



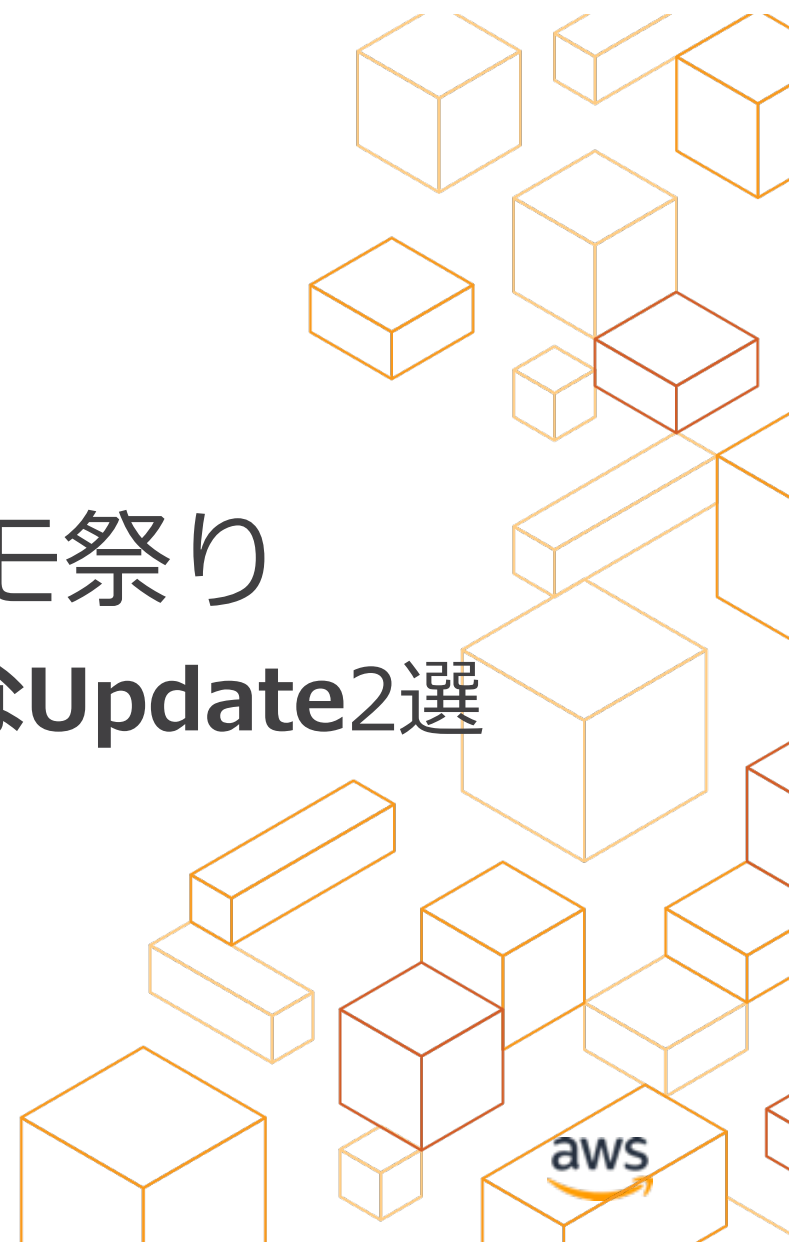
ちょっぴりDD#13

re: Invent 2021 Liveデモ祭り

ちょっぴり地味かも？でも**便利なUpdate2選**

アマゾンウェブサービスジャパン
ソリューションアーキテクト
吉田 裕貴(Yuki Yoshida)

© 2020, Amazon Web Services, Inc. or its Affiliates.



吉田 裕貴(Yuki Yoshida)

- お仕事: ソリューションアーキテクト
- 趣味:
バイク/キャンプ/サウナ/筋トレ
- 好きなAWSサービス:
AWS Single Sign-On
AWS Identity and Access Management (IAM)



猟師になりたいSA





New Amazon Inspector

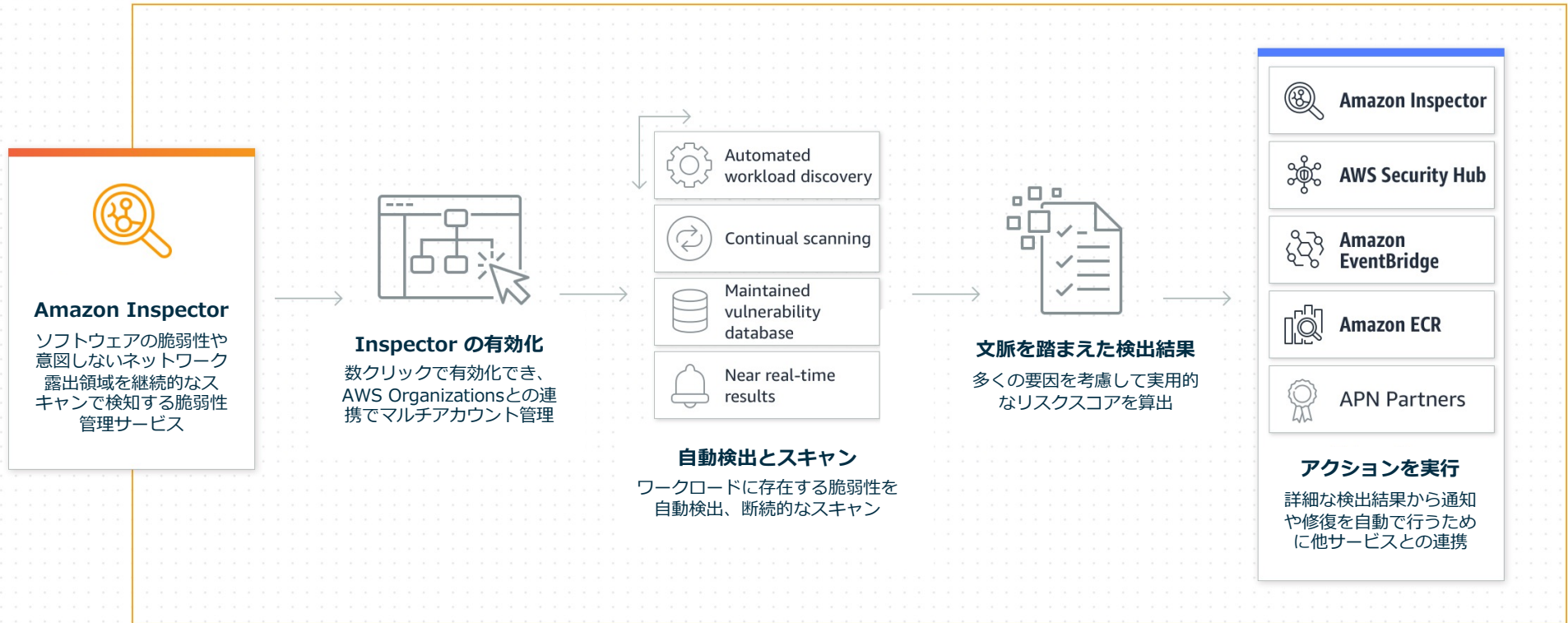


Amazon Inspector





Amazon Inspector の仕組み





Amazon Inspector のユースケース



**ニアリアルタイム
な脆弱性監視**



**パッチ管理の
迅速化**

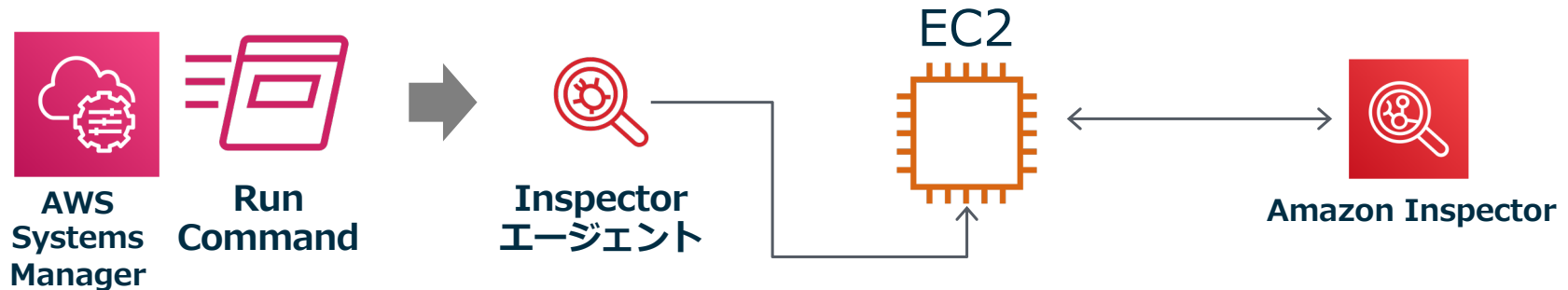


**コンプライアンス
要件に準拠**



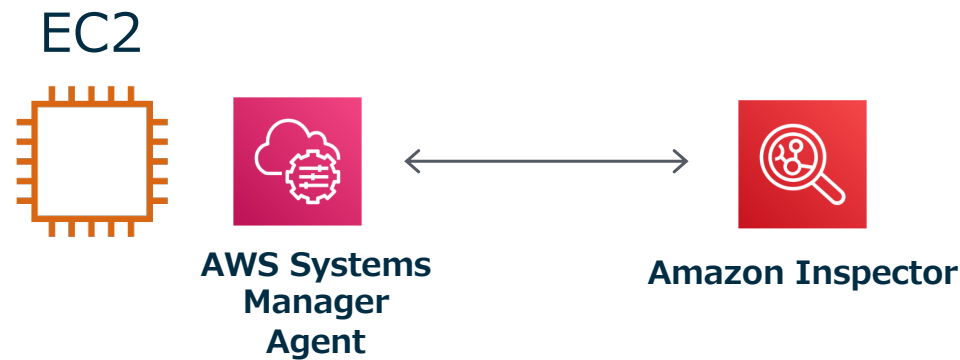
**脆弱性対応の
自動化**

Inspector Classicの導入



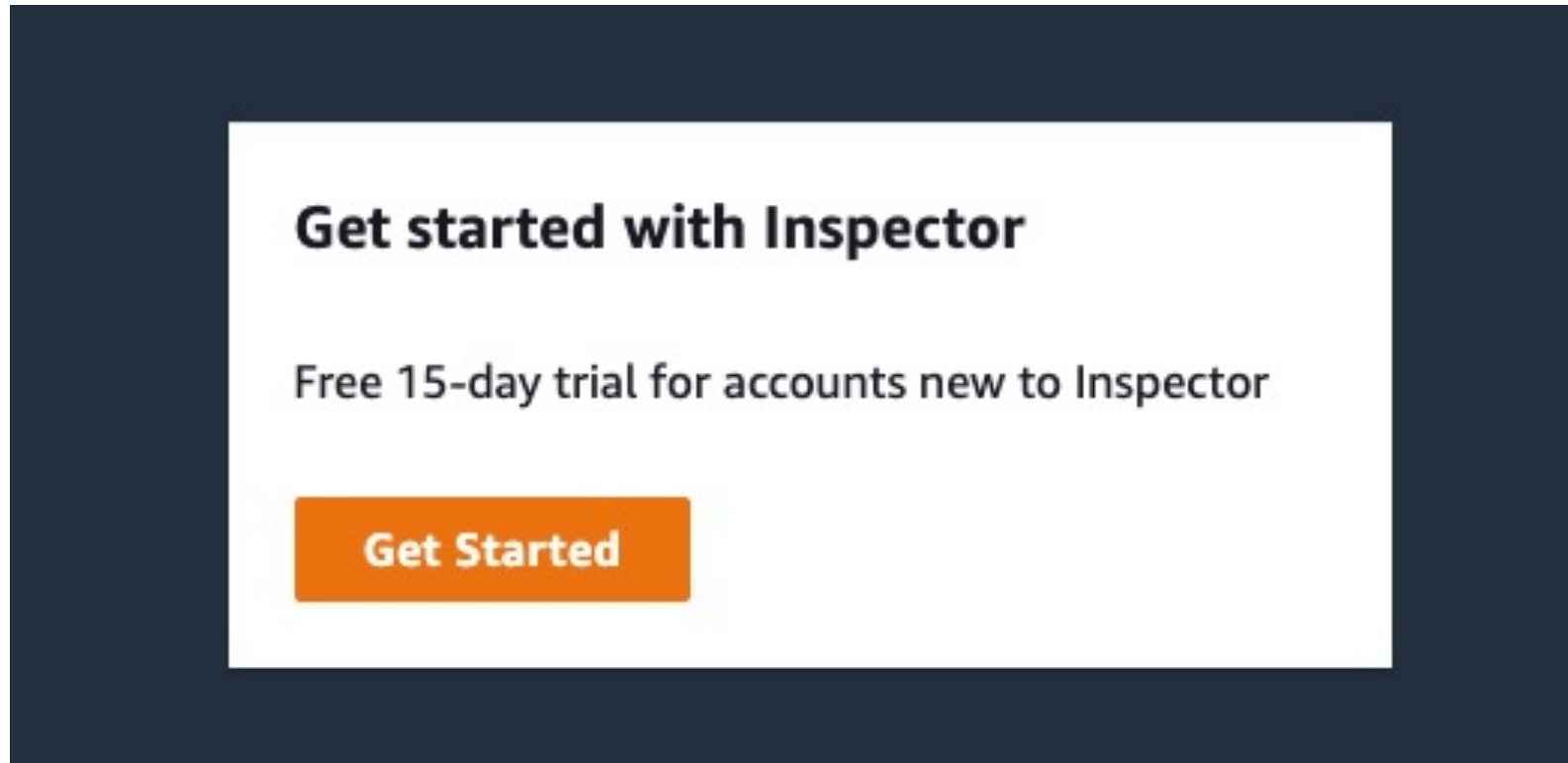
1. Inspectorのエージェントをインストール
2. Inspectorによる脆弱性検知を開始

Inspector v2の導入



**Amazon Linux AMIならSystems Manager Agentはインストール済み。
→個別の設定作業不要！**

①開始する



Get started with Inspector

Free 15-day trial for accounts new to Inspector

Get Started

②有効化する

Inspector ×

Enable Inspector

Switch to Inspector Classic [↗](#)

Enable Inspector 情報

Delegated administrator Delegate

Delegate permissions to manage Inspector for this organization

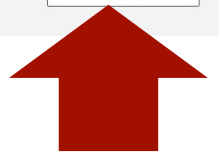
The delegated administrator is granted all of the permissions required to administer Inspector for your organization. When you choose a delegated administrator, Inspector is enabled for that account.

Delegated administrator account ID

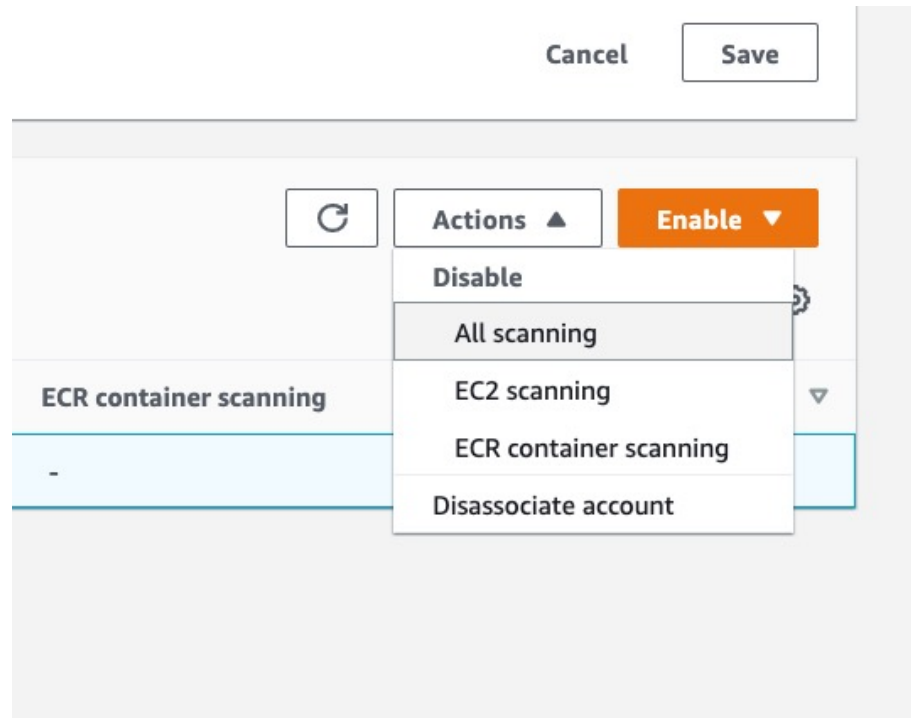
Service permissions View role permissions

When you enable Inspector, you grant Inspector permissions to discover, classify, and protect sensitive data in AWS on your behalf and to generate findings about potential security issues. This will enable Inspector for your account only.

Enable Inspector



③ Organizationsと連携する



メンバーアカウントに一括で設置可能。これは便利だ！

④新規アカウントも自動で有効化

Inspector > Settings > Account management

Account management 情報

Manage your accounts, and review the coverage of your instances and repositories.

Accounts | Instances | Repositories

▼ Auto-enable scanning for new member accounts

Automatically enable Inspector for all new member accounts

EC2 scanning
Scan all EC2 instances for vulnerabilities

ECR container scanning
Scan container images for vulnerabilities

Cancel Save

新しいメンバーアカウントが増えても自動で有効化してくれる
これは便利だ！！！！

ダッシュボード画面

Summary 情報

Viewing data from all accounts

適用範囲

Environment coverage

Your accounts, instances, and repositories that are enabled with Inspector.

Instances	Repositories
0%	100%
0 / 2 instances	1 / 1 repository

Criticalな件数

Critical findings

All active critical findings in your environment.

ECR container	EC2 instance	Network reachability
31 Critical	0 Critical	0 Critical
697 total findings	0 total findings	1 total finding

Risk based remediations

Vulnerabilities impacting the most instances and images.

Package name	Critical	All
libwebp	10	11
libwebp-dev	9	10
handlebars	4	12
node-sass	2	34
libexif-dev	2	8

[View all vulnerabilities](#)

ECR repositories with most critical findings

Elastic container registry (ECR) repositories with the most critical findings.

Repository name	AWS account	Critical	All
inspector-test	[REDACTED]	31	697

Inspectorが分析する範囲

Inspector で脆弱性を分析できるのは、ホスト上のどのようなソフトウェアパッケージですか？

Amazon Inspector は、エージェントがインストールされたオペレーティングシステムで、パッケージマネージャーやソフトウェアのインストールシステムに対してクエリを実行して、アプリケーションを検索します。つまり、パッケージマネージャーを使ってインストールされたソフトウェアは脆弱性を評価されます。このような方法でインストールされていないソフトウェアのバージョンやパッチレベルは、Inspector で認識されません。例えば、apt、yum、Microsoft Installer 経由でインストールされたソフトウェアは、Inspector で評価されます。make config や make install を使ってインストールされたソフトウェア、あるいは Puppet や Ansible といったオートメーションソフトウェアを使用してシステムに直接コピーされたバイナリファイルは、Inspector で評価されません。

<https://aws.amazon.com/jp/inspector/faqs/>

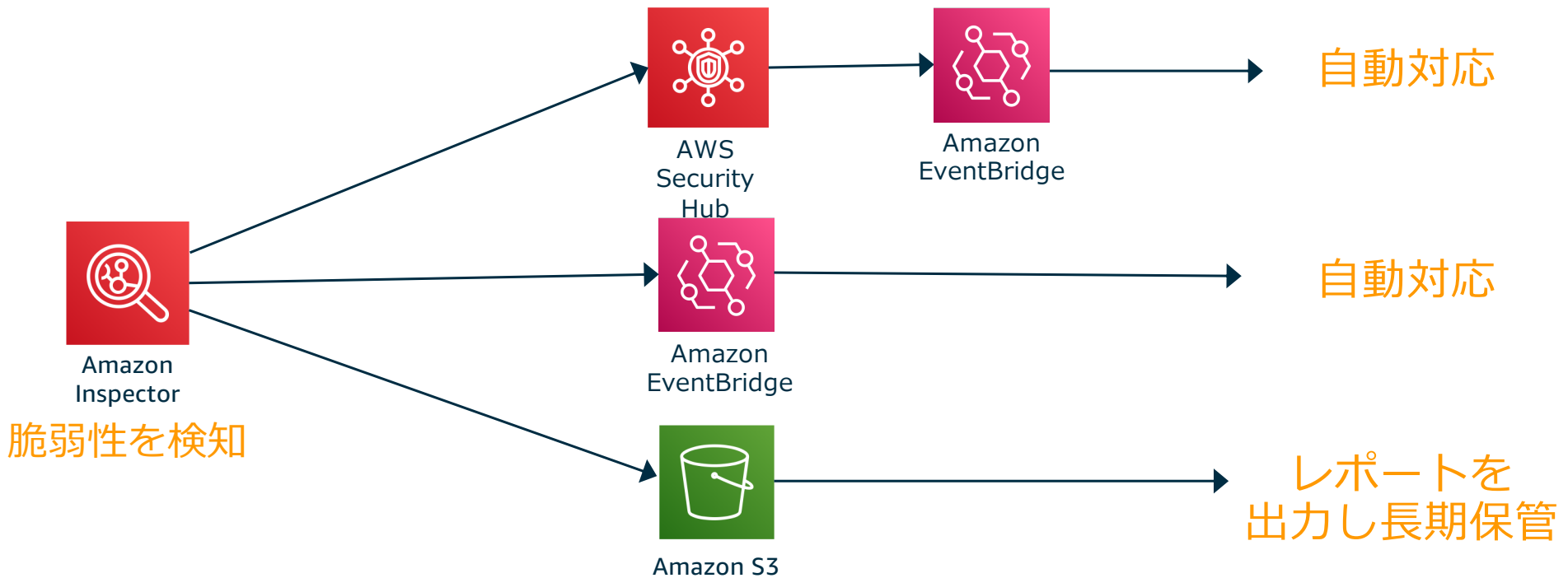
世の中銀の弾丸は無いので検知したい範囲によっては別のツールも併用する
でも、**何もしなくてもニアリアルタイムで全台スキャンできるのは良くないですか？**

v2もClassic同様検知までなのでパッチ適用はSystems Managerを利用します



対策措置のワークフロー自動化(5/5)

Amazon EventBridgeやAWS Security Hubとの連携による自動化で脆弱性の平均解決時間(MTTR)を短縮





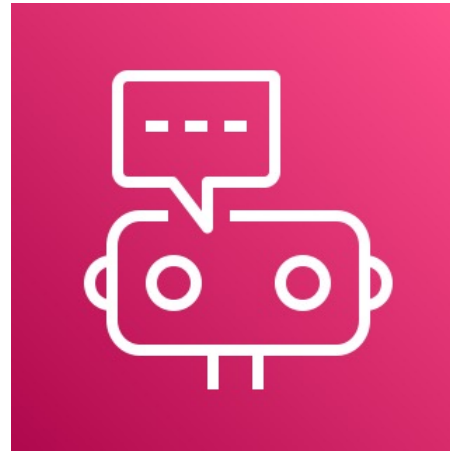
Amazon Inspector対応リージョン

19のリージョンでご利用可能

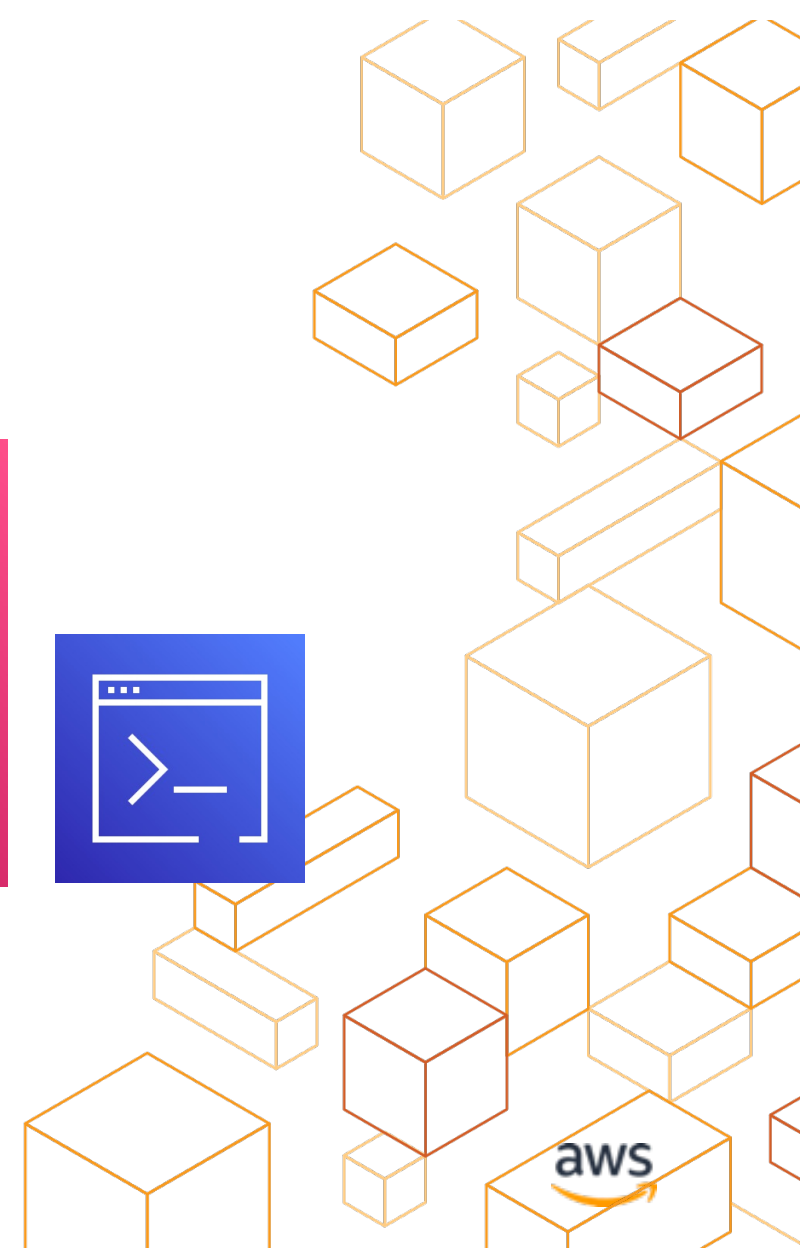
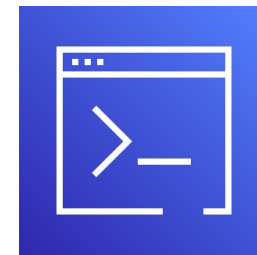
東京リージョンでも、使えます！！！！



AWS Chatbot CLI



AWS Chatbot



SlackでAWS CLIの実行が可能に！

AWS Chatbot が Slack での AWS リソースの管理をサポート (プレビュー)

投稿日: Nov 29, 2021

本日、AWS Chatbot を使用してAWS リソースを管理し、Slack チャンネルから AWS CLI コマンドを実行して AWS ワークロード内の問題を修正できる新機能の公開プレビューを発表いたします。以前は、AWS Chatbot を使用して AWS リソースをモニタリングし、診断情報を取得することしかできませんでした。

この機能を使用すると、お客様は、Slack チャンネルから直接 AWS リソースを管理することができます。お客様は、安全に AWS CLI コマンドを実行して EC2 インスタンスをスケーリングし、AWS Systems Manager ランプックを実行し、AWS Lambda の同時実行制限を変更できます。これで、お客様は、コンテキストを Slack と他の AWS 管理ツールの間で切り替えることなく、Slack チャンネルから AWS ワークロードをモニタリング、運用、トラブルシューティングできるようになりました。また、アカウントレベル設定を変更し、事前定義されたアクセス許可テンプレートを使用し、ガードレールポリシーを使用することで、セキュリティおよびコンプライアンスのニーズに合わせてチャンネルアクセス許可を設定することができます。

AWS Chatbot は、すべての商用 AWS リージョンでご利用になれます。AWS Chatbot の可用性の詳細については、[リージョン別の製品とサービスに関する表](#)をご参照ください。[生産ページ](#)にアクセスして、AWS Chatbot で AWS CLI コマンドを使用する AWS リソース管理の詳細をご確認ください。

<https://aws.amazon.com/jp/about-aws/whats-new/2021/11/aws-chatbot-management-resources-slack/>

寂しい絵ですが・・・



AWS Lambda挟んだり色々しなくて良いんですよ！？

設定も簡単

Tutorial: Using AWS Chatbot to run an AWS Lambda function remotely

[PDF](#) | [RSS](#)

In this tutorial you use AWS Chatbot to run a Lambda function remotely and check the status of the Lambda function using Amazon CloudWatch. A Lambda function is a self contained block of organized reusable code that you write. Lambda functions are useful because they are run without provisioning or managing servers. Additionally, they are only invoked when needed based on your specifications. There are steps at the end of this tutorial to delete the resources you created.

Topics

- [Prerequisites](#)
- [Step 1: Create a Lambda function](#)
- [Step 2: Create an SNS topic](#)
- [Step 3: Configure a CloudWatch alarm](#)
- [Step 4: Configure a Slack client for AWS Chatbot](#)
- [Step 5: Invoke a Lambda function from Slack](#)
- [Step 6: Test the CloudWatch alarm](#)
- [Step 7: Clean up resources](#)

Prerequisites

This tutorial assumes that you have some familiarity with the Lambda, AWS Chatbot, and CloudWatch consoles.

For more information, see the following topics:

- [Getting started with AWS Lambda](#) in the *AWS Lambda Developer Guide*.
- [Setting up AWS Chatbot](#) in the *AWS Chatbot Administrator Guide*.
- [Getting Set Up with CloudWatch](#) in the *Amazon CloudWatch User Guide*.

The AWS Region that you select while setting up these consoles should be the same Region you specify in your Slack channel when your first AWS Command Line Interface (AWS CLI) command in [Step 5: Invoke a Lambda function from Slack](#).

https://docs.aws.amazon.com/ja_jp/chatbot/latest/adminguide/chatbot-run-lambda-function-remotely-tutorial.html

かんたん設定

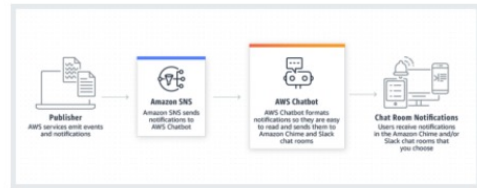
マネジメントとガバナンス

AWS Chatbot AWS の ChatOps

AWS Chatbot を使用しているチームでは、Amazon Chime と Slack チャットルームでの運用イベントをより迅速に識別し、共同でのトラブルシューティングが行えます。

仕組み

通知



コマンド



チャットクライアントを設定

チャットクライアント

チャットクライアントを選択

クライアントを設定

料金 (米国)

AWS Chatbot には追加料金はかかりません。AWS Chatbot を使用せずにサービスを利用した場合と同じように、基盤となるサービス (Amazon CloudWatch、Amazon Simple Notification Service、AWS GuardDuty など) の中で使用したものに対してのみ料金が発生します。

開始方法

AWS Chatbot とは何ですか?

AWS Chatbot の開始方法

AWS Chatbot のセットアップ

他の AWS サービスで AWS Chatbot を使用する

Slack からの AWS CLI コマンドの実行

チャットクライアントを設定

チャットクライアント

チャットクライアント...

Amazon Chime

Slack



AWS Chatbot is requesting permissions to access the AWS Slack workspace.

What will AWS Chatbot be able to do with my Slack workspace?

Content and info about channels & conversations

Content and info about your workspace

What will AWS Chatbot be able to do with my Slack workspace?

Perform actions in channels & conversations

Cancel

AWS Chatbot > 設定済みクライアント > Slack ワークスペース: AWS > Slack チャネルを設定

Slack チャネルを設定

設定の詳細

設定名
後で簡単に識別できるように、設定に名前を付けます。設定を作成した後は、この名前を変更できません。
my-awesome-configuration
名前は最大 128 文字です。使用できる文字は、a-z、A-Z、0-9、および - です。

ログ記録 - オプション

AWS Chatbot は、ユーザーが開始したコマンドの監査イベントを Amazon CloudWatch Logs に自動的にログ記録しますが、設定に関する追加のログ記録を有効にすることもできます。Amazon CloudWatch Logs へのログ記録には料金がかかります。 [詳細はこちら](#)

Amazon CloudWatch Logs にログを発行する

Slack チャネル

チャネル ID
Slack でチャネル ID を検索するには、チャネルリストでチャネルを右クリックし、リンクをコピーします。チャネル ID は URL の末尾にある文字列です。
チャネル ID または URL を入力
チャネル ID は、英数字の文字列 (C1111122233) またはチャネル URL 全体 (https://workspace.slack.com/messages/C1111122233) にすることができます。

アクセス許可

AWS Chatbot では、アクション (CLI コマンドの実行と、インタラクティブなメッセージへの応答) を実行するために IAM ロールが必要です。この IAM ロールは、ロール設定に応じてチャネルの IAM ロール、ユーザーロール、またはその両方とすることができます。どちらのロールタイプも、チャネルメンバーが持つアクセス許可を要求します。チャネルメンバーで実行可能なアクションは、チャネルガードレールにより制御されます。

ロール設定

ロール設定では、チャネルメンバーに付与するアクセス許可が決定されます。これと同じアクセス許可を必要とするチャネルメンバーがいる場合は、チャネル IAM ロールの使用が推奨されます。チャネルメンバーが異なるアクセス許可を必要とする場合は、ユーザーロールの使用が適切です。各チャネルメンバーが実行可能な処理は、ロールのアクセス許可とガードレールにより決定されます。

チャネル IAM ロール

すべてのチャネルメンバーが同じアクセス許可を共有しますが、それぞれのチャネルメンバーは、引き継ぎ独自の IAM ユーザーロールを使用できます。

ユーザーロール

チャネルメンバーは、アクションを実行するために IAM ユーザーロールを選択する必要があります。

チャネル IAM ロール

このロールは、チャネルメンバーが独自のロールを選択しない場合に使用されます。チャネルメンバーが実行する AWS アクションは、そのメンバーが使用するユーザーロールに依存なく、チャネルのガードレールで指定されたポリシーにより制御されます。

テンプレートを使用して IAM ロールを作成する

ロール名

AWSChatbot-role
名前は最大 64 文字です。使用できる文字は、a-z、A-Z、0-9、および +、.、@、- です。

ポリシーテンプレート

1 つ以上のポリシーテンプレートを選択すると、AWS Chatbot によってロールが自動的に作成されます。各ポリシーテンプレートがロールに追加するアクセス許可の詳細については、AWS Chatbot ユーザーガイドをご確認ください。 [詳細はこちら](#)

テンプレートを選択

通知のアクセス許可

AWS Chatbot が Amazon CloudWatch からメトリクスグラフを取得できるようにします。

Channel ガードレール

ポリシー名
チャネルのメンバーが実行可能なアクションは、チャネルのガードレールにより詳細に制御されます。これらのガードレールは、実行時にチャネル IAM ロールとユーザーロールの両方に適用されます。実行が許可されたチャネルメンバーは、ロールのアクセス許可とガードレールにより共通して定義されます。 [IAM コンソールでポリシーを表示する](#)

オプションを選択



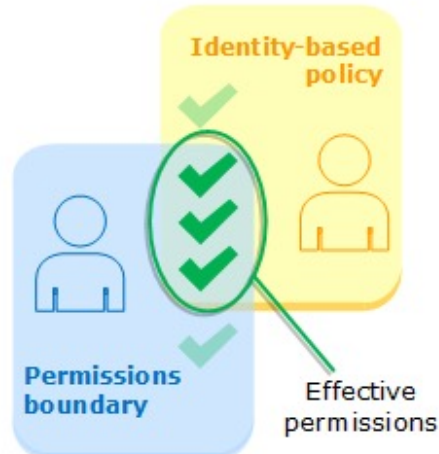
Channelガードレール

Channel ガードレール

ポリシー名

チャンネルのメンバーが実行可能なアクションは、チャンネルのガードレールにより詳細に制御されます。これらのガードレールは、実行時にチャンネル IAM ロールとユーザーロールの両方に適用されます。実行が許可されたチャンネルメンバーは、ロールのアクセス許可とガードレールにより共通して定義されます。[IAM コンソールでポリシーを表示する](#) .

オプションを選択



Permissions boundariesと同じ考え方ですね。

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html

今日紹介したChat botの機能はまだ
プレビューですのをご注意ください。

