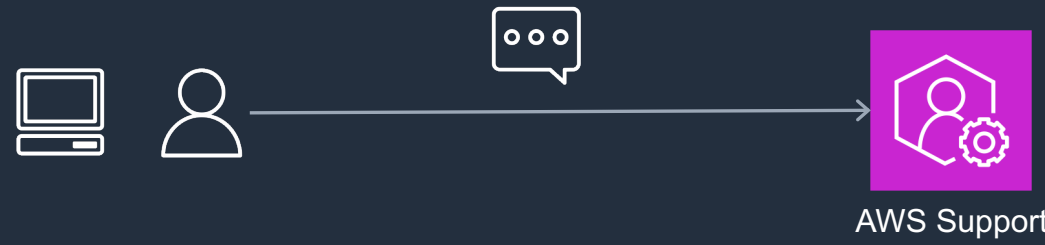
どこから調査していくべきか、わからない場合・・・

ひとまず、AWS サポートに問い合わせてみる場合も多いかと思います

運用中に問題が発生した場合



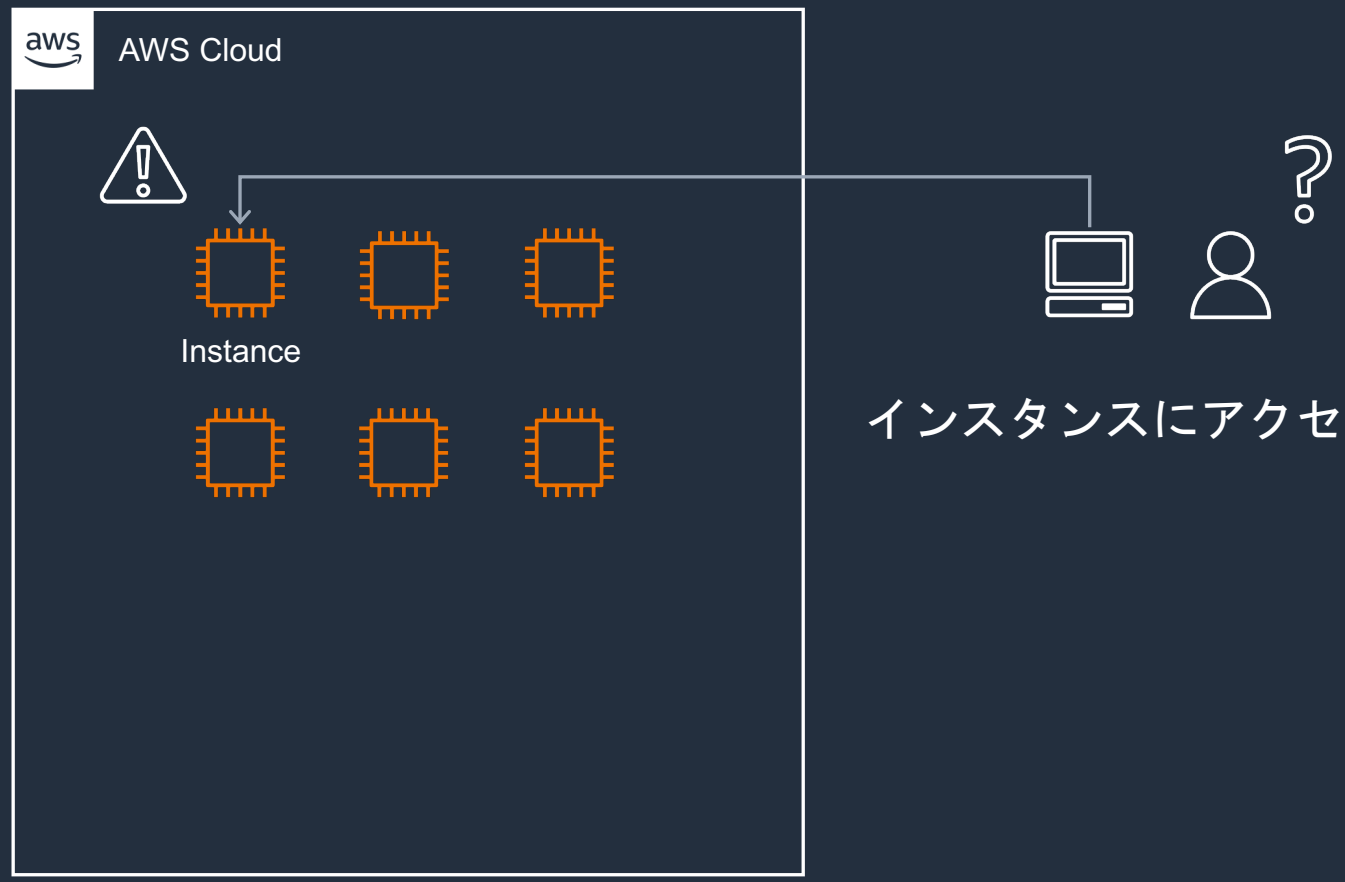
ご自身でできる対処は他にないでしょうか？



AWS サポートに問い合わせるために、情報の収集を行う必要があります
AWS サポートとのやり取りを進める必要があります

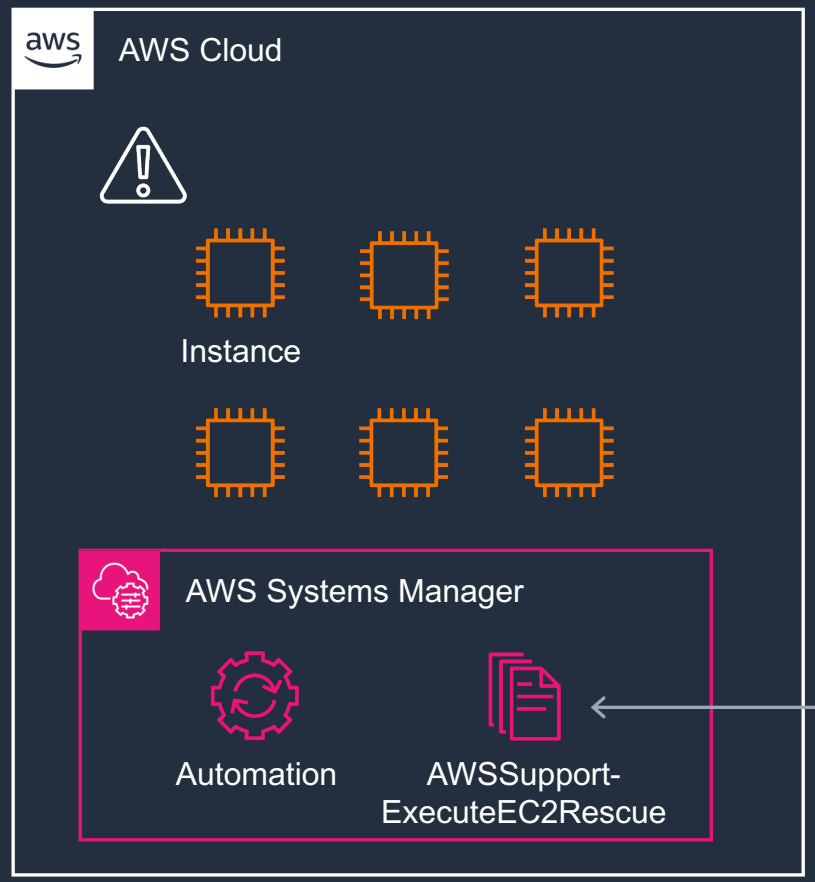
そこで AWS Support Automation Workflows(SAW) を使用していただくことで一般的な問題をご自身で対処できます

SAW を使用した場合



インスタンスにアクセスできなくなったことに気づきました

SAW を使用した場合

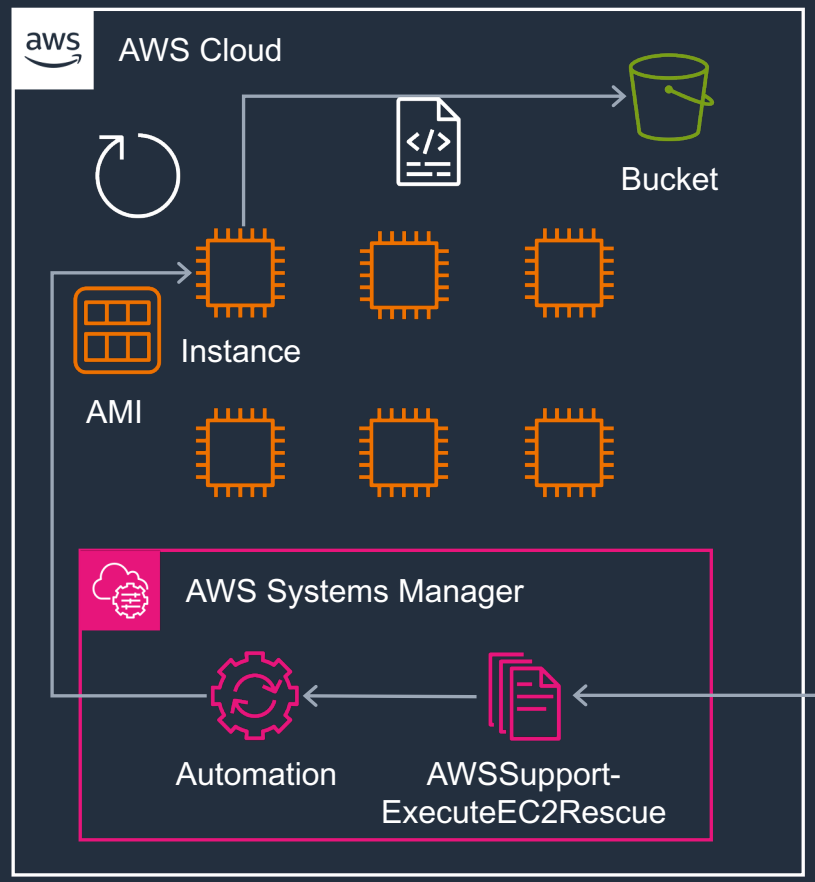


ここで AWSSupport-ExecuteEC2Rescue を使用します

SAW のランブックの 1 つである
AWSSupport-ExecuteEC2Rescue
をマネジメントコンソールから実行します

SAW の実行には
Automation の料金が課金されます
1 か月あたりの無料利用枠も存在します
料金の詳細については後述します

SAW を使用した場合



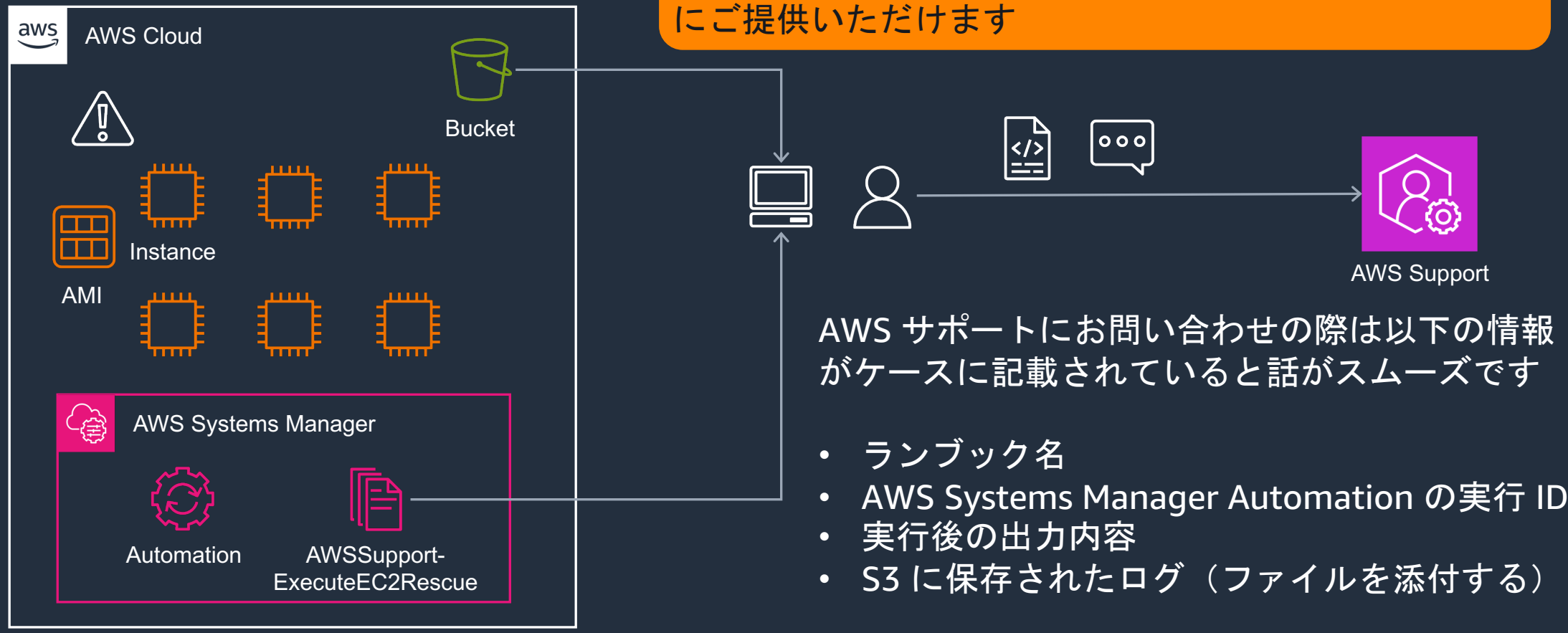
トラブルシューティングが自動的に実行され、可能な場合は修復が行われます

パラメーターで指定した Amazon S3 バケットにログが収集されます

EBS ボリュームへの操作の前に事前に AMI によるバックアップが行われます
対象のインスタンスは一時的に停止されます

SAW を使用した場合

もし、修復に成功しなくてもトラブルシューティングの結果やログの情報を AWS サポートへの問い合わせの際にご提供いただけます



AWS サポートにお問い合わせの際は以下の情報がケースに記載されていると話がスムーズです

- ランブック名
- AWS Systems Manager Automation の実行 ID
- 実行後の出力内容
- S3 に保存されたログ（ファイルを添付する）

SAW の概要と特徴

AWS Support Automation WorkFlow (SAW)

- AWS サポートチームがお客様の問題を解決することで得たベストプラクティスをもとに作成しています
- AWS Systems Manager(SSM) Automation のランブックを使用して、AWS 環境の一般的な問題をセルフサービスで解決します
- トラブルシューティング、ネットワークの問題の監視と特定、ログの収集と分析などを行います
- AWS のベストプラクティスにしたがって、手作業、管理上のオーバーヘッド、ヒューマンエラーを削減します

SAW の特徴とメリット

特徴

- AWS Systems Manager の機能の一つである Automation を使用して実行します
- お客様の AWS アカウントの環境で実行します
- お客様側で実行を開始します

メリット

- AWS サポートとのコミュニケーションコストを最適化
- お客様側でトラブルシューティングを行うことで、AWSサポートへの問い合わせ前に問題を解決できる可能性があります

AWSSupport と AWSPremiumSupport の違い

- SAW のランブックの名前には、AWSSupport と AWSPremiumSupport のいずれかのプレフィックスが付与されています
- それぞれ、使用する条件に以下のような違いがあります

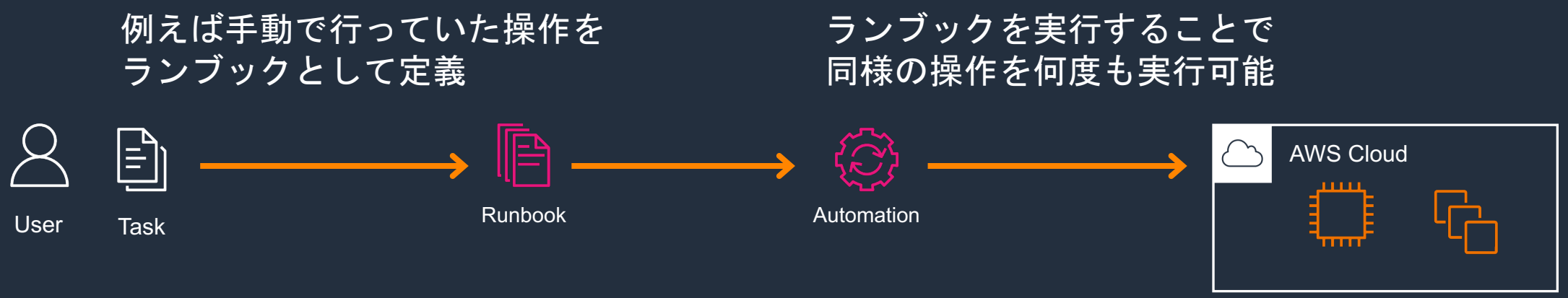
  - AWSSupport-* ランブック：すべての AWS アカウントでアクセス可能
  - AWSPremiumSupport-* ランブック：エンタープライズサポートまたはビジネスサポートへの加入が必要

- 条件を満たさない場合、AWSPremiumSupport-* ランブックは検索しても表示されません

ランブックの使用方法

AWS Systems Manager Automation とは

- AWS Systems Manager Automation は AWS クラウド上のリソースに対するオペレーションや管理タスクを自動化します
- 事前に定型的な作業をランブックとして定義し、手動あるいは自動的に実行します



ランブックとは

- 事前に定義された実行可能なタスクをランブックと言います
- 実行時にパラメータの指定が可能
- ランブックは JSON や YAML を使用して記述します
- 各処理はステップという単位で記述します
- 処理の内容はステップに紐つくアクションで決まります

- AWS Systems Manager コンソールからドキュメントビルダーを使用すると、JSON または YAML を直接編集しなくても、ランブックを作成、変更可能
- ただし、SAW は Amazon 所有のため変更できません

Automation のランブックの構造

```
{
  "schemaVersion": "0.3",
  "description": "The **AWSSupport-ExecuteEC2Rescue** runbook uses the EC2Rescue tool to troubleshoot and where possible repair common connectivity issues with the spe
  "parameters": {
    "UnreachableInstanceId": {
      "type": "AWS::EC2::Instance::Id",
      "description": "(Required) The ID of your unreachable EC2 instance. IMPORTANT: AWS Systems Manager Automation stops this instance, and creates an Amazon Machine
    },
    "LogDestination": {
      "type": "AWS::S3::Bucket::Name",
      "description": "(Optional) The Amazon Simple Storage Service (Amazon S3) bucket name in your account where you want to upload the troubleshooting logs. Make sure
      "default": ""
    },
    "EC2RescueInstanceType": {
      "type": "String",
      "description": "(Required) The EC2 instance type for the EC2Rescue instance. Recommended size: t2.medium.",
      "default": "t2.medium",
      "allowedValues": [
        "t2.small",
        "t2.medium",
        "t2.large",
        "t3.small",
        "t3.medium",
        "t3.large",
        "i3.large"
      ]
    },
    "SubnetId": {
      "type": "String",
      "description": "(Optional) The subnet ID for the EC2Rescue instance. By default, AWS Systems Manager Automation creates a new VPC. Alternatively, Use SelectedIns
      "default": "CreateNewVPC",
      "allowedPattern": "^SelectedInstanceSubnet$|^CreateNewVPC$|^subnet-[a-z0-9]{8,17}$"
    },
    "AssumeRole": {
      "type": "AWS::IAM::Role::Arn",
      "description": "(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform
      "default": ""
    }
  },
  "mainSteps": [
    {
      "name": "assertInstanceIsWindows",
      "action": "aws:assertAwsResourceProperty",
      "onFailure": "step:runEC2RescueForLinux",
      "description": "Asserts if the provided instance is Windows Server",
      "inputs": {
        "Service": "ec2",
        "Api": "DescribeInstances",
        "InstanceIds": [
          "{{ UnreachableInstanceId }}"
        ],
        "PropertySelector": "$.Reservations[0].Instances[0].Platform",
        "DesiredValues": [
          "windows"
        ]
      },
      "isCritical": "false",
      "nextStep": "runEC2RescueForWindows"
    },
    {
      "name": "runEC2RescueForWindows",
```

ランブック全体の設定

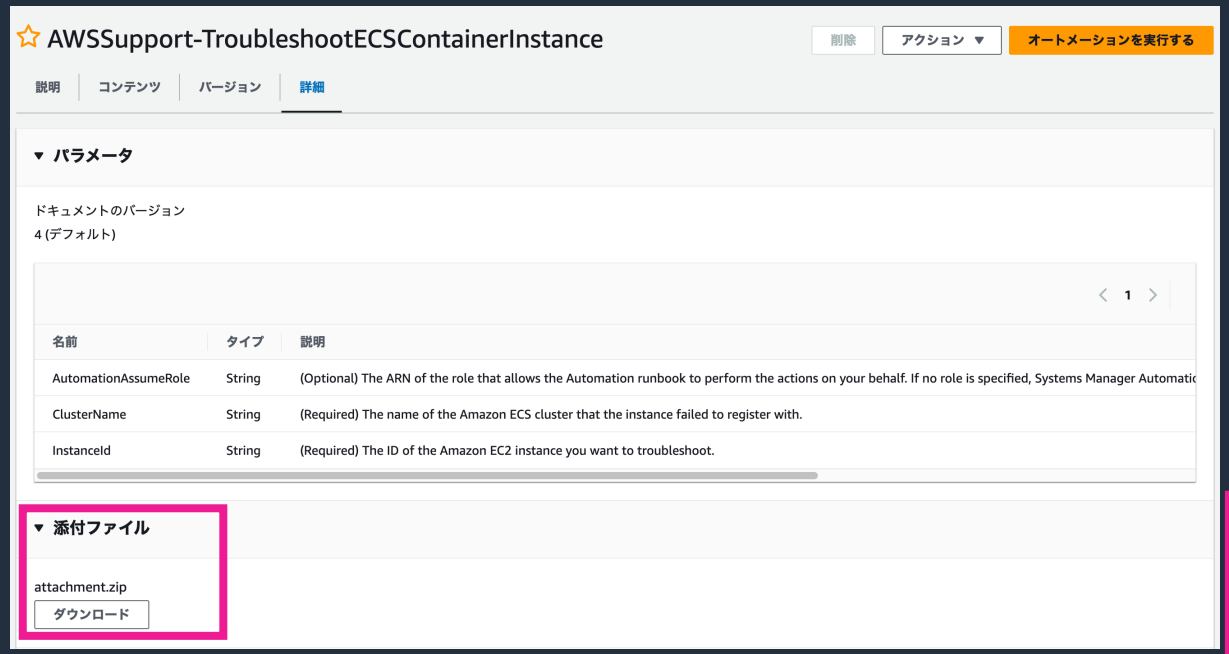
パラメータ

具体的な処理（ステップ）

具体的な処理は複数のステップとして記述されます
ステップには、アクションが１つ設定されており、アクションによって処理の内容が異なります

ランブックの添付ファイル

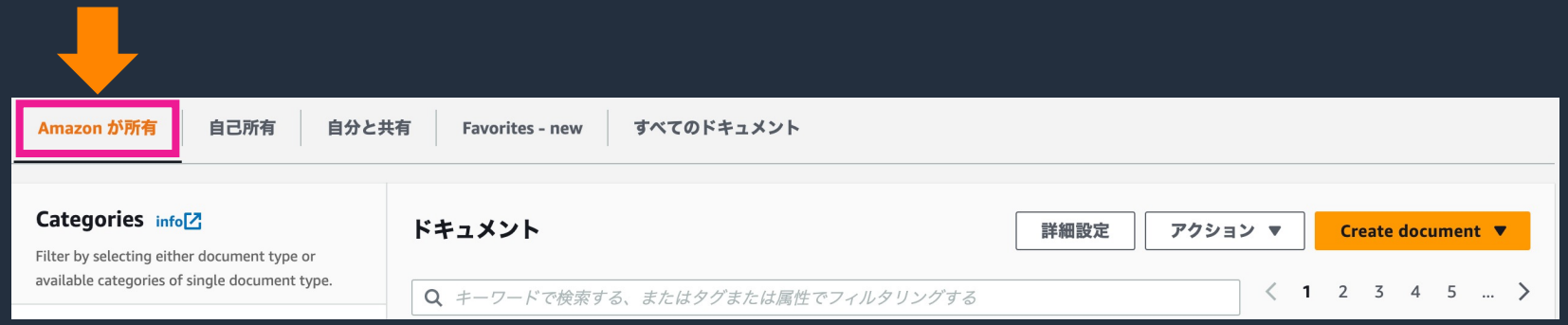
スクリプトが添付ファイルとなっている場合もあります
ランブックの詳細からダウンロードして内容を確認することが可能



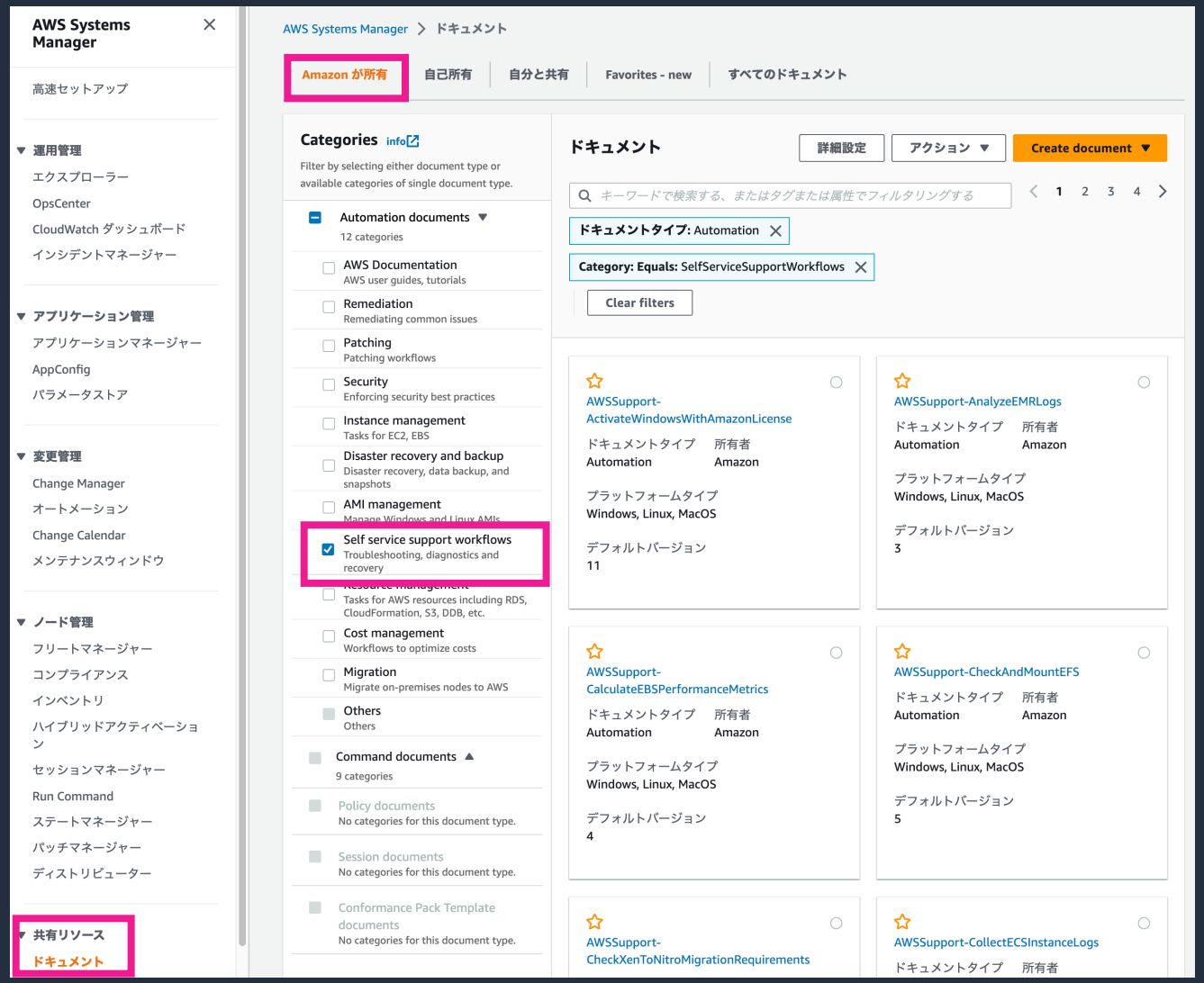

```
"mainSteps": [
  {
    "name": "executeChecker",
    "action": "aws:executeScript",
    "description": "Reviews whether the Amazon EC2 instance meets the prerequisites needed to register with ar
    "isCritical": true,
    "timeoutSeconds": 540,
    "inputs": {
      "Runtime": "python3.8",
      "InputPayload": {
        "InstanceId": "{{InstanceId}}",
        "ClusterName": "{{ClusterName}}"
      },
      "Handler": "lambda_handler",
      "Script": "import boto3\n\nfrom saw_ecs.ec2 import EC2Instance\nfrom saw_ecs.cluster import ECSCluster\r
      "Attachment": "attachment.zip"
    },
    "outputs": [
      {
        "Name": "stdout",
        "Selector": "$.Payload.stdout",
        "Type": "String"
      },
      {
        "Name": "info_codes",
        "Selector": "$.Payload.info_codes",
        "Type": "StringList"
      }
    ]
  }
],
"files": {
  "attachment.zip": {
    "checksums": {
      "sha256": "3aefd4b316c99e035759a1a03081468442f32cd9ec3ba862e6f847e5000776c8"
    }
  }
},
```

Amazon 所有のランブック

- 個別の AWS アカウントのリソースである自己所有のランブック以外に最初から提供されている Amazon 所有のランブックが存在します
- よくある管理タスクやトラブルシューティングなどの操作が定義されています
- ランブック（ドキュメント）の一覧の画面で「Amazonが所有」のタブを選択することで表示されます

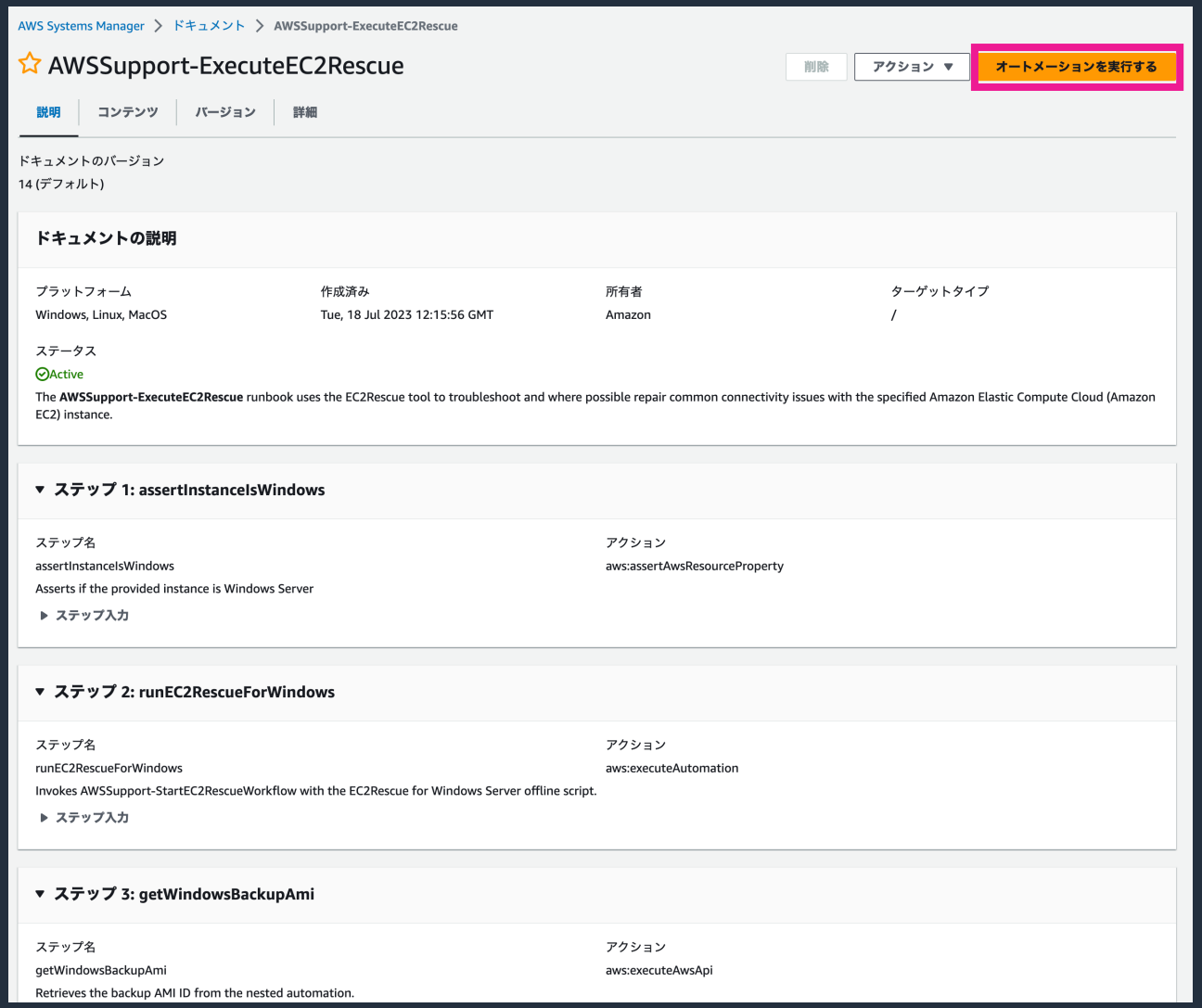


SAW の実行方法 – ランブックの検索



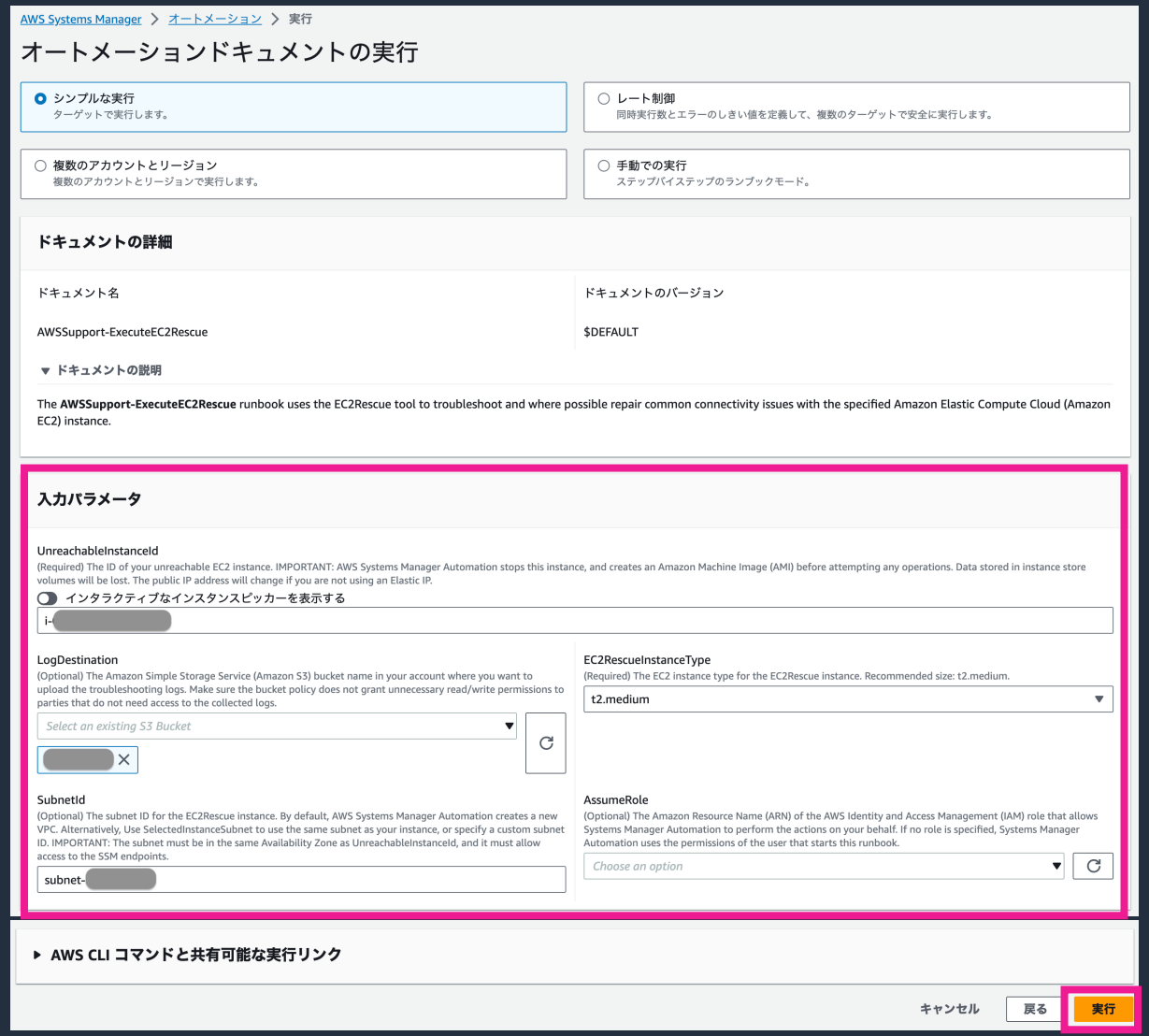
- AWS Systems Manager コンソールを表示し、左ペインの[ドキュメント]をクリックします
- [Amazon が所有] のタブを選択し、[Self service support workflows]をチェックします
- ランブックの一覧が表示されるので、実行したいランブックをクリックします

SAW の実行方法 – ランブックの実行



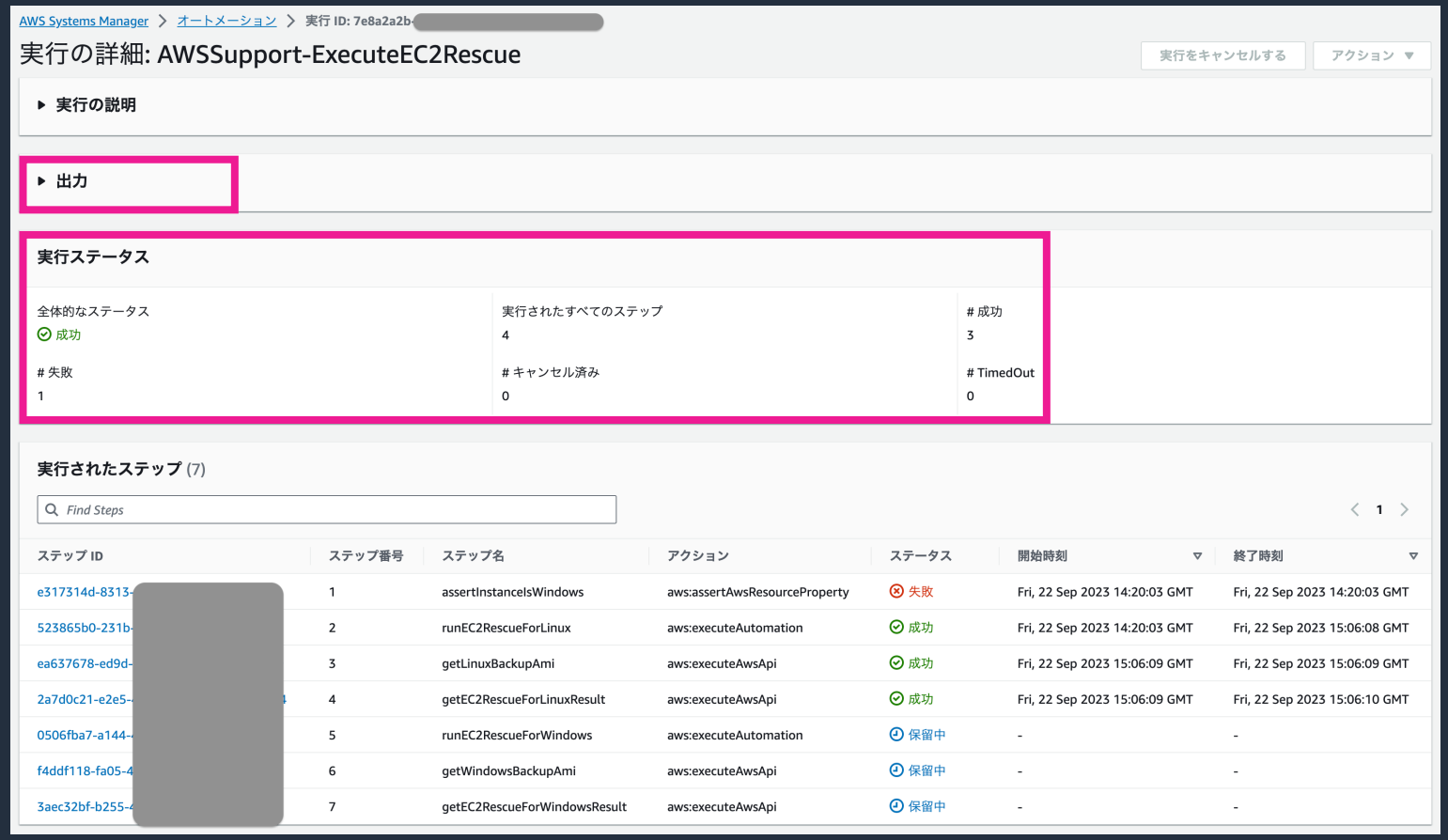
- ランブックの詳細が表示されます
- [オートメーションを実行する] をクリックします

SAW の実行方法 – ランブックの実行



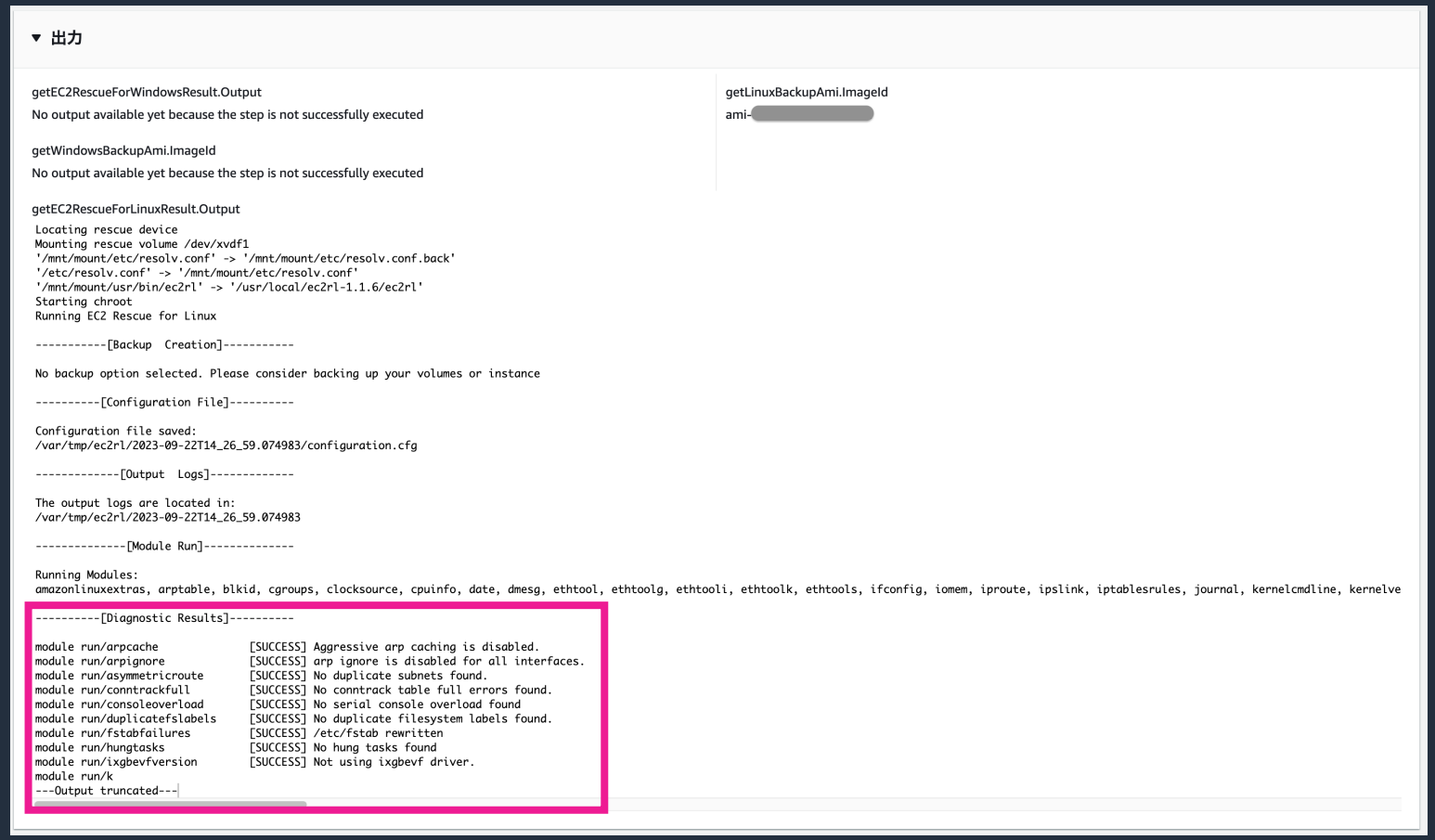
- [入力パラメータ] に必要な値を入力します
- 多くの場合、パラメータは対象のリソースIDや実行時の設定に関する値になります
- [実行] をクリックします

SAW の実行方法 – 実行結果の確認



- ランブックの実行が開始され、全体および各ステップの実行ステータスが表示されます
- 実行結果の詳細は最終的に [出力] に表示されます

SAW の実行方法 – 実行結果の確認



- 出力された実行結果の例
- [Diagnostic Results] で各項目のチェックが行われていることがわかります

AWS CLI でのランブックの実行

- SAW は AWS CLI からでも実行可能
- AutomationExecutionId（実行ID）が返却されます
- aws ssm get-automation-execution でステータスを確認します

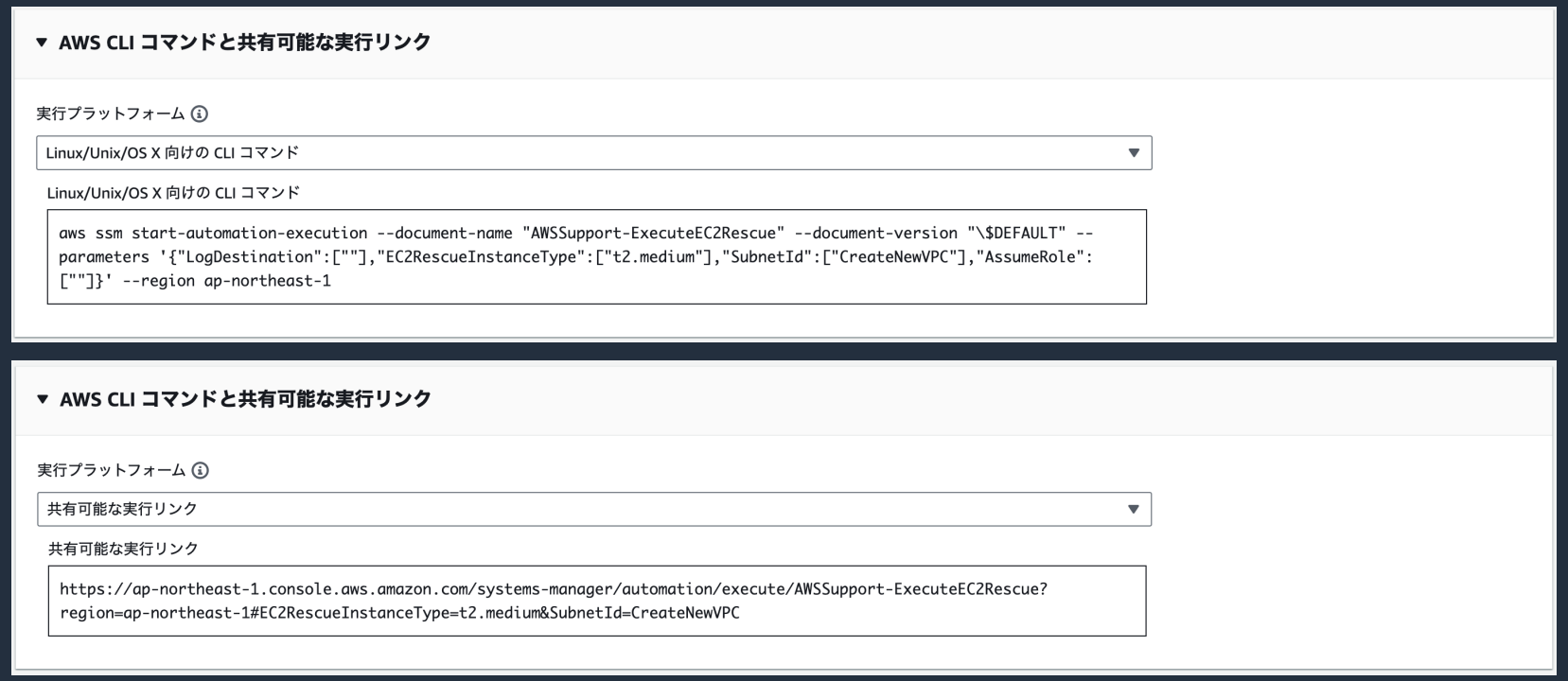
```
$ aws ssm start-automation-execution \
 --document-name "AWSSupport-ExecuteEC2Rescue" \
 --document-version "\$DEFAULT" \
 --parameters '{"UnreachableInstanceId":["i-XXXXXXXXXXXXXXXXX"],
  "LogDestination":[”bucket_name"],"EC2RescueInstanceType":["t2.medium"],"SubnetId":["subnet-YYYYYYYY"]}' \
 --region ap-northeast-1

{
   "AutomationExecutionId": "615eb4ea-1a67-40d5-a59b-ZZZZZZZZZZZZ"
}

$ aws ssm get-automation-execution \
 --automation-execution-id "615eb4ea-1a67-40d5-a59b-ZZZZZZZZZZZZ" \
 --region ap-northeast-1
```

AWS CLI でのランブックの実行

- コンソールの Automation の実行画面で、入力したパラメータを含む AWS CLI のコマンド、実行リンクの URL を生成することも可能



EC2 でよく使われる ランブックの例

今回ご紹介するランブック

よく使われるランブックとして以下の２つを解説します

名称	カテゴリ	概要
AWSSupport-ExecuteEC2Rescue	トラブルシューティング	Amazon EC2 インスタンスの問題の診断とトラブルシューティングを行います。
AWSSupport-TroubleshootManagedInstance	トラブルシューティング	Amazon EC2 インスタンスが AWS Systems Manager のマネージドノードとして管理対象にならない原因についてトラブルシューティングを行います。

双方のランブックともに Linux および Windows の Amazon EC2 インスタンスに対して使用可能

AWSSupport-ExecuteEC2Rescue

AWSSupport-ExecuteEC2Rescue

- Amazon EC2 インスタンスの問題の診断とトラブルシューティングを行います（Linux、Windows の両方に対応）
- インスタンス内部の設定でネットワーク疎通性が失われた場合などの復旧に役立ちます
- AWS CloudFormation を使用して一時的な VPC 、ヘルパーインスタンスを起動し、診断対象のインスタンスのルートボリュームをヘルパーインスタンスにアタッチして診断と修正を行った上で元のインスタンスにアタッチします
- 一連の操作の前に対象のインスタンスを停止して自動的にバックアップを取得します
- EC2Rescue は Linux、Windows の場合でそれぞれ異なる実装となっており、実行されるコマンドも異なります

到達不可能なインスタンスでの EC2Rescue ツールの実行
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/automation-ec2rescue.html

ランブックが行う調査の内容 (Linux の場合)

```
name: !!str arpignore
path: !!str
version: !!str 3.1
title: !!str Determines if any interfaces have been set to ignore arp requests
helptext: !!str |
  Determines if any interfaces have been set to ignore arp requests
  These being disabled can cause networking issues or result in an instance failing status checks
  Sudo is required for remediation
placement: !!str run
package:
  - !!str
language: !!str python
remediation: !!str True
content: !!str |
  """
  Determine if any interfaces have been set to ignore arp requests. These can cause networking issues
  or result in instances failing status checks.

  Functions:
      detect: Determine if arpignore is enabled on any interface.
      fix: Disable arpignore.
      run: Detect if arpignore is enabled and attempt to remediate if remediation is enabled.
  """
  from __future__ import print_function
  import os
  import re
  import subprocess
  import sys
```

- Linux 用の EC2Rescue はモジュールごとに診断とトラブルシューティングが実装されており、コマンド実行時のオプションで対象のモジュールを指定可能です
- モジュールはYAMLで記述されており、どのような診断、トラブルシューティングを行うかが定義されています
- 実際の処理は、シェルスクリプトや Python のコードで記述されています

https://github.com/awslabs/aws-ec2rescue-linux/blob/develop/docs/MODULE.md

ランブックが行う調査の内容 (Linux の場合)

- Linux のインスタンスの場合、以下のコマンドを実行するのと同様の診断、トラブルシューティングを行います

```
ec2rl run --remediate --fstabfailures --rebuildinitrd --selinuxpermissive --udevnetpersistent \
  --no=duplicatefsuuid,duplicatepartuuid
```

- Linux 用の EC2Rescue はコマンド実行時のオプションで対象のモジュールを指定可能です
- 上記のコマンドの場合、問題の修正、設定の変更を行うモジュールは以下の8つのみで、その他はインスタンス内部の情報収集のみを行います
  - arpignore, selinuxpermissive, tcprecycle, openssh, rebuildinitrd, arpcache, fstabfailures, udevpersistentnet
- これらのモジュールはインスタンス内部の設定変更を行う可能性があるので次のスライドで紹介します

  https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2rl_working.html

  https://github.com/awslabs/aws-ec2rescue-linux/blob/develop/docs/MODULE.md

ランブックが行う調査の内容 (Linux の場合)

- arpignore : ネットワークインターフェースが ARP リクエストを無視する設定となっていないか
- selinuxpermissive : selinux を permissive モードにする
- tcprecycle : IPv4 の tcp_tw_recycle を disable にする
- openssh : OpenSSH の設定を確認、修正する
- rebuildinitrd : 初期 RAM ディスクのリビルドを行う
- arpcache : ARP キャッシュの無効化を行う
- fstabfailures :「/etc/fstab」の全てのボリュームについて fsck を0に設定し、nofail を設定する
- udevpersistentnet :「 /etc/udev/rules.d/70-persistent-net.rules 」内の全行をコメントアウトする

https://github.com/awslabs/aws-ec2rescue-linux/tree/develop/docs/modules

ランブックが行う調査の内容 (Windows の場合)

- Windows のインスタンスの場合、以下のコマンドを実行した場合と同様のインスタンスの問題の診断とトラブルシューティングを行います

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

- 「/rescue:all」が指定されており、以下のすべての問題の修正を試みます
  - システム時刻
  - Windows ファイアウォール
  - リモートデスクトップ
  - EC2Config
  - EC2Launch
  - ネットワークインターフェイス

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/WindowsGuide/ec2rw-cli.html

EC2Rescue の制限

2023年10月時点

- Linux の場合の前提条件
- サポートされるオペレーティングシステム
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+

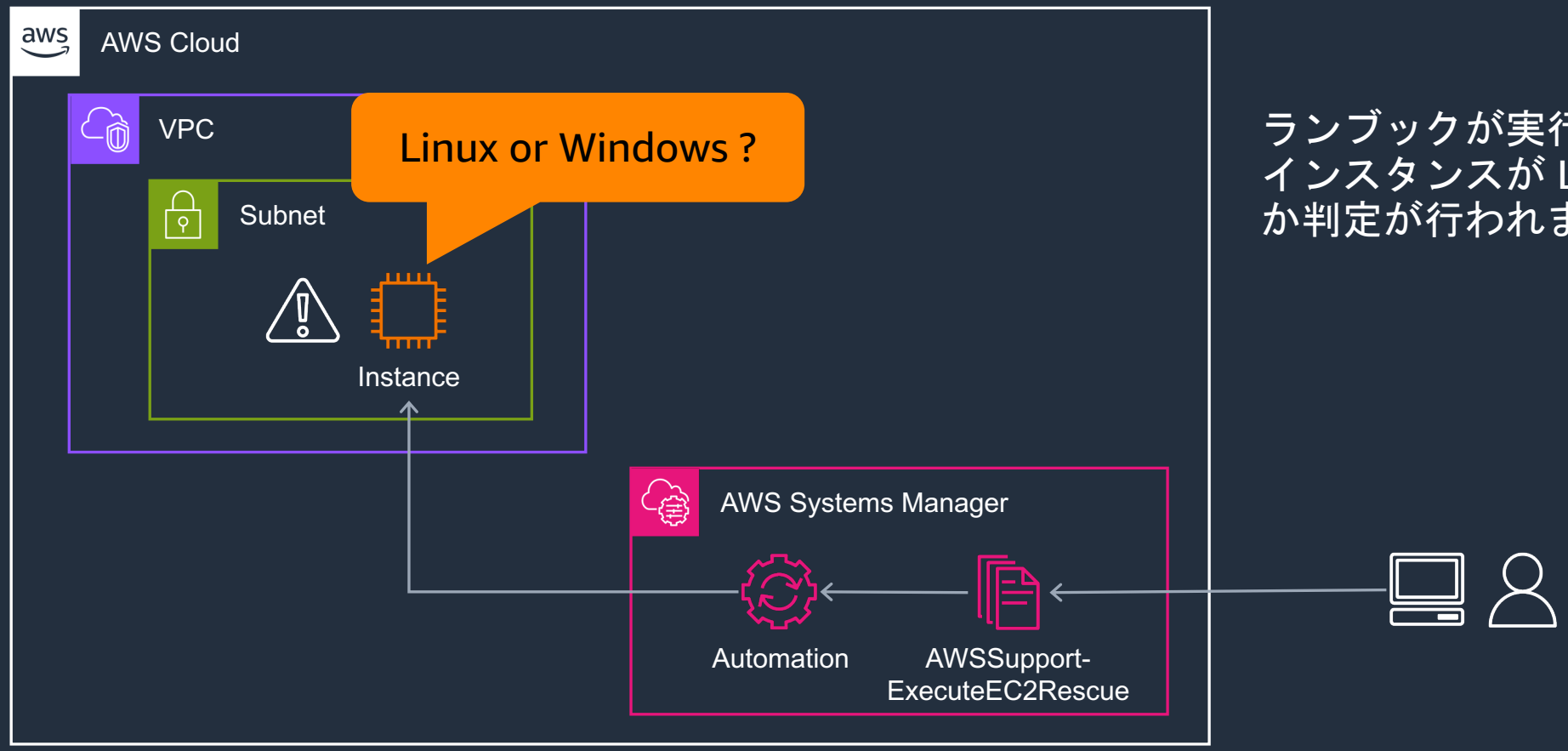
- ソフトウェア要件
  - Python 2.7.9+ または 3.2+

- Windows の場合の前提条件
  - Windows Server 2008 R2 以降

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2rl_install.html

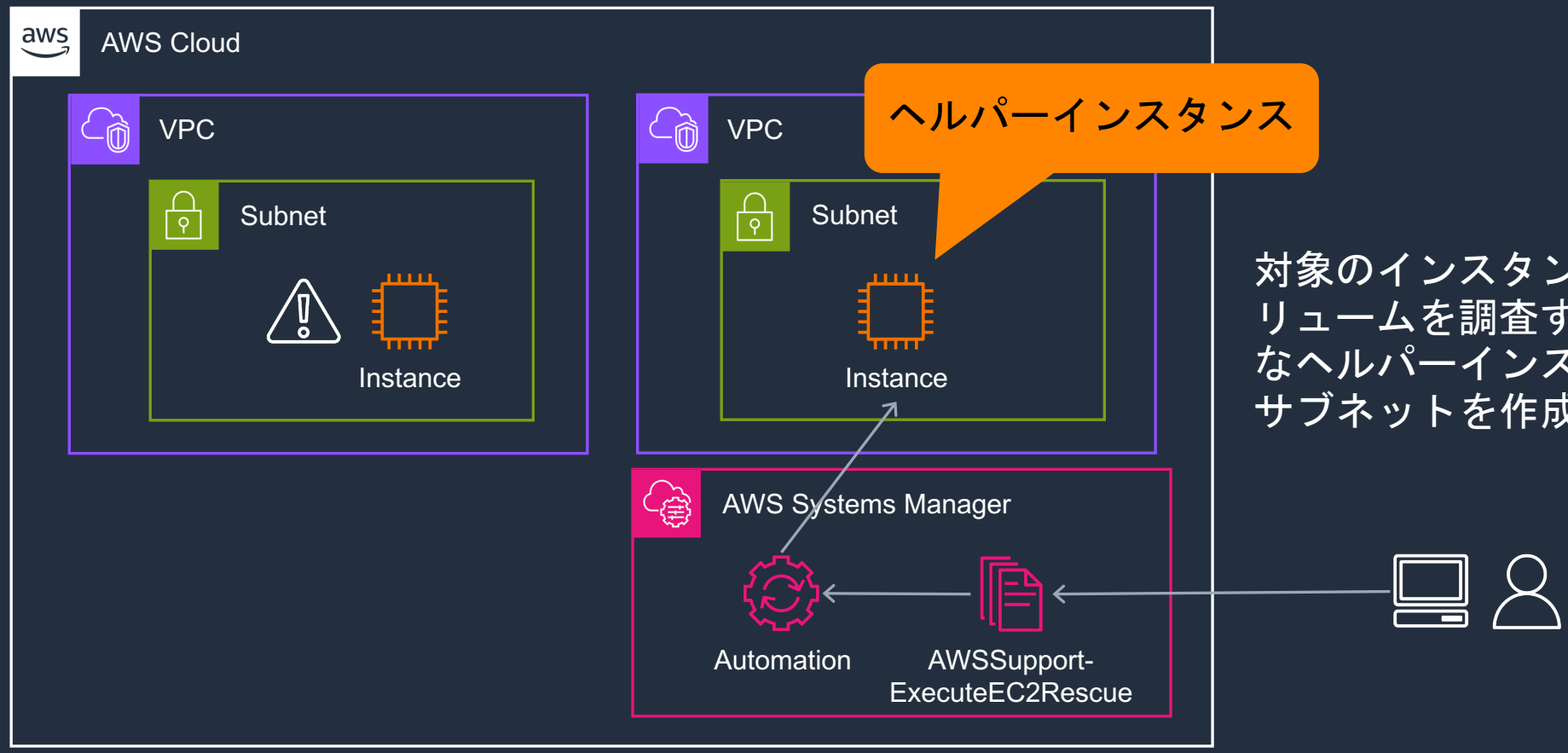
https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/WindowsGuide/Windows-Server-EC2Rescue.html

AWSSupport-ExecuteEC2Rescue の動作



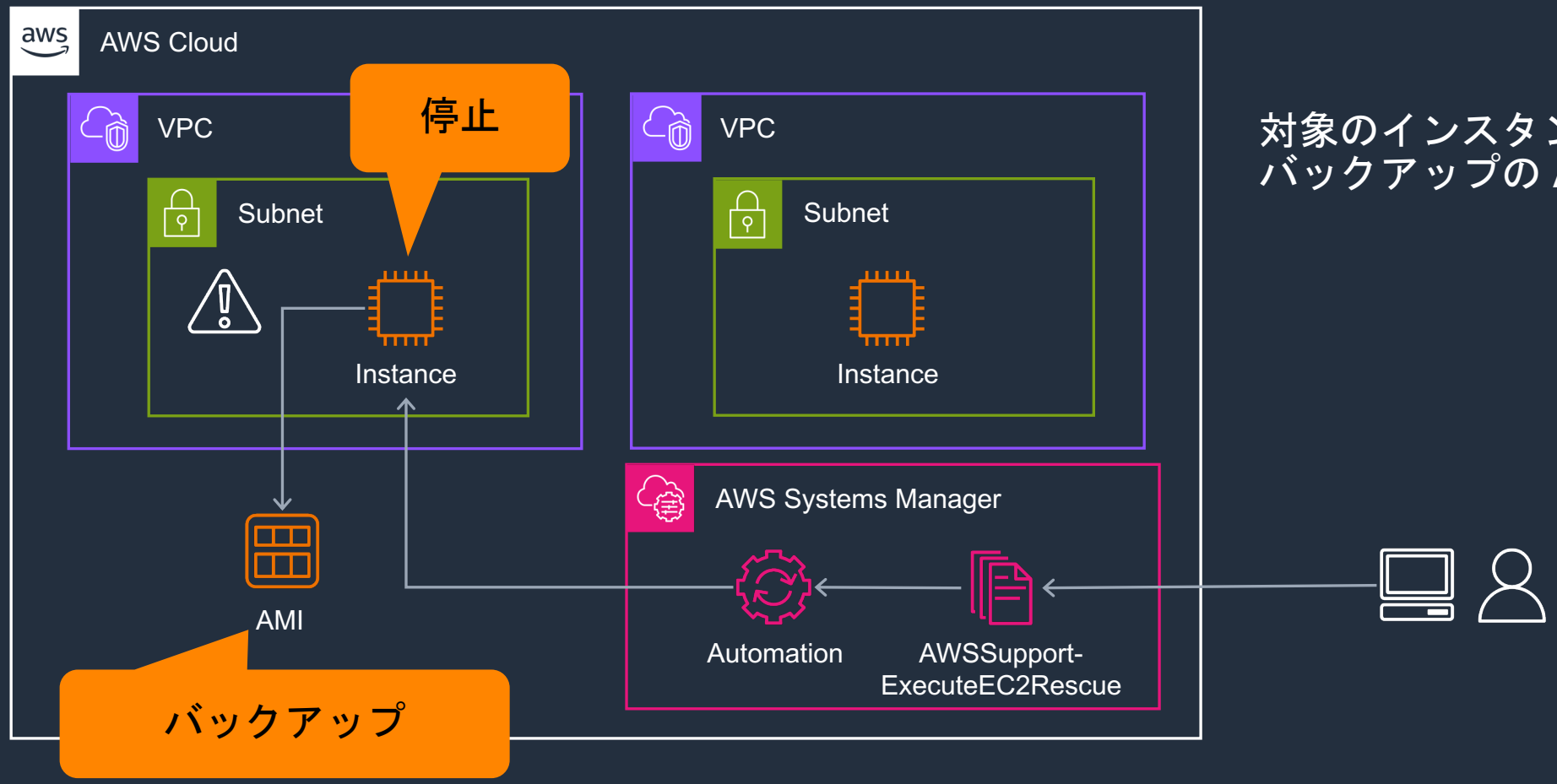
ランブックが実行されると対象のインスタンスが Linux か Windows か判定が行われます

AWSSupport-ExecuteEC2Rescue の動作



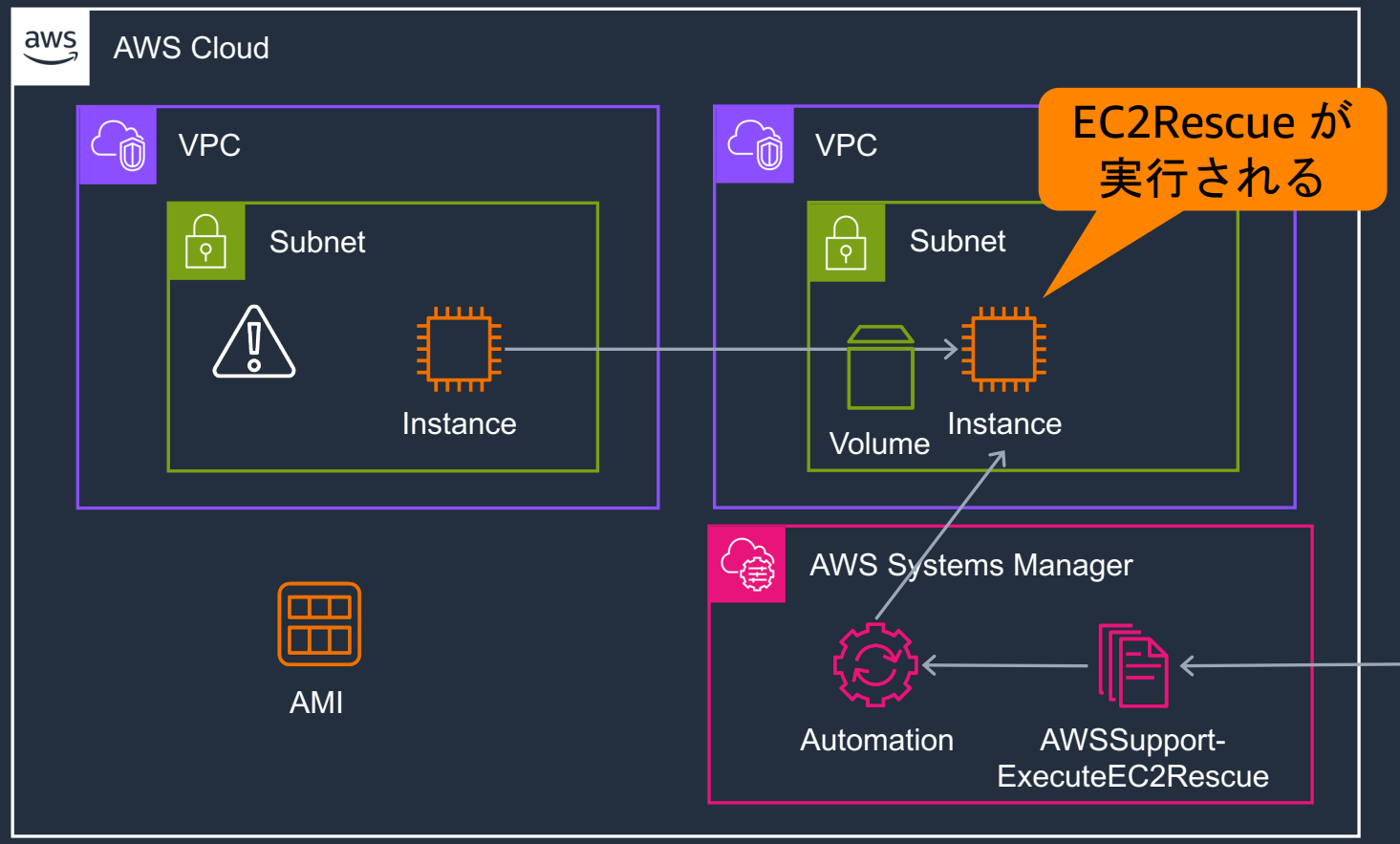
対象のインスタンスのルートボリュームを調査するために一時的なヘルパーインスタンス、VPC、サブネットを作成します

AWSSupport-ExecuteEC2Rescue の動作



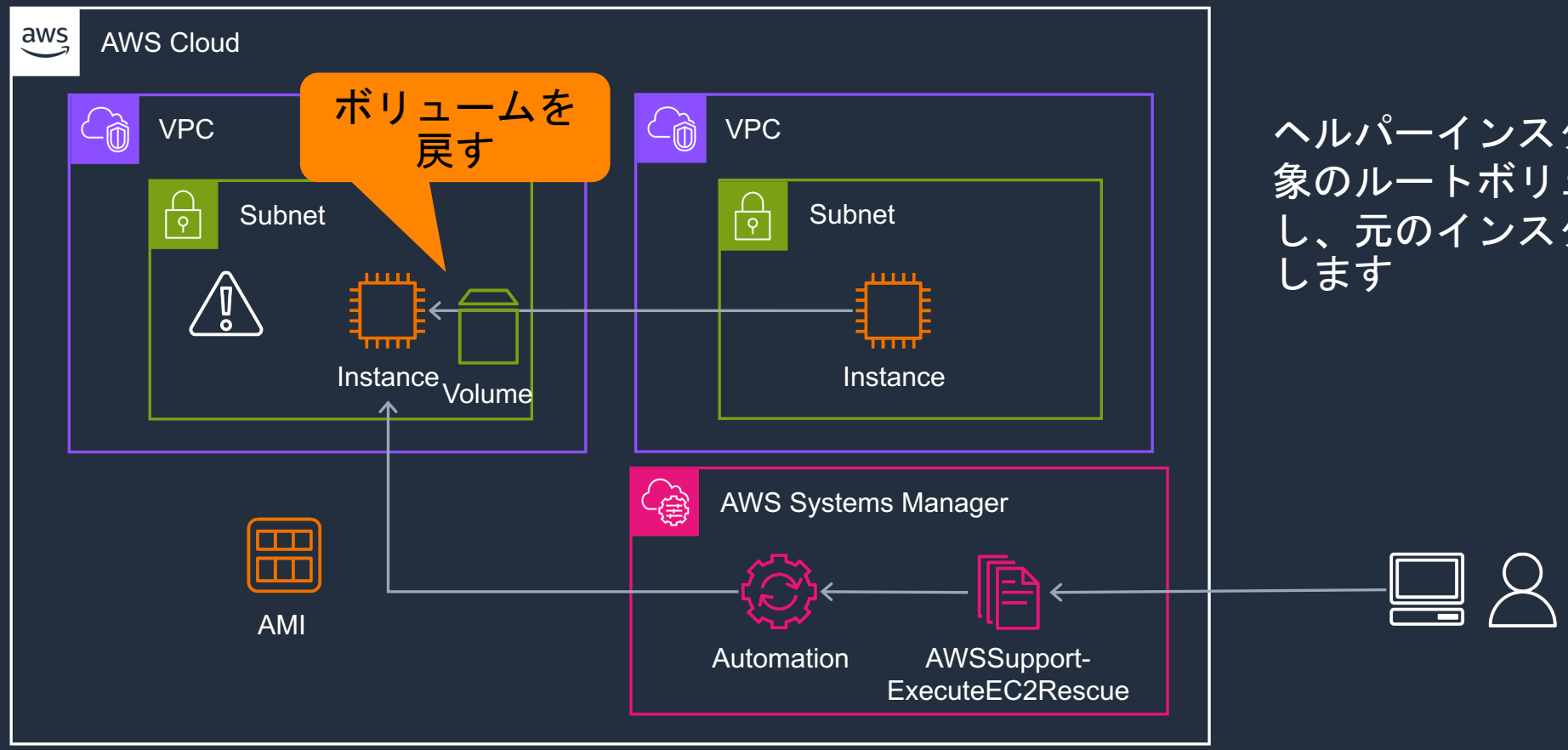
対象のインスタンスを停止して、
バックアップの AMI を取得します

AWSSupport-ExecuteEC2Rescue の動作



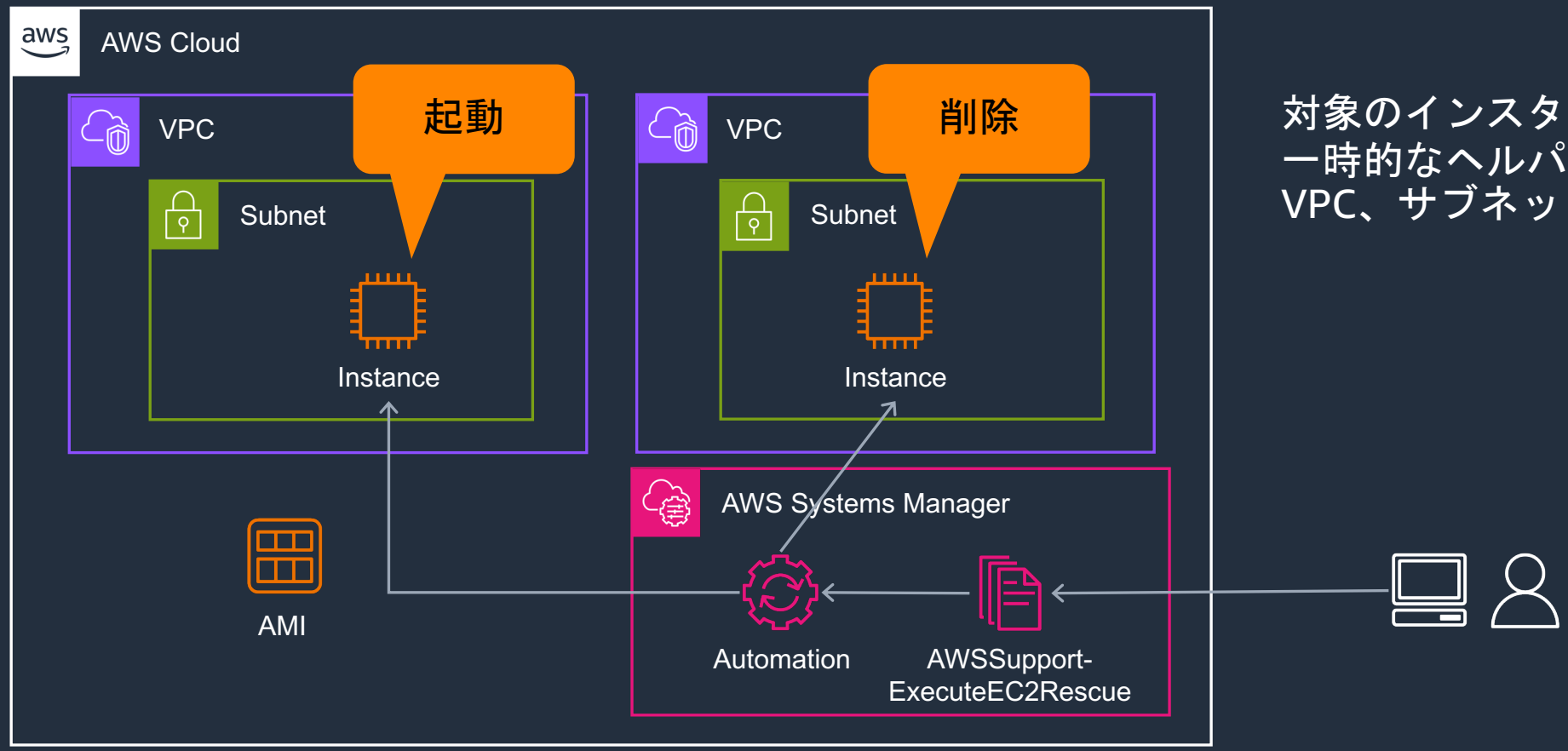
対象のインスタンスのルートボリュームをヘルパーインスタンスにアタッチします
EC2Rescue が実行されてルートボリュームの問題の修正を試み、オプションで指定した Amazon S3 バケットにログを保存します

AWSSupport-ExecuteEC2Rescue の動作



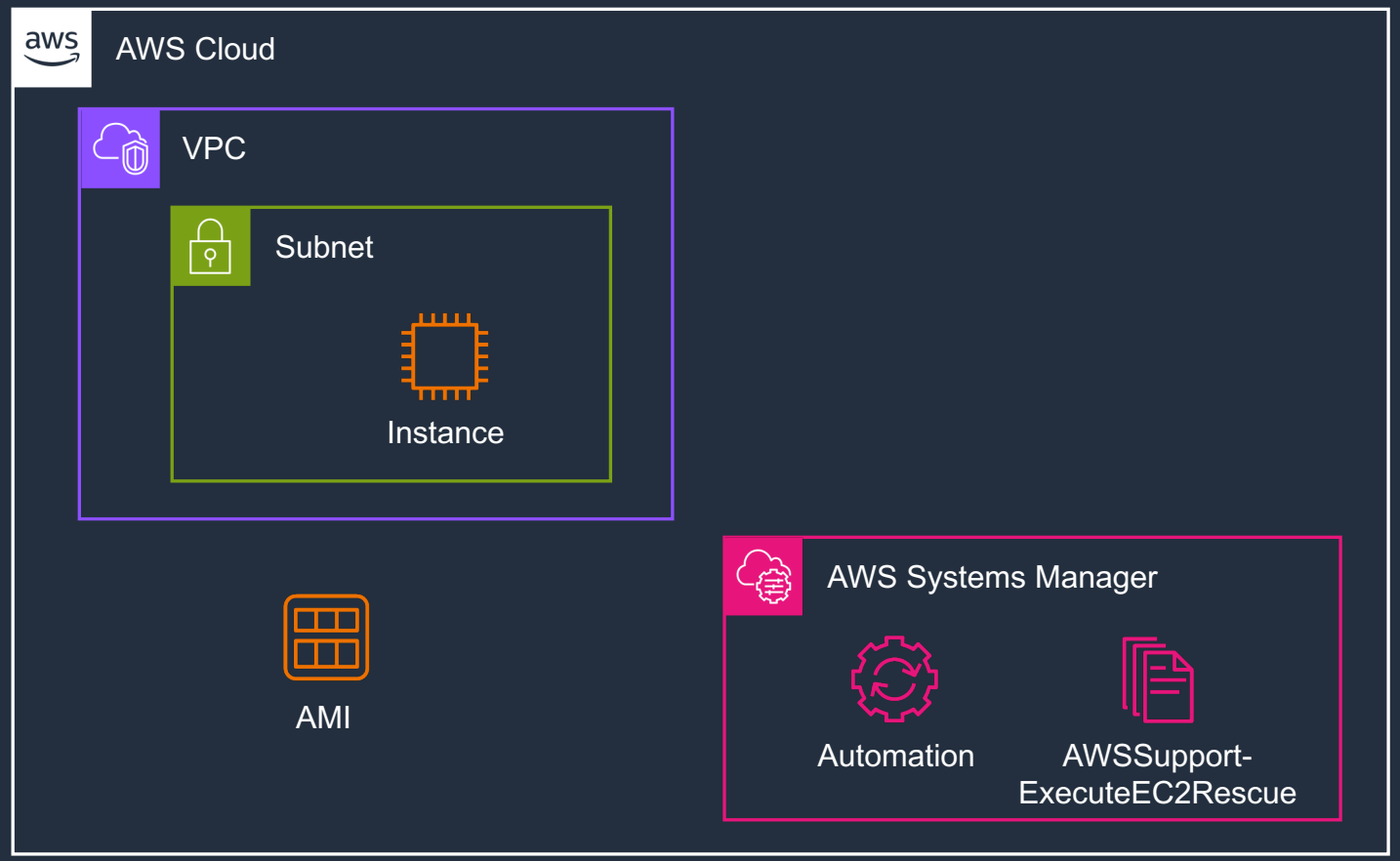
ヘルパーインスタンスから調査対象のルートボリュームをデタッチし、元のインスタンスにアタッチします

AWSSupport-ExecuteEC2Rescue の動作



対象のインスタンスを起動し、
一時的なヘルパーインスタンス、
VPC、サブネットを削除します

AWSSupport-ExecuteEC2Rescue の動作



ランブックの実行が完了します

ランブックの入力パラメーター

- UnreachableInstanceId (必須)
  - 接続できない調査対象の EC2 インスタンスの ID
- EC2RescueInstanceType (必須)
  - ヘルパーインスタンスの EC2 インスタンスタイプ
  - EC2Rescue 推奨サイズ: t2.small
- SubnetId (オプション)
  - ヘルパーインスタンスを起動するサブネットの ID 、デフォルトでは新しい VPC 、サブネットが作成されます

https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-executeec2rescue.html

ランブックの入力パラメーター

- LogDestination (オプション)
  - トラブルシューティングログをアップロードする Amazon S3 バケット名
- 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、ランブックを実行した IAM ユーザーの権限を使用

https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-executeec2rescue.html

ランブック実行時の注意点

- Amazon EBS ボリュームはアベイラビリティーゾーンに配置されるリソースであるため、SubnetId に既存のサブネットを指定する場合、UnreachableInstanceId で指定したインスタンスと同じアベイラビリティーゾーンである必要があります
- また、SubnetId で指定したサブネットから AWS SSM のエンドポイントにアクセス可能となっている必要があります
- 調査対象のインスタンスは一時的に停止され、操作を試みる前に AMI を作成します。インスタンスストアボリュームに保存されているデータは失われます。Elastic IP アドレスを使用していない場合、パブリック IP アドレスは変更されます

https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-executeec2rescue.html

AWSSupport-TroubleshootManagedInstance

AWSSupport-TroubleshootManagedInstance

- マネージドノードとなっていない Amazon EC2 インスタンスのトラブルシューティングを行います
- セキュリティグループ、ネットワーク ACL、VPC エンドポイント、ルートテーブルといった VPC の設定、インスタンスにアタッチされた IAM ロールをチェックします
- インスタンス内部の問題は、このランブックではチェックできません

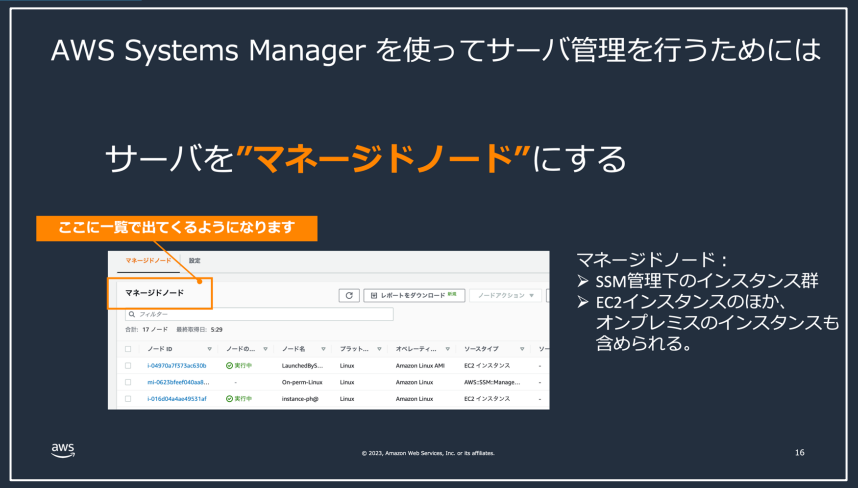
- 以下の記事で解説している問題について自動的にトラブルシューティングを行います

Systems Manager で EC2 インスタンスがマネージドノードとして表示されない、または 「接続が失われました」というステータスが表示されるのはなぜですか?

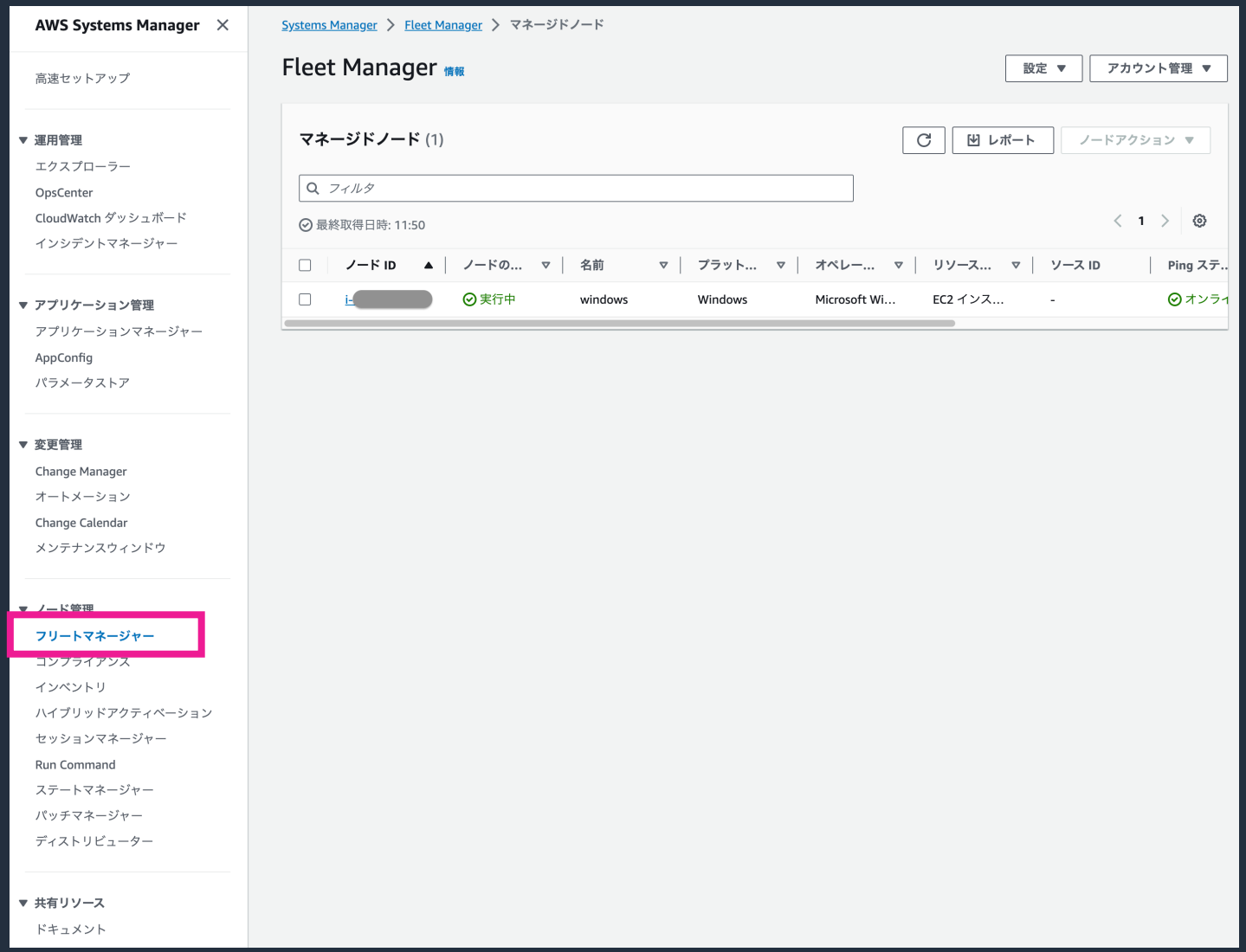
https://repost.aws/ja/knowledge-center/systems-manager-ec2-instance-not-appear

マネージドノード

- マネージドノードとは AWS SSM で管理するために設定された EC2 インスタンスなどのノードのことを指します
- SAW のランブックでは、インスタンス内部の操作を行うために対象のインスタンスがマネージドノードであることが前提条件となっているものも存在します
- マネージドノードの詳細は、AWS Black Belt Online Seminar の「AWS Systems Manager Overview」をご覧ください



マネージドノードの確認方法



- マネージドノードの一覧は AWS Systems Manager コンソールの [フリートマネージャー] から確認することが可能
- このランブックはインスタンス側でマネージドノードにするための設定を行なったものの、この一覧に対象のインスタンスが表示されないといった場合に使用します

ランブックが行う調査の内容

- インスタンスの VPC 設定
  - セキュリティグループルール
  - VPC エンドポイント
  - ネットワークアクセスコントロールリスト (ACL) ルール
  - ルートテーブル
- インスタンスにアタッチされているインスタンスプロファイルに、必要な権限を提供する管理ポリシーが含まれているか

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

ランブックの入力パラメーター

- InstanceId (必須)
  - システムマネージャーによって管理されていないと報告されている Amazon 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、ランブックを実行した IAM ユーザーの権限を使用

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

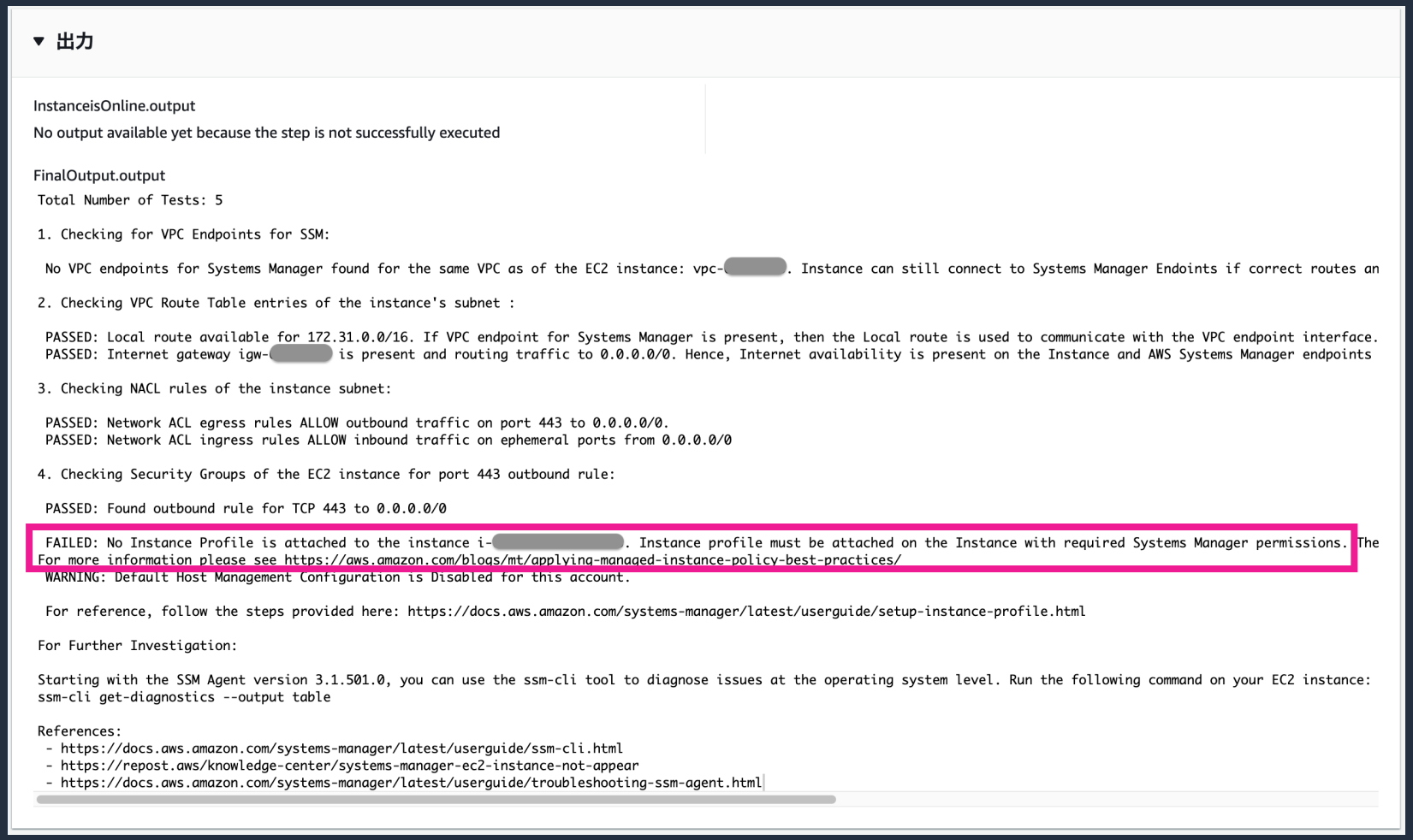
ランブック実行時の注意点

- ランブックの実行のみでは、インスタンス内部の問題については調査できません
- ssh などでインスタンスにログインし、「ssm-cli get-diagnostics」 コマンドを使用することでマネージドノードとなっていないインスタンス内部の原因の診断が可能です

```
[ec2-user@ip-[redacted] ~]$ sudo ssm-cli get-diagnostics --output table
```

Check	Status	Note
EC2 IMDS	Success	IMDS is accessible and has instance id i-09d4c1f4ed1a6aff6 in region ap-northeast-1
Hybrid instance registration	Skipped	Instance does not have hybrid registration
Connectivity to ssm endpoint	Success	ssm.ap-northeast-1.amazonaws.com is reachable
Connectivity to ec2messages endpoint	Success	ec2messages.ap-northeast-1.amazonaws.com is reachable
Connectivity to ssmmessages endpoint	Success	ssmmessages.ap-northeast-1.amazonaws.com is reachable
Connectivity to s3 endpoint	Success	s3.ap-northeast-1.amazonaws.com is reachable
Connectivity to kms endpoint	Success	kms.ap-northeast-1.amazonaws.com is reachable
Connectivity to logs endpoint	Success	logs.ap-northeast-1.amazonaws.com is reachable
Connectivity to monitoring endpoint	Success	monitoring.ap-northeast-1.amazonaws.com is reachable
AWS Credentials	Success	Credentials are for arn:aws:sts::092696531560:assumed-role/ec2-role-for-ssm/i-09d4c1f4ed1a6aff6 and will expire at 2023-09-27 10:26:57 +0000 UTC
Agent service	Failed	Agent is installed as a systemctl service but is not running
Proxy configuration	Skipped	No proxy configuration detected
SSM Agent version	Success	SSM Agent version is 3.2.1377.0, latest agent version in ap-northeast-1 is 3.2.1630.0

ランブックの実行例



▼ 出力

InstanceisOnline.output

No output available yet because the step is not successfully executed

FinalOutput.output

```
Total Number of Tests: 5

1. Checking for VPC Endpoints for SSM:

 No VPC endpoints for Systems Manager found for the same VPC as of the EC2 instance: vpc-[redacted]. Instance can still connect to Systems Manager Endoints if correct routes an

2. Checking VPC Route Table entries of the instance's subnet :

 PASSED: Local route available for 172.31.0.0/16. If VPC endpoint for Systems Manager is present, then the Local route is used to communicate with the VPC endpoint interface.
 PASSED: Internet gateway igw-[redacted] is present and routing traffic to 0.0.0.0/0. Hence, Internet availability is present on the Instance and AWS Systems Manager endpoints

3. Checking NACL rules of the instance subnet:

 PASSED: Network ACL egress rules ALLOW outbound traffic on port 443 to 0.0.0.0/0.
 PASSED: Network ACL ingress rules ALLOW inbound traffic on ephemeral ports from 0.0.0.0/0

4. Checking Security Groups of the EC2 instance for port 443 outbound rule:

 PASSED: Found outbound rule for TCP 443 to 0.0.0.0/0

 FAILED: No Instance Profile is attached to the instance i-[redacted]. Instance profile must be attached on the Instance with required Systems Manager permissions. The
For more information please see https://aws.amazon.com/blogs/mt/applying-managed-instance-policy-best-practices/
 WARNING: Default Host Management Configuration is Disabled for this account.

 For reference, follow the steps provided here: https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html

For Further Investigation:

Starting with the SSM Agent version 3.1.501.0, you can use the ssm-cli tool to diagnose issues at the operating system level. Run the following command on your EC2 instance:
ssm-cli get-diagnostics --output table

References:
 - https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-cli.html
 - https://repost.aws/knowledge-center/systems-manager-ec2-instance-not-appear
 - https://docs.aws.amazon.com/systems-manager/latest/userguide/troubleshooting-ssm-agent.html
```

問題のある項目は「FAILED」と表示されます

この例の場合では、インスタンスプロファイルに必要な権限が付与されていないことが指摘されています

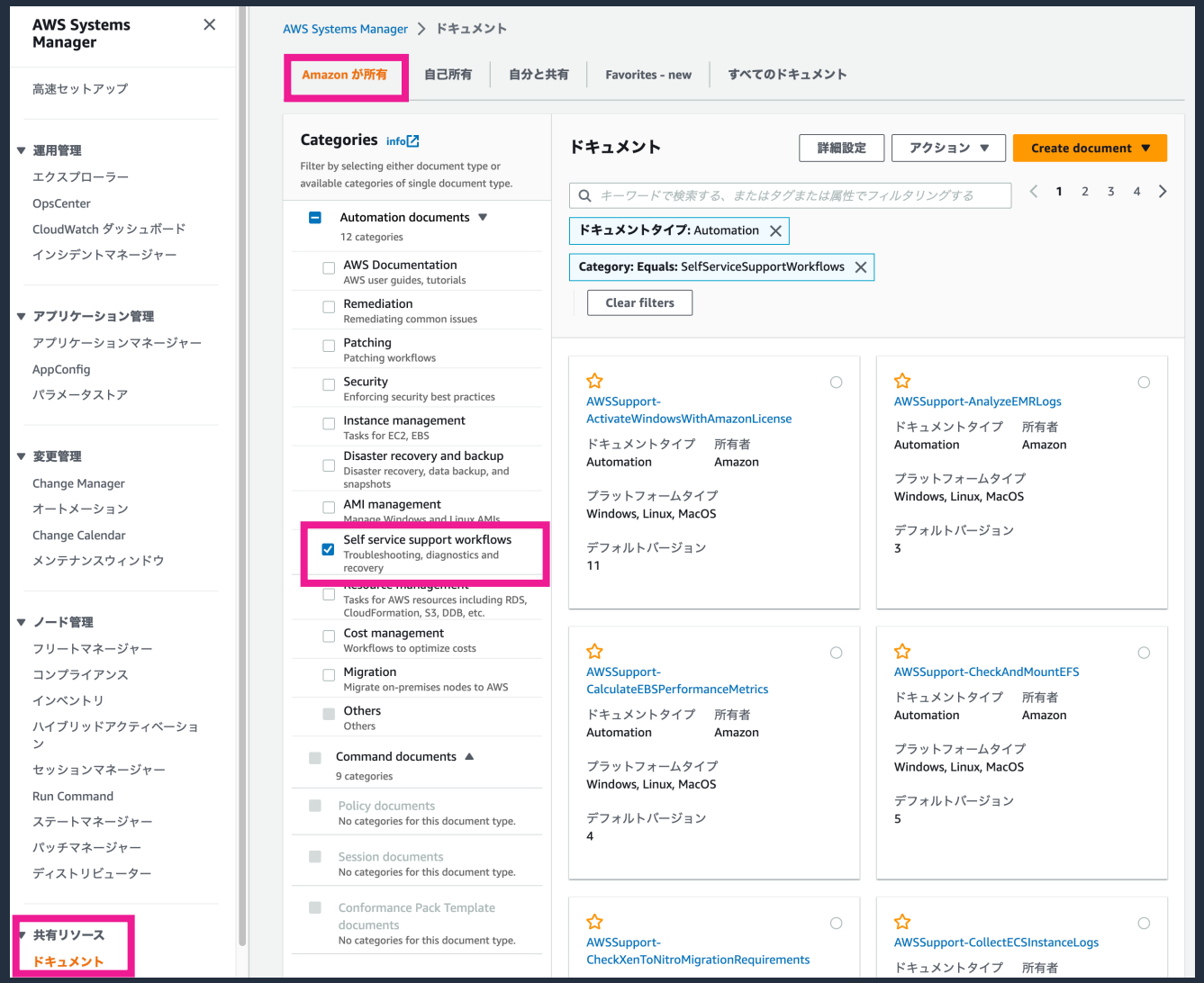
ランブックの探し方

ランブックの探し方

- SAWのランブックを探すには、以下のようにいくつかの方法があります

1. AWS SSM のコンソールから検索する
2. AWS SAW のランディングページから確認する
3. AWS re:Post やサービスのドキュメントから確認する

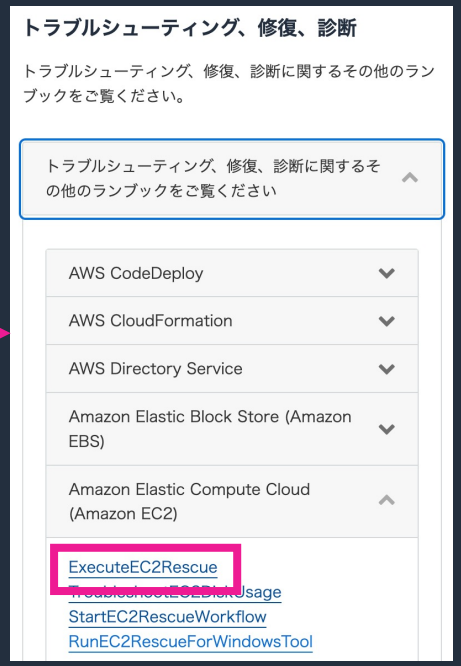
AWS Systems Manager のコンソールから検索する



- AWS Systems Manager コンソールを表示し、左ペインの [ドキュメント] をクリックします
- [Amazon が所有] のタブを選択し、[Self service support workflows] をチェックします
- ランブックの一覧が表示されるので、実行したいランブックをクリックします

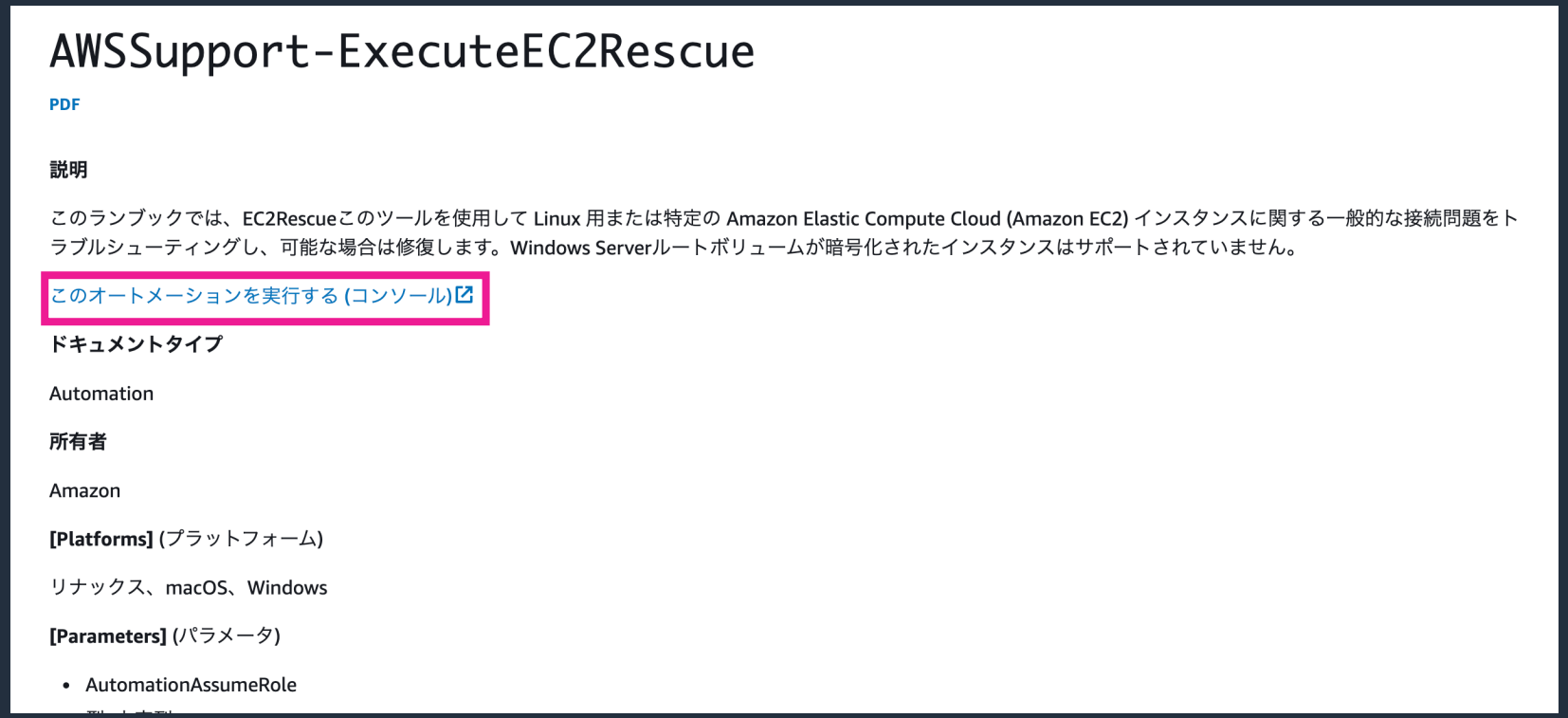
AWS SAW のランディングページから確認する

- 各ユースケースのドロップダウンリストをクリックするとサービスごとのランブックが表示されます



https://aws.amazon.com/jp/premiumsupport/technology/saw/

AWS SAW のランディングページから確認する



AWSSupport-ExecuteEC2Rescue

PDF

説明

このランブックでは、EC2Rescueこのツールを使用して Linux 用または特定の Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに関する一般的な接続問題をトラブルシューティングし、可能な場合は修復します。Windows Serverルートボリュームが暗号化されたインスタンスはサポートされていません。

このオートメーションを実行する (コンソール)

ドキュメントタイプ

Automation

所有者

Amazon

[Platforms] (プラットフォーム)

リナックス、macOS、Windows

[Parameters] (パラメータ)

- AutomationAssumeRole

- ランブックの詳細のページには、コンソールへのリンクが含まれており、このリンクからすぐに実行が可能

AWS re:Post やサービスのドキュメントから確認する

- ランブックによってはサービスのドキュメント自体に記述があるものがあり、使用方法が記述されています
- AWS re:Post で詳細な使用方法を説明している記事が存在する場合があります

https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/automation-ec2rescue.html
https://repost.aws/ja/knowledge-center/ec2rescue-windows-troubleshoot

料金の説明

SAW のコスト

2023年10月時点での料金

- AWS Systems Manager の Automation の料金が課金されます
  1. ステップカウント
     1 か月あたりアカウントごとに 100,000 ステップの無料利用枠
     無料利用枠を超えると、1 ステップあたり 0.002 USD
  2. ステップの実行時間
     aws:executeScript のステップには、1 か月あたり 5,000 秒の無料利用枠
     無料利用枠を超えると 1 秒あたり 0.00003 USD
- ランブックの実行によって発生する通信については標準の AWS データ転送料金で課金されます
- ランブックによって作成されたリソースは、それぞれ別途課金されます

まとめ

まとめ

- AWS Support Automation Workflows(SAW) はお客様の AWS アカウントの環境で実行することでトラブルシューティング、ログの収集や分析、管理タスクを自動化します
- AWS サポートとのコミュニケーションコストを最適化
- お客様側でトラブルシューティングを行うことで、AWSサポートへの問い合わせ前に問題を解決できる可能性があります

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

- 本資料では資料作成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)

Thank you!