直近の Amazon EKS アップデート

夏の AWS Kubernetes 祭り！

杉田 想士

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 想士 (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

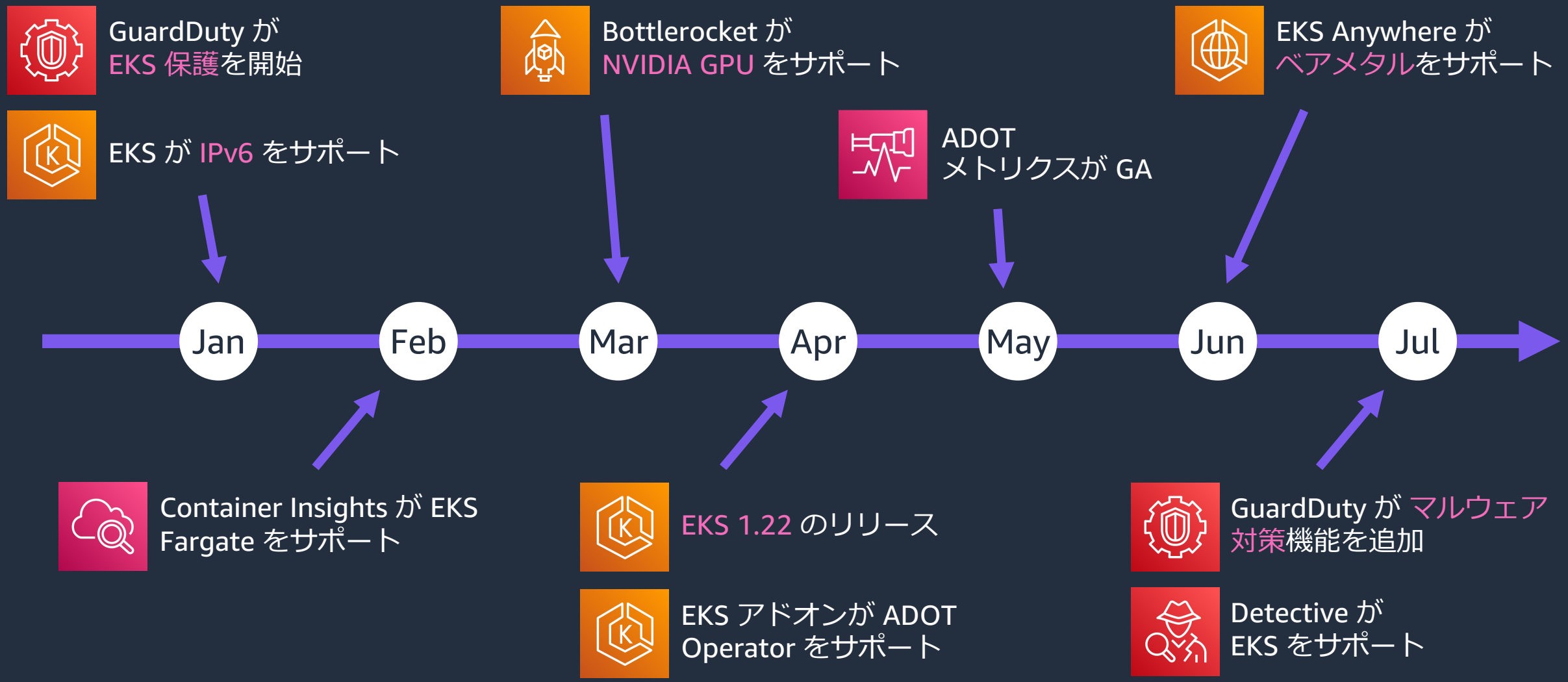
バックグランド

- 外資系 SIer 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。	• what's new • blog
👉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	• what's new • blog
👉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	• what's new • blog
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	• what's new
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	• blog
👉06/30	Amazon EKS Anywhere のベアメタルサポートを開始	• what's new • blog • blog

04/04 • what's new
• blog

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

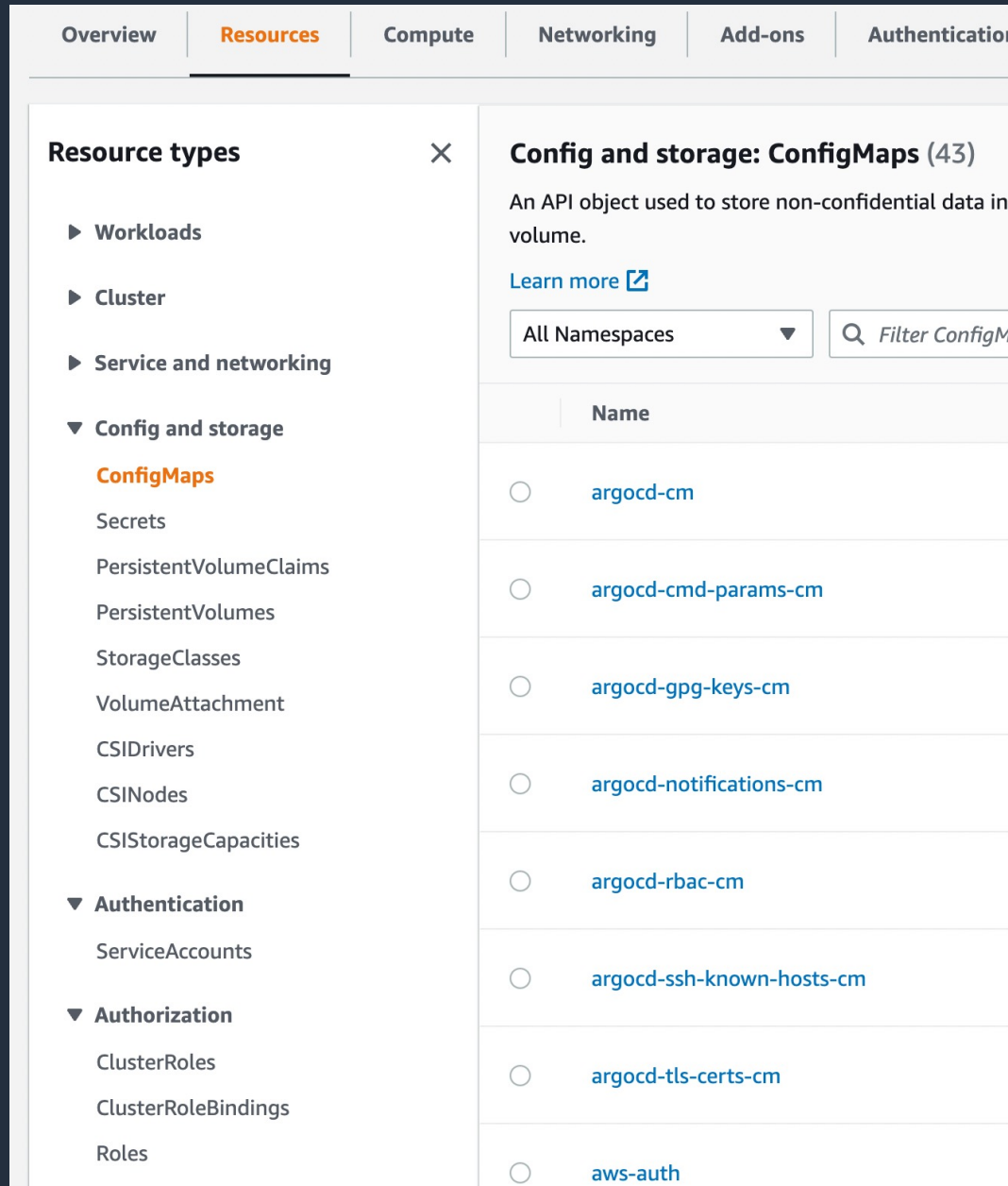
Kubernetes 1.22: Reaching New Peaks

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

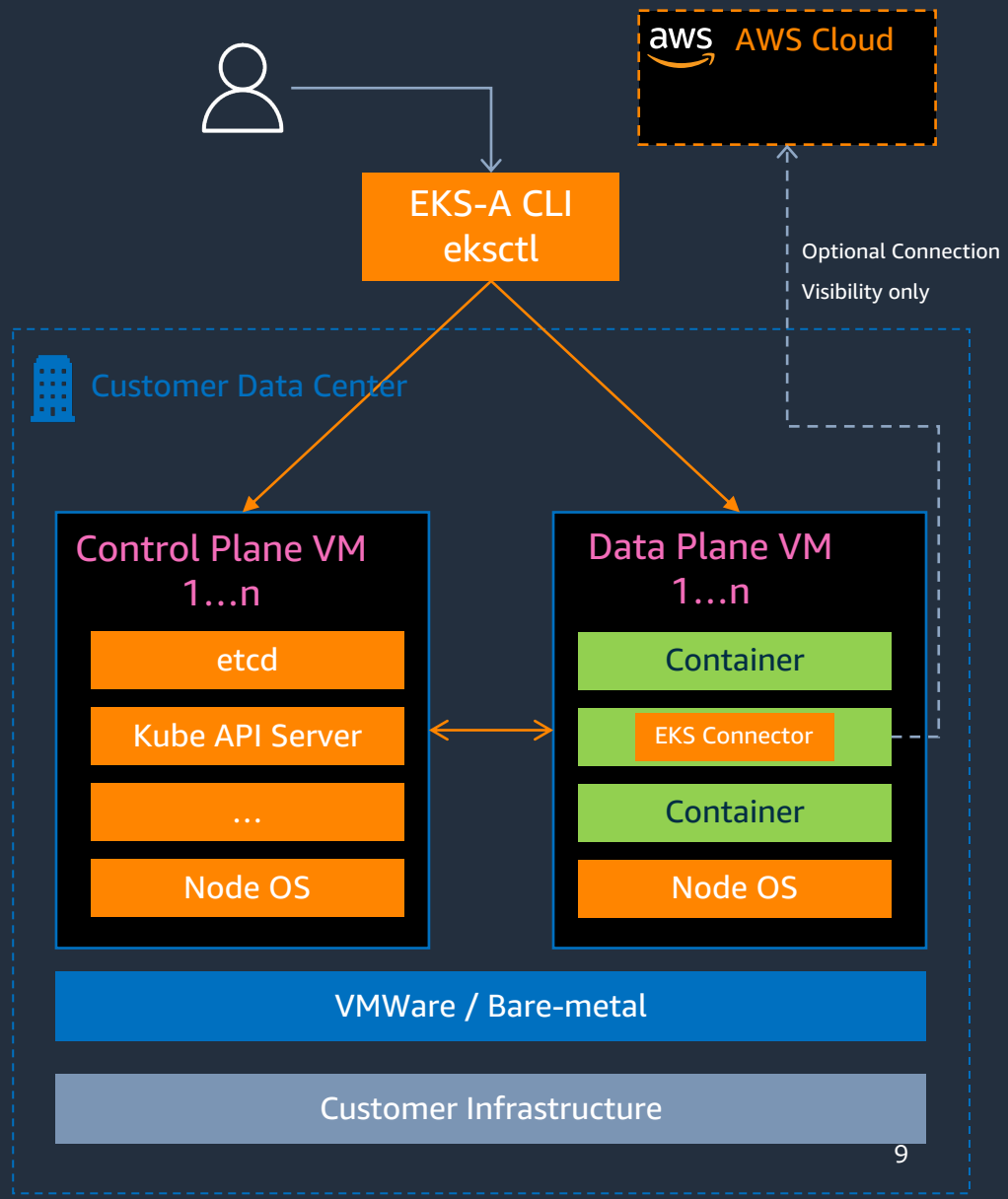
- EKS コンソールで Kubernetes の標準的なリソースを表示可能に
  - ワークロード
    - Pod, Deployment, DaemonSet など
  - クラスター
    - Node, Namespace など
  - ネットワーク
    - Service, Ingress, IngressClass など
  - 設定とストレージ
    - ConfigMap, Secret, PVC, PV など
  - 認証/認可
    - ServiceAccount, ClusterRole など



06/30 • what's new
• blog
• blog

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	• what's new • blog • blog
05/18	AWS App Mesh が Internet Protocol Version 6 (IPv6) をサポート	• what's new
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	• what's new

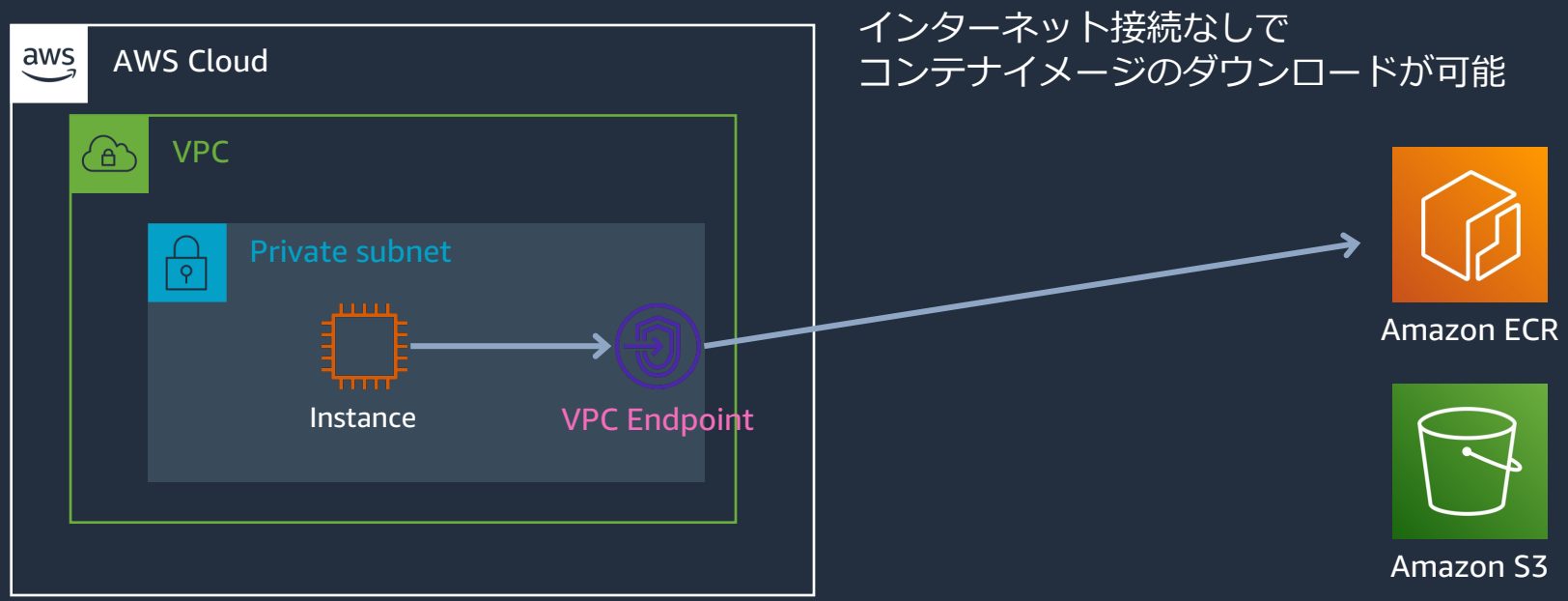
- what's new
- blog
- blog

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

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の多かった機能



コンピュート

EKS 関連アップデート (コンピュート)

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	• what's new • blog
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	• what's new
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	• what's new • blog
06/28	AWS Fargate のサービスクォータが vCPU ベースに変更予定	• blog

03/07 • what's new
• blog

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 バリアントが提供
  - 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 バリアント

サポート対象	バリアント
EKS	aws-k8s-1.19 aws-k8s-1.20 aws-k8s-1.21 aws-k8s-1.22 aws-k8s-1.23 aws-k8s-1.21-nvidia aws-k8s-1.22-nvidia aws-k8s-1.23-nvidia
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

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、オプトアプ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

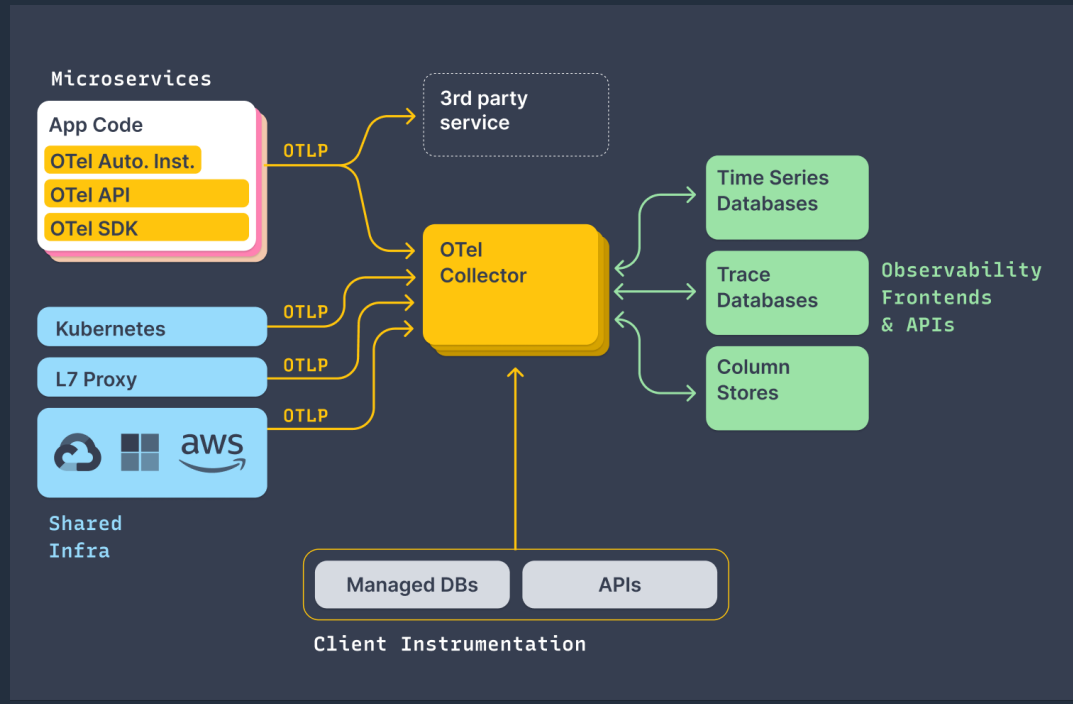
※ サービスクォータの使用量に基づいて CloudWatch アラームを設定している場合、新しいクォータでアラームの再作成が必要

オブザーバビリティ

OpenTelemetry / ADOT とは

https://opentelemetry.io/

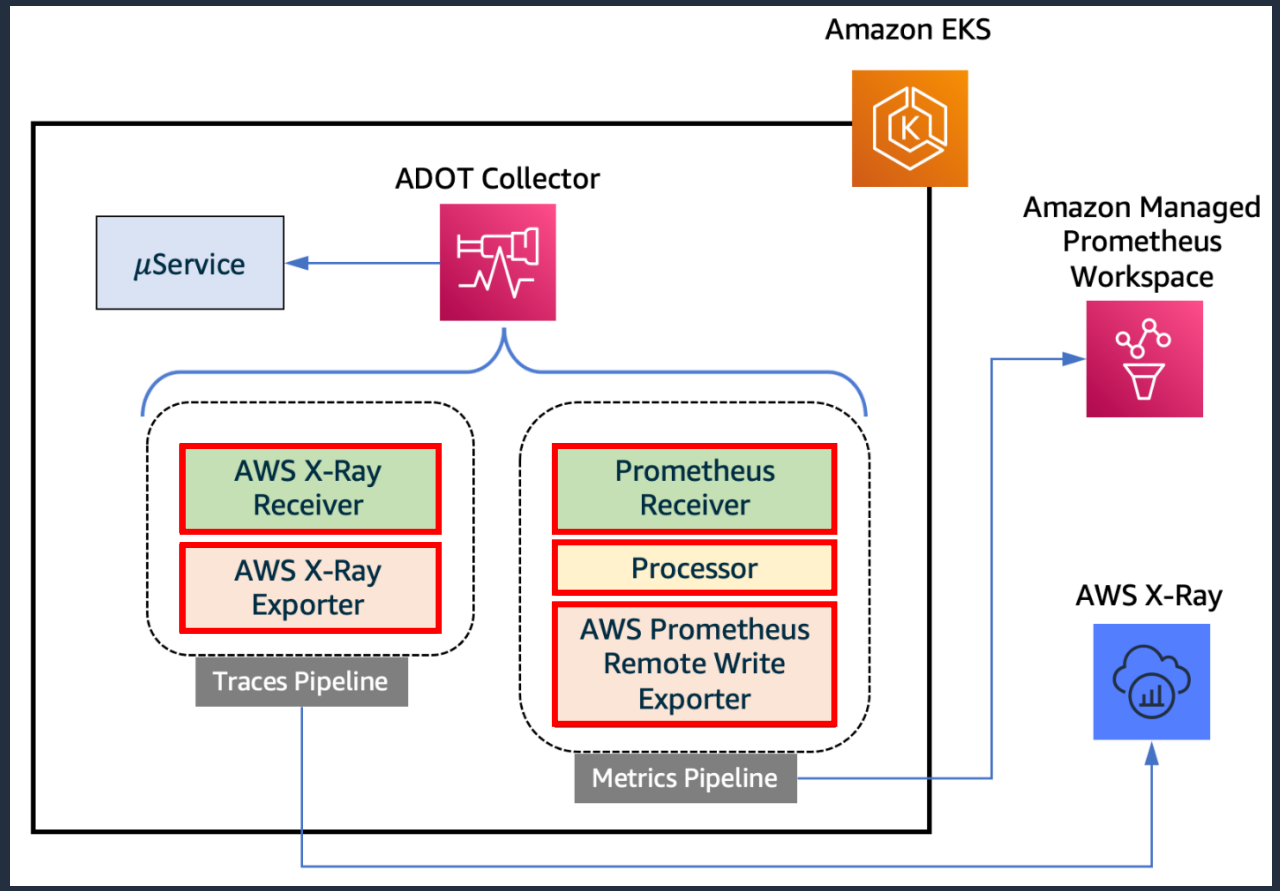
- OpenTelemetry とは
  - Cloud Native Computing Foundation (CNCF) でホストされるオープンソースプロジェクト
  - メトリクス、ログ、トレースなどのテレメトリーデータの計装 (インストルメンテーション) と送信の標準仕様と実装を提供
  - 具体的には以下を提供
    - Cross-language な仕様
    - Collector エージェント
    - 各言語の SDK
    - 自動計装 (オートインストルメンテーション)
- AWS Distro for OpenTelemetry (ADOT) とは
  - AWS 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
    - テレメトリーデータをバックエンドに送信

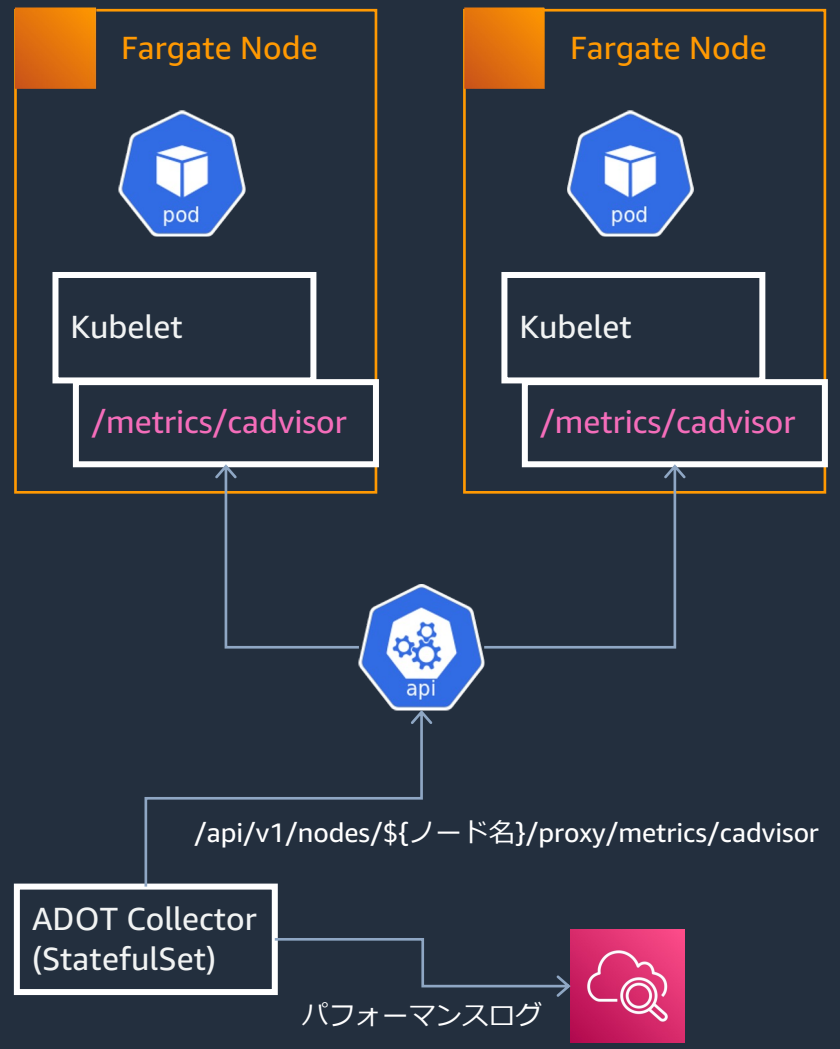


EKS 関連アップデート (オブザーバビリティ)

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	• what's new
👉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	• what's new • blog
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	• what's new
👉04/21	OpenTelemetry Operator の EKS アドオンサポートが一般提供開始	• what's new • blog
05/18	EKS Observability Accelerator の発表	• blog
👉05/19	AWS Distro for OpenTelemetry でメトリクスのサポートが利用可能に	• what's new • blog
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	• what's new

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

04/21 • what's new
• blog

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

04/21 • what's new
• blog

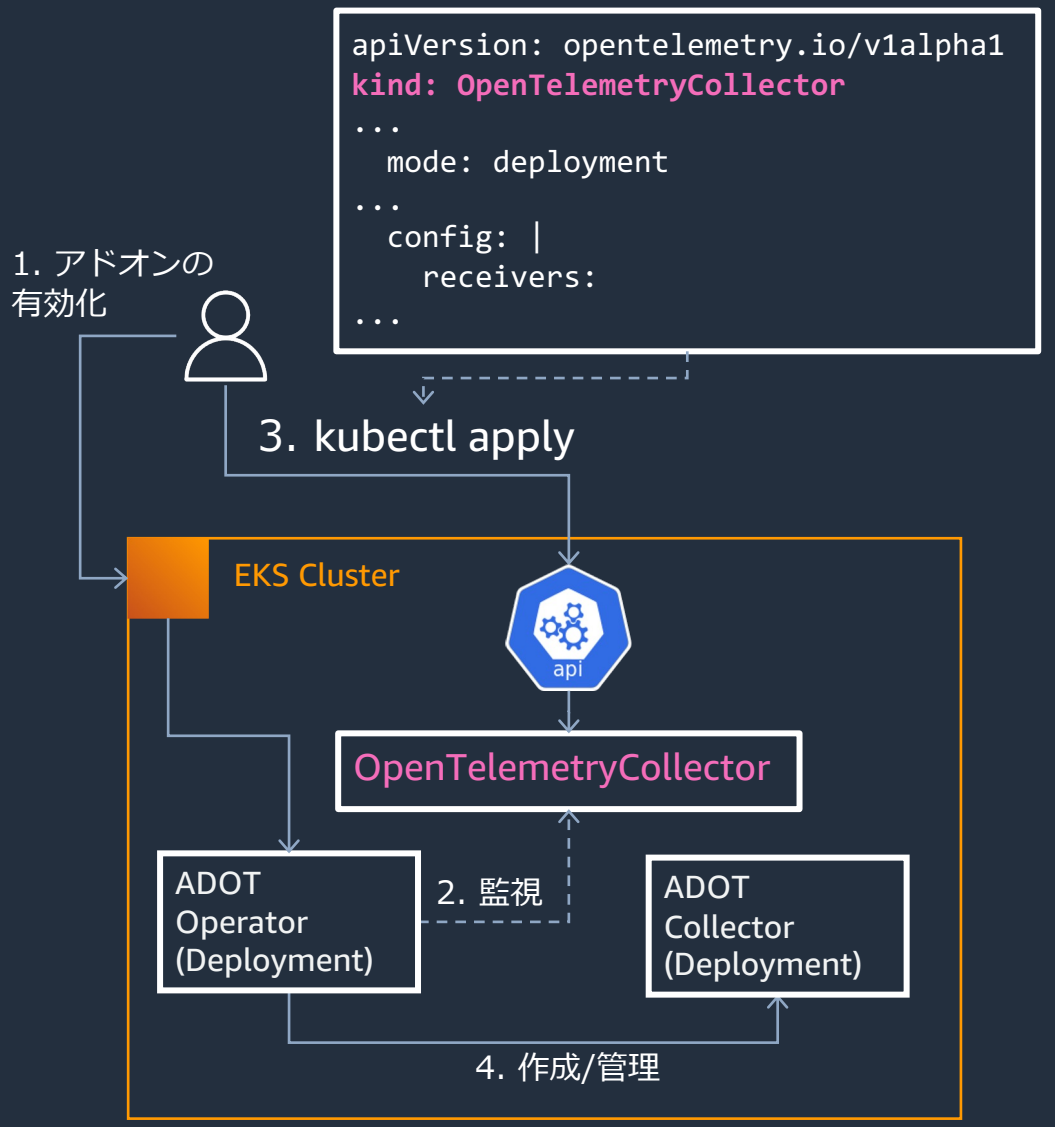
ADOT Operator の EKS アドオンが GA

- 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

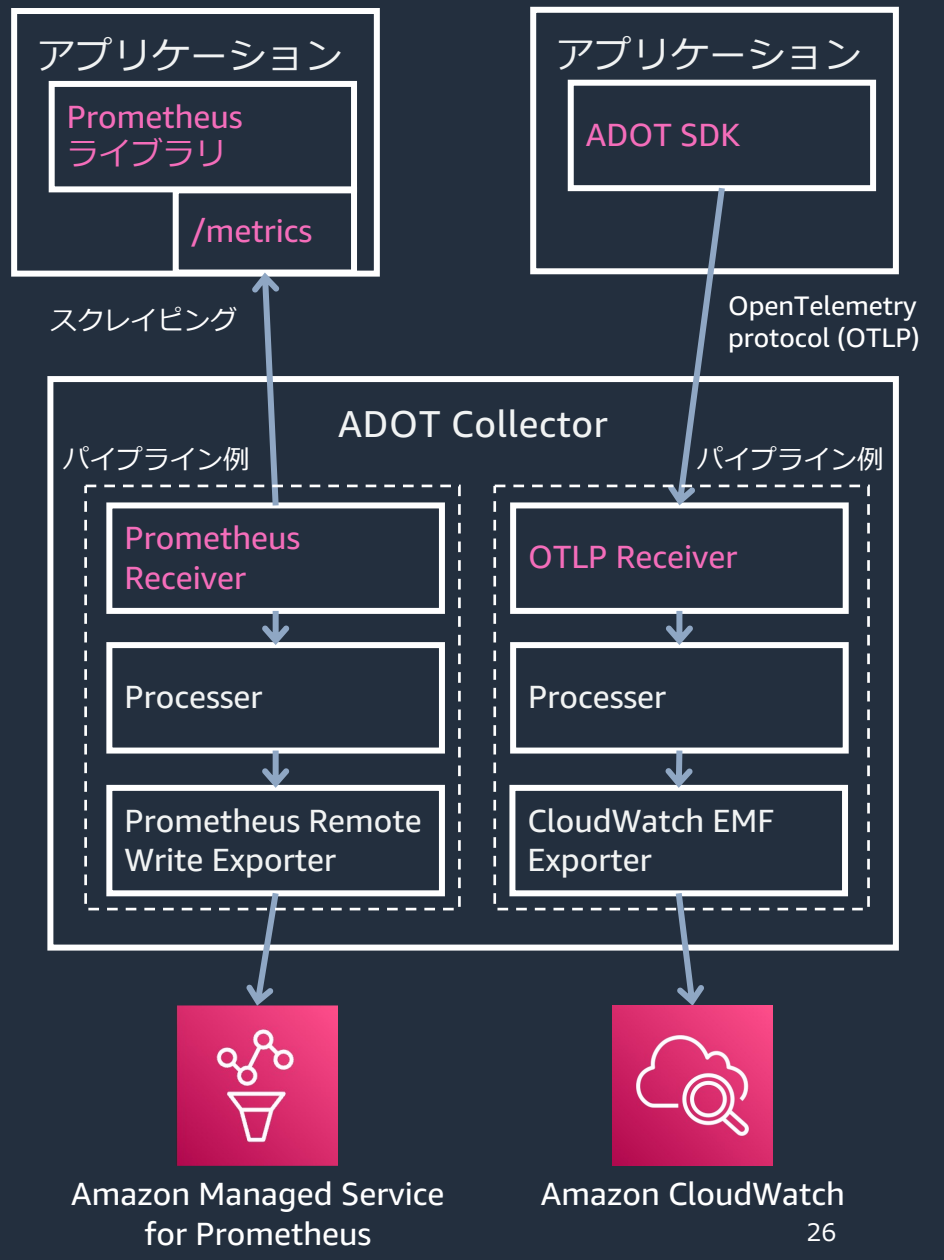
- 代表的な ADOT パイプライン設定のテンプレートはサンプルリポジトリで公開
  - https://github.com/aws-observability/aws-otel-community/tree/master/sample-configs/operator



05/19 • what's new
• blog

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
    - クラスター内の 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ルメントする 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

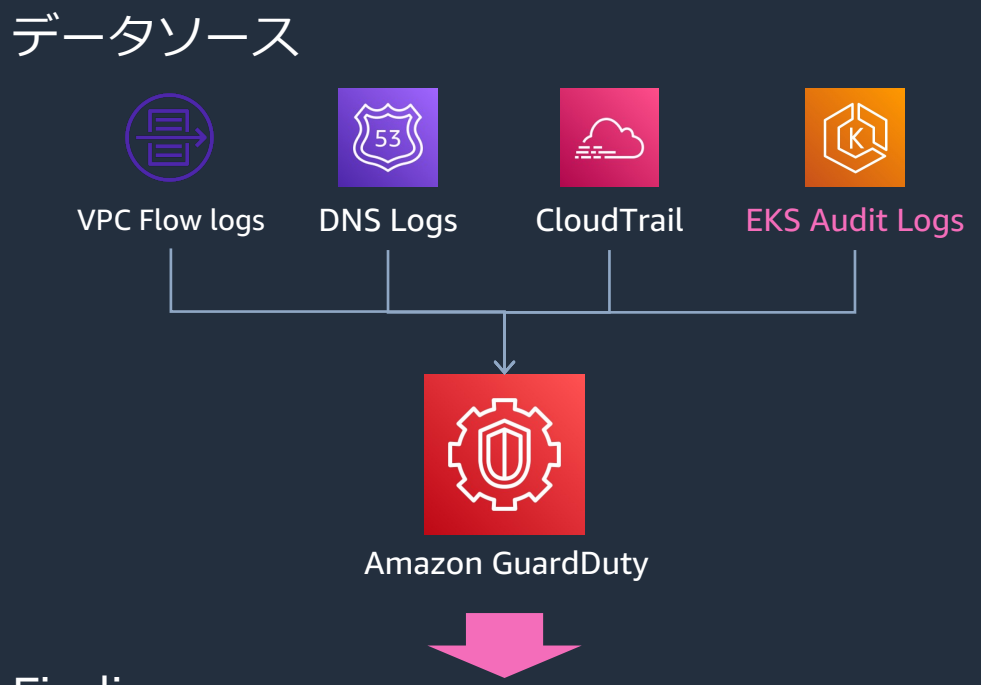
EKS 関連アップデート (セキュリティ)

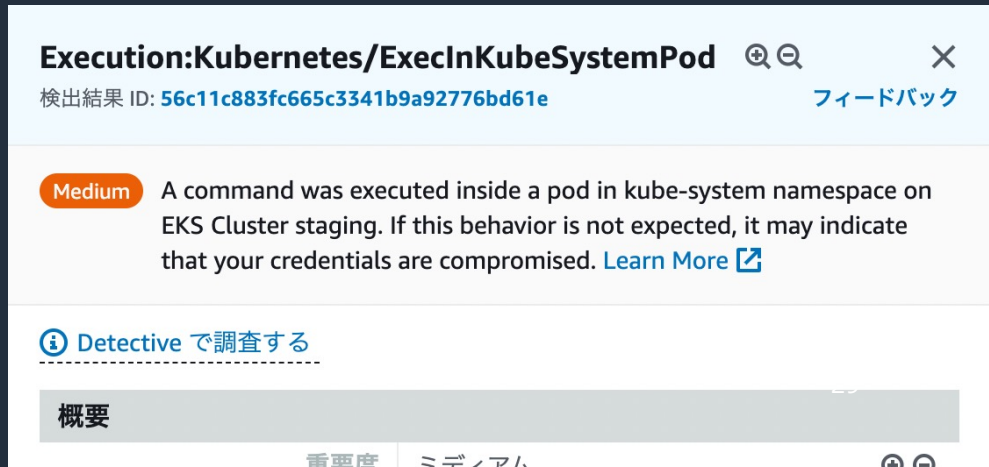
月/日	Update Title	関連 URL
01/04	ACM Private CA Kubernetes cert-manager プラグインが運用環境対応に	• what's new
👉01/26	Amazon GuardDuty が Amazon Elastic Kubernetes Service クラスターの保護を開始	• what's new • blog
👉06/25	Amazon Inspector が ECR 自動再スキャン期間の設定変更に対応	• user guide
👉07/26	Amazon GuardDuty がマルウェア対策機能を追加	• what's new • blog
👉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	• what's new • blog

- what's new
- blog

Amazon GuardDuty による EKS クラスターの保護

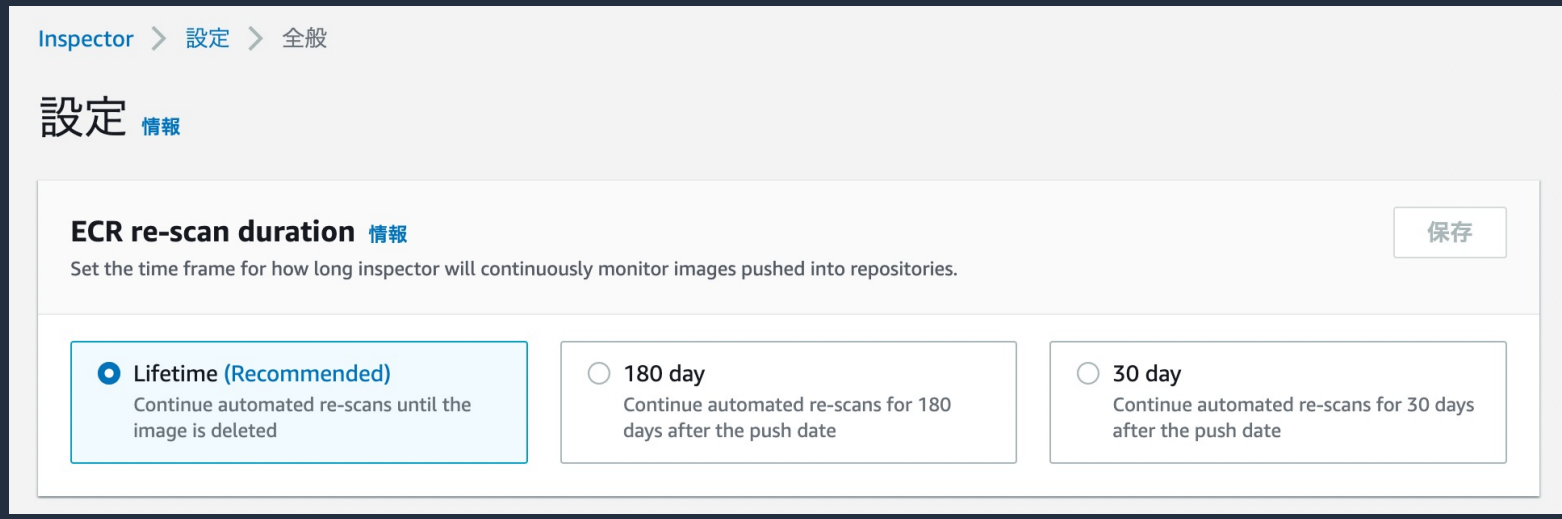
- GuardDuty が EKS の Kubernetes 監査ログを利用して疑わしいアクティビティを検出
  - GuardDuty で機能を有効化するだけで利用可能
  - 監査ログはネイティブ連携
- 現在、以下を始めとする 27 項目を検出
  - 特権コンテナ起動
  - kube-system 名前空間の Pod で exec
  - 既知の不正 IP から API にアクセス
  - 手動で脅威リストに登録した IP から API にアクセス
  - Tor から Kubernetes API にアクセス
  - ホストの /etc などをマウントしたコンテナを起動
  - default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





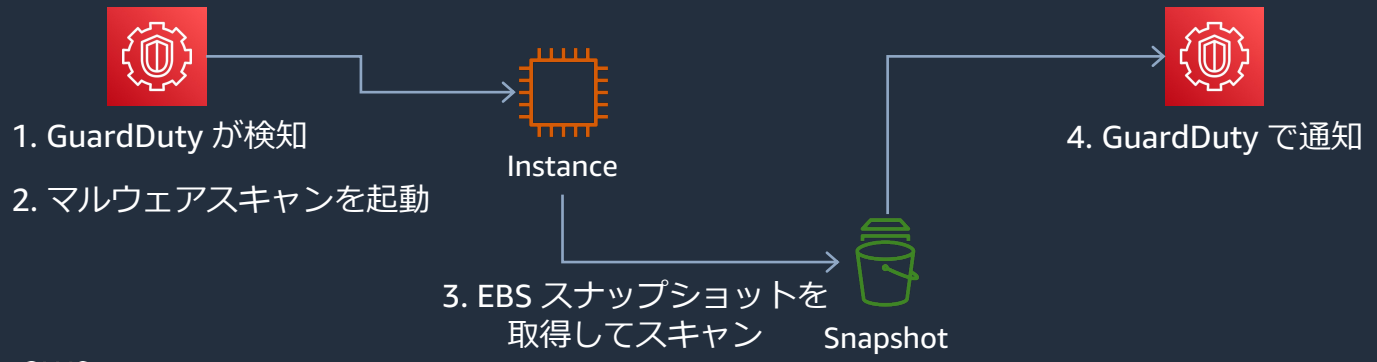
ECR Enhanced Scanning の継続スキャンの期間が設定可能に

- 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



Amazon GuardDuty がマルウェア対策機能を追加

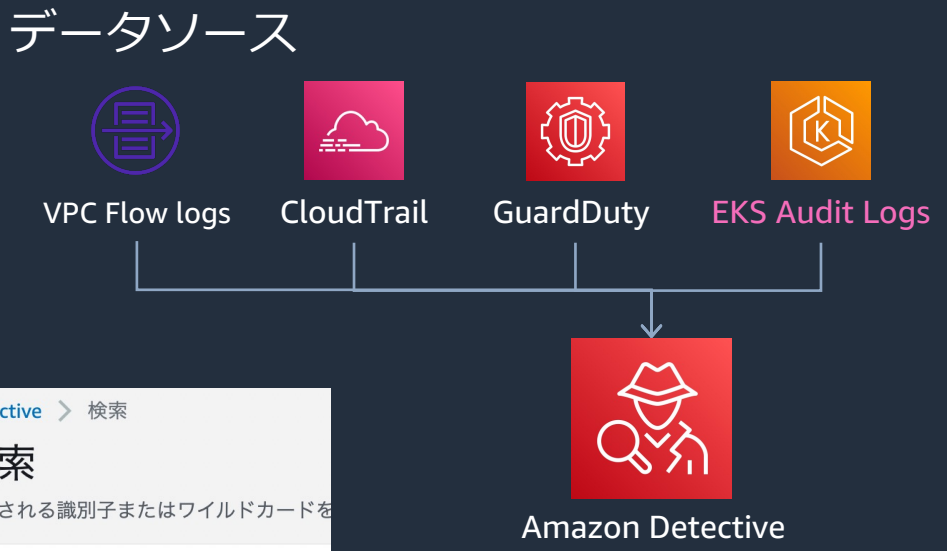
- セキュリティソフトウェアやエージェントをデプロイすることなく、Amazon EC2 インスタンスおよびコンテナワークロードの悪意のあるファイルを検出
- 以下のステップで動作する
  1. GuardDuty が疑わしいアクティビティを検出 (既存機能)
  2. マルウェアスキャンが起動
  3. GuardDuty が対象の EC2 インスタンスの EBS スナップショットを取ってマルウェアスキャンを実施
  4. マルウェアを見つけたら GuardDuty で通知

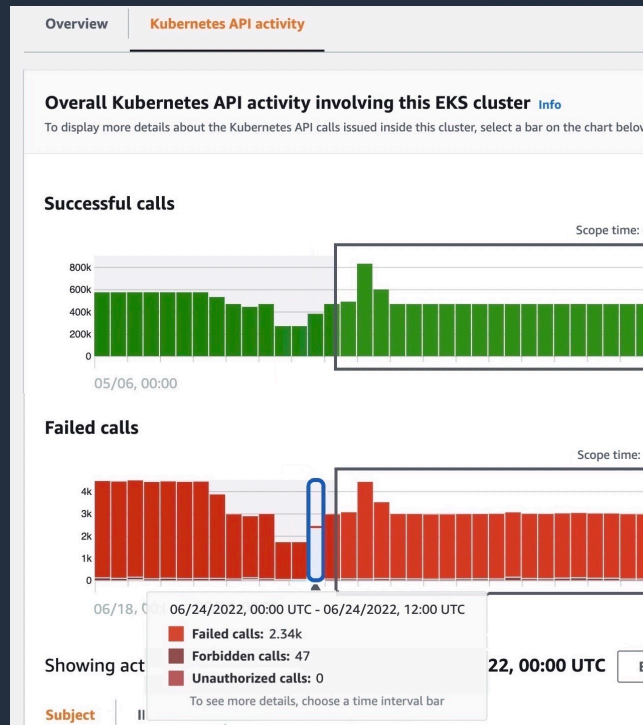


07/26 • what's new
• blog

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 クラスター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





その他のアップデート

EKS 関連アップデート (その他)

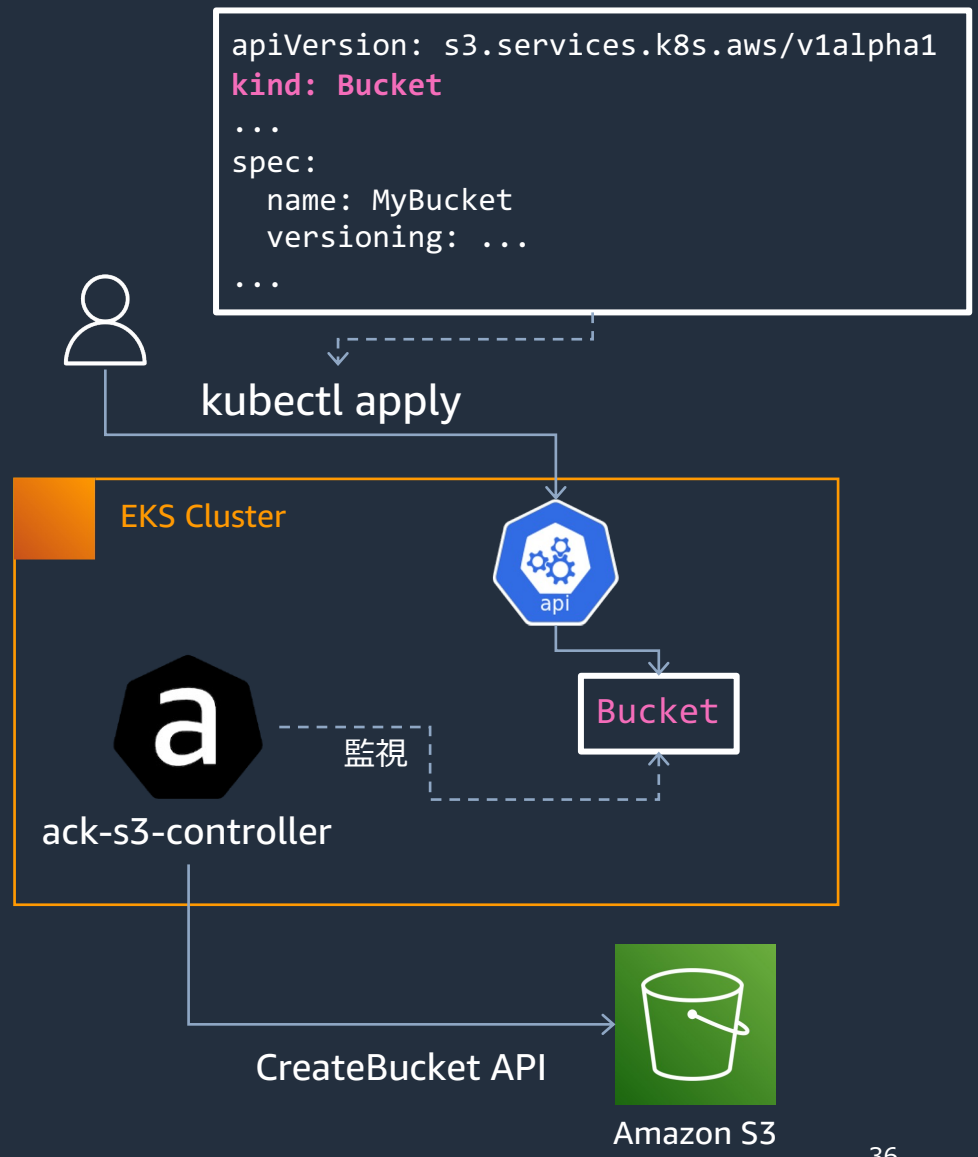
月/日	Update Title	関連 URL
01/04	Amazon EMR on EKS がカスタム Docker コンテナイメージのテストを簡素化するカスタムイメージ検証ツールをリリース	• what's new
01/05	Amazon EMR on EKS が、デバッグを簡素化するために DescribeJobRun API 応答にエラーメッセージの詳細を追加	• what's new
01/05	Amazon EMR on EKS が AWS Graviton ベースの EC2 インスタンス用にカスタマイズされたコンテナイメージのサポートを追加	• what's new
01/06	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	• what's new
02/25	AWS App Mesh が Agent for Envoy を導入	• what's new
03/28	AWS App Mesh Envoy Management Service (EMS) が AWS CloudTrail 統合をサポート	• what's new
04/07	Amazon MemoryDB 向け AWS Controllers for Kubernetes プレビューの発表	• what's new
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	• what's new

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	• release note
👉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	• what's new
👉04/20	EKS Blueprints の発表	• blog
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	• what's new
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	• what's new
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	• what's new

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/



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 クラスター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-blu
...
  cluster_version = "1.21"
...
  managed_node_groups = {
...
  }
}

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

  eks_cluster_id = module.eks_blueprints.eks_cluste

  # EKS Add-ons
  enable_amazon_eks_vpc_cni            = true
  enable_amazon_eks_coredns            = true
...

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

Thank you!