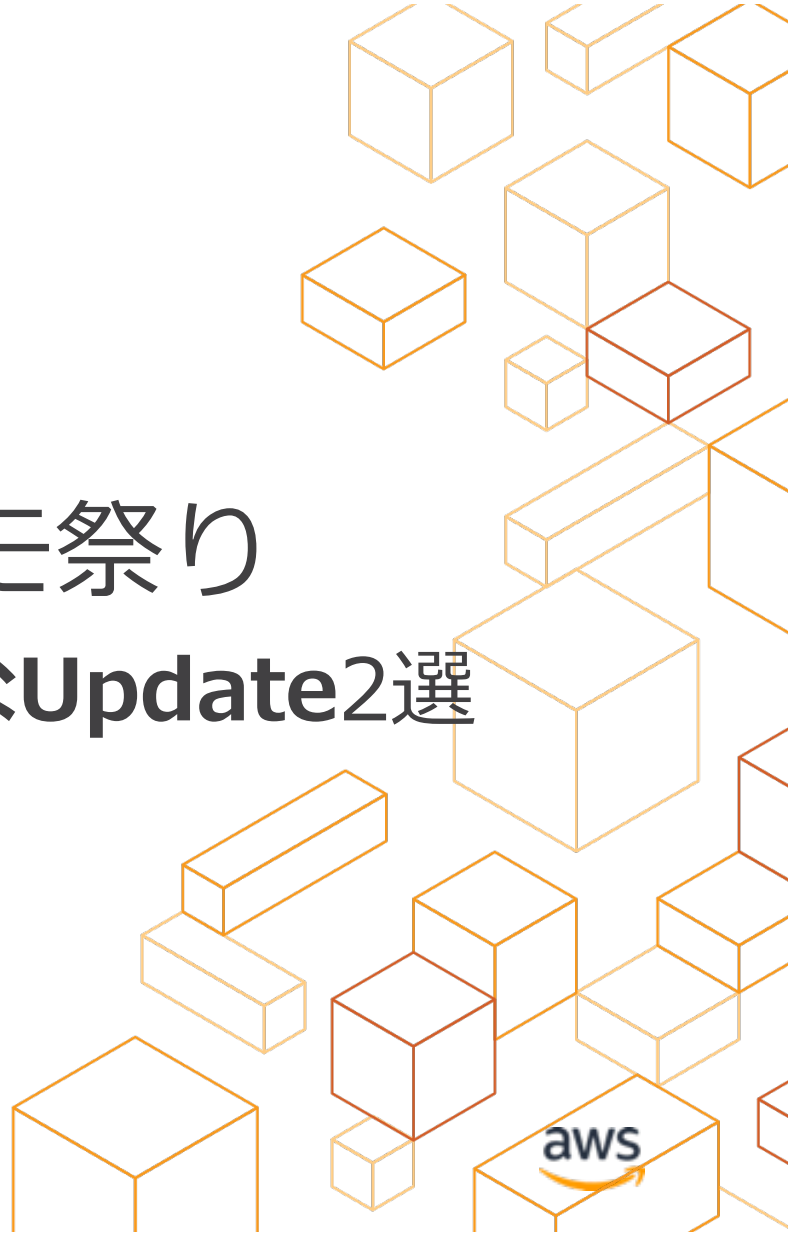


ちょっぴりDD#13

re: Invent 2021 Liveデモ祭り

ちょっぴり地味かも？でも**便利なUpdate**2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)

吉田 裕貴(Yuki Yoshida)

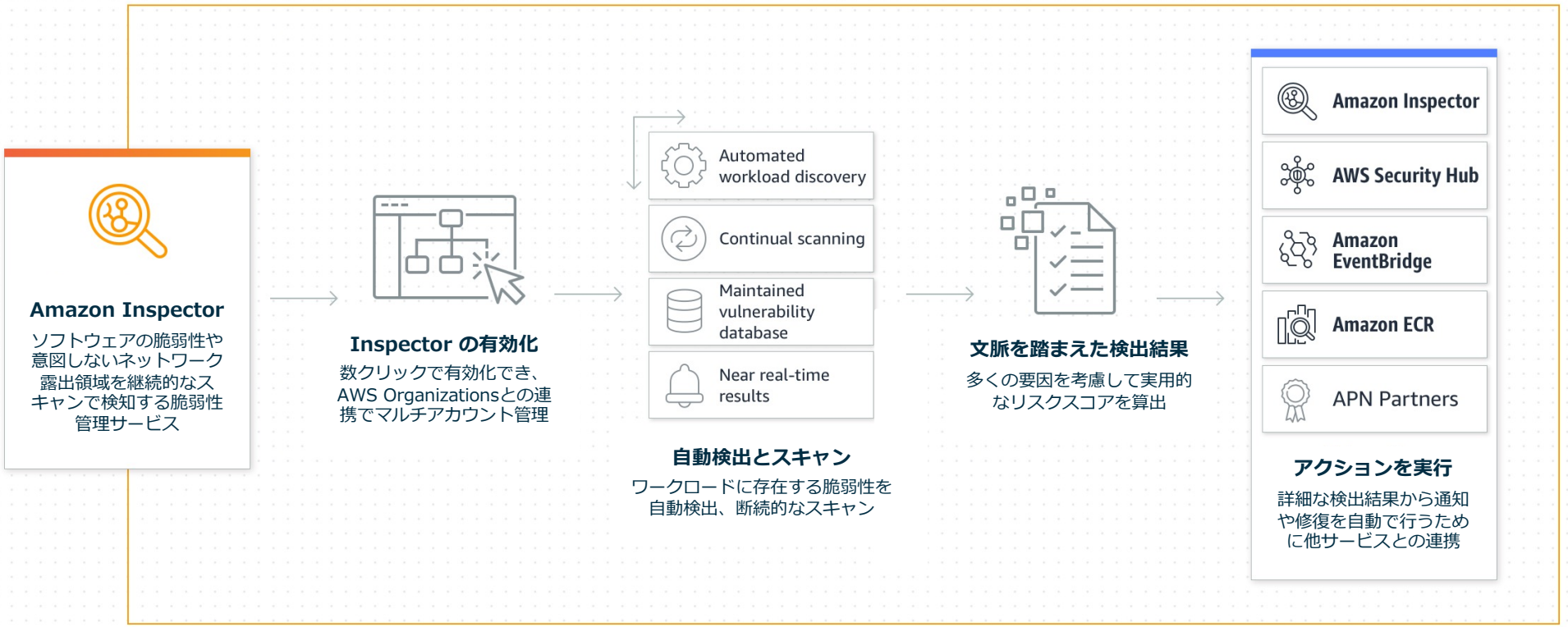
- お仕事: ソリューションアーキテクト
- 趣味:
  バイク/キャンプ/サウナ/筋トレ
- 好きなAWSサービス:
  AWS Single Sign-On
  AWS Identity and Access Management (IAM)

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

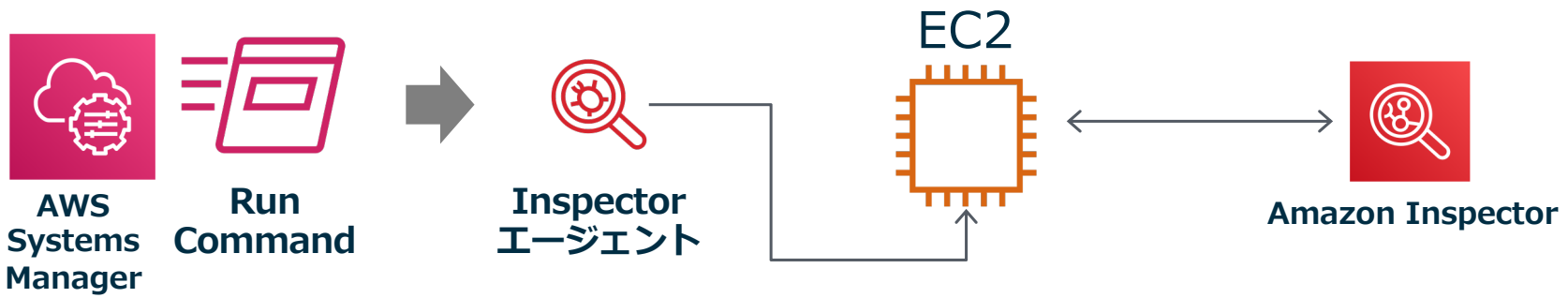
ニアリアルタイムな脆弱性監視

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

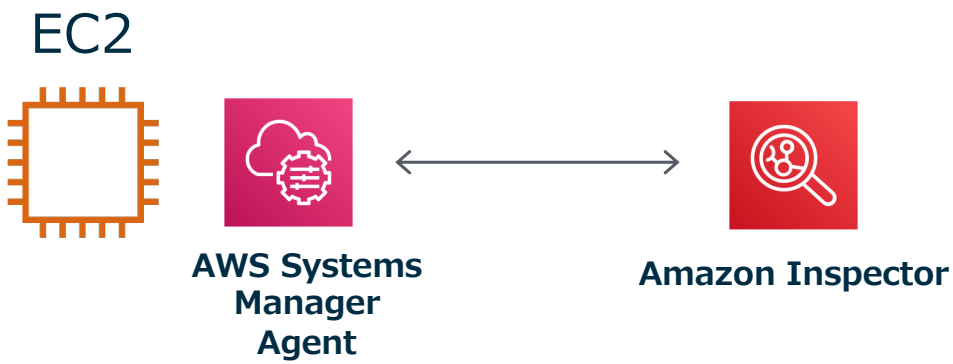
Inspector Classicの導入



1.Inspectorのエージェントをインストール

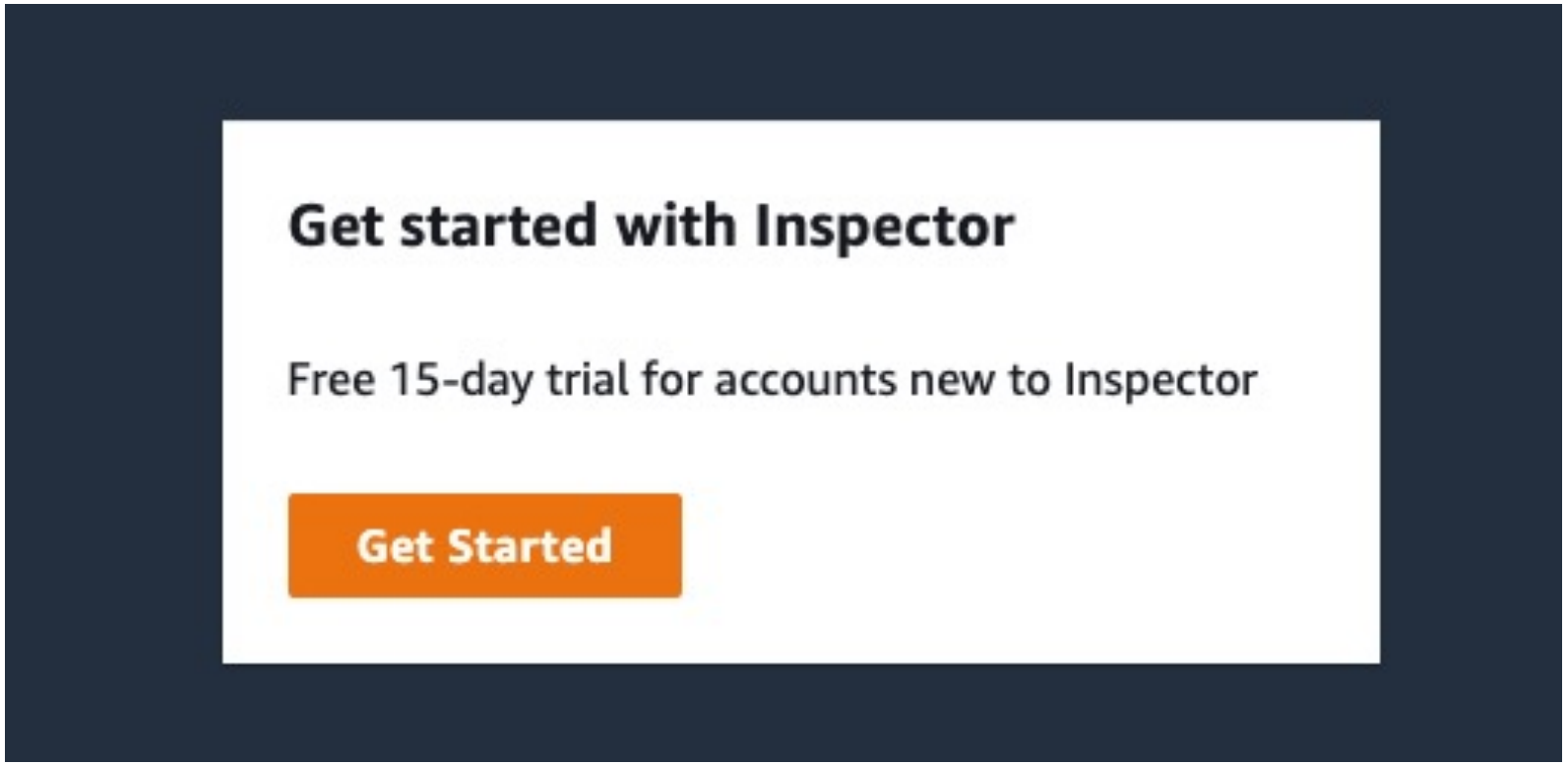
2.Inspectorによる脆弱性検知を開始

Inspector v2の導入

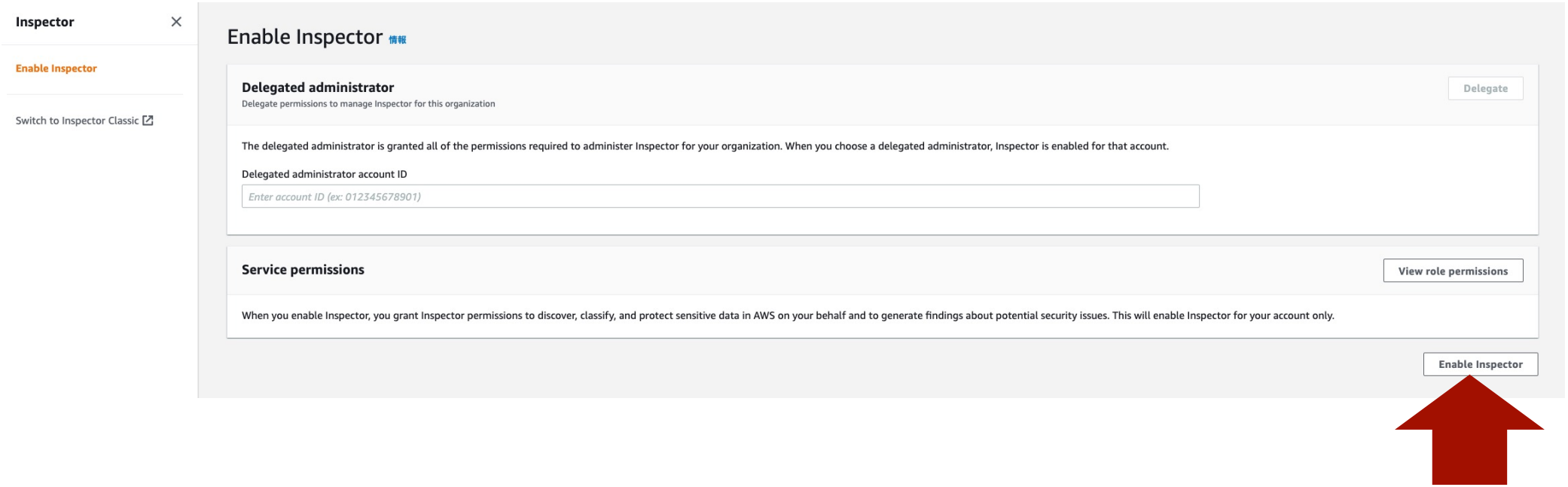


Amazon Linux AMIならSystems Manager Agentはインストール済み。
→個別の設定作業不要！

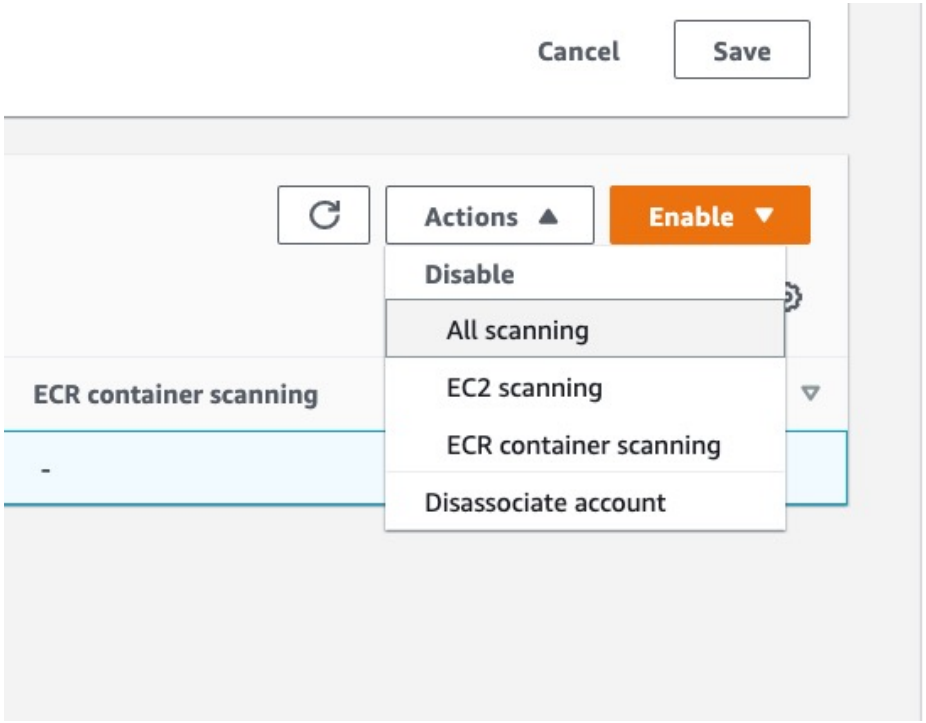
①開始する



②有効化する

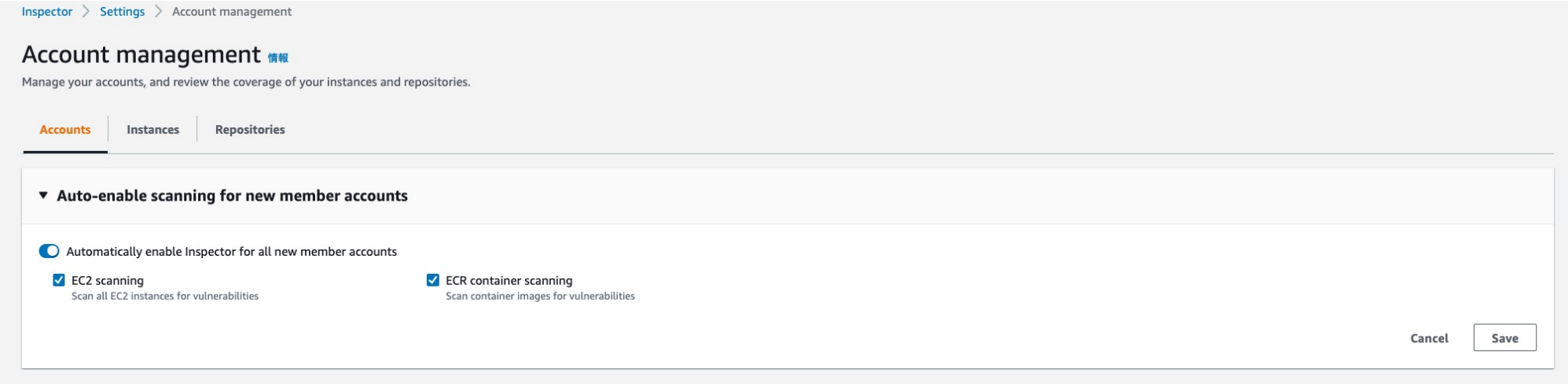


③Organizationsと連携する



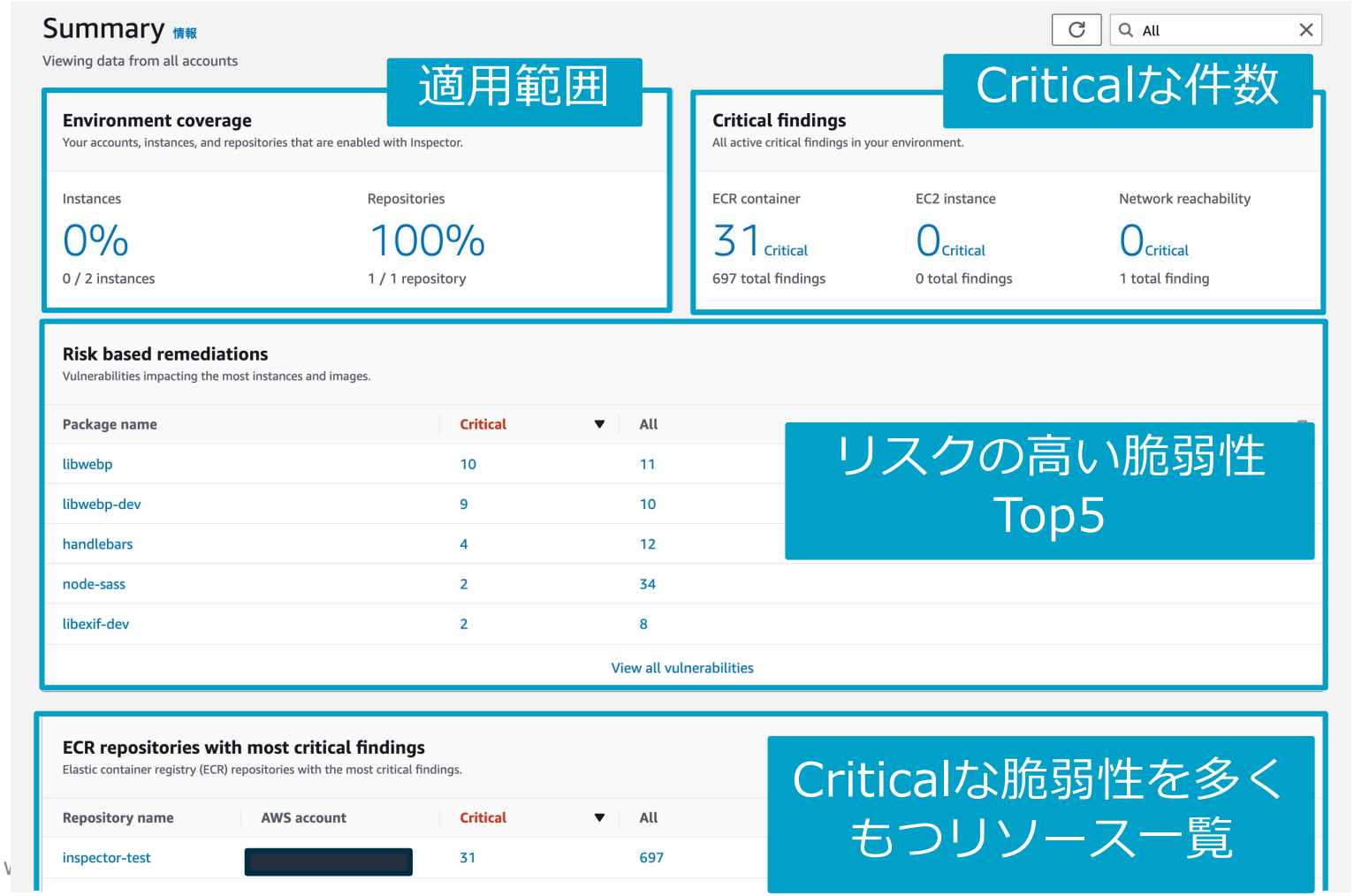
メンバーアカウントに一括で設置可能。これは便利だ❗

④新規アカウントも自動で有効化



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
コレは便利だ！！！

ダッシュボード画面



Inspecotr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。

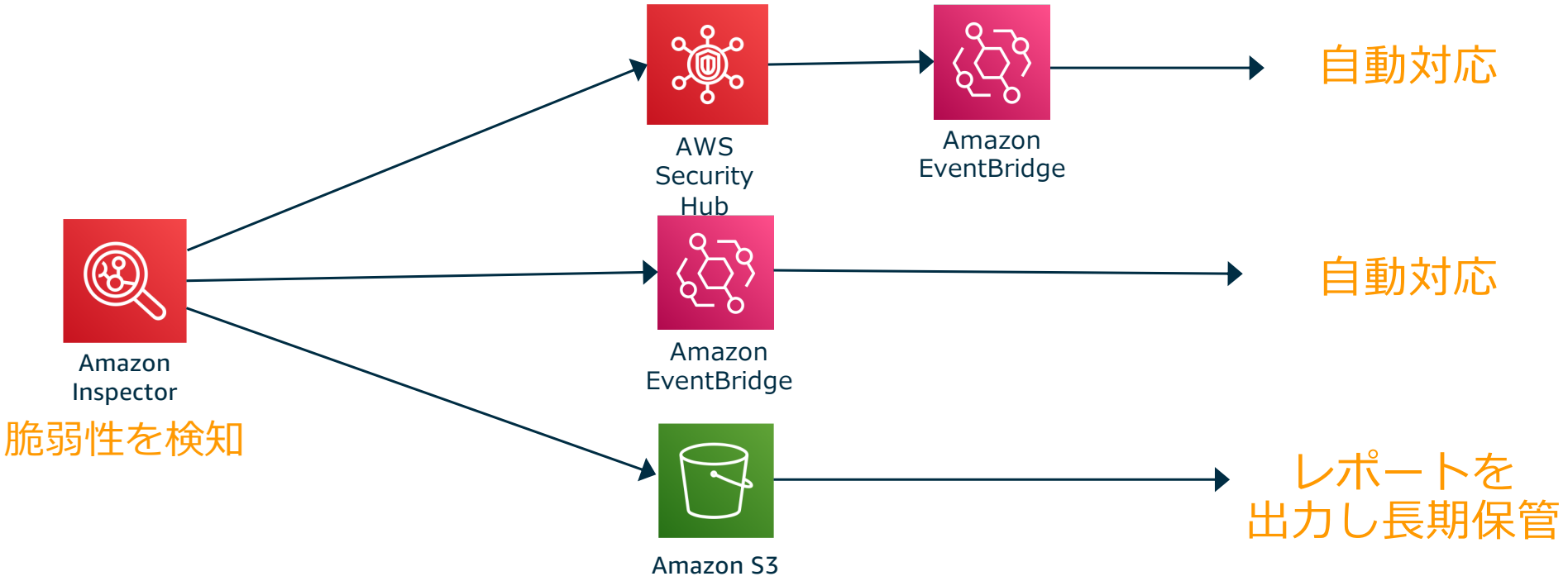
https://aws.amazon.com/jp/inspector/faqs/

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

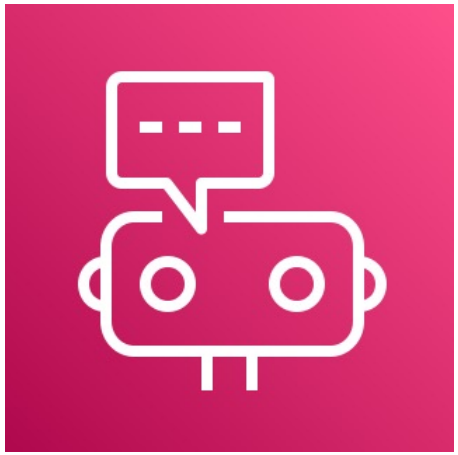


Amazon Inspector対応リージョン

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で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 ランブックを実行し、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るようにチャ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 resuable 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

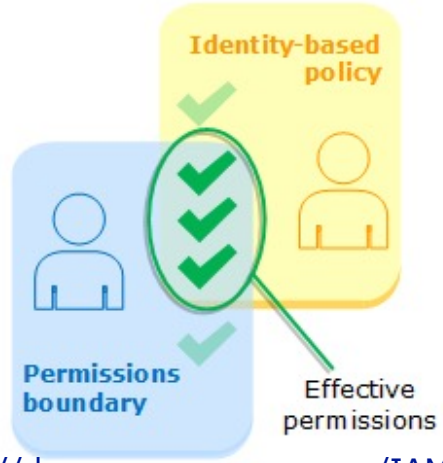
Channelガードレール

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



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
プレビューですのでご注意ください。