AWS Black Belt Online Seminar

# AWS SAW

## セルフサービス自動化ランブックを使用したトラフィック監視の視覚化 Amazon Virtual Private Cloud (Amazon VPC) 編

Yuki Nakamura

Cloud Support Engineer
2023/11

# 自己紹介

名前：中村 佑希 (Yuki Nakamura)

所属：技術支援本部（AWS サポート）

好きな AWS サービス：


Amazon Route 53

AWS Direct Connect

AWS Transit Gateway

# 本セミナーの対象者

- VPC からターゲットサーバーまでの疎通監視をご検討されている方

# 本セミナーの目的

- トラフィックを監視する AWS SAW ランブック「 AWSSupport-SetupIPMonitoringFromVPC 」の紹介
- トラフィックのログ取得に関する AWS SAW ランブックの紹介

# 本日お話しないこと

- AWS System Manager の全体的な説明
- AWS Support Automation Workflows (SAW) の説明

AWS SAW - セルフサービスな診断と運用の効率化 入門編
https://www.youtube.com/watch?v=P-UOXiedd9I

# アジェンダ

1. AWSSupport-SetupIPMonitoringFromVPC の紹介
2. AWSSupport-SetupIPMonitoringFromVPC の設定方法
3. AWSSupport-SetupIPMonitoringFromVPC の活用例
4. クリーンアップ
5. トラフィックのログ取得に関するランブックの紹介
6. 料金の説明

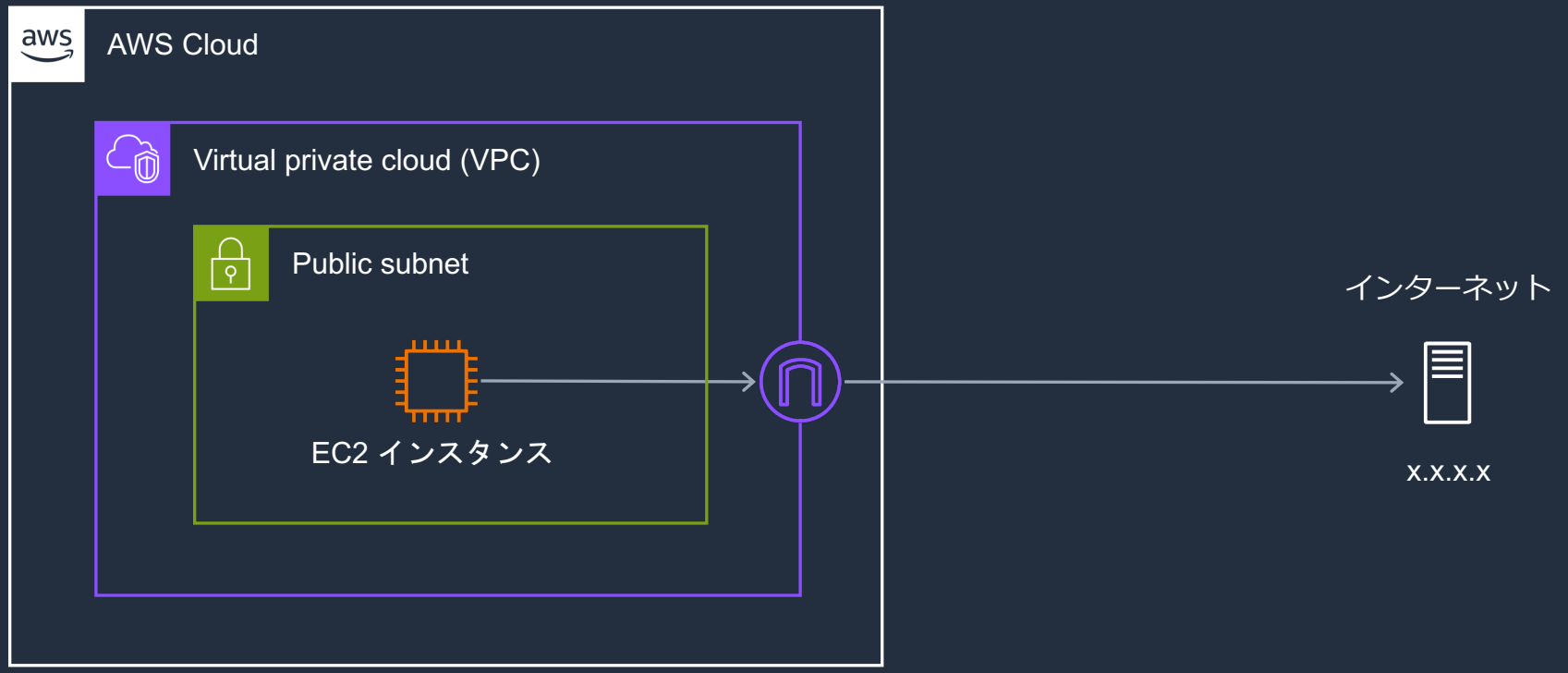
# AWSSupport-SetupIPMonitoringFromVPC とは？

# 概要

- VPC 上に EC2 インスタンスを作成し、
  ping / MTR / traceroute を指定した対象に継続的に実行して監視
- 実行結果は CloudWatch ログや CloudWatch メトリクス、
  CloudWatch ダッシュボードで確認可能
- 追加で CloudWatch アラームを作成し、
  しきい値を超えた場合のアラーム通知が可能

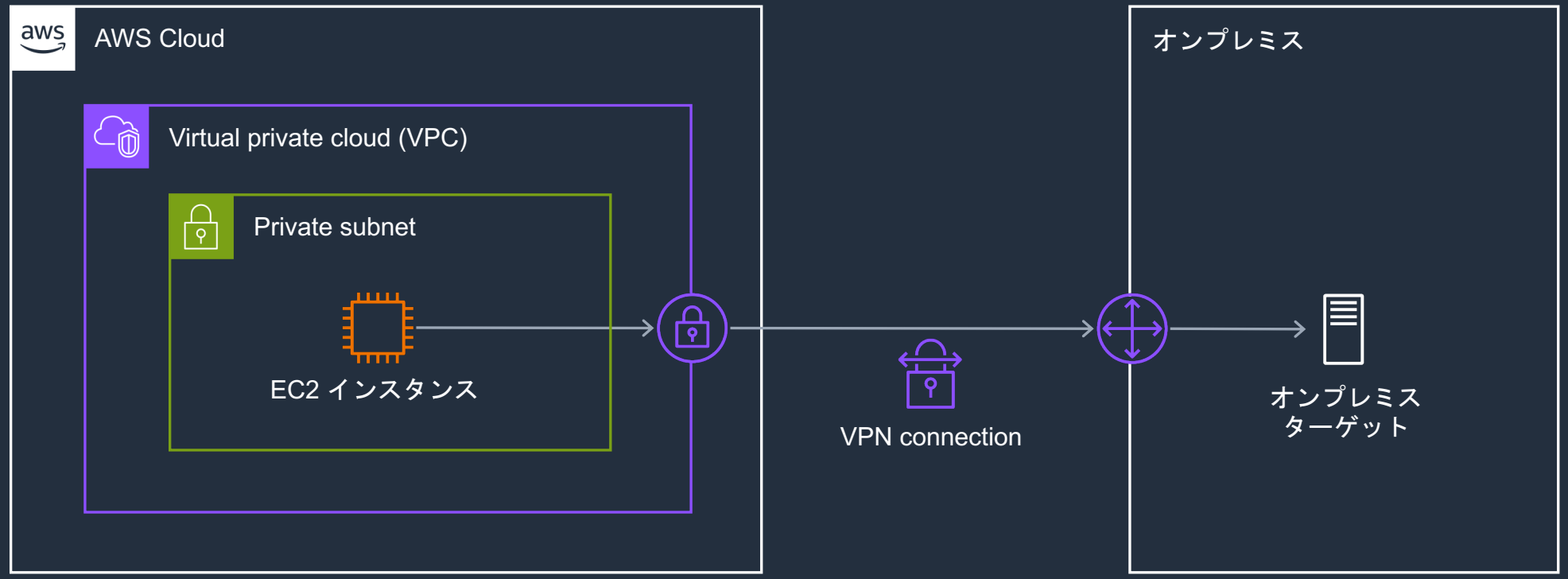
# 構成例 1

- インターネット上のサイトを監視
  提供するサービスやサイト等のレイテンシーとパケットロスを記録



# 構成例 2

- AWS Site-to-Site VPN や AWS Direct Connect を経由してオンプレミスのターゲットを監視



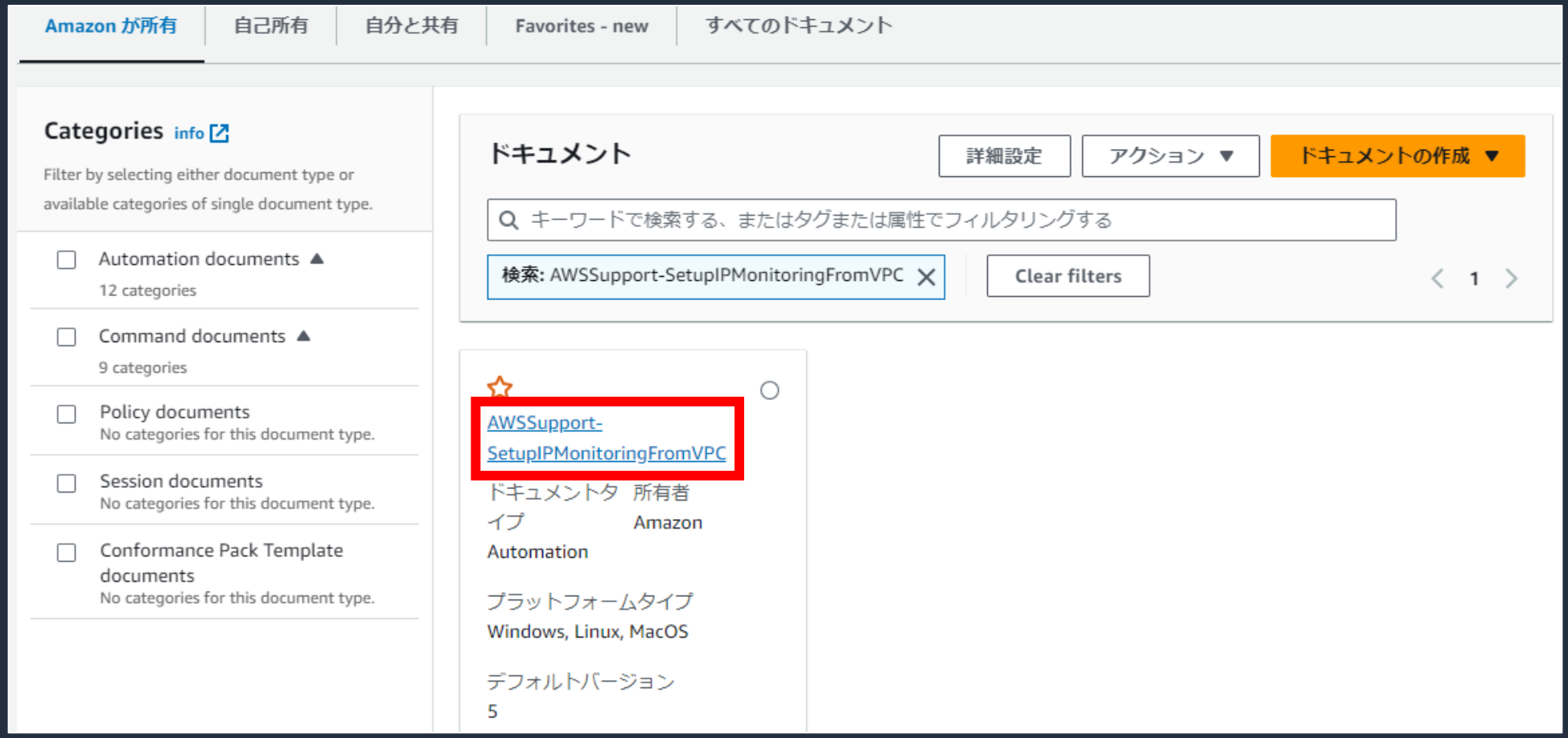
# 設定方法

# 設定方法

1. AWS Systems Manager コンソールからリージョンを指定し、「ドキュメント」を選択

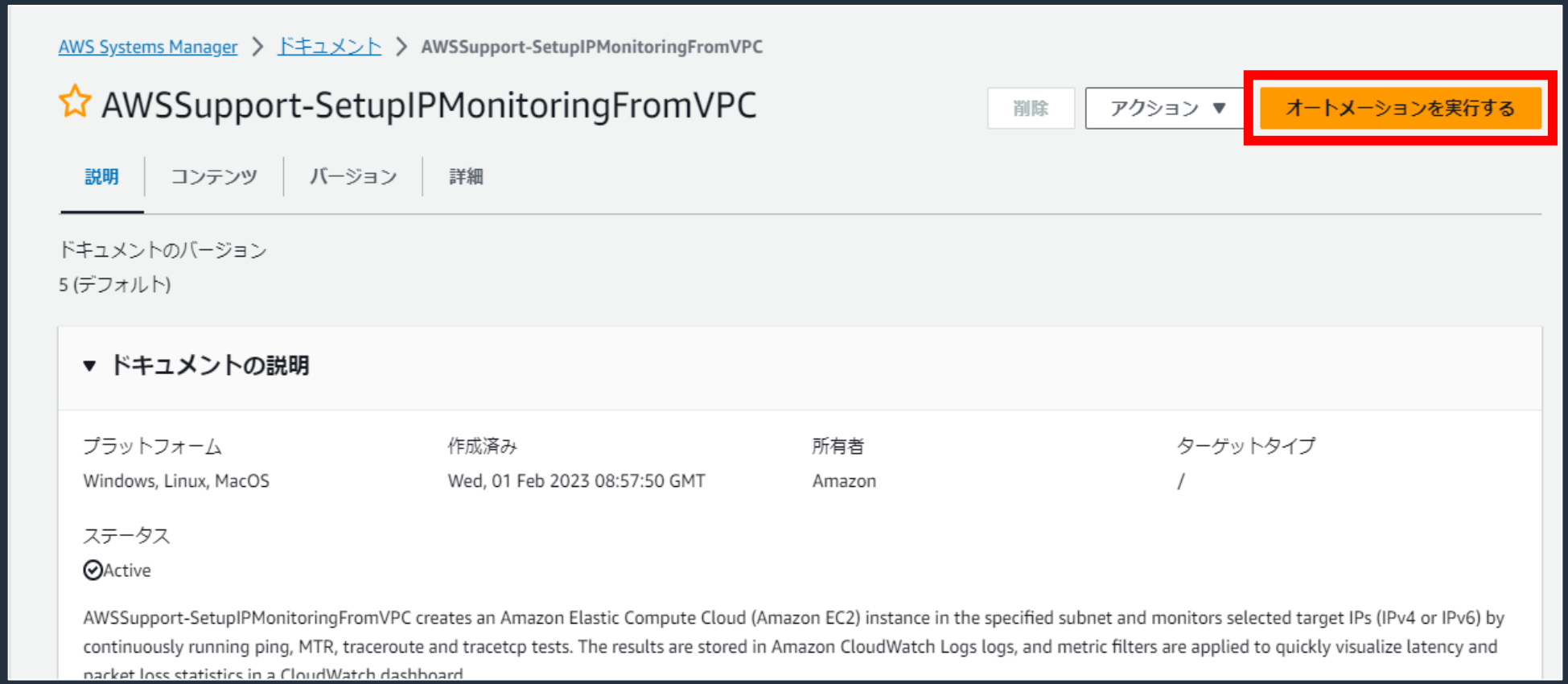
# 設定方法

2. 検索窓に「AWSSupport-SetupIPMonitoringFromVPC」を入力し、該当するドキュメントを選択



# 設定方法

3. 「オートメーションを実行する」を選択



# 設定方法

4. ランブック入力パラメーター
   - 「シンプルな実行」を選択
   - SubnetId：監視用の EC2 インスタンスを起動するサブネット
   - TargetIPs：監視対象サーバーの IP アドレス

※ オプションはデフォルトのままで実行可

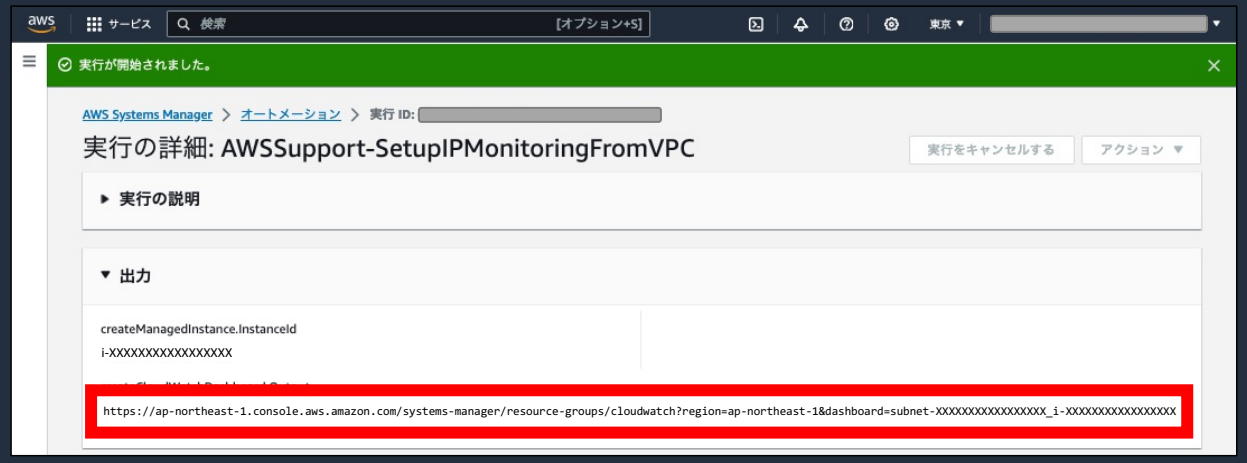
# 注意事項

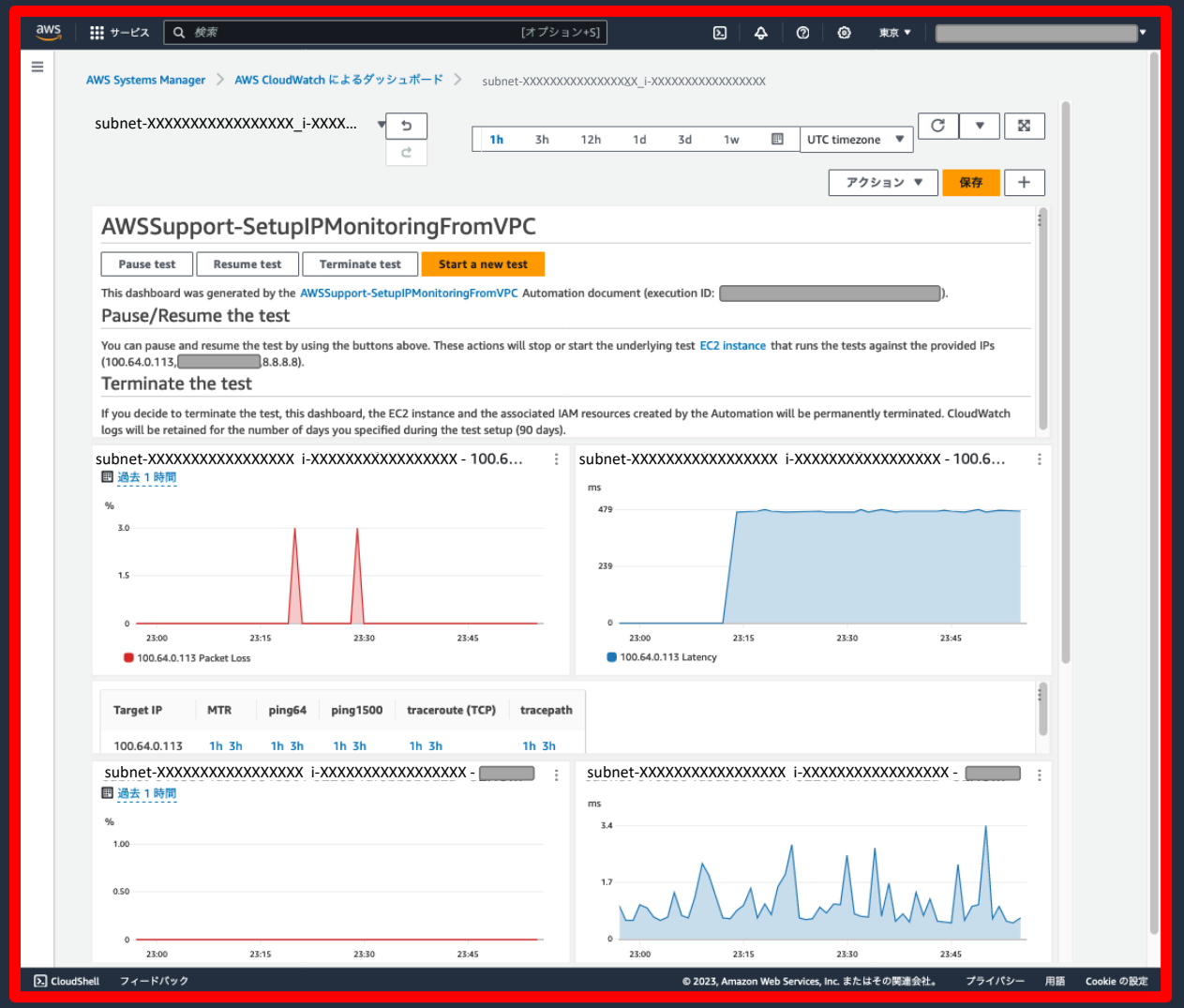
- 設定したパラメーターが有効でない場合は実行は失敗する
- ランブックが完了するまで 15 分程かかる
- 実行に必要な IAM アクセス許可はドキュメントを参照

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

# 活用例

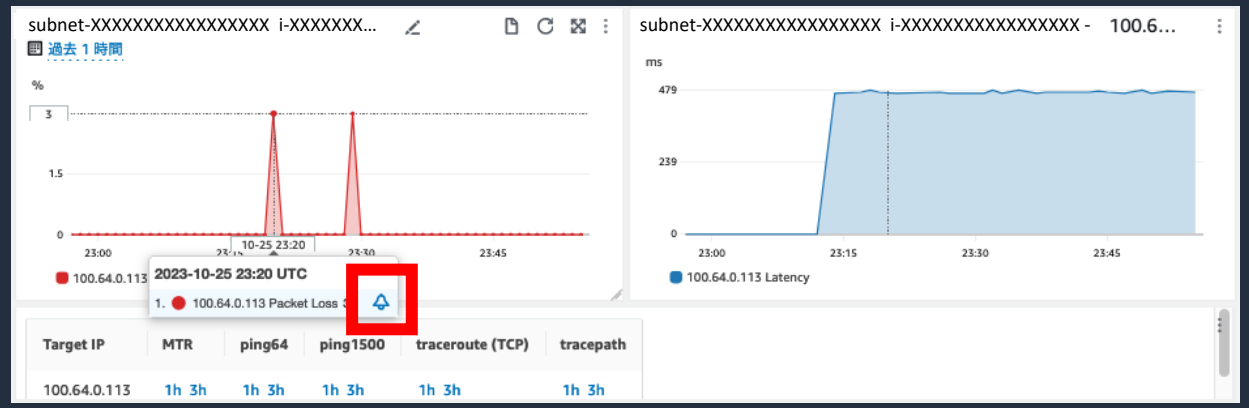
# CloudWatch ダッシュボード



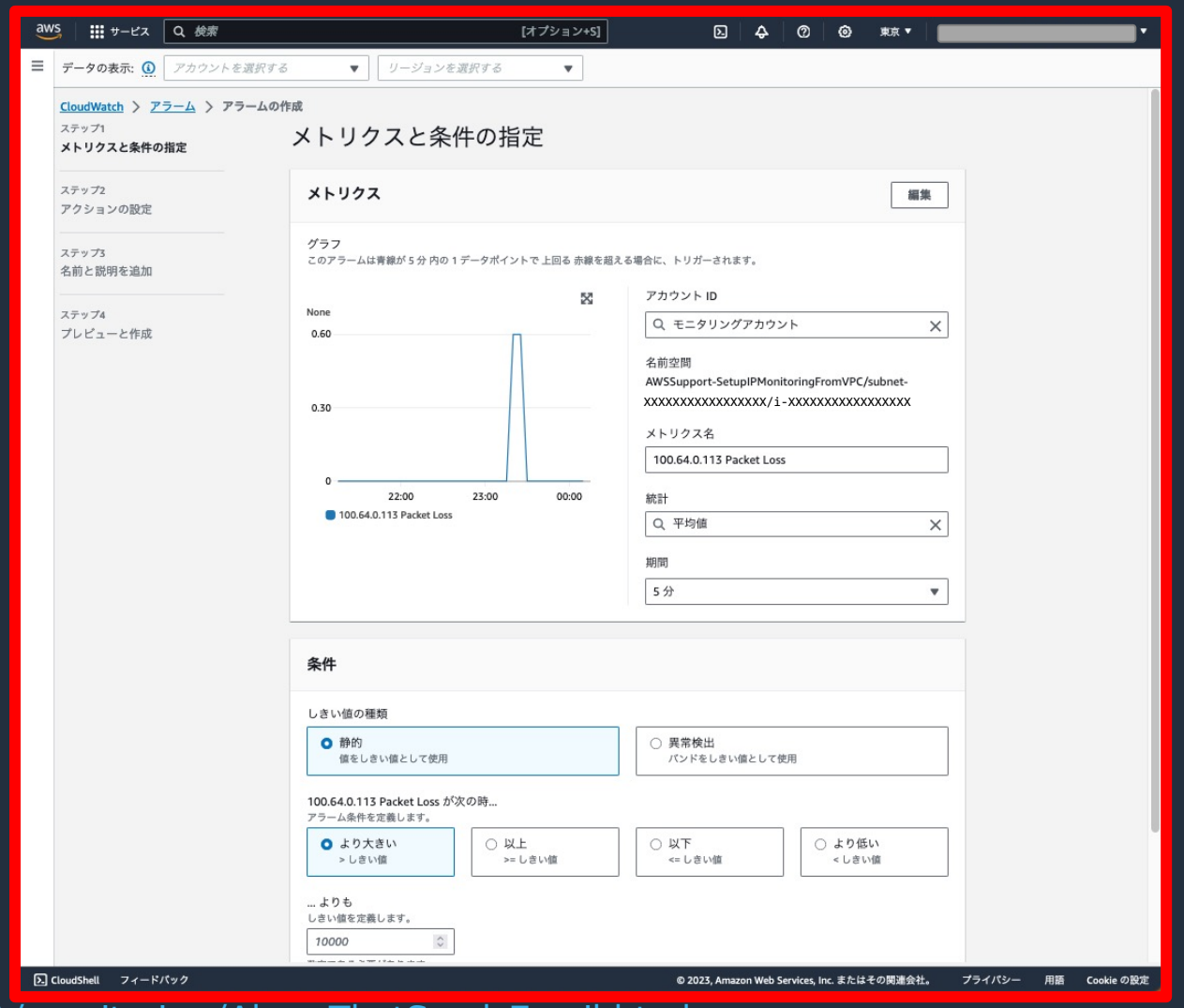




- ランブック実行結果の出力に表示される URL からアクセス
- Packet Loss や Latency のメトリクスを確認できる
- 複数の監視対象のメトリクスを一目で確認できる

# CloudWatch アラームとの併用

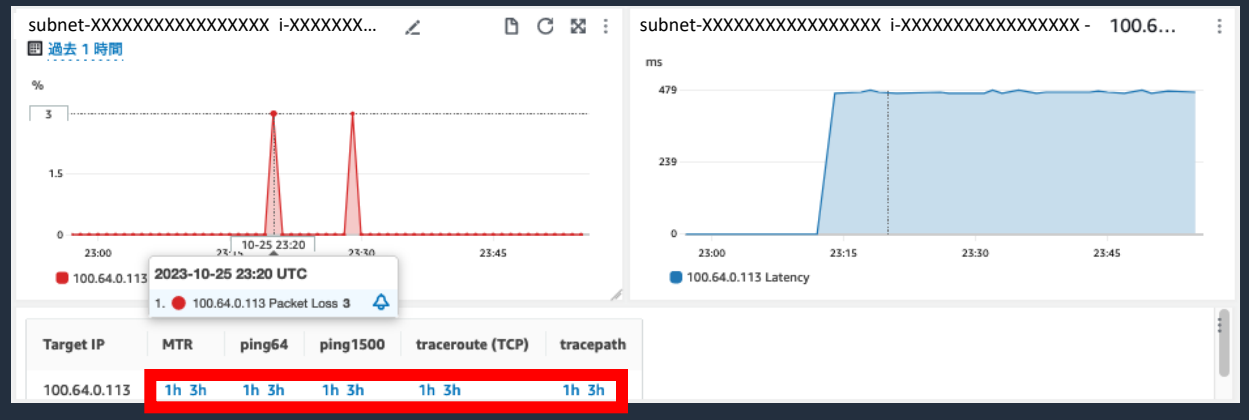


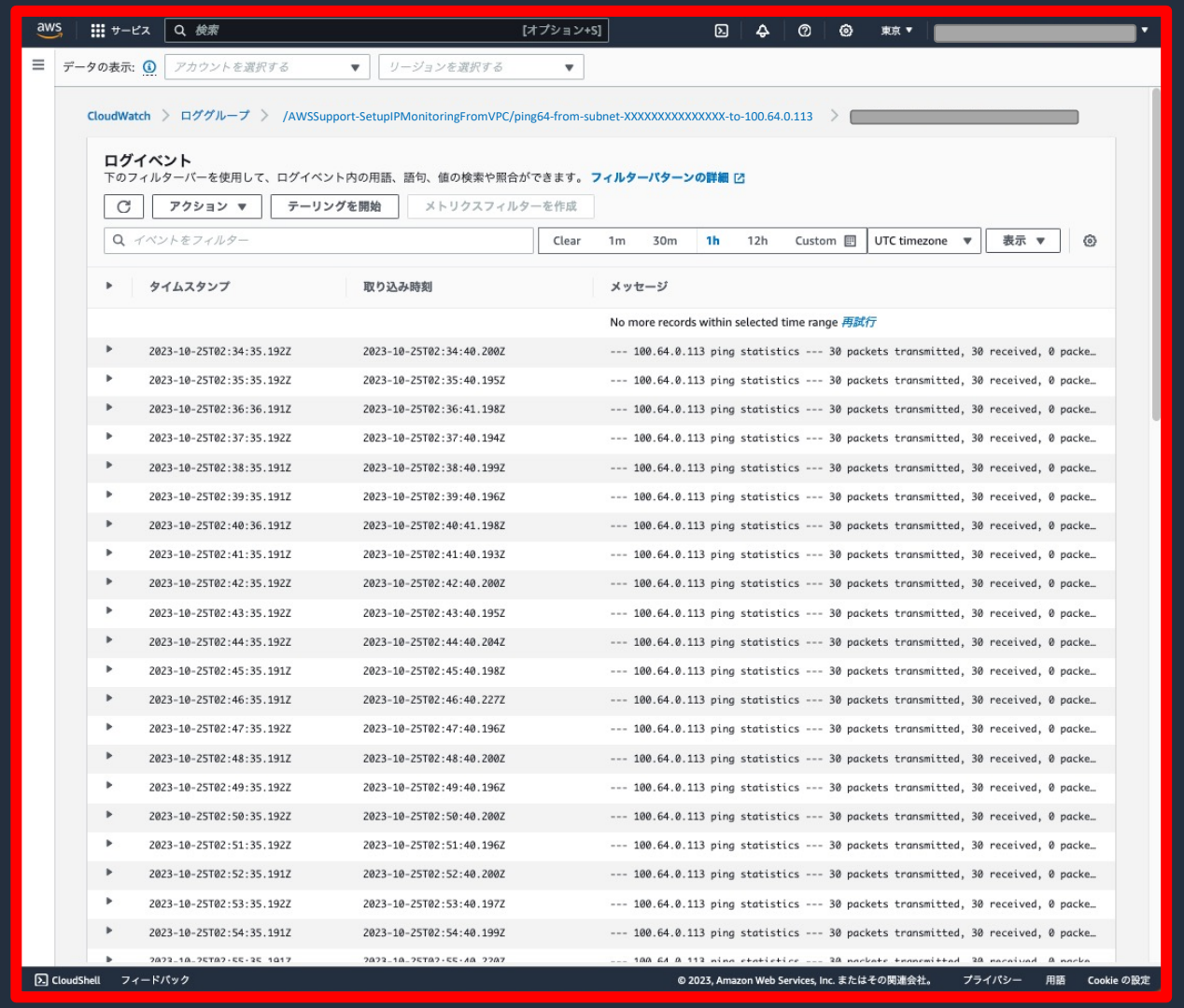

- データポイントの 🔔 から アラームの作成画面へ
- しきい値を超えた場合に Amazon SNS で通知することも可能




Amazon CloudWatch でのアラームの使用
https://docs.aws.amazon.com/ja_jp/AmazonCloudWatch/latest/monitoring/AlarmThatSendsEmail.html

# CloudWatch ログからの詳細

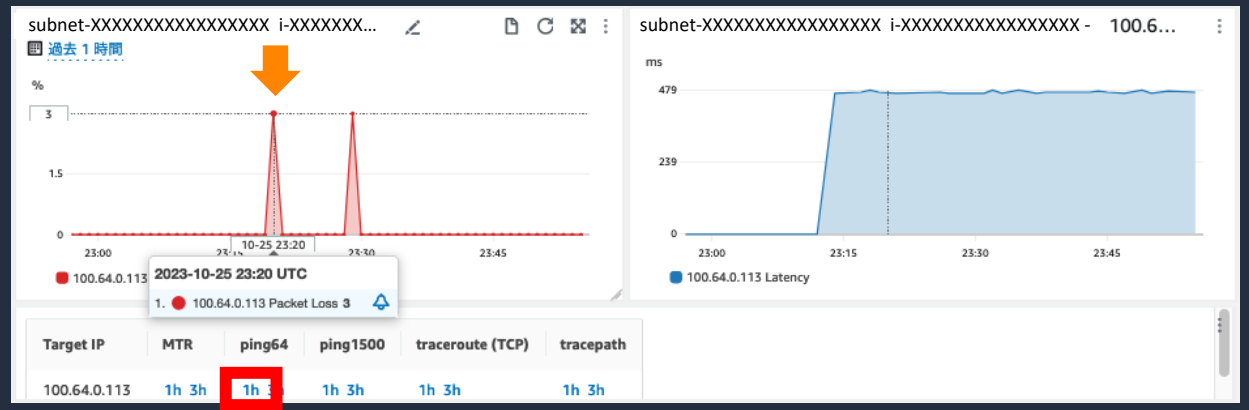


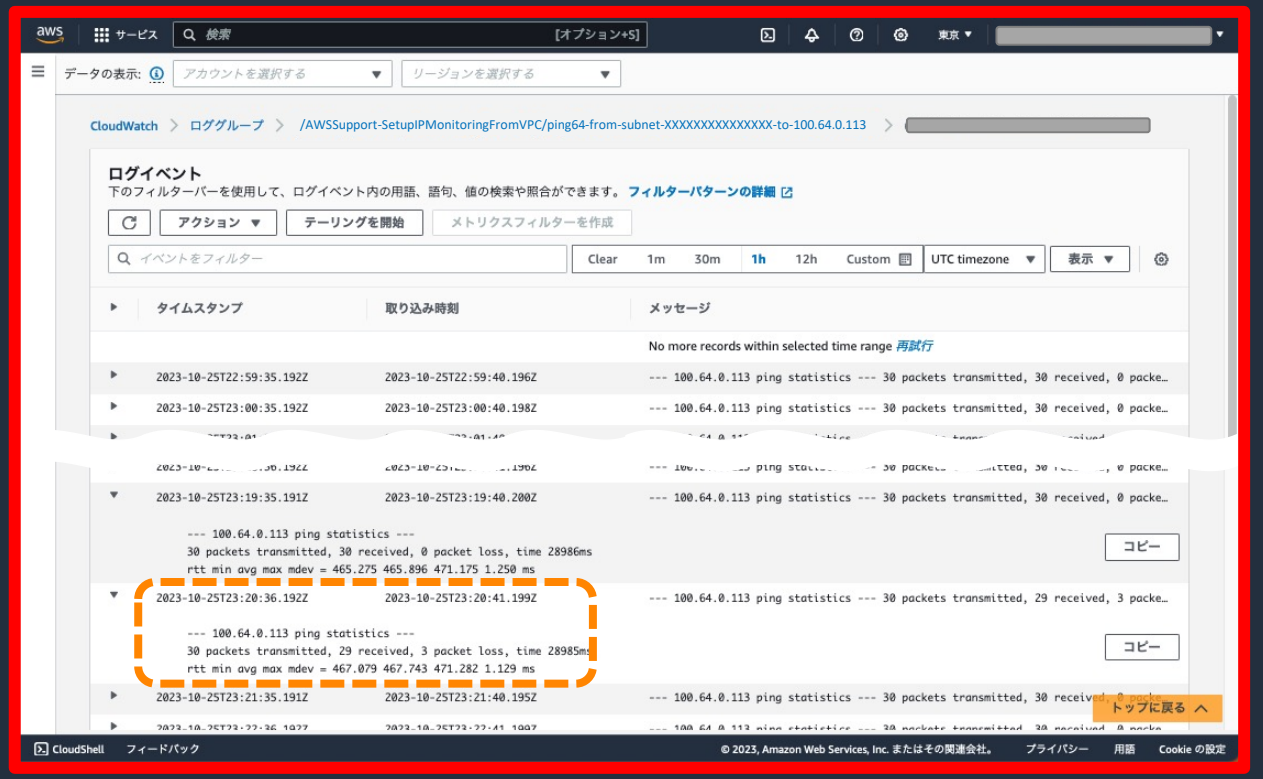




- 各コマンドの **1h** や **3h** から コマンド実行結果の確認画面へ
- 特定の時間における
  - ping 実行結果
  - traceroute (TCP) 実行結果

など確認が可能

# CloudWatch ログからの詳細 (Packet Loss)



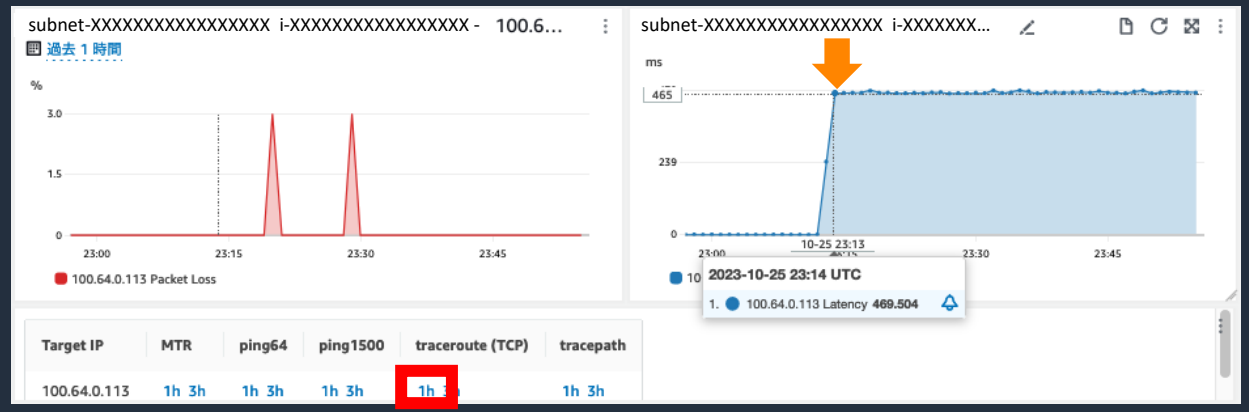

- 上記 Packet Loss 発生
- 1 分ごとの ping 結果が確認可能
  - どの程度の ping が落ちたか
  - 応答時間はどの程度かかったか

など確認が可能

```
2023-10-25T23:20:36.192Z          2023-10-25T23:20:41.199Z

--- 100.64.0.113 ping statistics ---
30 packets transmitted, 29 received, 3 packet loss, time 28985ms
rtt min avg max mdev = 467.079 467.743 471.282 1.129 ms
```

# CloudWatch ログからの詳細 (Latency)




- 上記 Latency の増加が発生
- 1 分ごとの traceroute 結果
  - 経路に変更があったか
  - Hop までどの程度時間がかかったか

など確認が可能

```
2023-10-25T23:13:07.274Z                2023-10-25T23:13:12.281Z

traceroute to 100.64.0.113 (100.64.0.113), 30 hops max, 60 byte packets
 1  100.64.0.113 [*]  5.095 ms  5.028 ms

2023-10-25T23:14:12.274Z                2023-10-25T23:14:17.284Z

traceroute to 100.64.0.113 (100.64.0.113), 30 hops max, 60 byte packets
 1  * *
 2  * *
 3  * *
 4  * *
 5  * *
 6  * *
 7  * *
 8  169.254.3.2 [*]  471.472 ms  471.425 ms
 9  100.64.15.177 [*]  477.198 ms  470.486 ms
10  100.64.0.113 [*]  480.471 ms  474.648 ms
```

経路が変更された可能性がある

- 人為的な操作ミス
- 経路の切り替わり

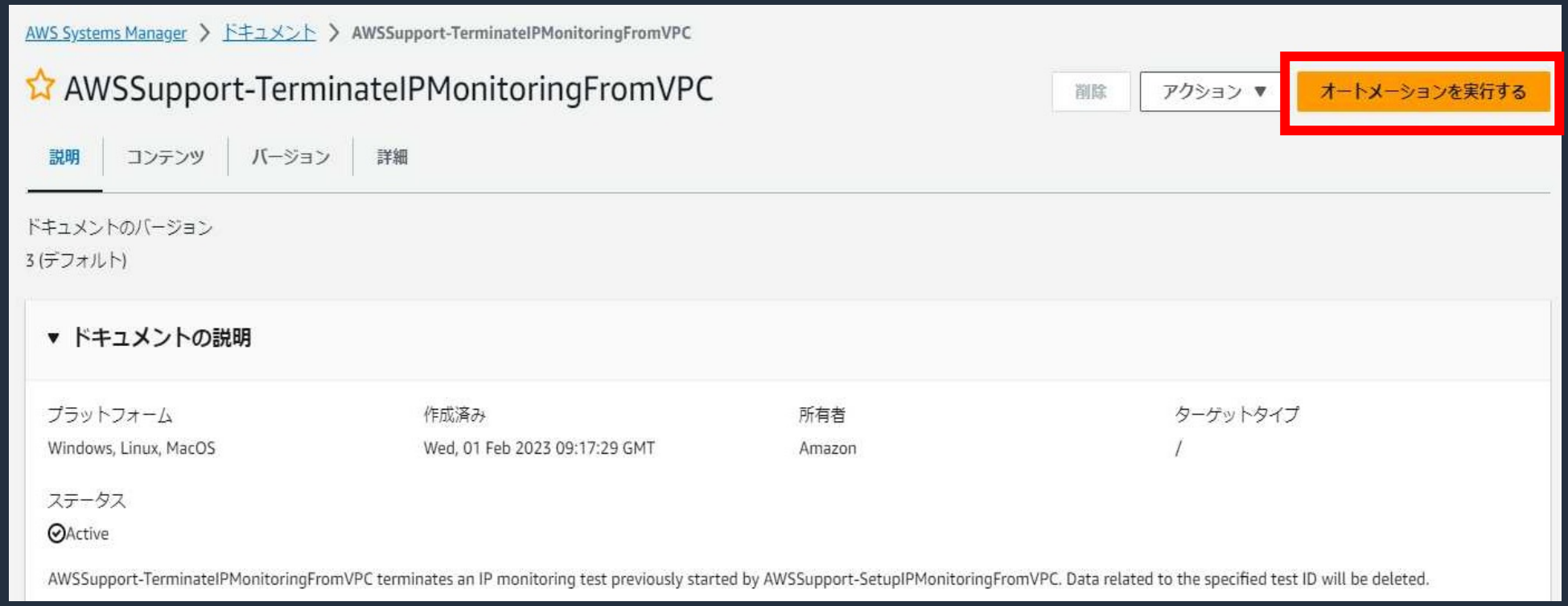
# クリーンアップ

# クリーンアップ

1. AWS Systems Manager の「ドキュメント」で「AWSSupport-TerminateIPMonitoringFromVPC」を検索し選択

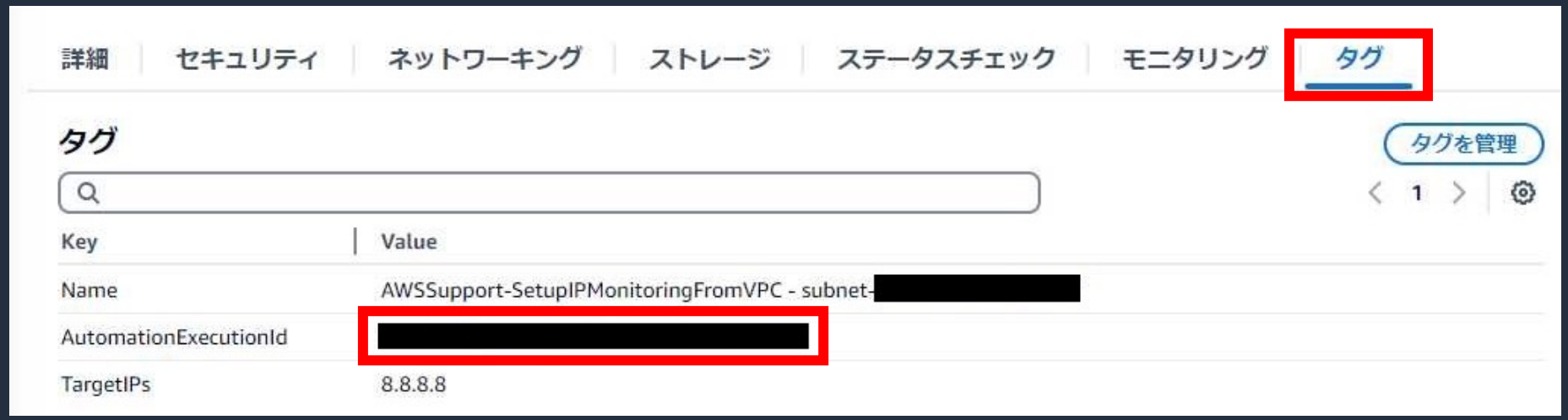
# クリーンアップ

2. 「オートメーションを実行する」を選択



# クリーンアップ

3. ランブック入力パラメーター
   - InstanceId：監視用 EC2 インスタンスの ID
   - AutomationExecutionId：監視用 EC2 インスタンスのタグから確認が可能
   - SubnetId： 監視用 EC2 インスタンスのサブネット ID




※ オプションはデフォルトのままで実行可

# その他の AWS SAW ランブック

# AWS SAW ランディングページ

- 現在提供されているランブックは以下のページに記載

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

- 今回はトラフィックのログ取得に役立つ２つのランブックを紹介

1. AWSSupport-EnableVPCFlowLogs：
   VPC フローログを設定するランブック

2. AWSSupport-ConfigureTrafficMirroring：
   トラフィックミラーリングを設定するランブック

# AWSSupport-EnableVPCFlowLogs

# AWSSupport-EnableVPCFlowLogs

- VPC フローログを自動で設定する

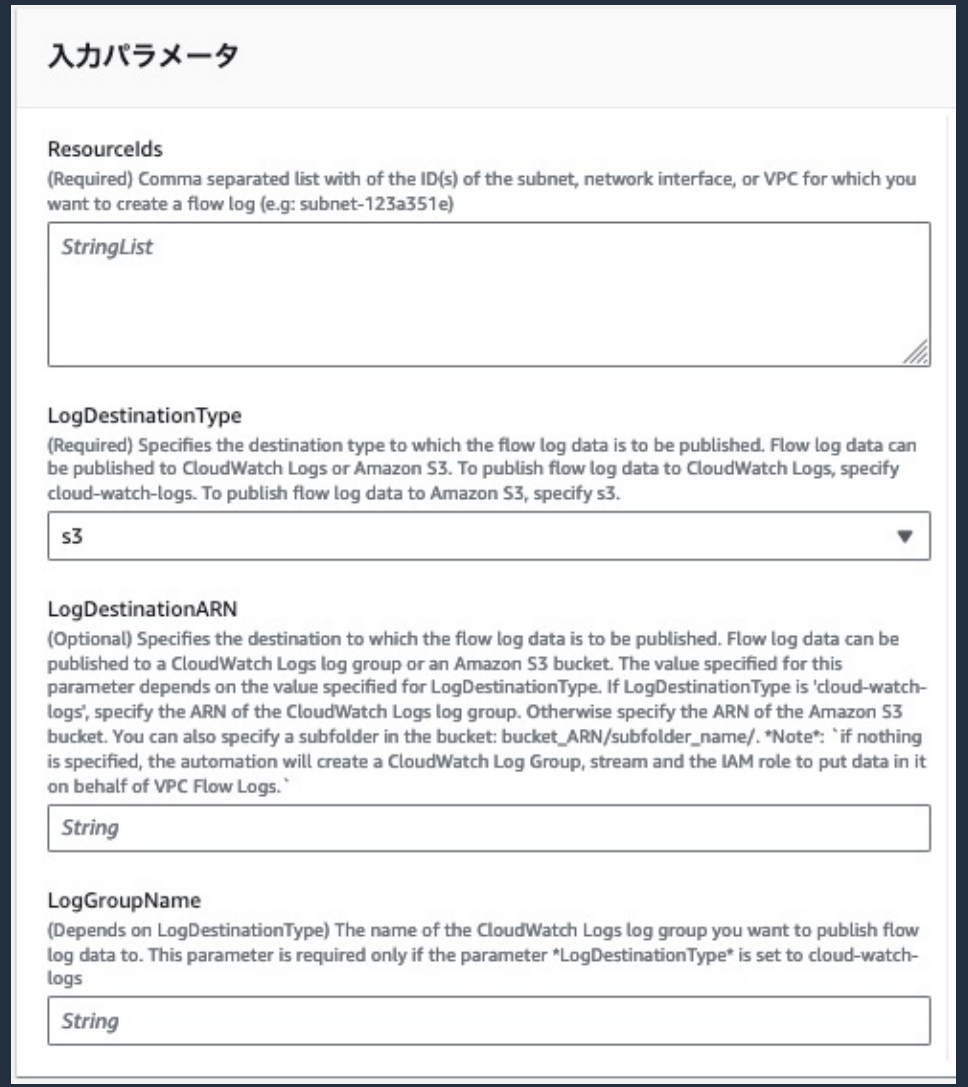
# VPC フローログ

- Elastic Network Interface を行き来する IP トラフィック情報を取得
- セキュリティグループルールの診断に役立つ
- インスタンスに到達するトラフィックの監視に役立つ
- 制限や詳細については下記公式ドキュメント参照

AWSSupport-EnableVPCFlowLogs
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-aws-enable-vpc-flowlogs.html
VPC フローログ
https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/flow-logs.html

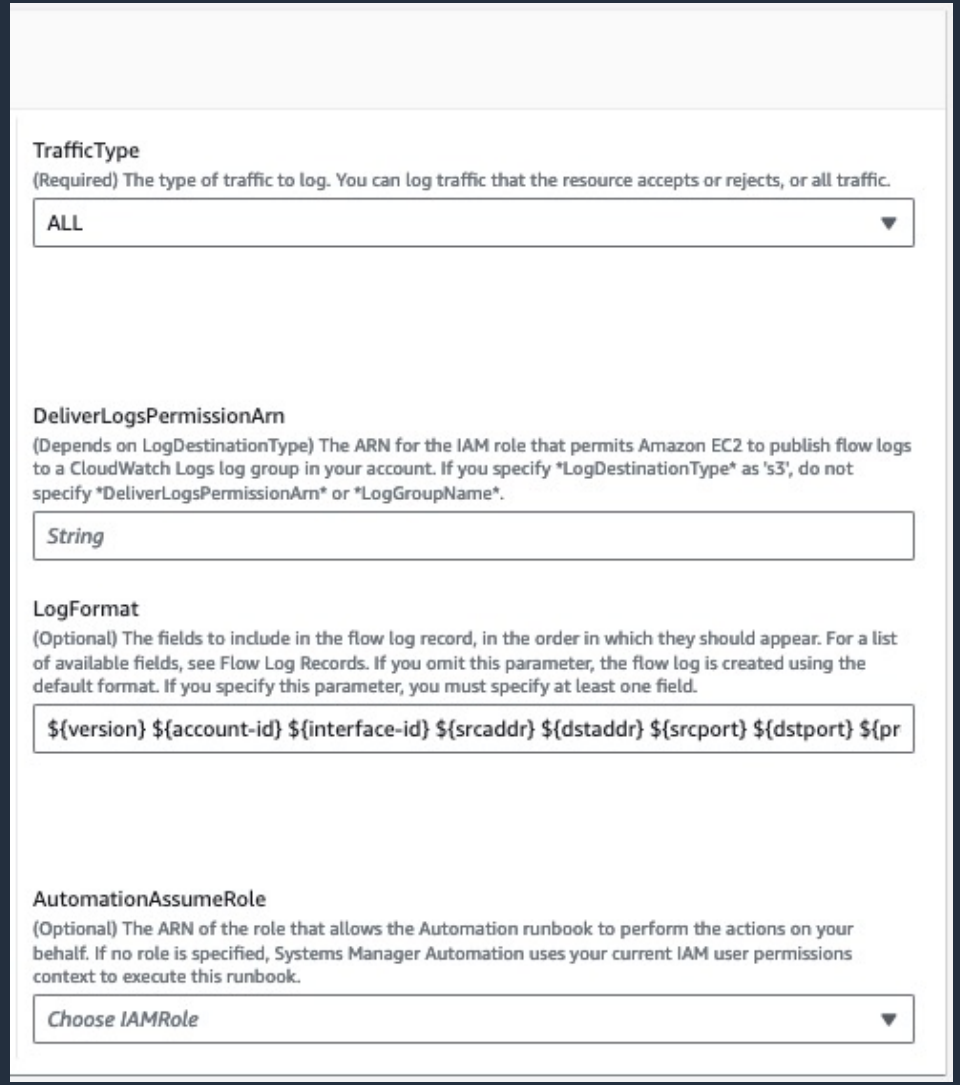
# ランブックの実行

| パラメータ | 説明 |
| --- | --- |
| **ResourceIds** | ログ取得対象のリソース ID<br>例： eni-0123456789abcef01,vpc-c15180a4 |
| **LogDestinationType** | ログ出力先リソースタイプ<br>有効な値: cloud-watch-log \| s3 |
| **LogDestinationARN** | ログ出力先の既存リソース ARN<br>※ cloud-watch-log (任意) / s3 (必須) |
| **LogGroupName** | ログ出力先の新規ロググループ名<br>※ cloud-watch-log (任意) / s3 (不要) |



# ランブックの実行

| パラメータ | 説明 |
| --- | --- |
| **TrafficType** | 記録するトラフィックのタイプ<br>有効な値: ACCEPT \| REJECT \| ALL |
| **DeliverLogsPermissionArn** | CloudWatchロググループにフローログの発行を許可するIAMロール<br>※ cloud-watch-log (必須) / s3 (不要) |
| **LogFormat** | フローログに含めるフィールドと、レコードに表示する順序の指定 |
| **AutomationAssumeRole** | SSMがユーザーに代わってアクションを実行できるようにするIAMロール |



# AWSSupport-ConfigureTrafficMirroring

# AWSSupport-ConfigureTrafficMirroring

- トラフィックミラーリングを自動で設定する

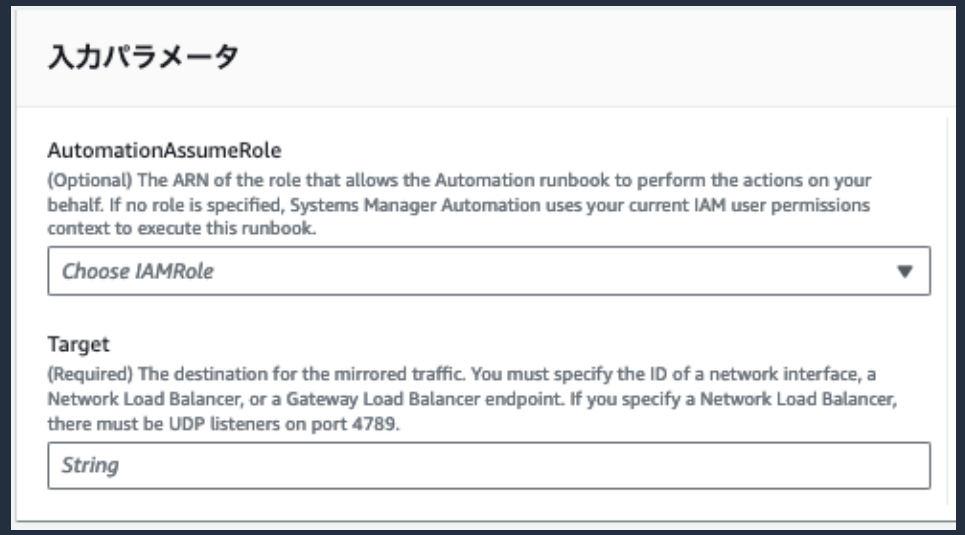
# トラフィックミラーリング

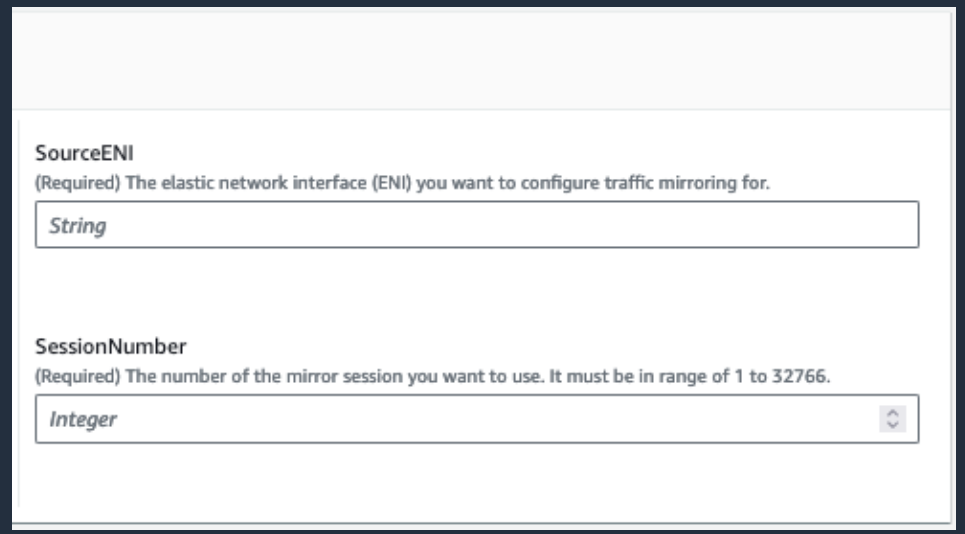
- Elastic Network Interface のトラフィックをコピー
- コピーしたトラフィックをターゲットに送信する
- パケットキャプチャの取得に役立つ
- 制限や詳細については下記公式ドキュメント参照

AWSSupport-ConfigureTrafficMirroring
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-aws-configuretrafficmirroring.html
トラフィックミラーリング
https://docs.aws.amazon.com/ja_jp/vpc/latest/mirroring/what-is-traffic-mirroring.html

# ランブックの実行

| パラメータ | 説明 |
| --- | --- |
| **AutomationAssumeRole** | SSMがユーザーに代わってアクションを実行できるようにする IAMロール |
| **Target** | ミラーリングされたトラフィックの宛先<br>例: NLB ARN や ENI ID |
| **SourceENI** | トラフィックをミラーリングしたい ENI |
| **SessionNumber** | 使用するミラーセッションの番号<br>有効な値: 1 - 32766 |



# 料金の説明

# SAWのコスト

2023年11月時点での料金

- AWS Systems Manager の Automation の料金が課金される。

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 が課金される
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 が課金される

- 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る
- ランブックによって作成されたリソースについては、それぞれ別途課金される

# 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!