



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

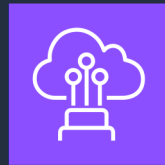
名前：中村 佑希 (Yuki Nakamura)

所属：技術支援本部 (AWS サポート)

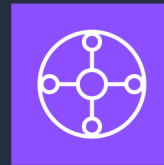
好きな AWS サービス：



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

本日本話しないこと

- 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

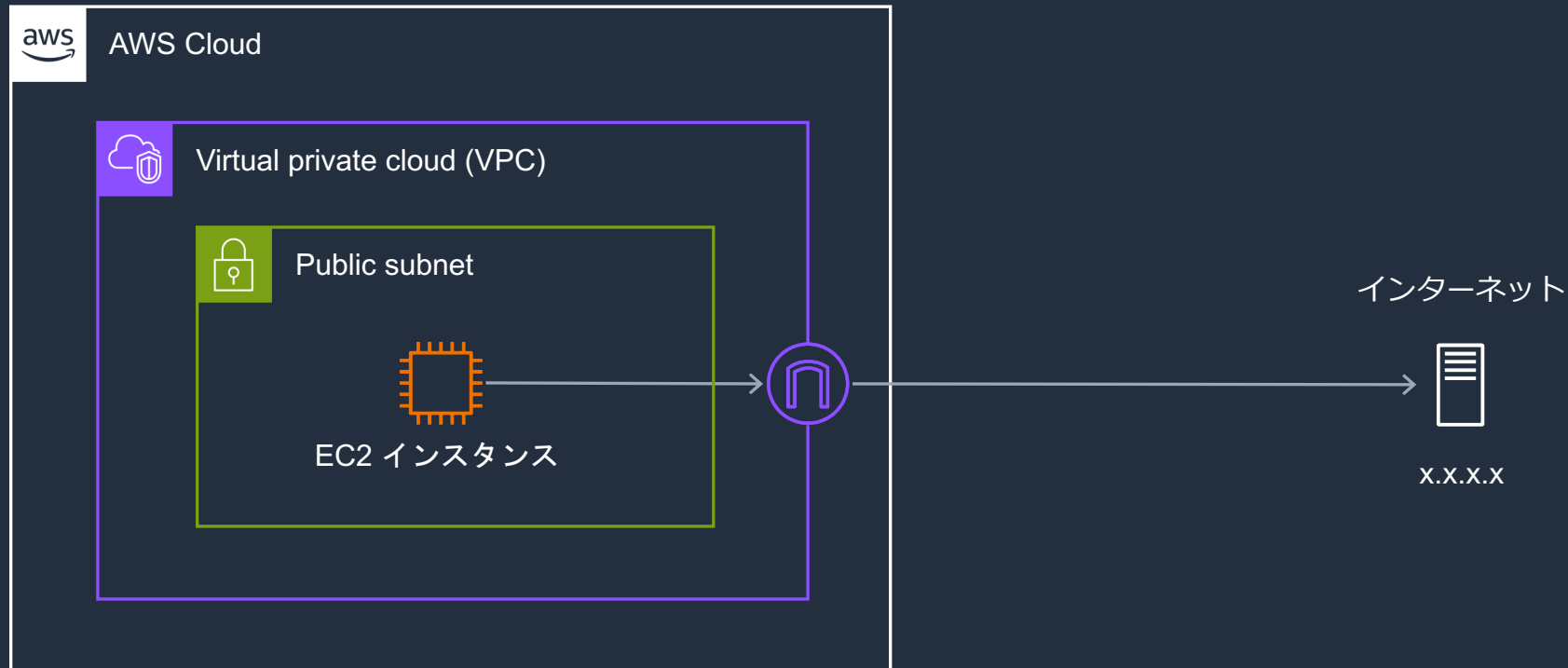
AWS Support- Setup IP Monitoring From VPC とは？

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

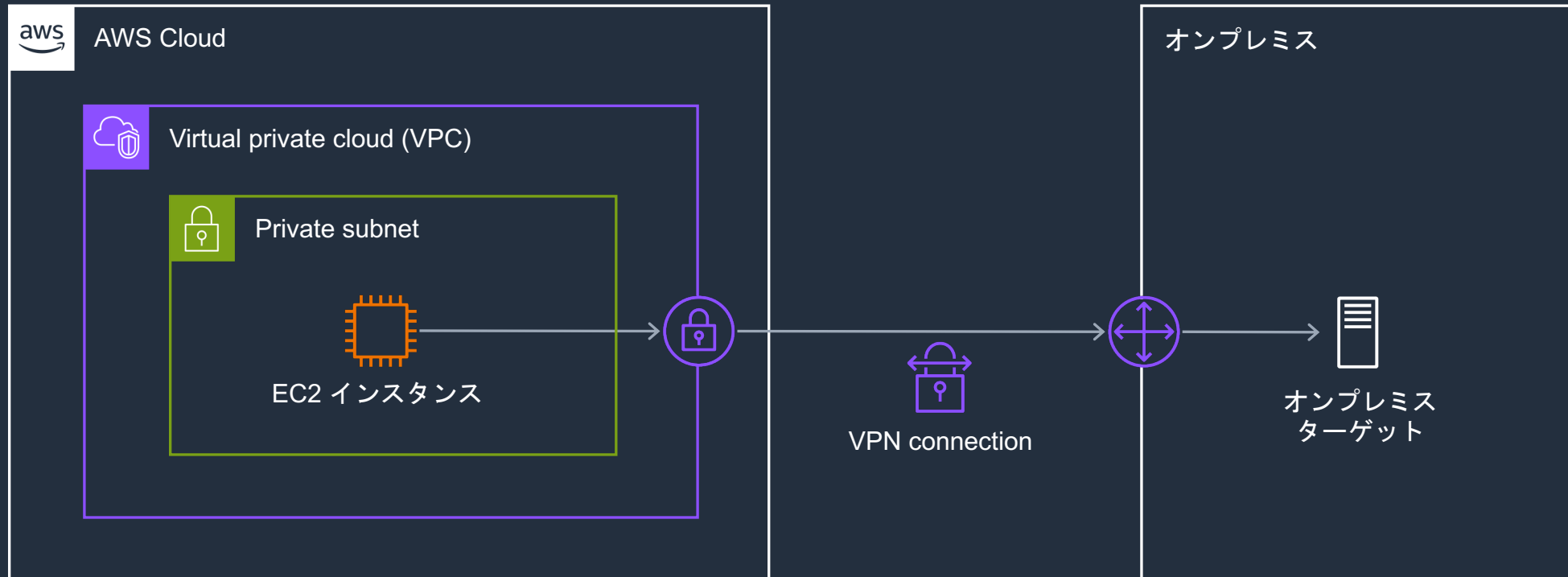
構成例 1

- 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

Amazon が所有 | 自己所有 | 自分と共有 | Favorites - new | すべてのドキュメント

Categories [info](#) [🔗](#)

Filter by selecting either document type or available categories of single document type.

- Automation documents ▲
12 categories
- Command documents ▲
9 categories
- Policy documents
No categories for this document type.
- Session documents
No categories for this document type.
- Conformance Pack Template documents
No categories for this document type.

ドキュメント

詳細設定 | アクション ▼ | ドキュメントの作成 ▼

🔍 キーワードで検索する、またはタグまたは属性でフィルタリングする

検索: AWSsupport-SetupIPMonitoringFromVPC ✕ | Clear filters | < 1 >

★ **AWSsupport-SetupIPMonitoringFromVPC** ○

ドキュメントタイプ 所有者
イブ Amazon
Automation

プラットフォームタイプ
Windows, Linux, MacOS

デフォルトバージョン
5

設定方法

3. 「オートメーションを実行する」を選択

The screenshot shows the AWS Systems Manager console interface for a document named 'AWSSupport-SetupIPMonitoringFromVPC'. The breadcrumb navigation is 'AWS Systems Manager > ドキュメント > AWSSupport-SetupIPMonitoringFromVPC'. The document title is '★ AWSSupport-SetupIPMonitoringFromVPC'. In the top right corner, there are three buttons: '削除' (Delete), 'アクション' (Actions) with a dropdown arrow, and 'オートメーションを実行する' (Run Automation), which is highlighted with a red rectangular box. 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 selected. Underneath, it says 'ドキュメントのバージョン' (Document version) and '5 (デフォルト)' (5 (Default)). A section titled '▼ ドキュメントの説明' (▼ Document description) contains a table with the following data:

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, 01 Feb 2023 08:57:50 GMT	Amazon	/

Below the table, the status is shown as 'ステータス' (Status) with a radio button selected for 'Active'. A descriptive paragraph follows: 'AWSSupport-SetupIPMonitoringFromVPC creates an Amazon Elastic Compute Cloud (Amazon EC2) instance in the specified subnet and monitors selected target IPs (IPv4 or IPv6) by continuously running ping, MTR, traceroute and tracetcp tests. The results are stored in Amazon CloudWatch Logs logs, and metric filters are applied to quickly visualize latency and market loss statistics in a CloudWatch dashboard.'

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も実行可

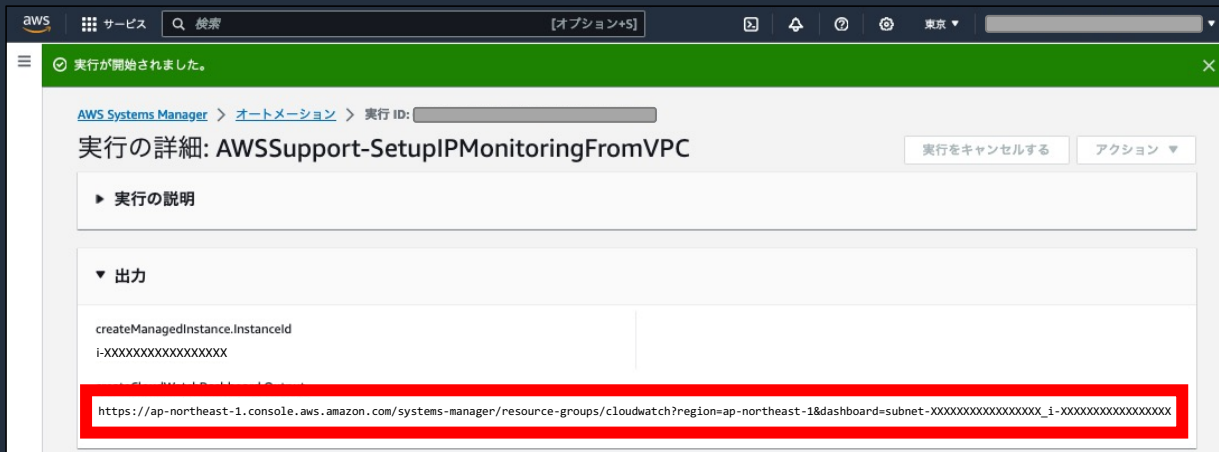
注意事項

- 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

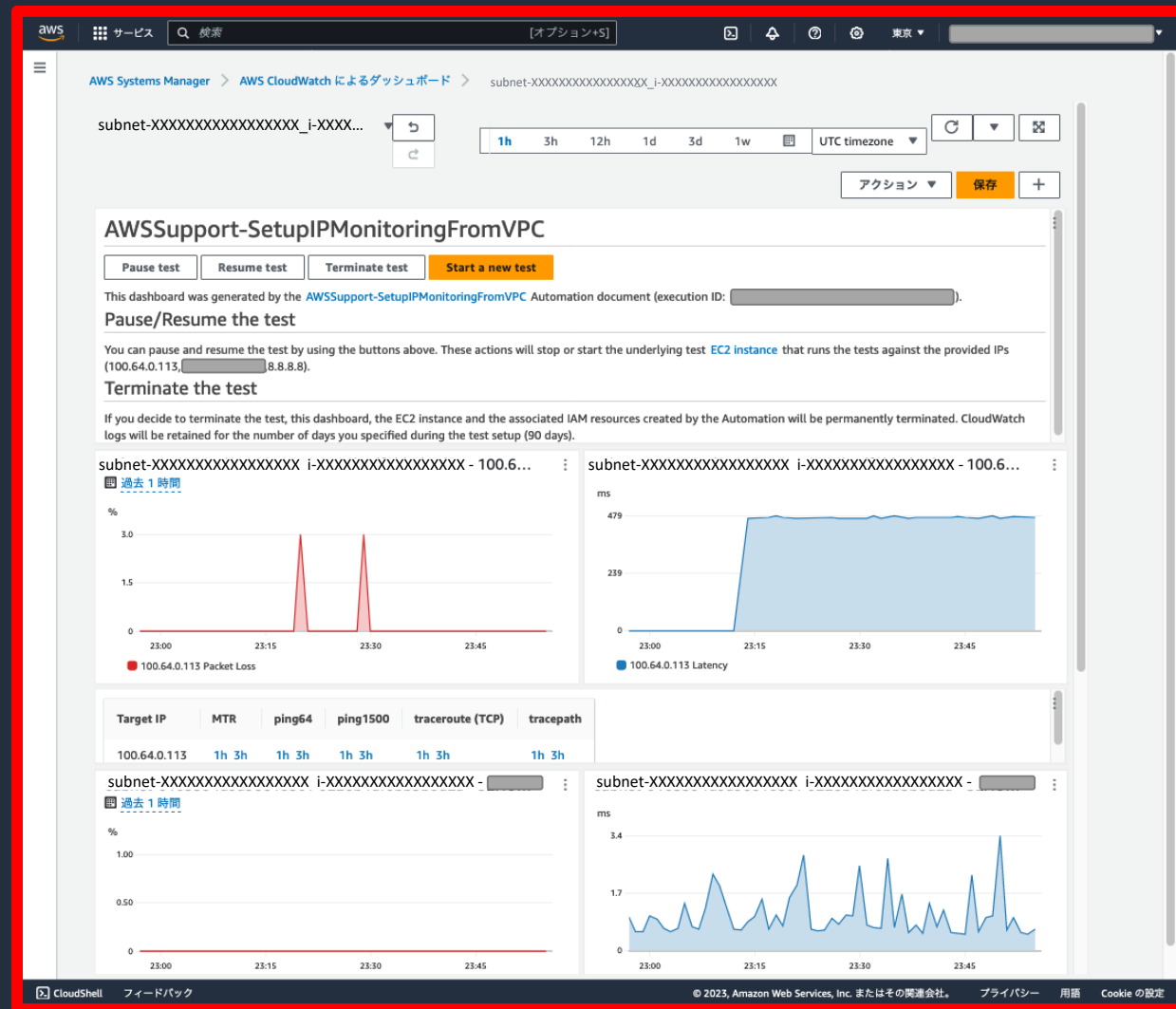
https://docs.aws.amazon.com/ja_jp/systems-manager-automation-runbooks/latest/userguide/automation-awssupport-setupipmonitoringfromvpc.html

活用例

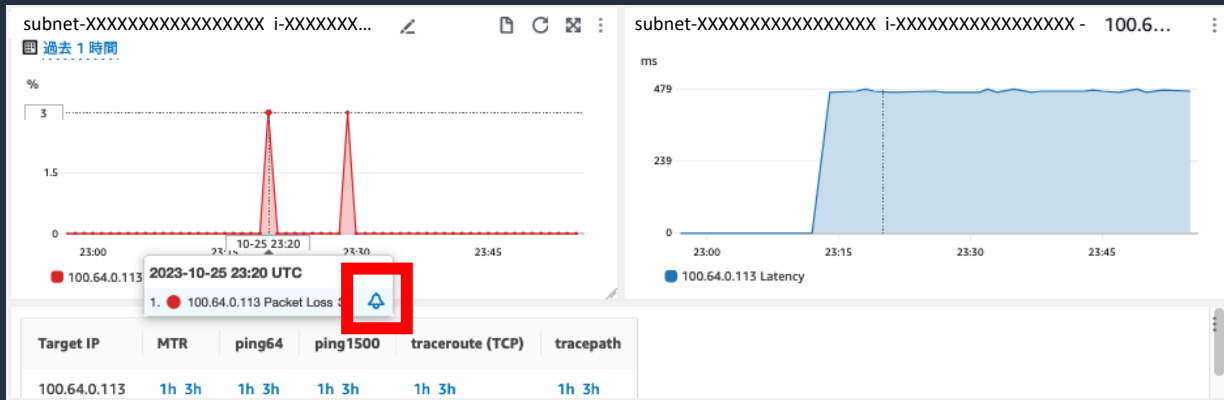
CloudWatch ダッシュボード




- 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



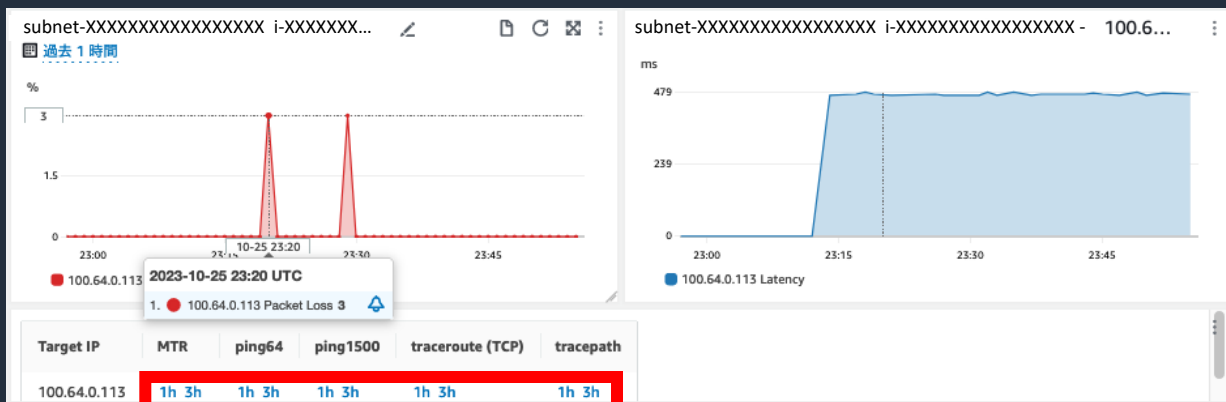
- データポイントの  からアラームの作成画面へ
- しきい値を超えた場合に Amazon SNS で通知することも可能

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

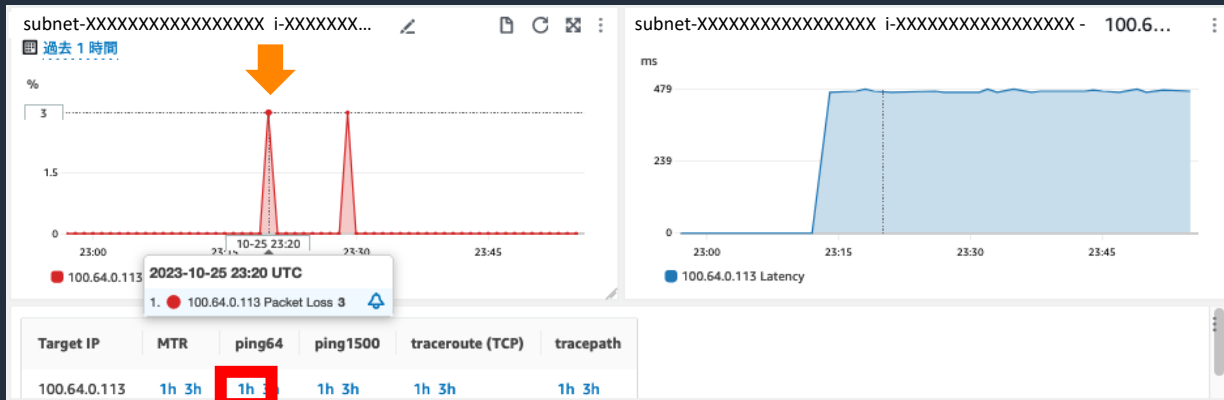


- 各コマンドの **1h** や **3h** からコマンド実行結果の確認画面へ
- 特定の時間における
 - ping 実行結果
 - traceroute (TCP) 実行結果

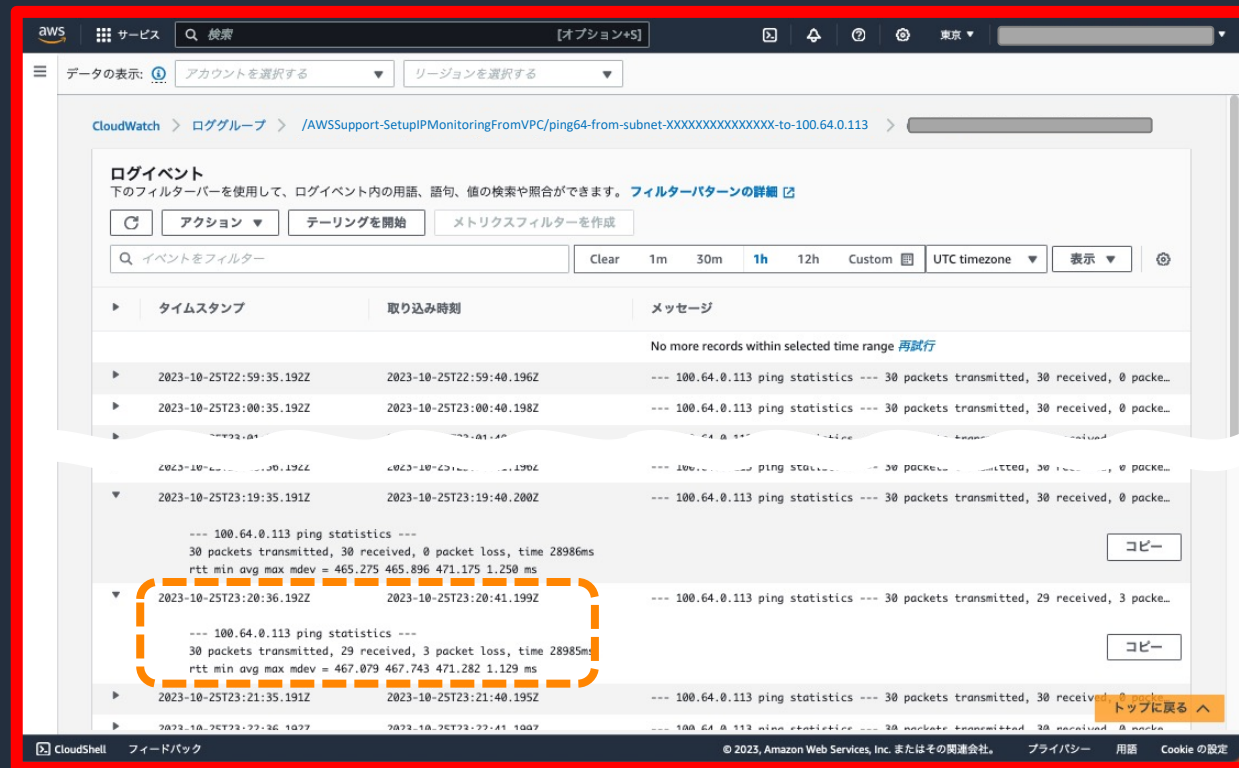
など確認が可能

タイムスタンプ	取り込み時刻	メッセージ
2023-10-25T02:34:35.192Z	2023-10-25T02:34:40.200Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:35:35.192Z	2023-10-25T02:35:40.195Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:36:36.191Z	2023-10-25T02:36:41.198Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:37:35.192Z	2023-10-25T02:37:40.194Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:38:35.191Z	2023-10-25T02:38:40.199Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:39:35.191Z	2023-10-25T02:39:40.196Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:40:36.191Z	2023-10-25T02:40:41.198Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:41:35.191Z	2023-10-25T02:41:40.193Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:42:35.192Z	2023-10-25T02:42:40.200Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:43:35.192Z	2023-10-25T02:43:40.195Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:44:35.192Z	2023-10-25T02:44:40.204Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:45:35.191Z	2023-10-25T02:45:40.198Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:46:35.191Z	2023-10-25T02:46:40.227Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:47:35.192Z	2023-10-25T02:47:40.196Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:48:35.191Z	2023-10-25T02:48:40.200Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:49:35.192Z	2023-10-25T02:49:40.196Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:50:35.192Z	2023-10-25T02:50:40.200Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:51:35.192Z	2023-10-25T02:51:40.196Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:52:35.191Z	2023-10-25T02:52:40.200Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:53:35.192Z	2023-10-25T02:53:40.197Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time
2023-10-25T02:54:35.191Z	2023-10-25T02:54:40.199Z	--- 100.64.0.113 ping statistics --- 30 packets transmitted, 30 received, 0 packets lost, 0 bytes in 0.000 seconds round-trip time

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

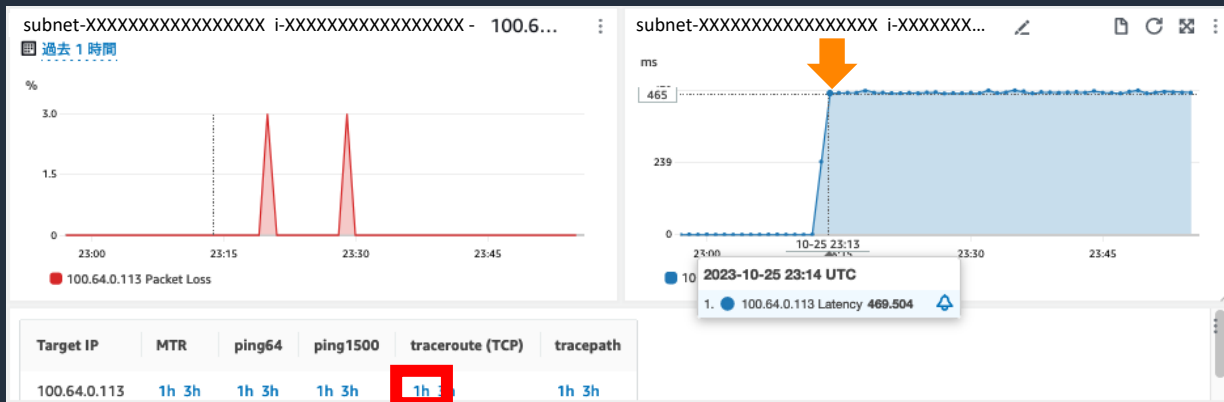
2023-10-25T23:20:41.199Z

--- 100.64.0.113 ping statistics ---

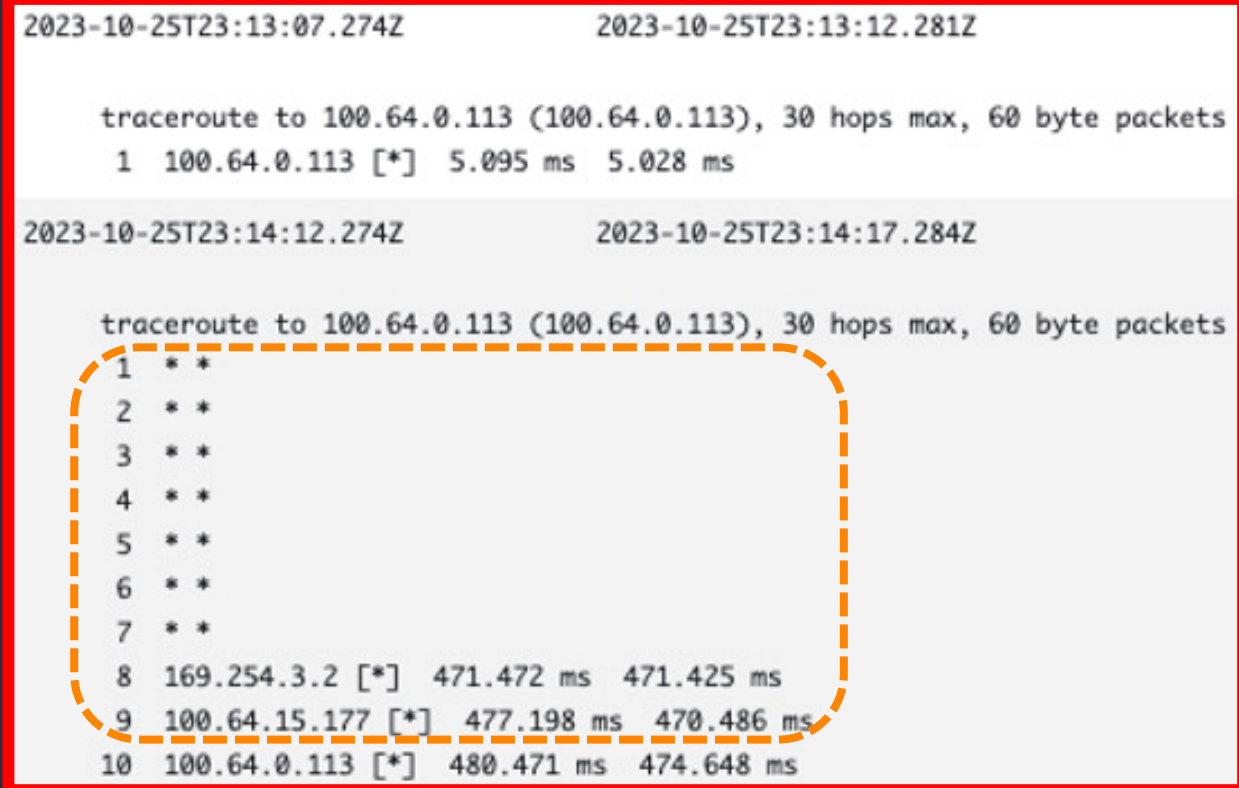
30 packets transmitted, 29 received, 3 packet loss, time 28985ms

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



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

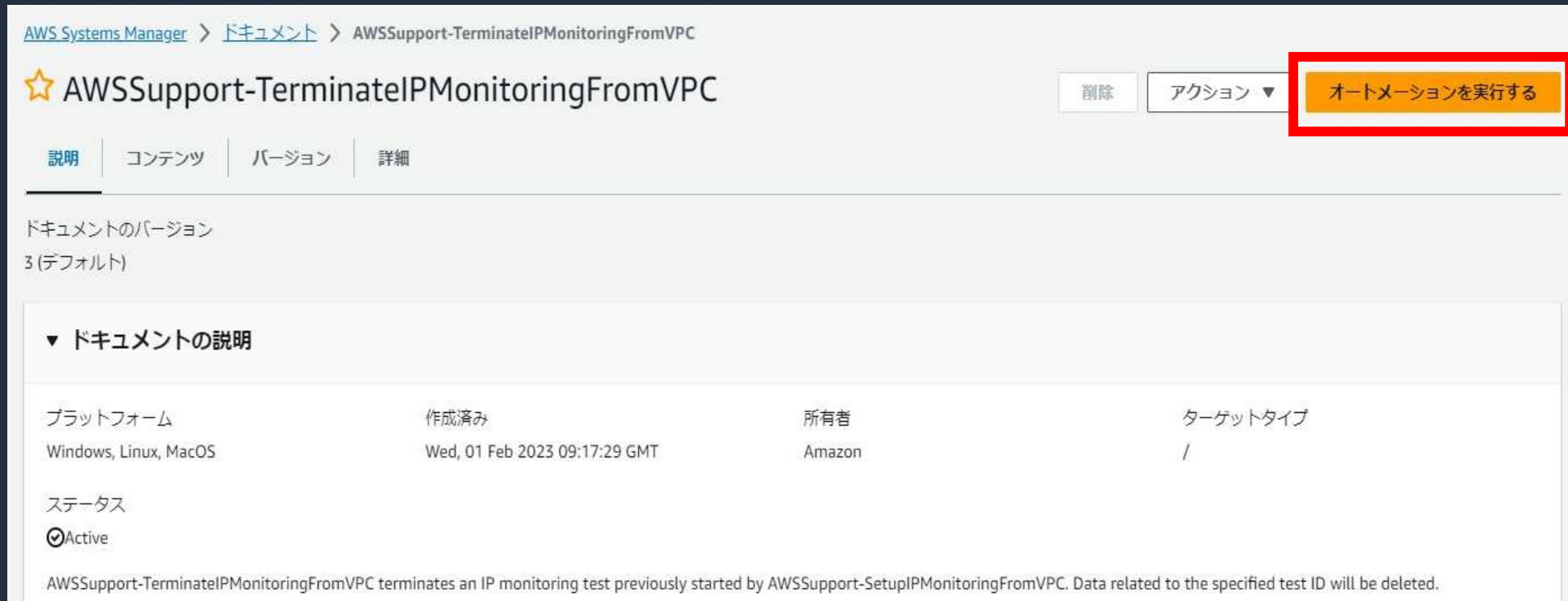
クリーンアップ

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

The screenshot shows the AWS Systems Manager console interface. At the top, there are tabs for document ownership: "Amazon が所有", "自己所有", "自分と共有", "Favorites - new", and "すべてのドキュメント". The left sidebar shows a "Categories" section with filters for document types: "Automation documents" (12 categories), "Command documents" (9 categories), "Policy documents" (No categories), "Session documents" (No categories), and "Conformance Pack Template documents" (No categories). The main content area is titled "ドキュメント" and includes a search bar with the text "キーワードで検索する、またはタグまたは属性でフィルタリングする". Below the search bar, the search results are displayed, showing a document titled "AWSSupport-TerminateIPMonitoringFromVPC" which is highlighted with a red box. The document details include "ドキュメントタイプ 所有者", "Automation Amazon", "プラットフォームタイプ", "Windows, Linux, MacOS", and "デフォルトバージョン", "3".

クリーンアップ

2. 「オートメーションを実行する」を選択



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

☆ AWSSupport-TerminateIPMonitoringFromVPC

削除 アクション ▼ **オートメーションを実行する**

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
3 (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, 01 Feb 2023 09:17:29 GMT	Amazon	/

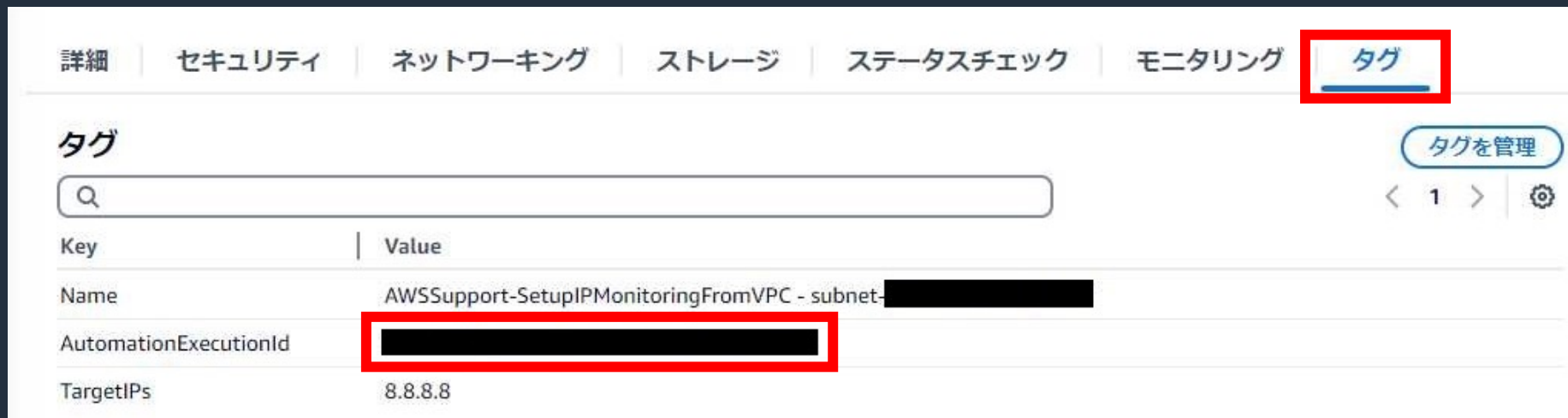
ステータス
☑ Active

AWSSupport-TerminateIPMonitoringFromVPC terminates an IP monitoring test previously started by AWSSupport-SetupIPMonitoringFromVPC. Data related to the specified test ID will be deleted.

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



The screenshot shows the AWS Management Console interface for a resource's tags. The 'タグ' (Tags) tab is selected and highlighted with a red box. Below the search bar, a table lists the tags. The 'AutomationExecutionId' tag value is highlighted with a red box.

Key	Value
Name	AWSSupport-SetupIPMonitoringFromVPC - subnet-██████████
AutomationExecutionId	██████████
TargetIPs	8.8.8.8

※ オプションはデフォルトのまま実行可

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

AWS Support-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 例 : eni-0123456789abcef01,vpc-c15180a4
LogDestinationType	ログ出力先リソースタイプ 有効な値: cloud-watch-log s3
LogDestinationARN	ログ出力先の既存リソース ARN ※ cloud-watch-log (任意) / s3 (必須)
LogGroupName	ログ出力先の新規ロググループ名 ※ cloud-watch-log (任意) / s3 (不要)

入力パラメータ

ResourceIds

(Required) Comma separated list with of the ID(s) of the subnet, network interface, or VPC for which you want to create a flow log (e.g: subnet-123a351e)

LogDestinationType

(Required) Specifies the destination type to which the flow log data is to be published. Flow log data can be published to CloudWatch Logs or Amazon S3. To publish flow log data to CloudWatch Logs, specify cloud-watch-logs. To publish flow log data to Amazon S3, specify s3.

LogDestinationARN

(Optional) Specifies the destination to which the flow log data is to be published. Flow log data can be published to a CloudWatch Logs log group or an Amazon S3 bucket. The value specified for this parameter depends on the value specified for LogDestinationType. If LogDestinationType is 'cloud-watch-logs', specify the ARN of the CloudWatch Logs log group. Otherwise specify the ARN of the Amazon S3 bucket. You can also specify a subfolder in the bucket: bucket_ARN/subfolder_name/. *Note*: `if nothing is specified, the automation will create a CloudWatch Log Group, stream and the IAM role to put data in it on behalf of VPC Flow Logs.`

LogGroupName

(Depends on LogDestinationType) The name of the CloudWatch Logs log group you want to publish flow log data to. This parameter is required only if the parameter *LogDestinationType* is set to cloud-watch-logs

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 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 ※ 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

TrafficType
(Required) The type of traffic to log. You can log traffic that the resource accepts or rejects, or all traffic.

ALL ▼

DeliverLogsPermissionArn
(Depends on LogDestinationType) The ARN for the IAM role that permits Amazon EC2 to publish flow logs to a CloudWatch Logs log group in your account. If you specify *LogDestinationType* as 's3', do not specify *DeliverLogsPermissionArn* or *LogGroupName*.

String

LogFormat
(Optional) The fields to include in the flow log record, in the order in which they should appear. For a list of available fields, see Flow Log Records. If you omit this parameter, the flow log is created using the default format. If you specify this parameter, you must specify at least one field.

`\${version} \${account-id} \${interface-id} \${srcaddr} \${dstaddr} \${srcport} \${dstport} \${pr

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 ▼

AWS Support-Configure Traffic Mirroring

AWS Support-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

AWS Support-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 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 有効な値: 1 - 32766

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

Target

(Required) The destination for the mirrored traffic. You must specify the ID of a network interface, a Network Load Balancer, or a Gateway Load Balancer endpoint. If you specify a Network Load Balancer, there must be UDP listeners on port 4789.

String

SourceENI

(Required) The elastic network interface (ENI) you want to configure traffic mirroring for.

String

SessionNumber

(Required) The number of the mirror session you want to use. It must be in range of 1 to 32766.

Integer

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=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBIqY>



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)



Thank you!