Google Cloud

# 忙しい人のための Google Cloud Next ‘22 Recap (Application Modernization 編)

Google Cloud
アプリケーション モダナイゼーション スペシャリスト
内間 和季

Table of Contents

01

# ソフトウェア サプライチェーン

# Software Delivery Shield

ソフトウェア サプライ チェーンのセキュリティを強化する
フルマネージドのエンド ツー エンド ソリューション

ポリシー

開発

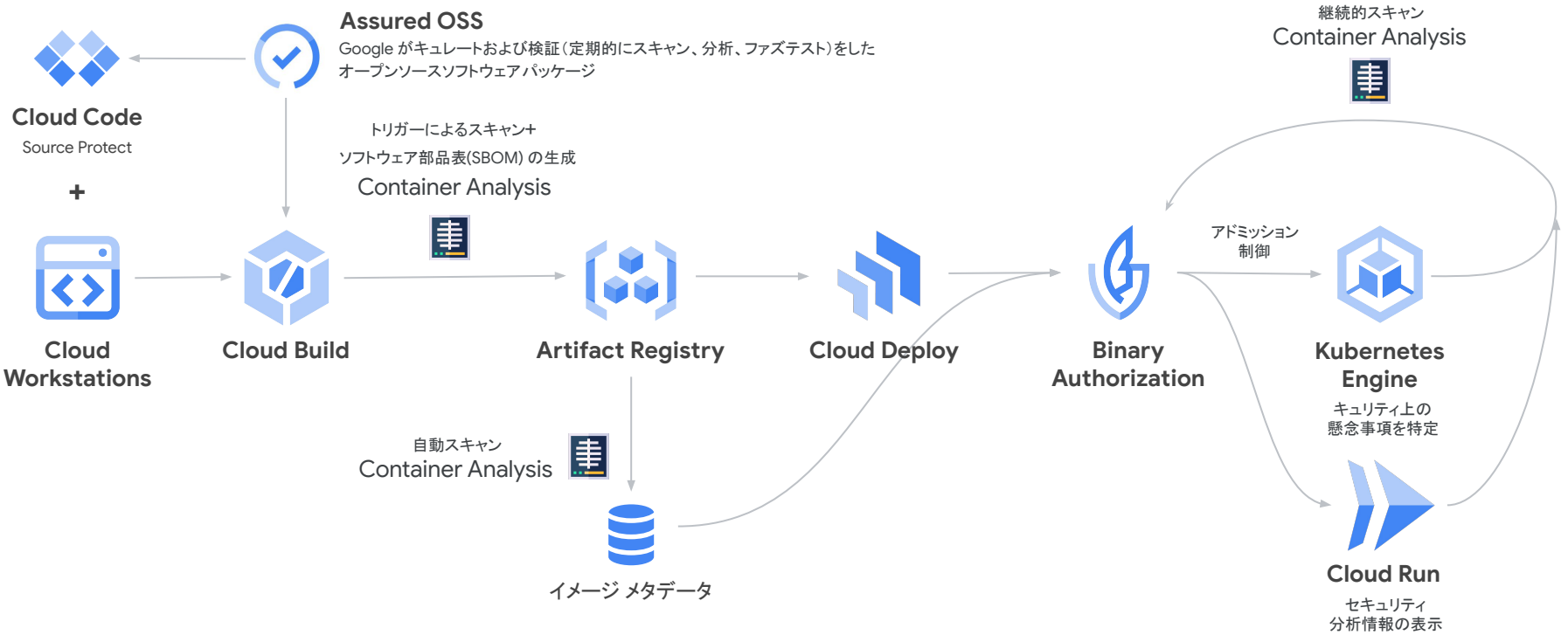
サプライ

CI / CD

実行環境

Google Cloud

# Software Delivery Shield を構成する Google Cloud のサービス群

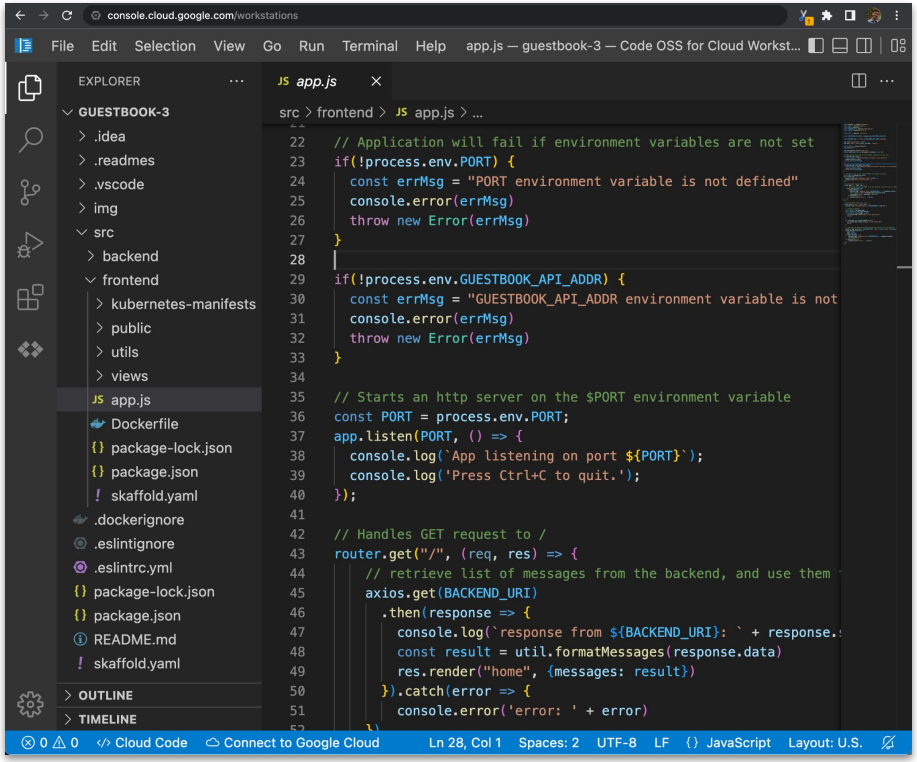


Public Preview

# フルマネージドな開発環境

## Cloud Workstations

- どこからでも接続できるオンデマンド環境
- セキュリティ ポリシーの設定
- マネージド ベースイメージ
- VPC Service Controls 対応

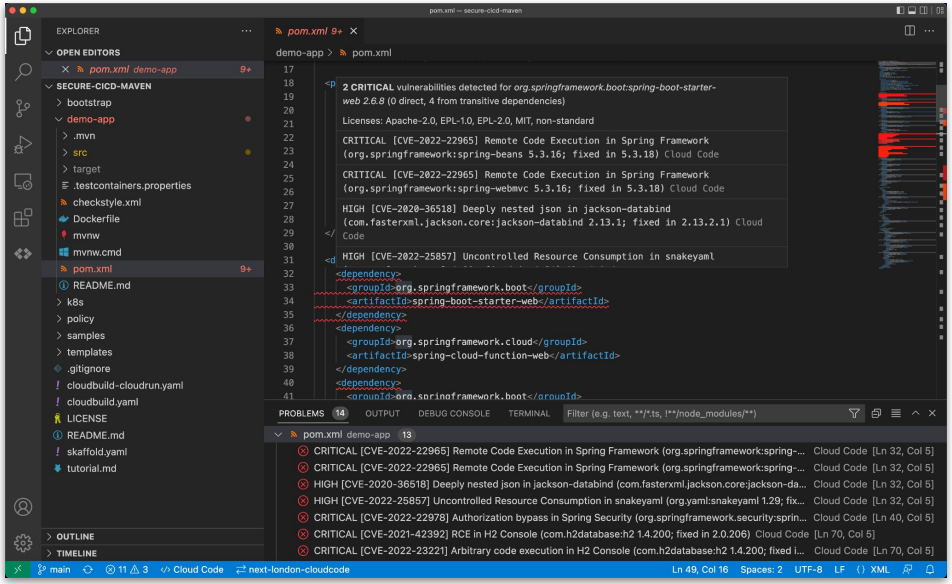


Public Preview

# IDE でのセキュリティ支援

## Cloud Code source protect

- コーディング中の脆弱性検知
- 遷移的依存関係のスキャンもサポート
- 依存するライセンスに関するレポート



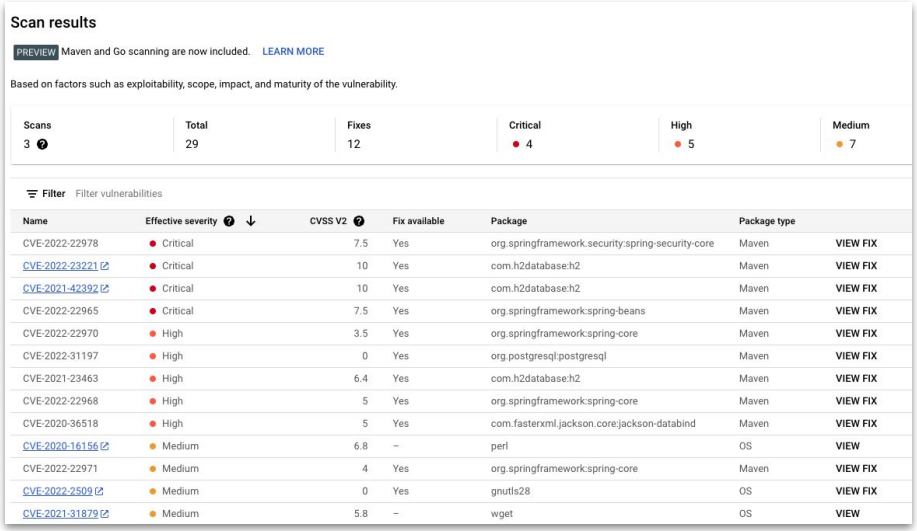
Public Preview

# 依存関係とアーティファクトのセキュリティ改善

## Artifact Registry & Container Analysis

## Assured Open Source Software

- 250 を超える Java と Python の
  キュレートおよび検証済みパッケージの提供
- 各種リポジトリの利用
  - **Private** repos
  - **Remote** repos: upstream の依存関係を
    キャッシュし、脆弱性もスキャン
  - **Virtual** repos: 一つのエンドポイントで
    Private と Remote を検索順序つきで統合
- Maven と Go の脆弱性スキャン
- ソフトウェア部品表 (SBOM) の生成



Scan results

PREVIEW Maven and Go scanning are now included. LEARN MORE

Based on factors such as exploitability, scope, impact, and maturity of the vulnerability.

| Scans | Total | Fixes | Critical | High | Medium |
|---|---|---|---|---|---|
| 3 | 29 | 12 | 4 | 5 | 7 |

Filter Filter vulnerabilities

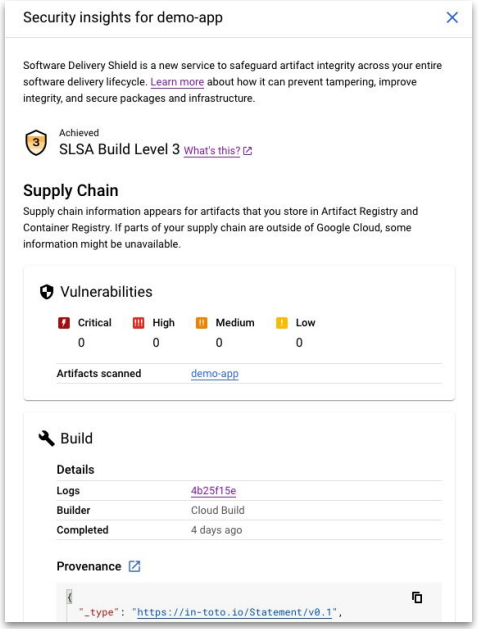
| Name | Effective severity | CVSS V2 | Fix available | Package | Package type | |
|---|---|---|---|---|---|---|
| CVE-2022-22978 | Critical | 7.5 | Yes | org.springframework.security:spring-security-core | Maven | VIEW FIX |
| CVE-2022-23221 | Critical | 10 | Yes | com.h2database:h2 | Maven | VIEW FIX |
| CVE-2021-42392 | Critical | 10 | Yes | com.h2database:h2 | Maven | VIEW FIX |
| CVE-2022-22965 | Critical | 7.5 | Yes | org.springframework:spring-beans | Maven | VIEW FIX |
| CVE-2022-22970 | High | 3.5 | Yes | org.springframework:spring-core | Maven | VIEW FIX |
| CVE-2022-31197 | High | 0 | Yes | org.postgresql:postgresql | Maven | VIEW FIX |
| CVE-2021-23463 | High | 6.4 | Yes | com.h2database:h2 | Maven | VIEW FIX |
| CVE-2022-22968 | High | 5 | Yes | org.springframework:spring-core | Maven | VIEW FIX |
| CVE-2020-36518 | High | 5 | Yes | com.fasterxml.jackson.core:jackson-databind | Maven | VIEW FIX |
| CVE-2020-16156 | Medium | 6.8 | – | perl | OS | VIEW |
| CVE-2022-22971 | Medium | 4 | Yes | org.springframework:spring-core | Maven | VIEW FIX |
| CVE-2022-2509 | Medium | 0 | Yes | gnutls28 | OS | VIEW FIX |
| CVE-2021-31879 | Medium | 5.8 | – | wget | OS | VIEW |

Public Preview

# CI パイプラインのセキュリティ強化

## Cloud Build

- SLSA Level 3 のビルドをサポート
- コンテナ化アプリケーションと
  Maven および Python パッケージの
  認証済み & 改ざんできないビルド来歴の生成
- セキュリティに関する分析情報の表示
  - SLSA レベル
  - 脆弱性
  - 来歴など
- ビルドをトリガーできる外部サービスの制御
- VPC Service Controls 対応



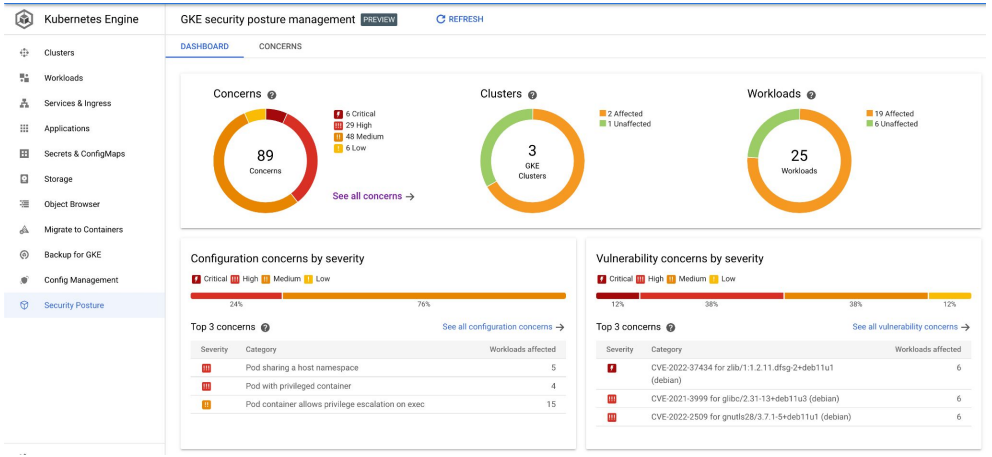
Public Preview

# 実行時のセキュリティ分析

## GKE security posture

## Cloud Run security insights

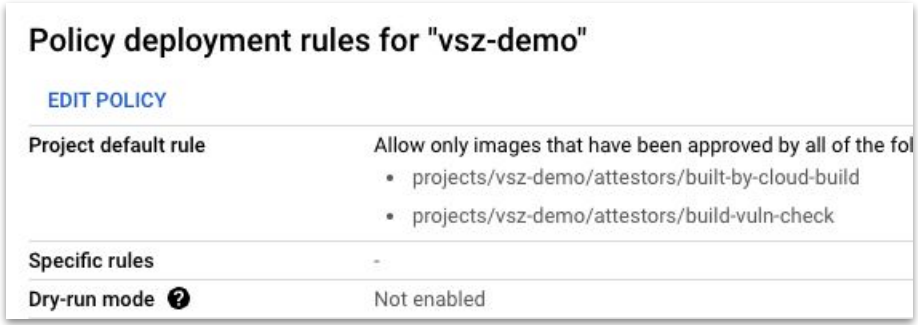
- GKE: 継続的な実行時脆弱性・設定スキャン
- Cloud Run: セキュリティ分析情報の表示
  - ターゲットレベル
  - 脆弱性
  - ビルド来歴



# 信頼ベースのポリシー

Binary Authorization

- 信頼ベースの開発ライフサイクルポリシー
  - 例 1. ホスト名が前方一致したイメージのみのデプロイを許可
  - 例 2. 署名したイメージのみを許可
- アプリケーション実行時のポリシー強制



02

# Cloud Functions

GA

# Cloud Functions 2nd gen（第 2 世代）

## より多くのコンピュート

より多くの CPU やメモリ割り当てが必要なワークロードにも対応

## より多くのイベント

より多くの Google Cloud サービスやサードパーティ製品とのインテグレーション

## よりコントロール可能に

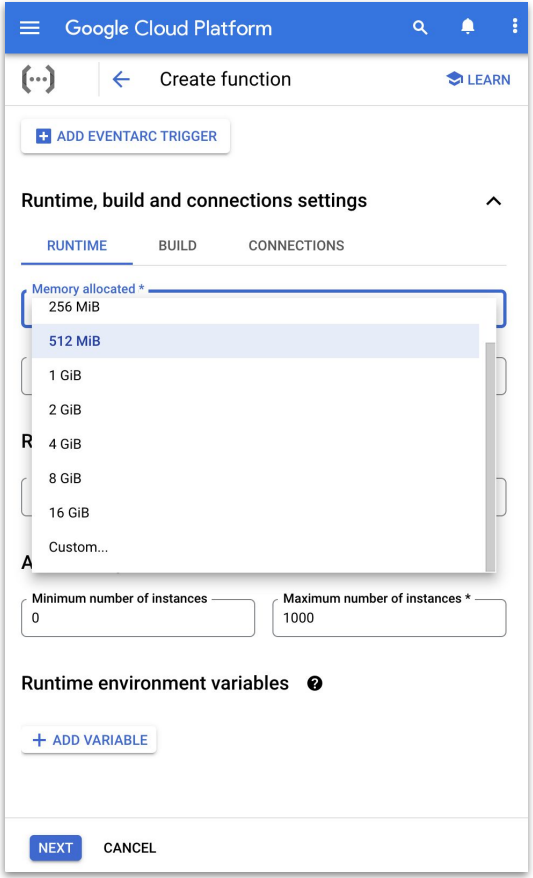
コストやパフォーマンス要件に合うような構成や制御がしやすく

Cloud Functions

# リソース上限の向上

最大で 8 vCPU、32 GiB メモリを構成することが可能に

より多くの CPU やメモリ割り当てが必要なワークロードもサポート

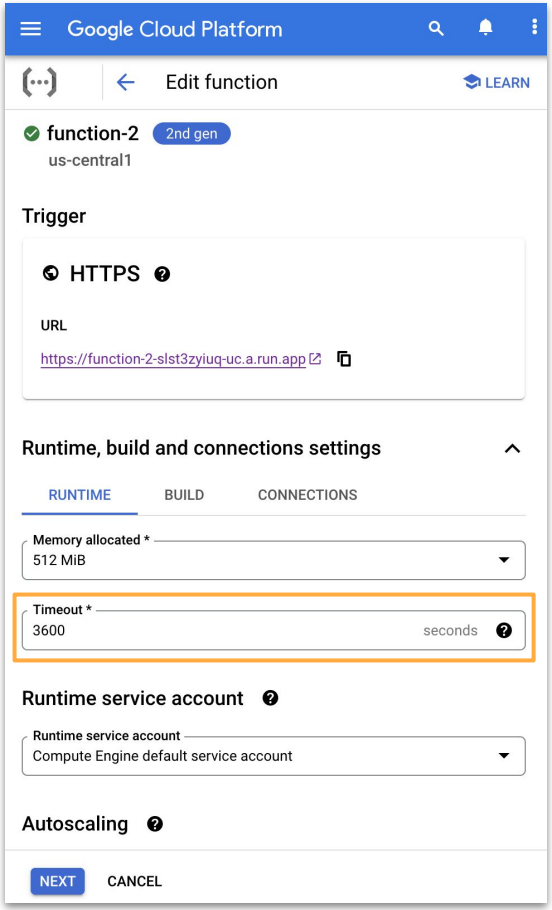


Cloud Functions

# タイムアウト値が 6 倍に

HTTP トリガーの関数で最大 60 分のタイムアウト値を構成可能に

処理完了まで時間のかかっていたワークロードもサポート



Cloud Functions

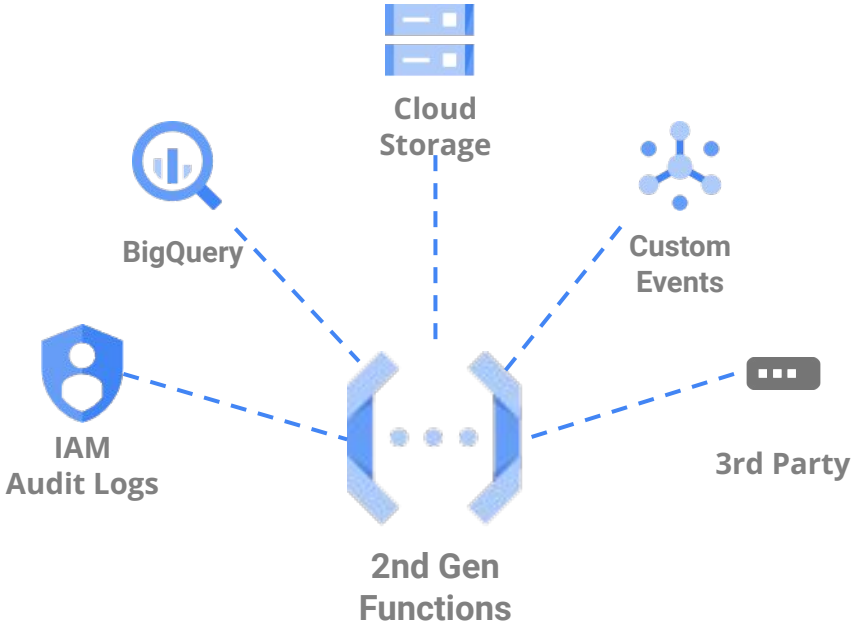
# 10 倍のイベントソース

125 以上の Google Cloud イベントソースをサポート

Audit Log による Google Cloud プロダクトのサポートを 10 倍以上拡大

4 社のパートナー企業から追加のサードパーティ イベントをサポート

オープンソースの CloudEvent 仕様を利用可能に



# BigQuery リモート関数

Cloud Functions を使って BigQuery のリモート関数を作成

Google Cloud AI/ML や Vertex APIs 等も含んだ外部 API とのインテグレーションが可能に

JavaScript や Python, Java 等 7 つの言語をサポート

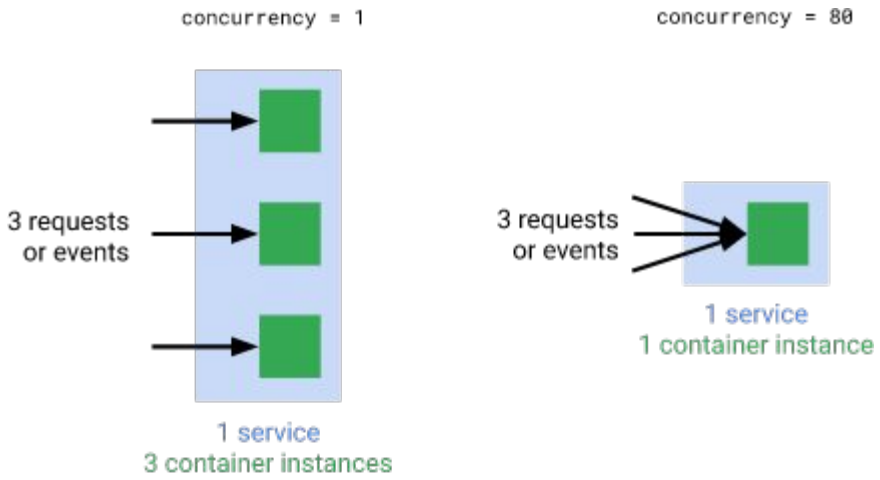
```
CREATE FUNCTION `project`.`table`.`bq-function-name`(
      input INT
) RETURNS BOOL
REMOTE WITH CONNECTION 'your-connection'
OPTIONS (endpoint =
'https://your-cloud-function-url');
```

# 同時実行

インスタンス毎に 1,000 同時実行までサポート

コールドスタートを回避することができ、パフォーマンスの改善が期待できる

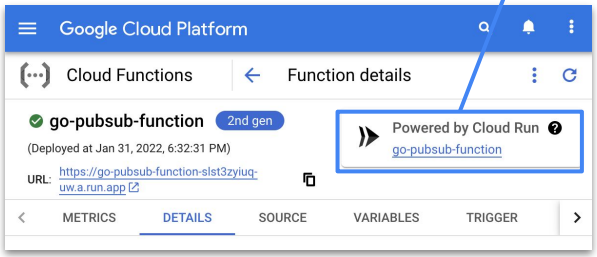
CPU やメモリリソースを複数の呼び出しで共有することにより、コストの削減にも繋がる

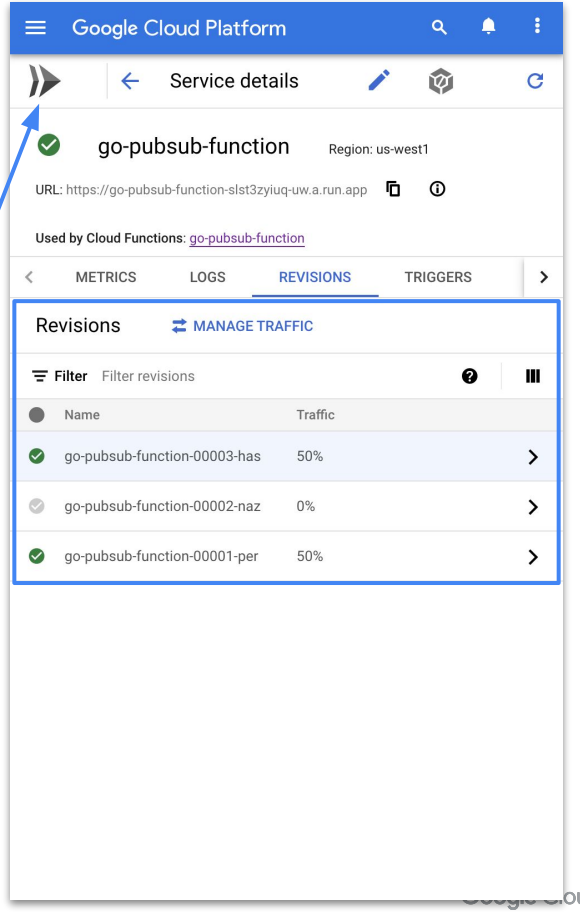


# 簡単なロールバック

デプロイメント毎に新しいリビジョンが自動的に作られており、簡単に以前のリビジョンにロールバックすることができる

トラフィックの分割機能により、最新バージョンへ段階的に移行することも可能



03

# Cloud Run

Cloud Run

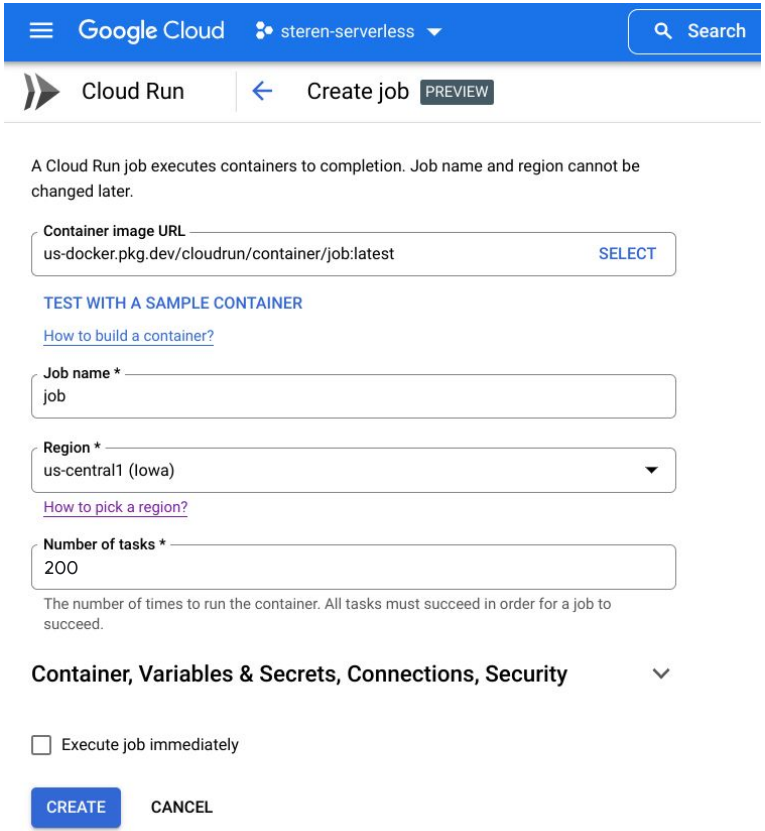
# Jobs

Public Preview

データ処理のユースケースで活用

- スケジュールされたスクリプト
- バックグラウンド処理
- バッチデータ処理

全ての Google Cloud リージョンで利用可能



Public Preview

# ヘルスチェック


## Startup probe

**コンテナがトラフィックを受信できる状態か？**

Protocol: TCP, HTTP or gRPC

例:

- 機械学習モデルのロード
- 初期化のために非同期ライブラリを待機

デフォルトの TCP probe では $PORT がリッスンできているかを確認する

## Liveness probe

**コンテナが健全な状態か？そうでなければ再起動する**

Protocol: HTTP or gRPC

例:

- データベースとのコネクションが切断されたら再起動する
- ローカルステートの破損から復旧する
- N 分後に強制的に再起動する

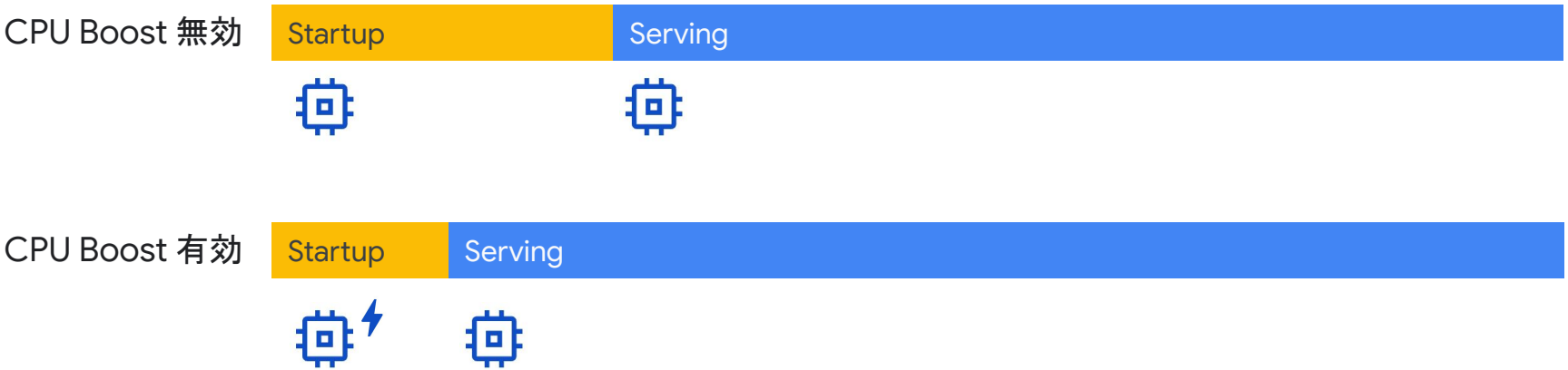
Cloud Run

Public Preview

# Startup CPU Boost

コンテナ起動時に一時的に CPU 割り当てを増加させることにより、起動速度を向上させる

CPU Boost 機能を有効化すると、起動時に Boost された CPU 分の料金が追加で課金される



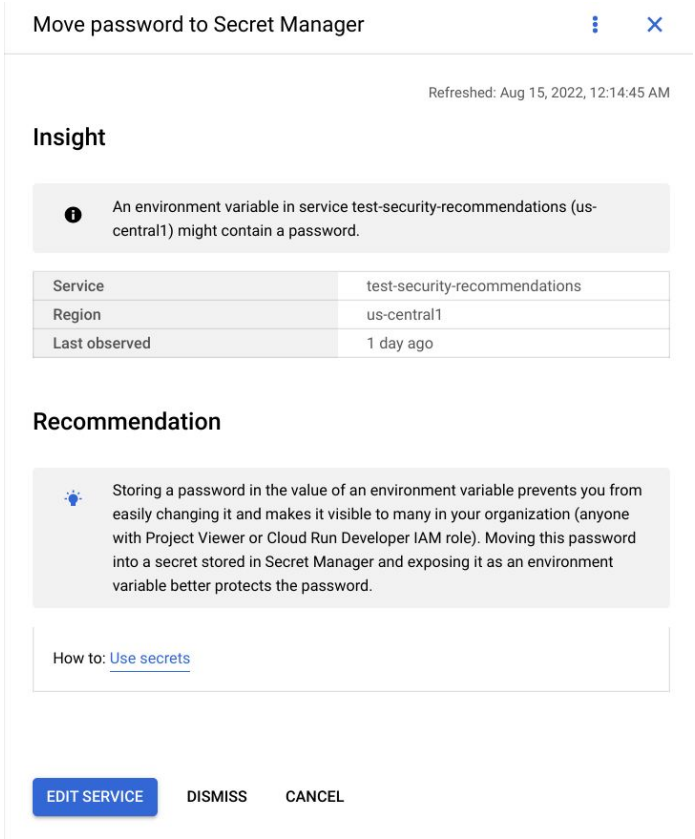
Cloud Run

Public Preview

# Security Recommendations

Cloud Run サービスに対するプロアクティブな推奨事項の提供

デフォルト サービスアカウントの利用や、パスワードや API キーなどの機密データが含まれている可能性のある環境変数等を検出し、よりセキュアな構成方法を推奨する

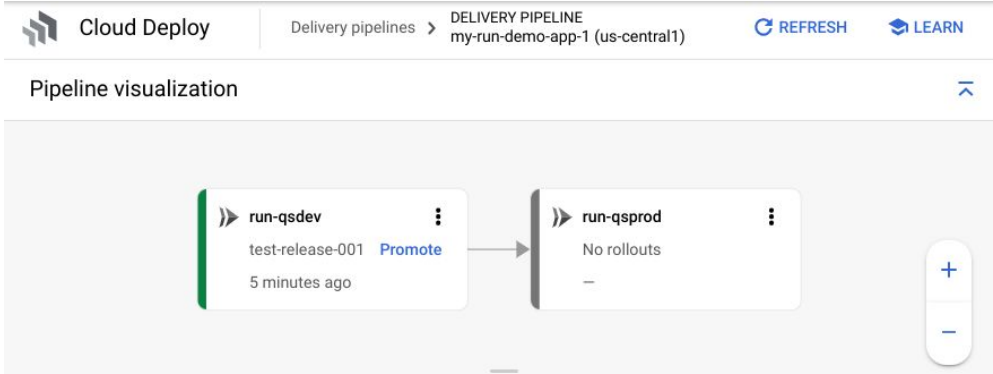


# Cloud Deploy サポート

Public Preview

Cloud Deploy のデプロイターゲットとして
Cloud Run を選択することが可能に

Knative マニフェストでデプロイする Cloud Run サービス仕様を定義




```
apiVersion: deploy.cloud.google.com/v1
kind: Target
metadata:
 name: dev
description: development service
run:
  location: projects/my-app/locations/us-central1
```

Cloud Run

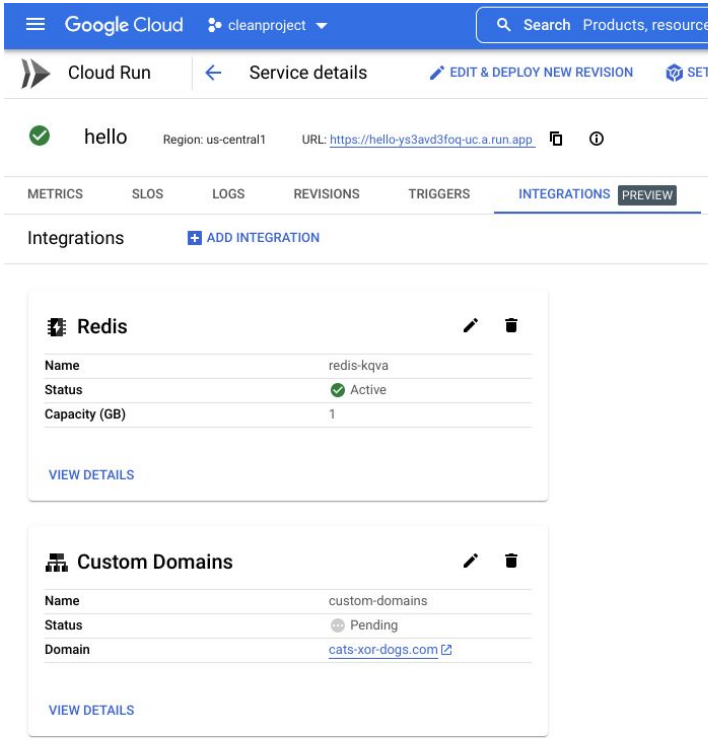
# Integrations

Public Preview

数クリック / 1 つのコマンドで Cloud Run と他サービスの連携が可能に

現在対応しているサービス

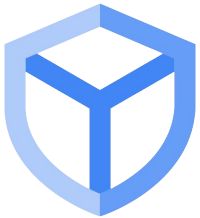
- Redis - Memorystore
- Custom Domains - Google Cloud Load Balancing



04

# Google Kubernetes Engine (GKE)

Public Preview

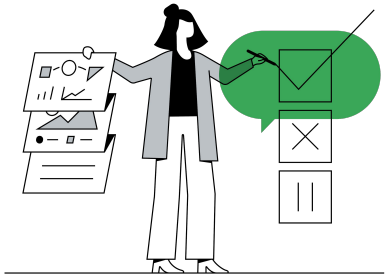


# GKE Security Posture Management

Google Cloud

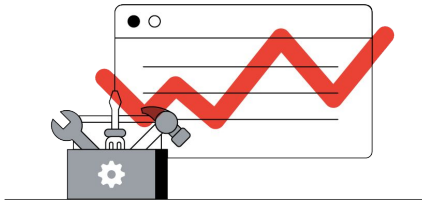
Google Kubernetes Engine

# GKE Security Posture Management



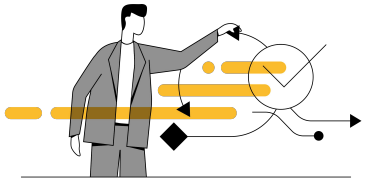
## セキュリティ ガイダンス

実行可能なセキュリティ ガイダンスを提供することで、 要求される Kubernetes セキュリティの知識を最小化



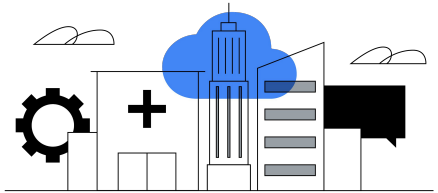
## ビルトイン ツール

GKE がビルトインのセキュリティツールを提供することで、セキュリティツールの乱立を回避



## 可視化

環境全体の統合的なビューとコントロールを提供



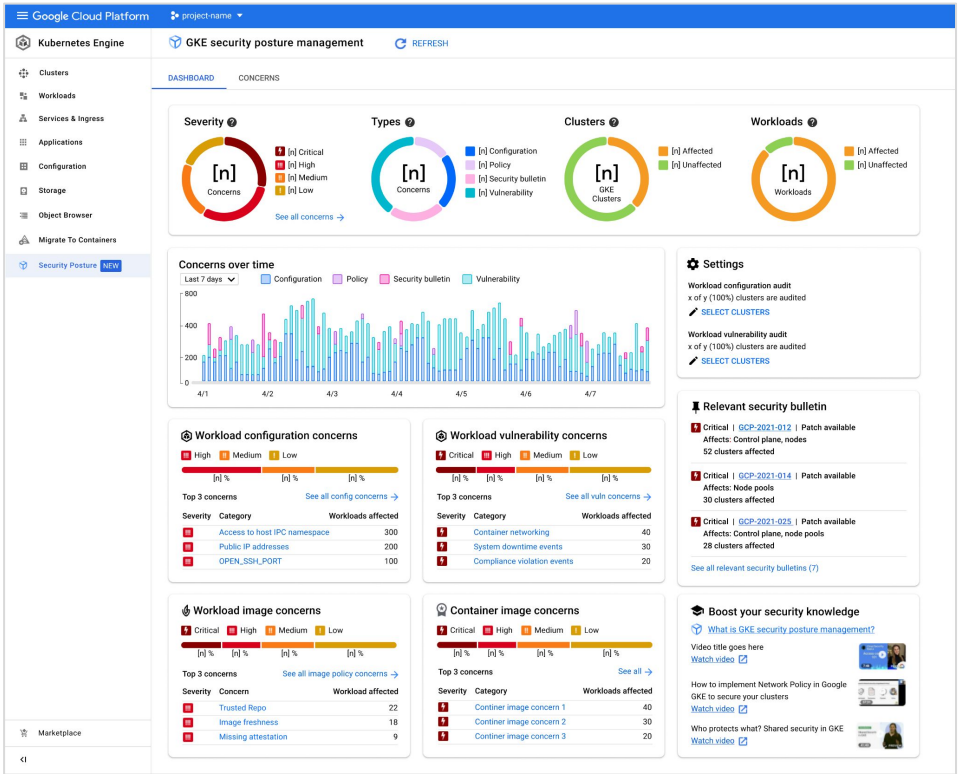
## GKE 機能の一部

GKE に含まれている機能なので、追加費用なしで利用可能

Google Kubernetes Engine

# 分かりやすいダッシュボード

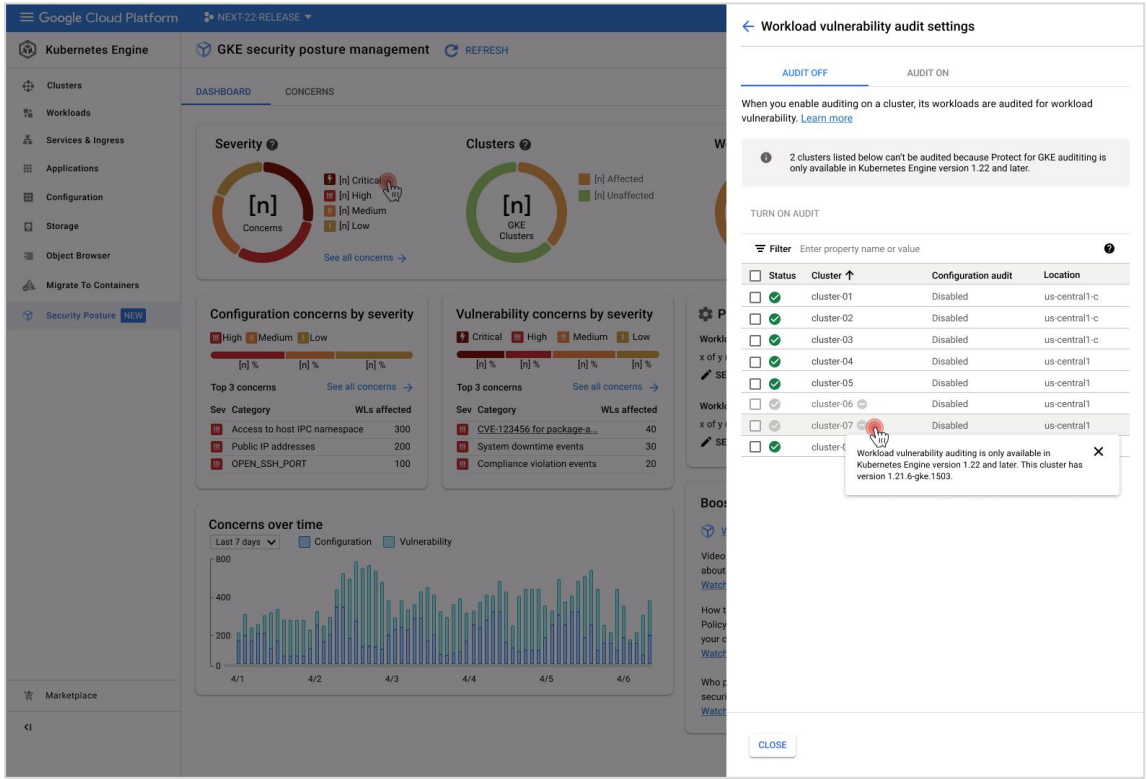
一目でセキュリティに関する懸念事項や
傾向が分かりやすいダッシュボード



Google Kubernetes Engine

# 細かなチューニングや管理が不要

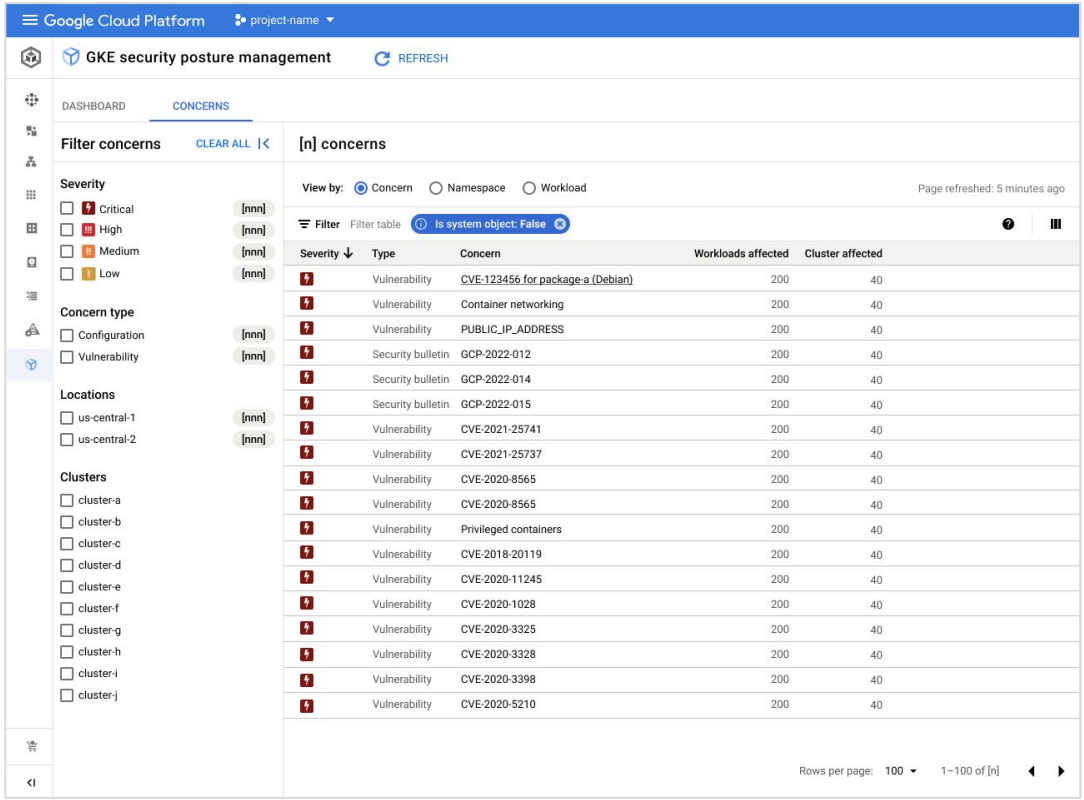
クラスタ毎に Security Posture 機能を有効化



Google Kubernetes Engine

# リスク指向

全ての表面化した懸念事項は重大度でカテゴリされており、具体的な推奨事項（対処方法）も提示



# ワークロード構成スキャン

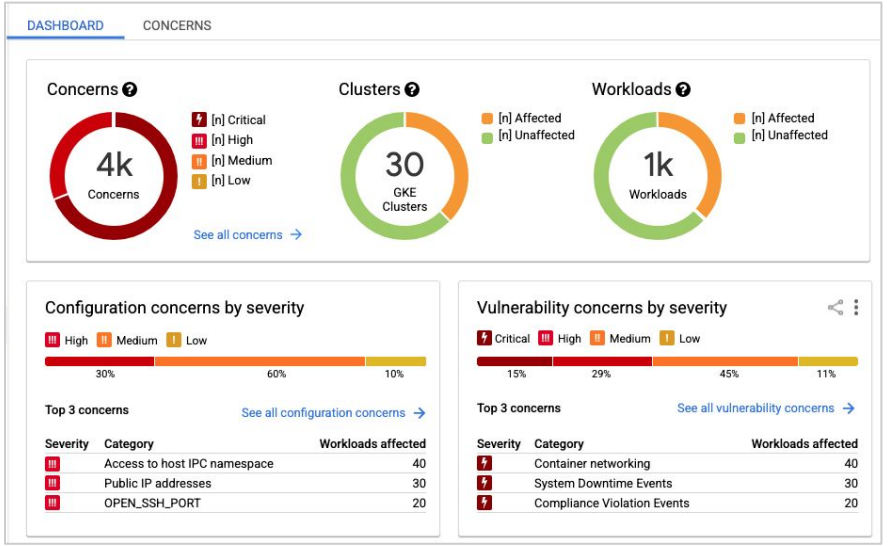
ワークロードの構成を自動的にスキャンし、

**Kubernetes のベストプラクティスに沿っていない、潜在的なリスクがあるワークロードを報告**

発見された懸念事項は Cloud Console ダッシュボードや Cloud Logging のログエントリーから確認可能

検知するリスクの例:

- ホストのネームスペースの共有
- 特権コンテナの利用
- runAsNonRoot が有効になっていない
- 権限昇格が可能になっている



# Blue / Green アップグレード

Node レベル Blue / Green アップグレードの一連の手順を自動的に実行

問題発生時のロールバックを迅速に行うことが可能


*1 デフォルト 1 時間 (3,600 秒)、最大 7 日間 (604,800 秒)

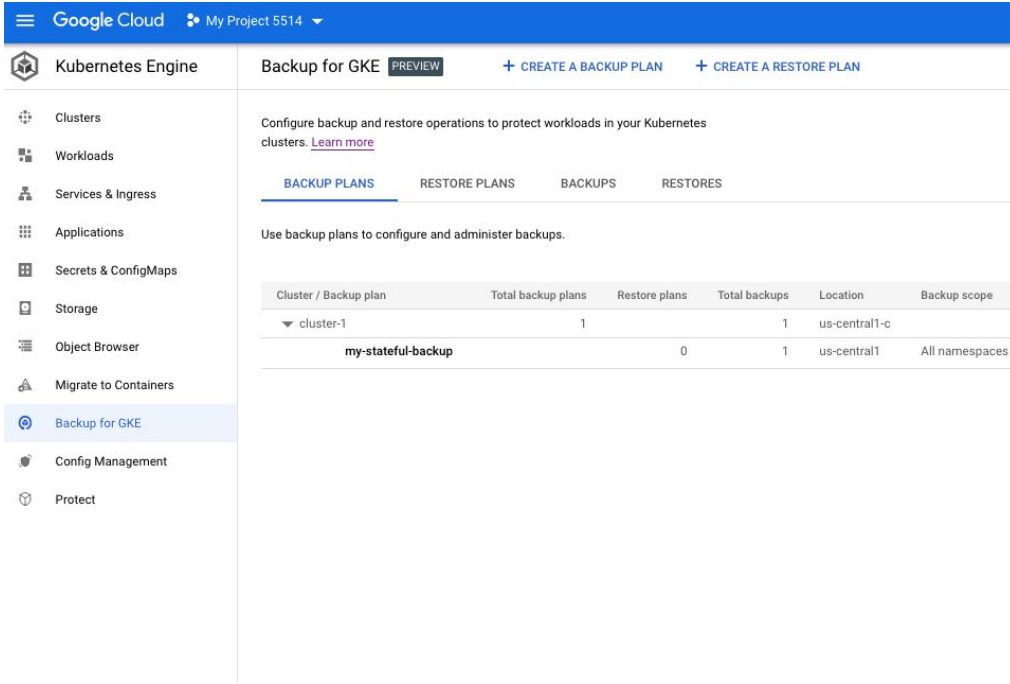
Google Kubernetes Engine

GA

# Backup for GKE

## GKE 上のワークロードのバックアップ・リストア機能を提供

- バックアップ・リストアプランのきめ細かな制御
- IAM ベースのポリシーコントロール
- 同一クラスタもしくは別クラスタへのリストア



Google Kubernetes Engine

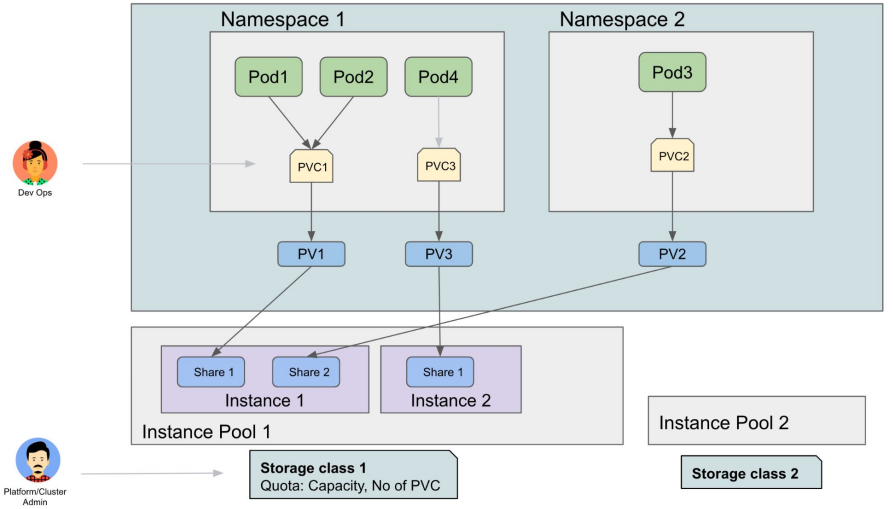
GA

# Filestore multishares for GKE

1 つの Filestore instance を複数の Persistent Volume で共有できるように

PV あたりのサイズも最小 100 GB から利用可能に

（以前までは PV の最小サイズが 1 TB）



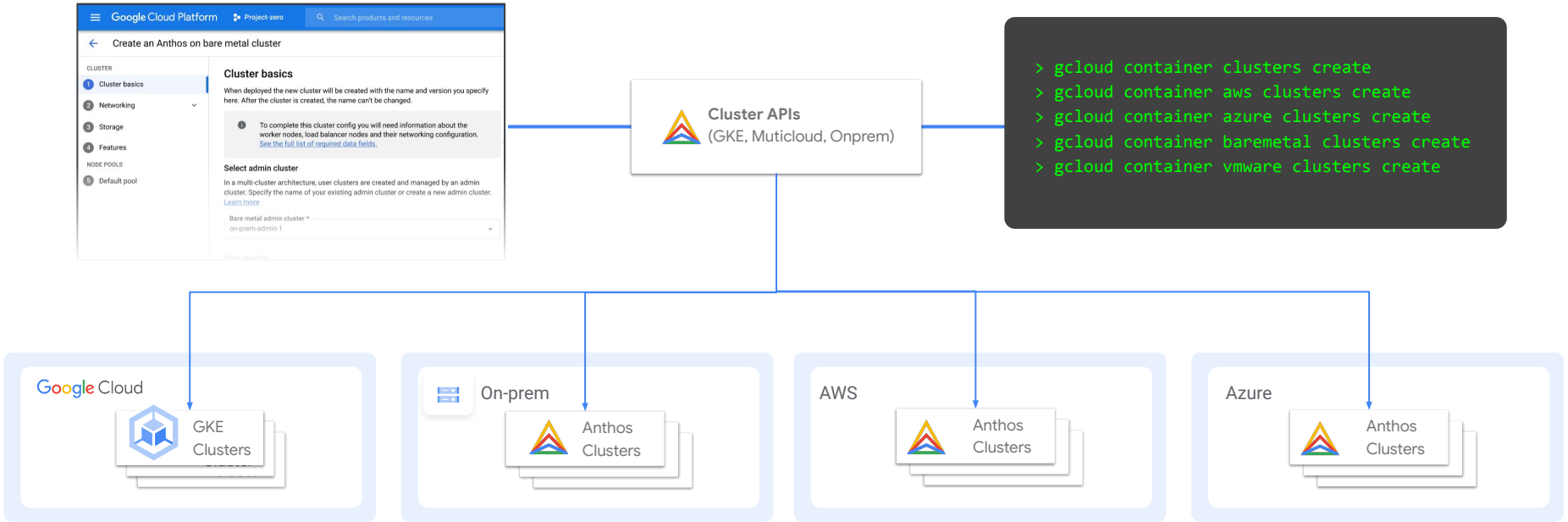
05

# Anthos

Anthos

# コンソールや API によるクラスタ ライフサイクル管理

Anthos clusters のライフサイクル（構築 / アップグレード等）を gcloud コマンドや
Google Cloud コンソールから管理

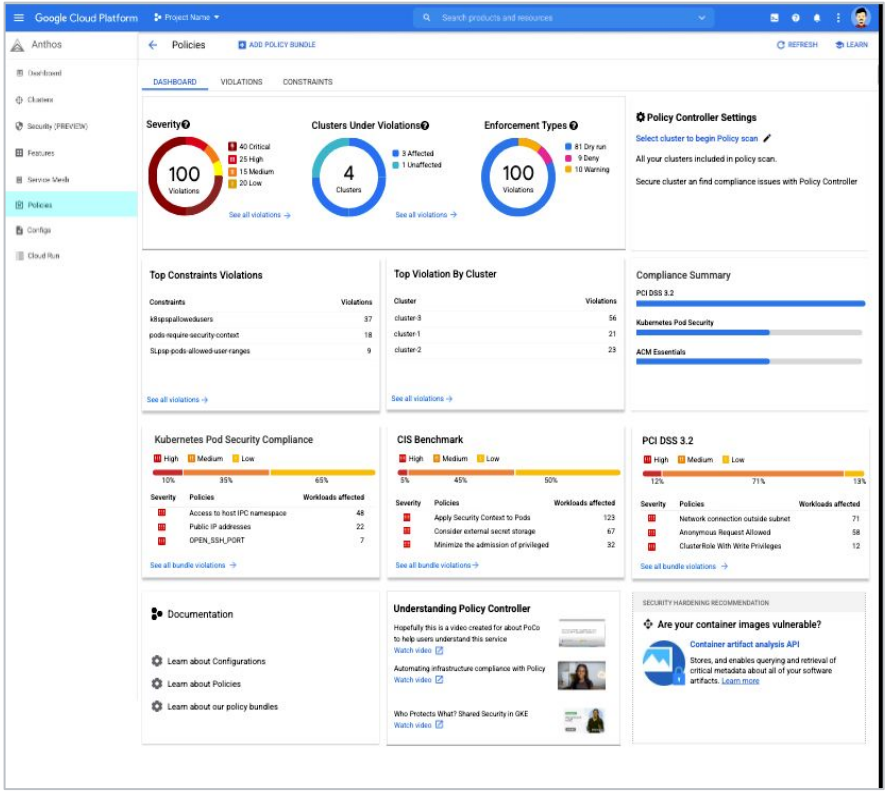


Anthos

# 新しい Policy Controller UI

Policy Controller によりセキュリティやコンプライアンス違反を防止

コンプライアンス準拠状況や重大な制約違反のハイライトをコンソール上から確認可能に



# Anthos for VMs

- 仮想マシンとコンテナで統合された開発・運用体験を提供
- 開発者がセルフサービスで仮想マシンをプロビジョニング
- 仮想マシンの宣言的なデプロイ
- ポリシー強制による一貫したコンプライアンス

# Thank you.

Google Cloud