



# 直近の Amazon EKS アップデート

## 夏の AWS Kubernetes 祭り！

杉田 想土

アマゾン ウェブ サービス ジャパン合同会社  
プロフェッショナルサービス本部

# 自己紹介

杉田 想土 (Soto Sugita)

## 所属

- プロフェッショナルサービス



AWS Professional Services



## 好きな AWS サービス

- Amazon Elastic Kubernetes Service (Amazon EKS)



Amazon EKS

## バックグラウンド

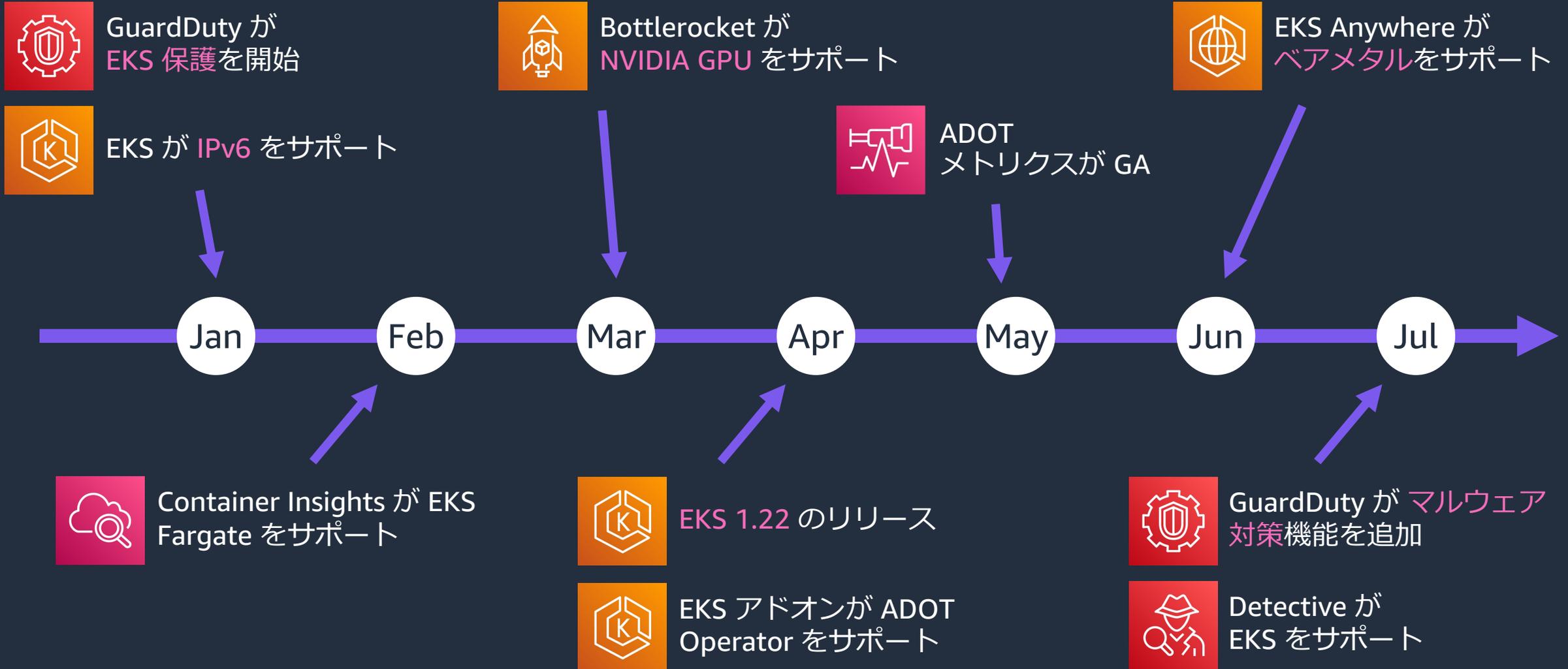
- 外資系 Sler の SE



# アジェンダ

- 2022 年上半期の主要アップデート
- カテゴリ別アップデート
  - コア機能
  - ネットワーク
  - コンピュート
  - オブザーバビリティ
  - セキュリティ
  - その他

# 2022 年上半期の主要アップデート



# コア機能

# EKS 関連アップデート (コア機能)

月/日	Update Title	関連 URL
03/31	EBS CSI ドライバーの EKS アドオンサポートが一般提供になりました。	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
 04/04	Amazon EKS、Amazon EKS Distro、および Amazon EKS Anywhere で Kubernetes バージョン 1.22 のサポートを開始	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
 05/03	クラスター管理を簡素化するために Amazon EKS コンソールがすべての標準 Kubernetes リソースのサポートを開始しました	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
06/24	Amazon Elastic Kubernetes Service 向けの AWS Fargate がアマゾン ウェブ サービス中国 (北京と寧夏) リージョンで利用可能に	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li></ul>
06/27	Amazon EKS がコントロールプレーンのスケーリングとアップデートの速度を最大 4 倍向上	<ul style="list-style-type: none"><li>• <a href="#">blog</a></li></ul>
 06/30	Amazon EKS Anywhere のベアメタルサポートを開始	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li><li>• <a href="#">blog</a></li></ul>

# Amazon EKS が Kubernetes 1.22 をサポート

- Kubernetes 1.22 をサポート
  - 1.22 では多くの非推奨 API が削除
    - Ingress の extensions/v1beta1 など
  - Kubernetes のリリース頻度が年 3 回に変更
  - EKS は少なくとも 4 つの Kubernetes バージョンをサポート
  - 1.22 のアップデート詳細については、アップストリームのリリースノートや、EKS のリリースブログを参照
    - <https://aws.amazon.com/jp/blogs/news/amazon-eks-now-supports-kubernetes-1-22/>
- Dockershim のサポートは EKS 1.23 から削除
  - <https://docs.aws.amazon.com/eks/latest/userguide/dockershim-deprecation.html>
  - EKS 最適化 AMI ではユーザーデータでコンテナランタイムを containerd に切り替えてテストすることが可能



Kubernetes 1.22: Reaching New Peaks

## EKS リリースカレンダー

Kubernetes version	Upstream release	Amazon EKS release	Amazon EKS EOS
1.18	2020/03/23	2020/10/13	2022/03/31
1.19	2020/08/26	2021/02/16	2022/08/01
1.20	2020/12/08	2021/05/18	2022/11/01
1.21	2021/04/08	2021/07/19	2023/02
1.22	2021/08/04	2022/04/04	2023/05
1.23	2021/12/07	2022/08	2023/10

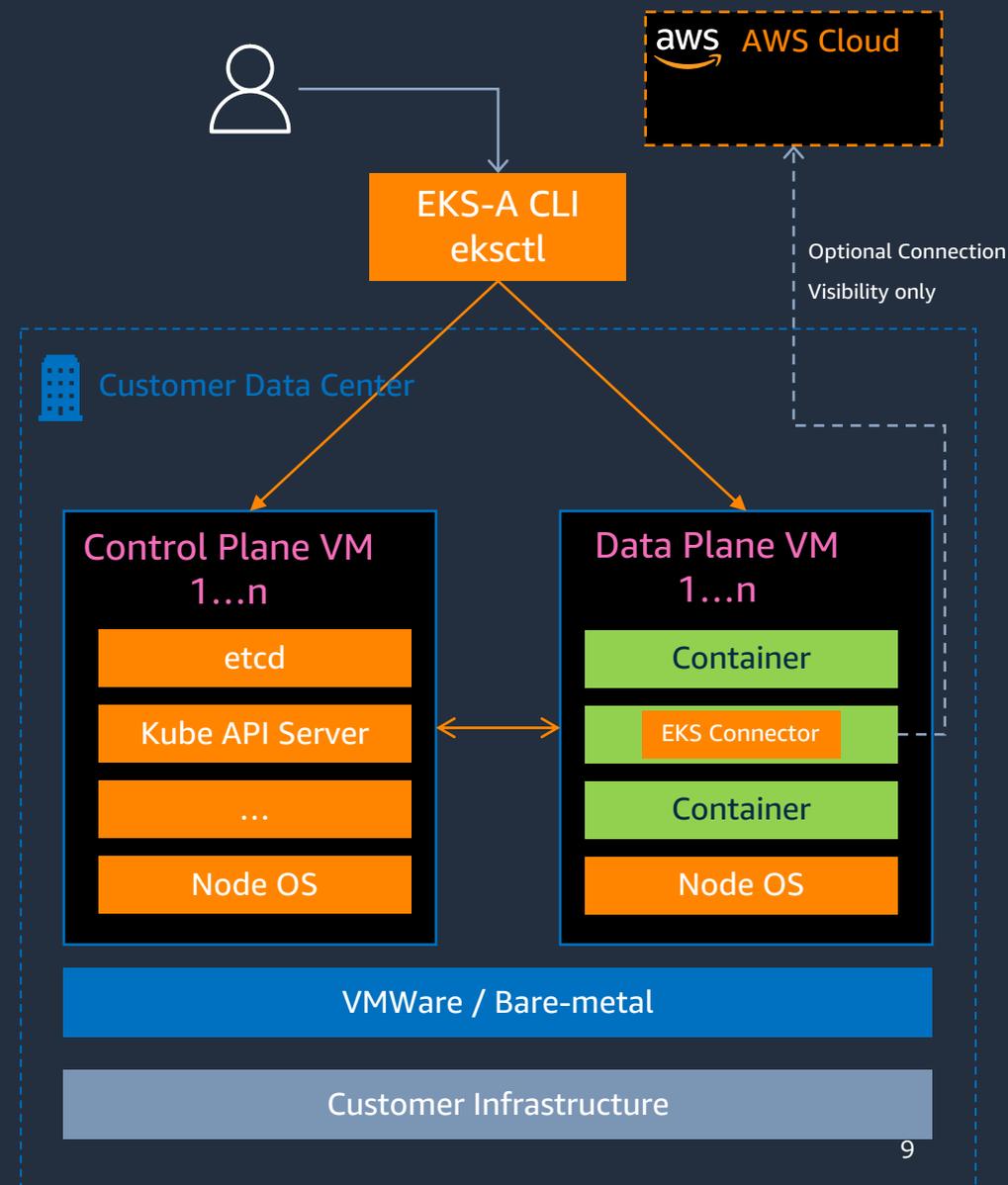
# EKS コンソールでのリソース表示の拡充

- EKS コンソールで **Kubernetes** の標準的なリソースを表示可能に
  - ワークロード
    - Pod, Deployment, DaemonSet など
  - クラスタ
    - Node, Namespace など
  - ネットワーク
    - Service, Ingress, IngressClass など
  - 設定とストレージ
    - ConfigMap, Secret, PVC, PV など
  - 認証/認可
    - ServiceAccount, ClusterRole など

The screenshot displays the AWS EKS console interface. At the top, there are navigation tabs: Overview, Resources (selected), Compute, Networking, Add-ons, and Authentication. The left sidebar, titled 'Resource types', lists various Kubernetes resource categories. Under the 'Config and storage' section, 'ConfigMaps' is highlighted in orange. Other listed resources include Secrets, PersistentVolumeClaims, PersistentVolumes, StorageClasses, VolumeAttachment, CSIDrivers, CSINodes, CSISStorageCapacities, Authentication (ServiceAccounts), and Authorization (ClusterRoles, ClusterRoleBindings, Roles). The main content area is titled 'Config and storage: ConfigMaps (43)'. It includes a description: 'An API object used to store non-confidential data in volume.' and a 'Learn more' link. Below this is a search bar with 'All Namespaces' selected and a 'Filter ConfigM' input field. A table lists several ConfigMaps, each with a radio button and a name: argocd-cm, argocd-cmd-params-cm, argocd-gpg-keys-cm, argocd-notifications-cm, argocd-rbac-cm, argocd-ssh-known-hosts-cm, argocd-tls-certs-cm, and aws-auth.

# Amazon EKS Anywhere がベアメタルをサポート

- Amazon EKS Anywhere は **オンプレミス** 上に Kubernetes クラスターを作成、運用が可能なツールセット
  - Amazon EKS で利用されているのと同じオープンソースの Kubernetes ディストリビューションである Amazon EKS Distro を利用
  - eksctl CLI のプラグインである **eksctl-anywhere** プラグインとして提供される
- VMware vSphere に加えて、このアップデートで **ベアメタルサーバー** をサポート
- Amazon EKS Anywhere はオープンソース
  - 本番環境での利用には **Amazon EKS Anywhere Subscription** を契約することで24 時間 365 日のサポートを受けることができる
  - 前提としてエンタープライズサポートが必要



# ネットワーク

# EKS 関連アップデート (ネットワーク)

月/日	Update Title	関連 URL
👉 01/06	Amazon EKS が Internet Protocol version 6 (IPv6) をサポート	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li><li>• <a href="#">blog</a></li></ul>
05/18	AWS App Mesh が Internet Protocol Version 6 (IPv6) をサポート	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li></ul>
👉 06/21	Amazon ECR が AWS アジアパシフィック (大阪) リージョンで AWS PrivateLink のサポートを開始	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li></ul>

# Amazon EKS が IPv6 をサポート

- EKS で IPv6 対応のクラスターが作成可能
  - EKS CreateCluster API に **ipFamily** パラメータが追加
  - VPC は IPv4/IPv6 デュアルスタックである必要がある
- VPC の **IP アドレスが枯渇する**という課題に対応
  - Kubernetes の IPv4/IPv6 デュアルスタック機能とは異なる機能
  - Pod と Service は IPv6 のアドレスのみを受け取る

▼ クラスター情報 [情報](#)

Kubernetes バージョン [情報](#) 1.21 ステータス   
 アクティブ

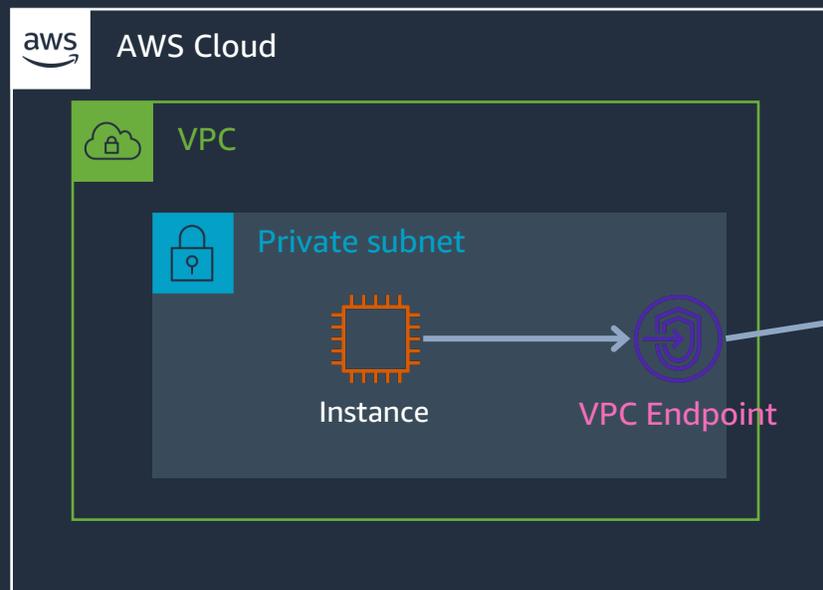
概要 | リソース | コンピューティング | **ネットワーキング** | アド

### ネットワーキング

VPC <a href="#">情報</a> vpc-0681b0609b23a5203 <a href="#">🔗</a>	サブネット subnet-07bb60223916b0e81 subnet-0031bd1edec6c7e5c subnet-08ac5475fdcde7cff <a href="#">🔗</a> subnet-0814f7d21e070dedc subnet-0fdedb1a49f4087ef <a href="#">🔗</a> subnet-07505f02a9071fe9c <a href="#">🔗</a>
<b>クラスター IP アドレスファミリー <a href="#">情報</a></b> IPv6	
サービス IPv6 の範囲 <a href="#">情報</a> fd3d:82ac:23e8::/108	

# 大阪リージョンで ECR の PrivateLink をサポート

- 大阪リージョンで Amazon ECR の VPC エンドポイント (PrivateLink) が利用可能に
  - インターネット接続を利用することなく ECR にアクセス可能
  - 閉域で EKS を利用されており、かつ大阪リージョンを利用した災害対策の要件があるお客様からは要望が多かった機能



インターネット接続なしで  
コンテナイメージのダウンロードが可能



Amazon ECR



Amazon S3

# コンピューート

# EKS 関連アップデート (コンピューート)

月/日	Update Title	関連 URL
 03/07	Bottlerocket が NVIDIA を搭載した GPU ベースの EC2 インスタンスタイプのサポートを追加	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
03/14	Kubernetes 1.21 以降の EKS での containerd ランタイム向け Windows サポートの発表	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li></ul>
 04/13	AWS Fargate でアプリケーションのより高速なスケーリングが可能に	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
 06/28	AWS Fargate のサービスクォータが vCPU ベースに変更予定	<ul style="list-style-type: none"><li>• <a href="#">blog</a></li></ul>

# Bottlerocket が NVIDIA GPU をサポート

- Bottlerocket は オープンソースのコンテナの実行に最適化された OS
- EKS 用の **NVIDIA Bottlerocket バリエーション** が提供
  - GPU の利用に必要なライブラリとカーネルモジュールがイメージ内で利用可能
  - GPU ドライバーをインストールまたは設定したり、k8s-device-plugin を実行したりする必要がない
  - マネージド型ノードグループは未サポート

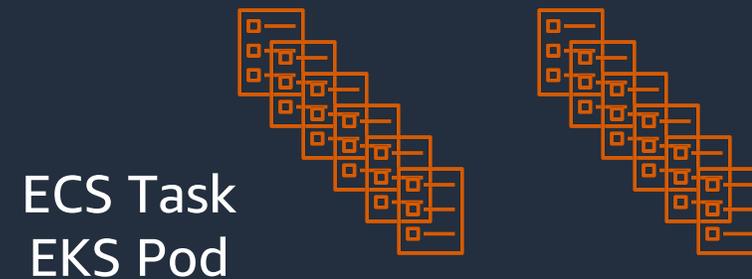


現在利用可能な Bottlerocket バリエーション

サポート対象	バリエーション
EKS	aws-k8s-1.19 aws-k8s-1.20 aws-k8s-1.21 aws-k8s-1.22 aws-k8s-1.23 <b>aws-k8s-1.21-nvidia</b> <b>aws-k8s-1.22-nvidia</b> <b>aws-k8s-1.23-nvidia</b>
ECS	aws-ecs-1 aws-ecs-1-nvidia
VMware	vmware-k8s-1.20 vmware-k8s-1.21 vmware-k8s-1.22 vmware-k8s-1.23
Bare Metal	metal-k8s-1.21 metal-k8s-1.22 metal-k8s-1.23

# AWS Fargate でより高速なスケールリングが可能に

- Fargate での ECS タスク / EKS Pod の起動レートリミット
  - トークンバケットアルゴリズムを利用してバースト可能
    - バケットの最大サイズは 100 トークン
    - リフィルレートは 20 トークン / 秒
  - 持続的な起動レートは 20 (タスク / Pod) / 秒
- 昨年比 20 倍



AWS Fargate

クォータ (リージョン毎)	バースト レート	持続可能 なレート	調整 可能
Fargate On-Demand Task / Pod 起動レート	100 / 秒	20 / 秒	Yes
Fargate Spot Task 起動レート	100 / 秒	20 / 秒	Yes

# AWS Fargate のクォータが vCPU ベースに変更予定

- 現在、Fargate で起動できるタスク / Pod は「数」ベースのクォータ
  - ソフトリミットであり Service Quotas コンソールから引き上げのリクエストが可能
- Fargate のタスク / Pod は 0.25 vCPU ~ 4 vCPU
- より実際のコンピュートリソースの使用量を反映したクォータとするため、「vCPU」ベースのクォータに移行予定
- 移行スケジュール
  - 8月から新しいクォータのオプトインが可能
  - 9月から10月に全てのアカウントが自動的に新しいクォータに移行、ただし移行を遅らせるためにオプトアウトすることも可能
  - 11月以降、オプトアウトしたアカウントも含め全てのアカウントが移行

クォータ (リージョン毎)	デフォルトのクォータ	調整可能
Fargate On-Demand resource count	1000	Yes
Fargate Spot resource count	1000	Yes



クォータ (リージョン毎)	デフォルトのクォータ	調整可能
Fargate On-Demand vCPU resource count	4000 vCPU	Yes
Fargate Spot vCPU resource count	4000 vCPU	Yes

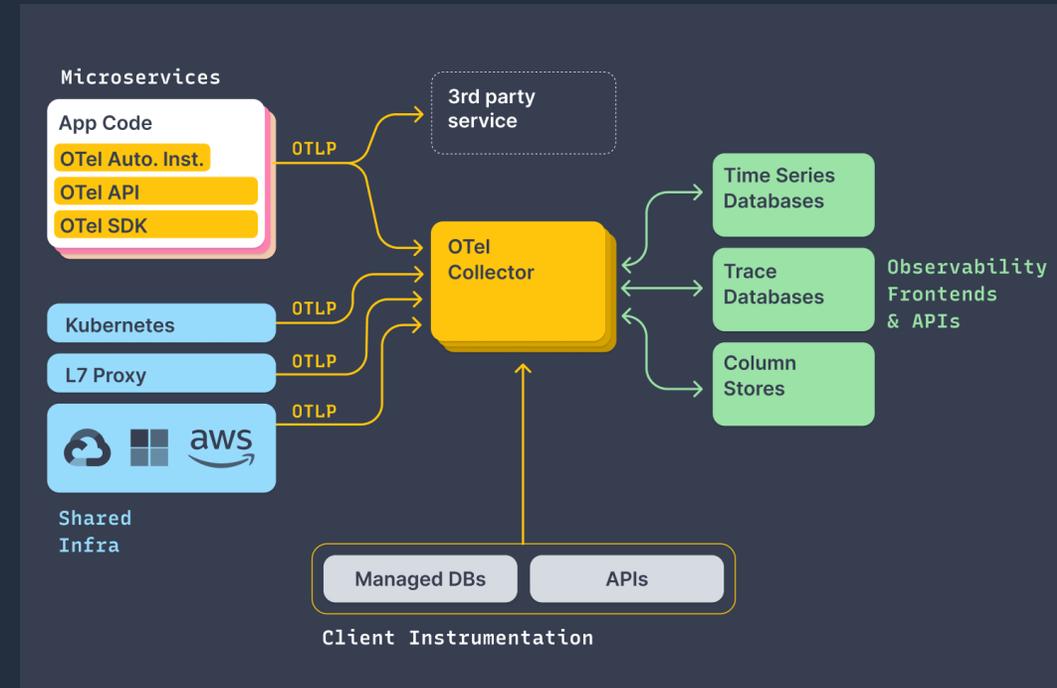
※ サービスクォータの使用量に基づいて CloudWatch アラームを設定している場合、新しいクォータでアラームの再作成が必要

# オブザーバビリティ

# OpenTelemetry / ADOT とは

<https://opentelemetry.io/>

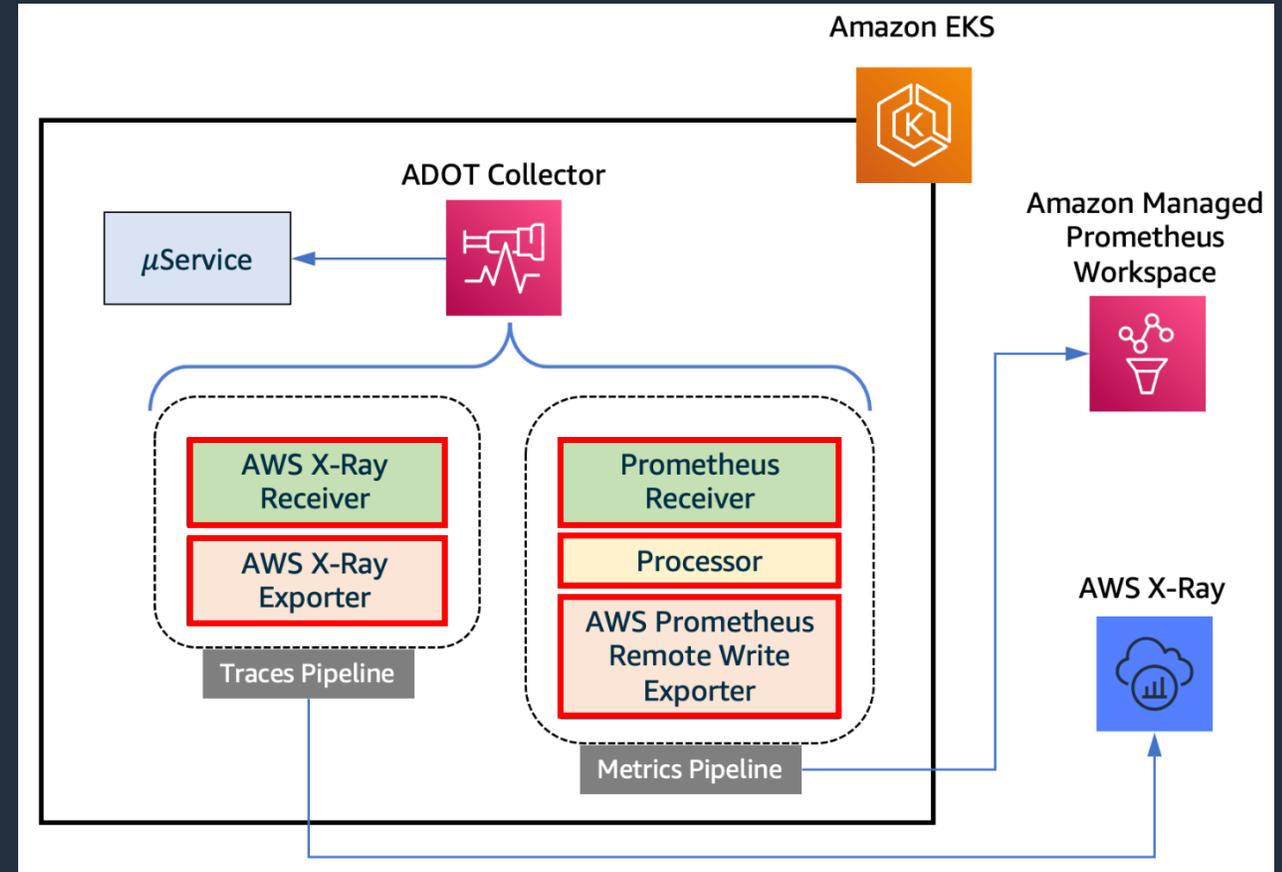
- **OpenTelemetry** とは
  - Cloud Native Computing Foundation (CNCF) でホストされるオープンソースプロジェクト
  - メトリクス、ログ、トレースなどのテレメトリーデータの計装 (インストルメンテーション) と送信の**標準仕様と実装を提供**
  - 具体的には以下を提供
    - Cross-language な仕様
    - Collector エージェント
    - 各言語の SDK
    - 自動計装 (オートインストルメンテーション)
- **AWS Distro for OpenTelemetry (ADOT)** とは
  - AWS がサポートするセキュアで Production Ready な OpenTelemetry ディストリビューション
  - **AWS 上で使いやすいように機能を拡張**



<https://aws-otel.github.io/>

# OpenTelemetry Collector / ADOT Collector とは

- テレメトリデータの収集、整形、バックエンドへの送信のためのエージェント
- Collector を分離することで、各言語 SDK が各バックエンドに向けた実装を持たなくてよくなる
- 3つの要素でパイプラインを構成
  - Receiver
    - 特定のフォーマットでデータを受け取る
    - プル型とプッシュ型
  - Processor
    - データのバッチ処理、フィルタリング、変換など
  - Exporter
    - テレメトリデータをバックエンドに送信



# EKS 関連アップデート (オブザーバビリティ)

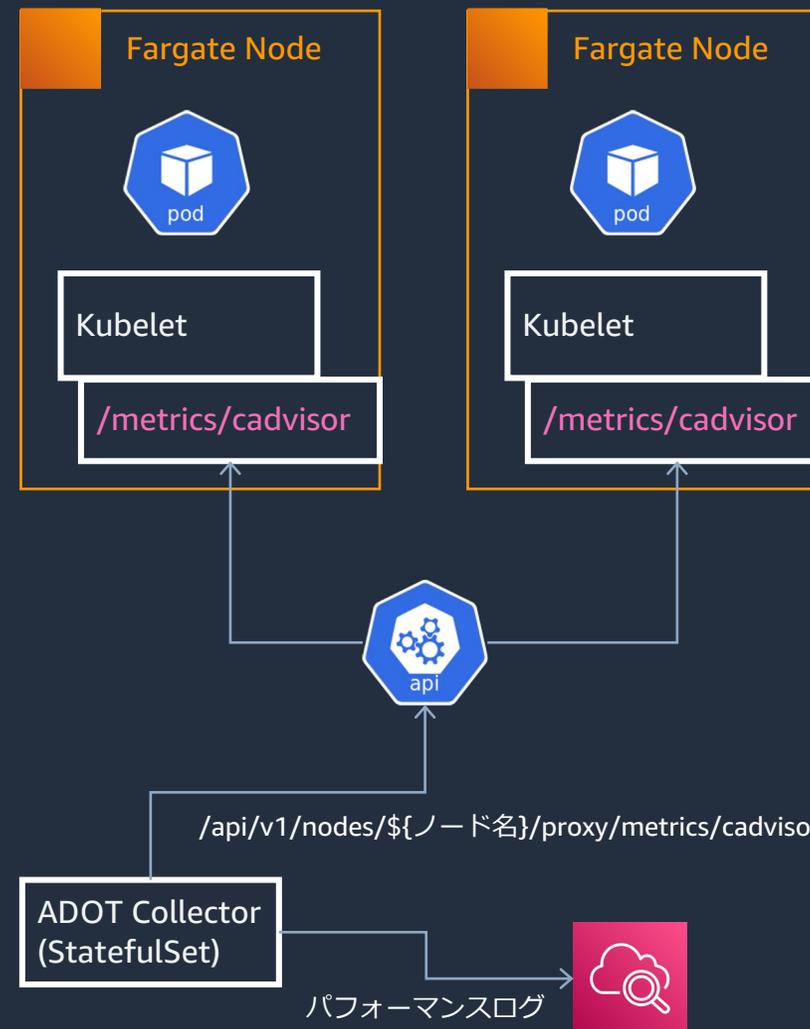
月/日	Update Title	関連 URL
01/07	Amazon ECR がリポジトリプル統計をモニタリングする機能を追加	<ul style="list-style-type: none"><li><a href="#">what's new</a></li></ul>
02/17	Amazon CloudWatch Container Insights は、AWS Distro for OpenTelemetry を使用した Amazon EKS Fargate をサポート対象に追加	<ul style="list-style-type: none"><li><a href="#">what's new</a></li><li><a href="#">blog</a></li></ul>
02/28	Amazon CloudWatch Container Insights は AWS Distro for OpenTelemetry を使用した Helm チャートをサポート対象に追加	<ul style="list-style-type: none"><li><a href="#">what's new</a></li></ul>
04/21	OpenTelemetry Operator の EKS アドオンサポートが一般提供開始	<ul style="list-style-type: none"><li><a href="#">what's new</a></li><li><a href="#">blog</a></li></ul>
05/18	EKS Observability Accelerator の発表	<ul style="list-style-type: none"><li><a href="#">blog</a></li></ul>
05/19	AWS Distro for OpenTelemetry でメトリクスのサポートが利用可能に	<ul style="list-style-type: none"><li><a href="#">what's new</a></li><li><a href="#">blog</a></li></ul>
06/21	AWS Fargate が AWS for Fluent Bit によるマルチラインロギングの完全サポートを開始	<ul style="list-style-type: none"><li><a href="#">what's new</a></li></ul>

# Container Insights が EKS Fargate をサポート

- CloudWatch Container Insights がこれまでサポート対象外だった EKS Fargate をサポート
  - メトリクスの収集のために ADOT Collector をデプロイする
  - ADOT Collector が Kubernetes API Server のプロキシ経由で各ノードの Kubelet の `/metrics/cadvisor` エンドポイントにアクセスし、メトリクスを収集
  - ADOT Collector はパフォーマンスログイベントを EMF (組み込みメトリクスフォーマット) で CloudWatch Logs に送信
  - Container Insights のダッシュボードで表示可能

## 取得できるメトリクス

- pod\_cpu\_utilization\_over\_pod\_limit
- pod\_cpu\_usage\_total
- pod\_cpu\_limit
- pod\_memory\_utilization\_over\_pod\_limit
- pod\_memory\_working\_set
- pod\_memory\_limit
- pod\_network\_rx\_bytes
- pod\_network\_tx\_bytes



# ADOT Operator の EKS アドオンが GA

- EKS アドオンは Kubernetes の運用に必要なソフトウェアを EKS で管理する機能
- 新たに ADOT Operator を EKS アドオンとしてサポート

The screenshot displays the AWS EKS console's 'Add-ons' page. The navigation bar at the top includes tabs for '概要', 'リソース', 'コンピューティング', 'ネットワーキング', 'アドオン', '認証', 'ログ記録', '更新履歴', and 'タグ'. The 'アドオン' tab is selected. Below the navigation bar, there's a section titled 'アドオン (5) 情報' with buttons for '編集', '削除', and '新規を追加'. The main content area shows five add-on cards, each with a title, type, status, and version. The 'adot' add-on is highlighted with a red border. All add-ons are currently active.

アドオン名	タイプ	ステータス	バージョン
adot	可観測性	アクティブ	v0.51.0-eksbuild.1
aws-ebs-csi-driver	ストレージ	アクティブ	v1.9.0-eksbuild.1
coredns	ネットワーキング	アクティブ	v1.8.7-eksbuild.1
kube-proxy	ネットワーキング	アクティブ	v1.22.6-eksbuild.1 <a href="#">今すぐ更新</a>
vpc-cni	ネットワーキング	アクティブ	v1.10.1-eksbuild.1 <a href="#">今すぐ更新</a>

# ADOT Operator の EKS アドオンが GA

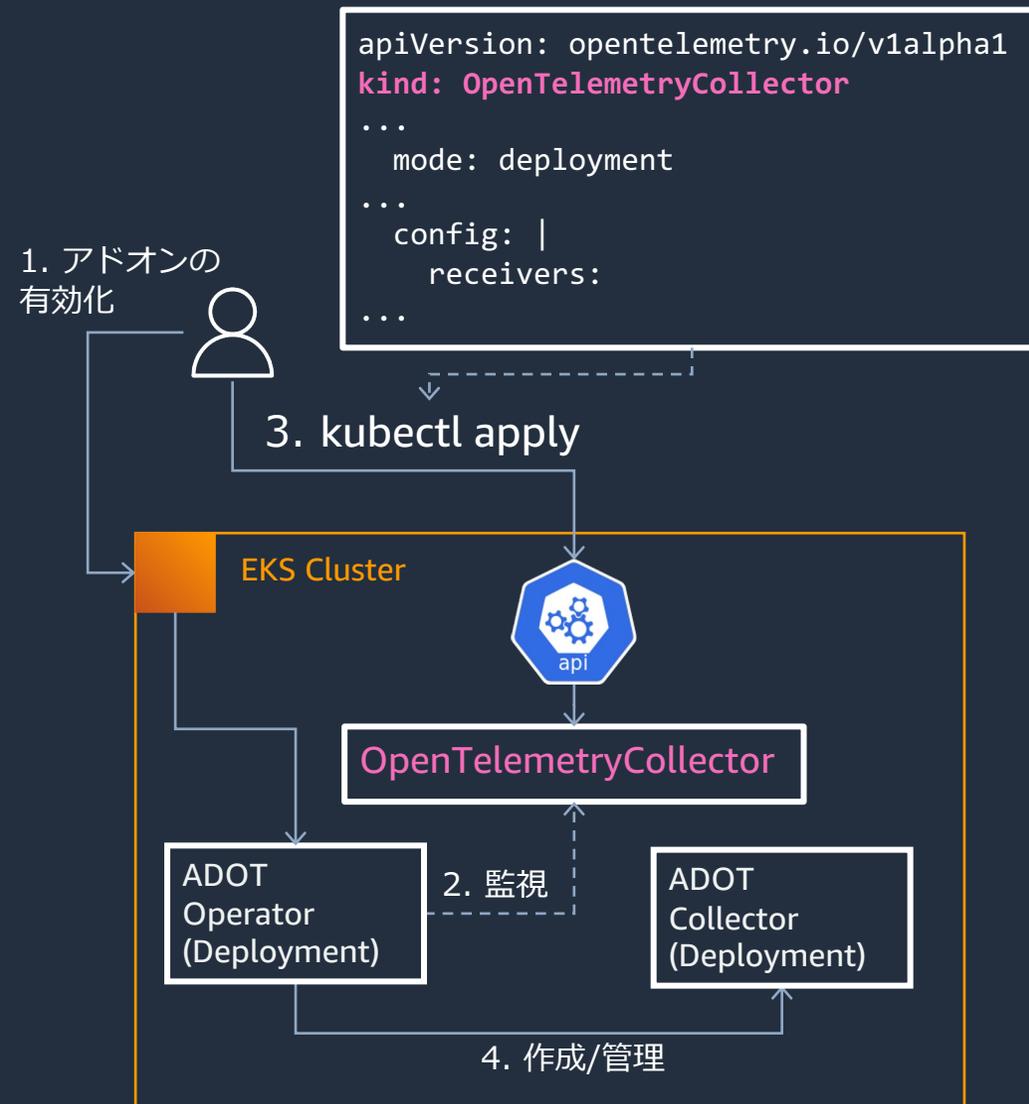
- ADOT アドオンの動作

※ アドオンの有効化の前に前提条件として権限付与と cert-manager のインストールが必要

1. アドオンを有効化するとクラスターに ADOT Operator がデプロイされる
2. ADOT Operator は OpenTelemetryCollector カスタムリソースを監視
3. ユーザーが ADOT Collector のパイプライン設定を含む OpenTelemetryCollector カスタムリソースを作成
4. ADOT Operator が ADOT Collector をデプロイする

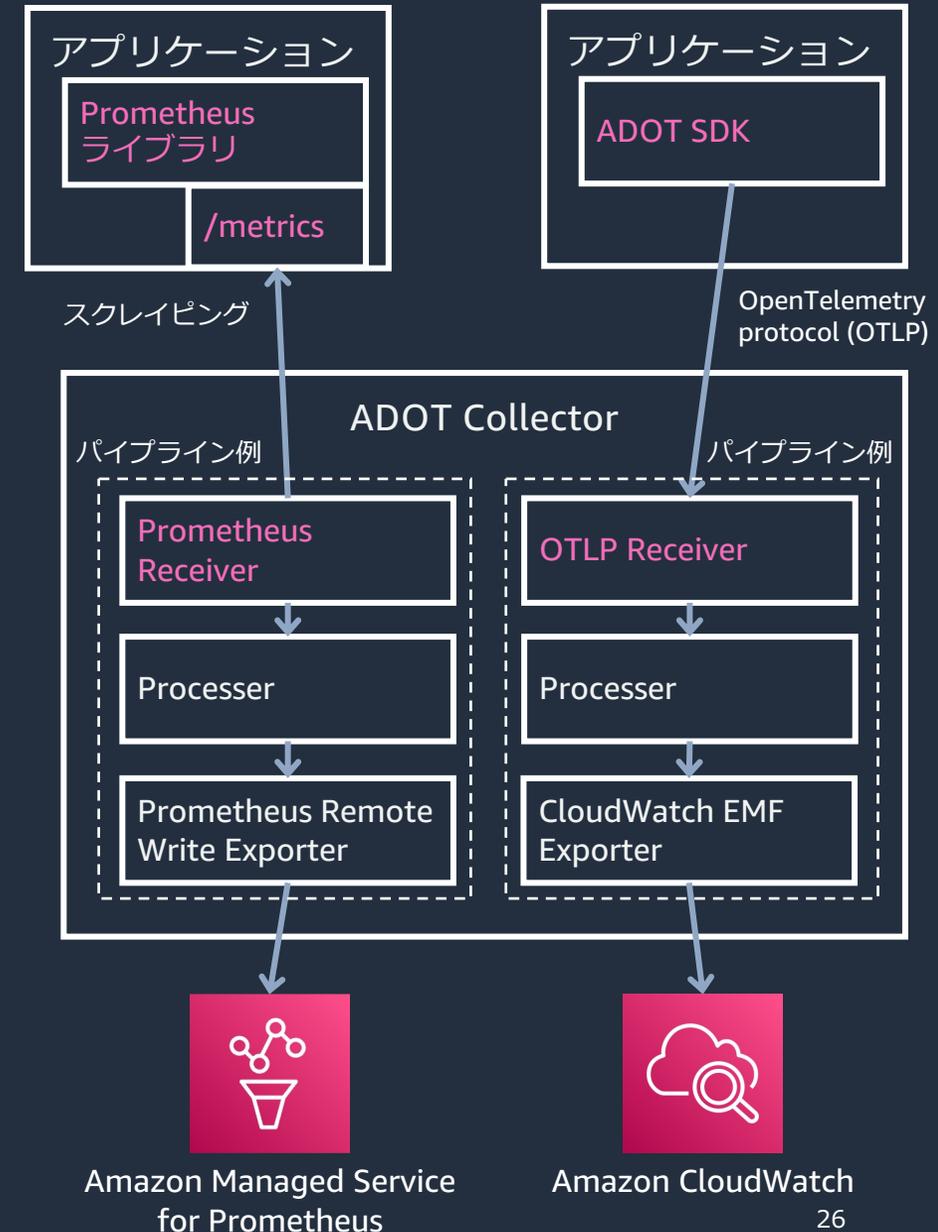
- 代表的な ADOT パイプライン設定のテンプレートはサンプルリポジトリで公開

- <https://github.com/aws-observability/aws-otel-community/tree/master/sample-configs/operator>



# ADOT のメトリクスサポートが GA

- ADOT のトレースサポートは 2021 年 9 月に GA
  - <https://aws.amazon.com/jp/blogs/news/new-for-aws-distro-for-opentelemetry-tracing-support-is-now-generally-available/>
- ADOT のメトリクスサポートも GA
  - ADOT Collector は Production Ready
    - クラスタ内の Prometheus の代替として ADOT Collector を使用してスクレイピング
    - Prometheus Remote Write Exporter を使用して Amazon Managed Service for Prometheus にメトリクスを送信可能
- アプリケーションをインストールする 2 つの選択肢
  - OpenTelemetry SDK (Java, .NET, Python) を使用
  - Prometheus ライブラリを使用
    - ADOT Collector の Prometheus Receiver によるスクレイピング



# セキュリティ

# EKS 関連アップデート (セキュリティ)

月/日	Update Title	関連 URL
01/04	ACM Private CA Kubernetes cert-manager プラグインが運用環境対応に	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li></ul>
 01/26	Amazon GuardDuty が Amazon Elastic Kubernetes Service クラスターの保護を開始	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
 06/25	Amazon Inspector が ECR 自動再スキャン期間の設定変更に対応	<ul style="list-style-type: none"><li>• <a href="#">user guide</a></li></ul>
 07/26	Amazon GuardDuty がマルウェア対策機能を追加	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>
 07/26	Amazon Detective が Amazon EKS 上のワークロードのセキュリティ調査をサポート	<ul style="list-style-type: none"><li>• <a href="#">what's new</a></li><li>• <a href="#">blog</a></li></ul>

# Amazon GuardDuty による EKS クラスターの保護

- GuardDuty が EKS の **Kubernetes 監査ログ** を利用して疑わしいアクティビティを検出
  - GuardDuty で機能を有効化するだけで利用可能
  - 監査ログはネイティブ連携
- 現在、以下を始めとする 27 項目を検出
  - 特権コンテナ起動
  - kube-system 名前空間の Pod で exec
  - 既知の不正 IP から API にアクセス
  - 手動で脅威リストに登録した IP から API にアクセス
  - Tor から Kubernetes API にアクセス
  - ホストの /etc などをマウントしたコンテナを起動
  - default サービスアカウントに管理者権限を付与

## データソース



Amazon GuardDuty

## Findings

**Execution:Kubernetes/ExecInKubeSystemPod** 🔍 ×  
検出結果 ID: [56c11c883fc665c3341b9a92776bd61e](#) [フィードバック](#)

**Medium** A command was executed inside a pod in kube-system namespace on EKS Cluster staging. If this behavior is not expected, it may indicate that your credentials are compromised. [Learn More](#)

[Detective](#) で調査する

概要

# ECR Enhanced Scanning の継続スキャンの期間が設定可能に

- Amazon Inspector を使用したコンテナイメージの脆弱性スキャン (Enhanced Scanning) では継続スキャンが設定可能
  - データベースに新しい CVE が追加されるたびにコンテナイメージがスキャンされる
- 自動再スキャンはこれまではイメージ Push 後 ~ 30 日間がスキャン対象だったが、**180 日間または Lifetime が選択可能に**
  - 今後新規作成するアカウントでは Lifetime がデフォルト設定
  - 既存アカウントの設定は自動で変更されない
  - 設定変更時点でスキャン対象のイメージのみが設定変更後もスキャン対象

The screenshot shows the AWS Inspector console settings for ECR re-scan duration. The breadcrumb navigation is 'Inspector > 設定 > 全般'. The main heading is '設定 情報'. Below it, the section is 'ECR re-scan duration 情報' with a '保存' button. The description reads: 'Set the time frame for how long inspector will continuously monitor images pushed into repositories.' There are three radio button options: 'Lifetime (Recommended)' (selected), '180 day', and '30 day'. Each option has a sub-description: 'Continue automated re-scans until the image is deleted', 'Continue automated re-scans for 180 days after the push date', and 'Continue automated re-scans for 30 days after the push date' respectively.

# Amazon GuardDuty がマルウェア対策機能を追加

- セキュリティソフトウェアやエージェントをデプロイすることなく、Amazon EC2 インスタンスおよび **コンテナワークロード** の悪意のあるファイルを検出
- 以下のステップで動作する
  1. GuardDuty が疑わしいアクティビティを検出 (既存機能)
  2. マルウェアスキャンが起動
  3. GuardDuty が対象の EC2 インスタンスの **EBS スナップショット** を取ってマルウェアスキャンを実施
  4. マルウェアを見つけたら GuardDuty で通知



## Execution:Kubernetes/MaliciousFile 🔍

検出結果 ID: 10c11f45aff181fc6d28eb8cf3d5fbf1

フィードバック

**High** 2 security risk(s) detected including EICAR-Test-File (not a virus) on EKS Cluster mycluster. [情報](#)

[Detective](#) で調査する

### 概要

重要度	高い	🔍
リージョン	ap-northeast-1	
カウント	1	
アカウント ID	████████████████████	🔍
リソース ID	mycluster <a href="#">🔗</a>	
作成時刻	2022-07-27 16:24:54 (10分前)	
更新時刻	2022-07-27 16:24:54 (10分前)	
スキャン ID	66f8d014e7b601e55493531a5f63a2a3	🔍

### 検出された脅威 (2)

#### 1. EICAR-Test-File (not a virus)

Name	EICAR-Test-File (not a virus)	🔍
Severity	HIGH	🔍
Hash	275a021bbfb6489e54d471899f7db9...	🔍
File path	eicar.com	
File name	eicar.com	

# Amazon Detective が EKS をサポート

- Amazon Detective は潜在的なセキュリティ問題や疑わしい活動の分析、調査、根本原因の特定を容易にするフルマネージドサービス
  - 前提条件として GuardDuty の有効化が必要
  - ユーザーアクティビティ (CloudTrail) やネットワークアクティビティ (VPC Flow logs)、GuardDuty の検出結果を自動的に関連付け
  - GuardDuty の検出結果や IP アドレスといった「プロファイル」毎に関連情報をまとめて可視化
- Detective が EKS Audit Logs をサポート
  - EKS クラスタでコントロールプレーンのロギングを有効化するなどの設定変更は不要
  - Kubernetes API アクティビティの概要を確認したり、詳細のドリルダウンが可能

## データソース



VPC Flow logs



CloudTrail



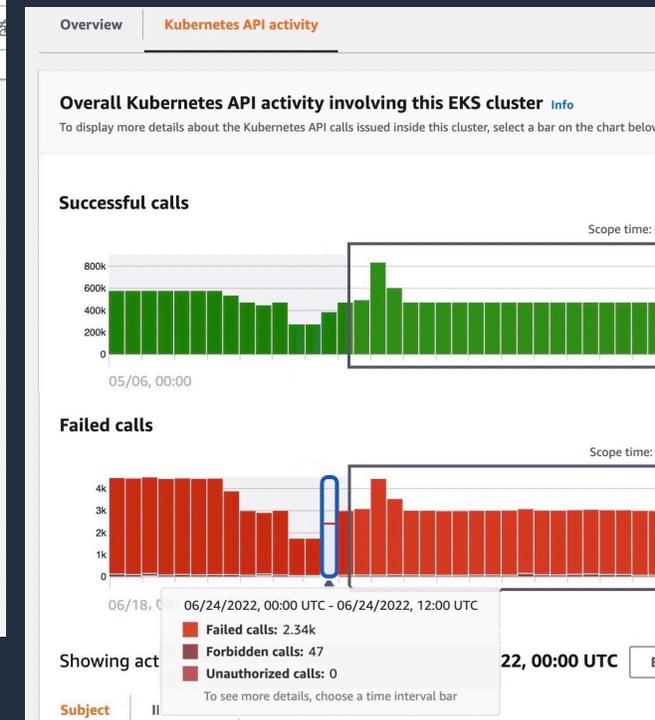
GuardDuty



EKS Audit Logs



Amazon Detective



# その他のアップデート

# EKS 関連アップデート (その他)

月/日	Update Title	関連 URL
01/04	Amazon EMR on EKS がカスタム Docker コンテナイメージのテストを簡素化するカスタムイメージ検証ツールをリリース	• <a href="#">what's new</a>
01/05	Amazon EMR on EKS が、デバッグを簡素化するために DescribeJobRun API 応答にエラーメッセージの詳細を追加	• <a href="#">what's new</a>
01/05	Amazon EMR on EKS が AWS Graviton ベースの EC2 インスタンス用にカスタマイズされたコンテナイメージのサポートを追加	• <a href="#">what's new</a>
01/06	Amazon EMR on EKS、マネージドエンドポイントを使用して実行されるインタラクティブジョブのカスタマイズされたコンテナイメージのサポートを追加	• <a href="#">what's new</a>
02/25	AWS App Mesh が Agent for Envoy を導入	• <a href="#">what's new</a>
03/28	AWS App Mesh Envoy Management Service (EMS) が AWS CloudTrail 統合をサポート	• <a href="#">what's new</a>
04/07	Amazon MemoryDB 向け AWS Controllers for Kubernetes プレビューの発表	• <a href="#">what's new</a>
04/12	Amazon ECR Public がナビゲーションパンくずリンクの実装やドロップダウンからのイメージ識別子のコピーなどのギャラリーの変更を発表	• <a href="#">what's new</a>

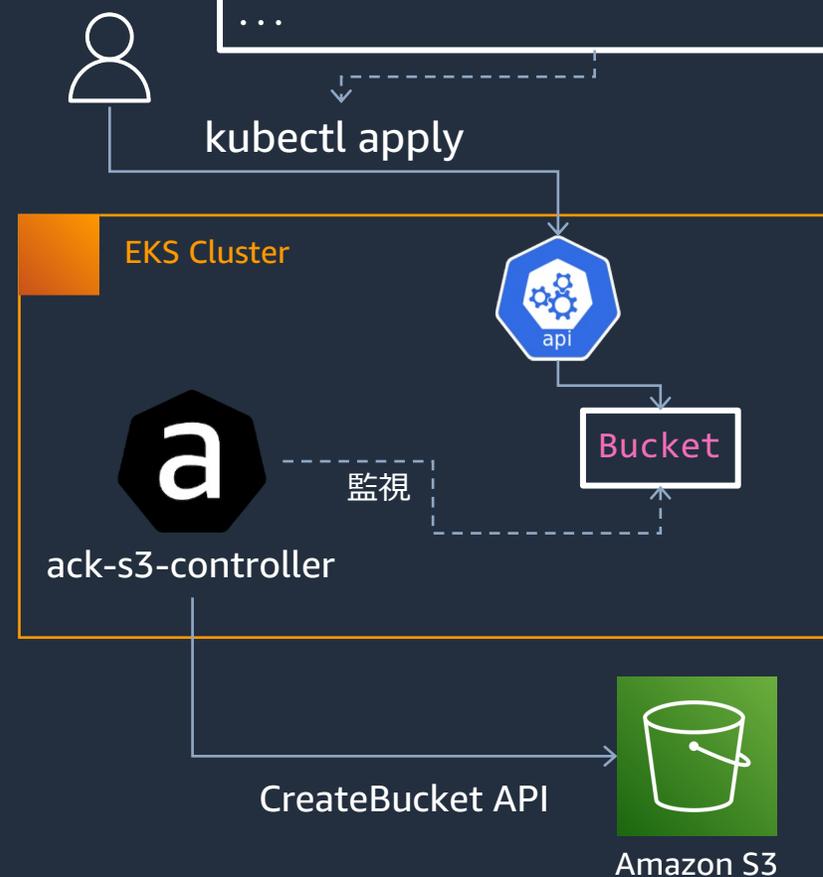
# EKS 関連アップデート (その他)

月/日	Update Title	関連 URL
04/14	Amazon VPC CNI Plugin for K8s の v1.11.0 で新しいモードが追加され Calico Network Policy や NodeLocal DNS Cache と Security group for Pods が併用可能に	• <a href="#">release note</a>
 04/19	Amazon EKS、Amazon ECR、Amazon DynamoDB、Amazon S3、AWS Application Autoscaling、AWS API Gateway v2 の ACKコントローラーが一般提供を開始	• <a href="#">what's new</a>
 04/20	EKS Blueprints の発表	• <a href="#">blog</a>
04/26	Amazon Elastic Kubernetes Service (EKS) が、ポッドアフィニティをサポートする Karpenter v0.9.0 を発表	• <a href="#">what's new</a>
05/13	Amazon EKS Anywhere キュレーションパッケージの公開プレビューを開始	• <a href="#">what's new</a>
05/16	Kubeflow v1.4.1 をサポートする Kubeflow の AWS ディストリビューションの一般提供開始	• <a href="#">what's new</a>

# いくつかのサービス用の ACK コントローラーが GA

- AWS Controllers for Kubernetes (ACK) は **AWS サービスを Kubernetes から管理**することを可能にするカスタムコントローラー
- 以下のサービス用のカスタムコントローラーが GA
  - Amazon EKS
  - Amazon ECR
  - Amazon DynamoDB
  - Amazon S3
  - AWS Application Auto Scaling
  - Amazon API Gateway v2 (HTTP API)
- その他のサポートされている AWS サービスやリリースフェーズはドキュメントを参照
  - <https://aws-controllers-k8s.github.io/community/docs/community/services/>

```
apiVersion: s3.services.k8s.aws/v1alpha1
kind: Bucket
...
spec:
  name: MyBucket
  versioning: ...
...
```



# EKS Blueprints の発表

- EKS の導入をより簡単かつ迅速にする新しいオープンソースプロジェクト
- EKS Blueprints は IaC モジュールのコレクション
- HashiCorp Terraform と AWS CDK で実装
- EKS アドオンだけでなく、人気のある幅広いオープンソースアドオンを使用して EKS クラスタをブートストラップ可能
  - Prometheus
  - Karpenter
  - AWS Load Balancer Controller
  - Argo CD など多数
- 各アドオンはアップストリームの Helm チャートリポジトリを指しており、チャートの values をカスタマイズすることも可能

## Terraform の例

```
module "eks_blueprints" {
  source = "github.com/aws-ia/terraform-aws-eks-bl...
  ...
  cluster_version = "1.21"
  ...
  managed_node_groups = {
  ...
  }
}

module "kubernetes_addons" {
  source = "github.com/aws-ia/terraform-aws-eks-bl...

  eks_cluster_id = module.eks_blueprints.eks_cluster_id

  # EKS Add-ons
  enable_aws_iam_roles_for_eks_nodes = true
  enable_aws_load_balancer_controller = true
  ...

  # Self-managed Add-ons
  enable_aws_for_fluentbit = true
  enable_aws_load_balancer_controller = true
  ...
}
```



Thank you!