

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

ソフトウェア サプライチェーン	01
Cloud Functions	02
Cloud Run	03
Google Kubernetes Engine (GKE)	04
Anthos	05

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

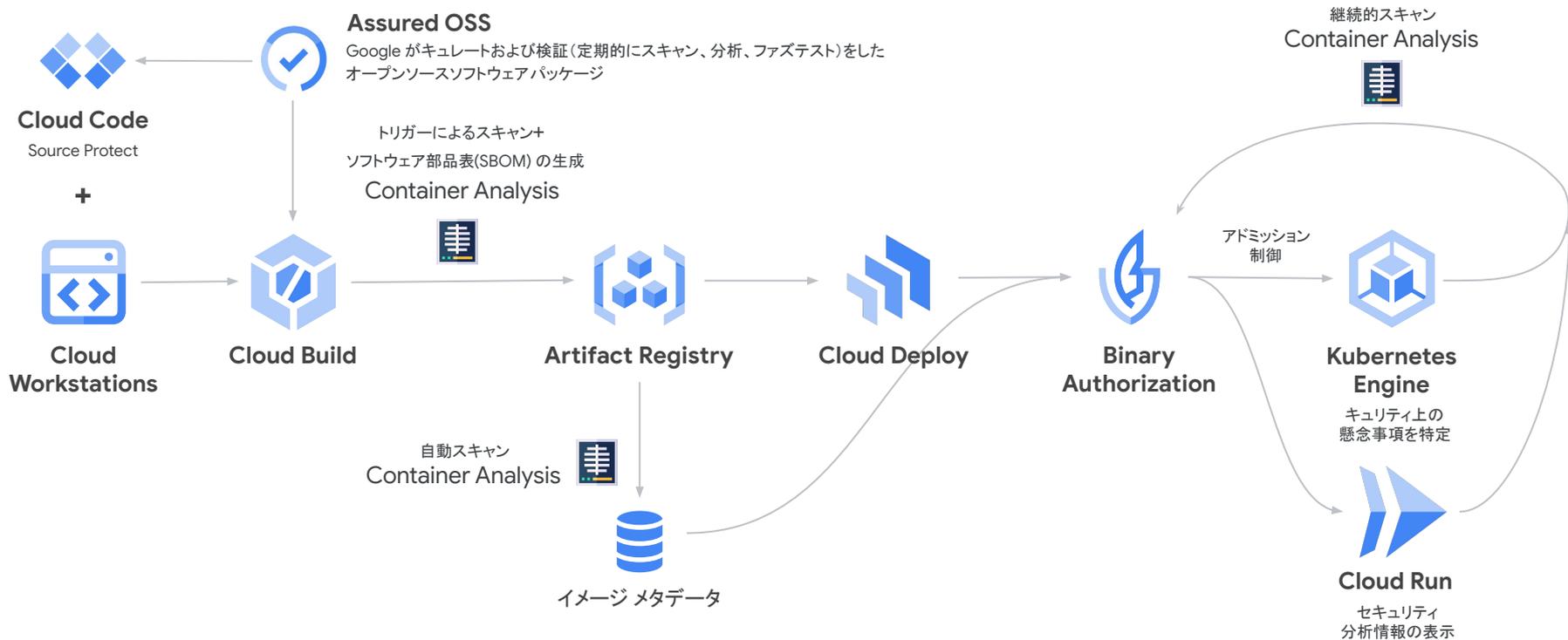
開発

サプライ

CI / CD

実行環境

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



フルマネージドな開発環境



Cloud Workstations

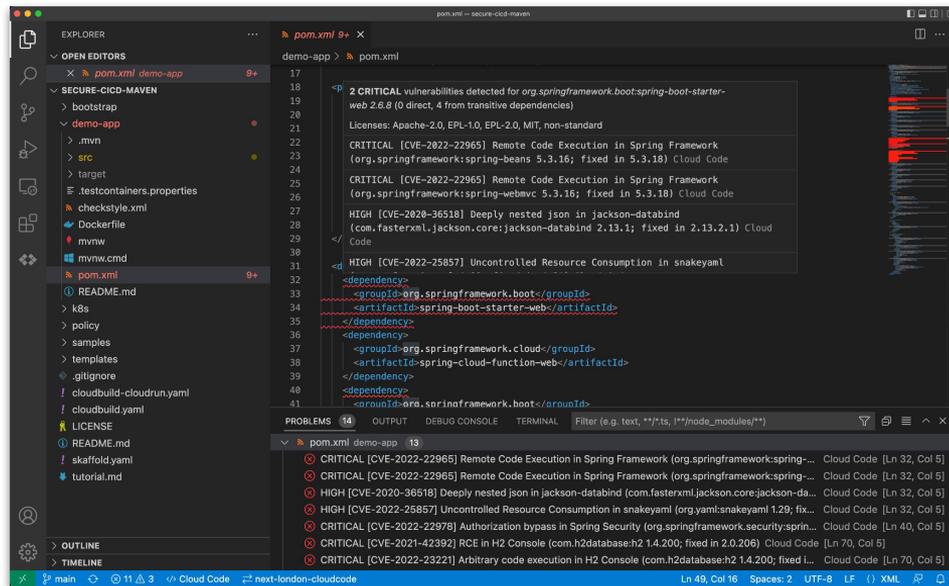
- どこからでも接続できるオンデマンド環境
- セキュリティポリシーの設定
- マネージド ベースイメージ
- VPC Service Controls 対応

```
src > frontend > JS app.js > ...
22 // Application will fail if environment variables are not set
23 if(!process.env.PORT) {
24   const errMsg = "PORT environment variable is not defined"
25   console.error(errMsg)
26   throw new Error(errMsg)
27 }
28
29 if(!process.env.GUESTBOOK_API_ADDR) {
30   const errMsg = "GUESTBOOK_API_ADDR environment variable is not
31   console.error(errMsg)
32   throw new Error(errMsg)
33 }
34
35 // Starts an http server on the $PORT environment variable
36 const PORT = process.env.PORT;
37 app.listen(PORT, () => {
38   console.log(`App listening on port ${PORT}`);
39   console.log('Press Ctrl+C to quit.');
```

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



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 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	gnuts28	OS	VIEW FIX
CVE-2021-31879	Medium	5.8	-	wget	OS	VIEW

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

Security insights for demo-app

Software Delivery Shield is a new service to safeguard artifact integrity across your entire software delivery lifecycle. [Learn more](#) about how it can prevent tampering, improve integrity, and secure packages and infrastructure.

Achieved
SLSA Build Level 3 [What's this?](#)

Supply Chain
Supply chain information appears for artifacts that you store in Artifact Registry and Container Registry. If parts of your supply chain are outside of Google Cloud, some information might be unavailable.

Vulnerabilities

Critical	High	Medium	Low
0	0	0	0

Artifacts scanned: [demo-app](#)

Build

Details

Logs	4b25f15e
Builder	Cloud Build
Completed	4 days ago

Provenance [View](#)

```
..._type": "https://in-toto.io/Statement/v0.1",
```

実行時のセキュリティ分析

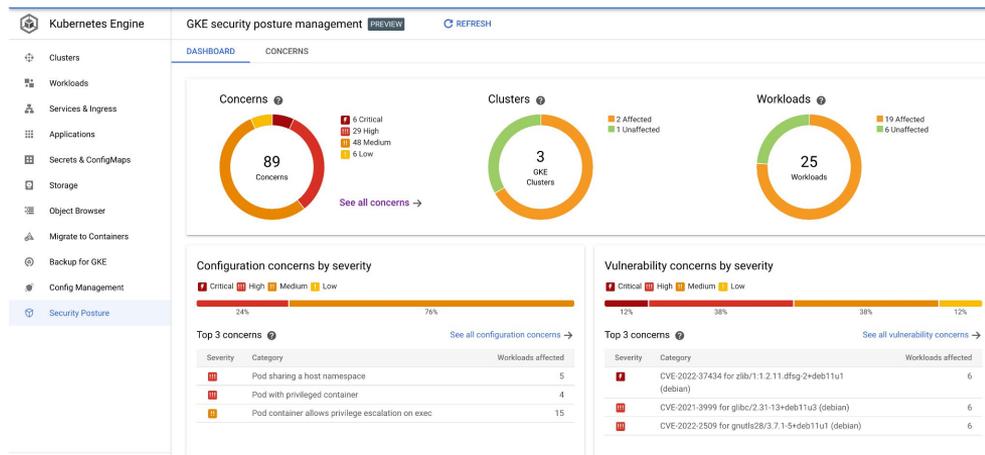


GKE security posture



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

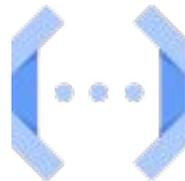
- 信頼ベースの開発ライフサイクルポリシー
 - 例 1. ホスト名が前方一致したイメージのみのデプロイを許可
 - 例 2. 署名したイメージのみを許可
- アプリケーション実行時のポリシー強制

Policy deployment rules for "vsz-demo"	
EDIT POLICY	
Project default rule	Allow only images that have been approved by all of the following attestors: <ul style="list-style-type: none">• projects/vsz-demo/attestors/built-by-cloud-build• projects/vsz-demo/attestors/build-vuln-check
Specific rules	-
Dry-run mode	Not enabled

02

Cloud Functions

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

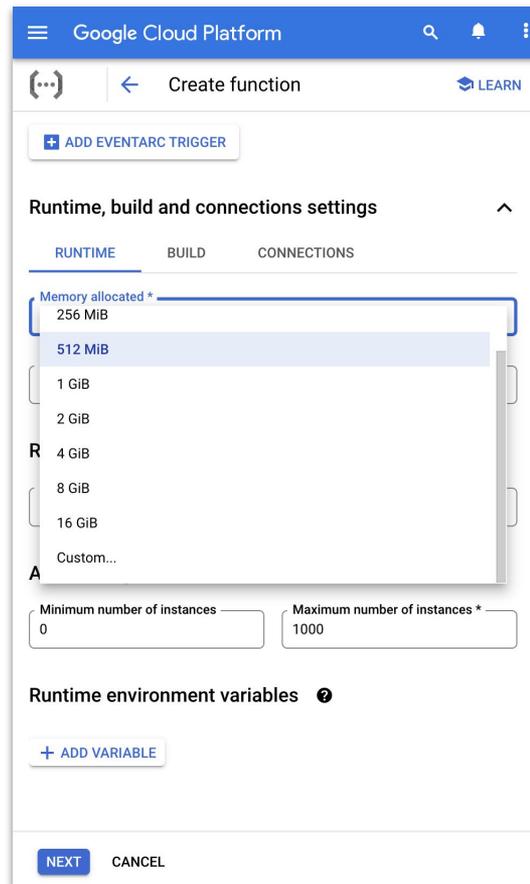
よりコントロール可能に

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

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

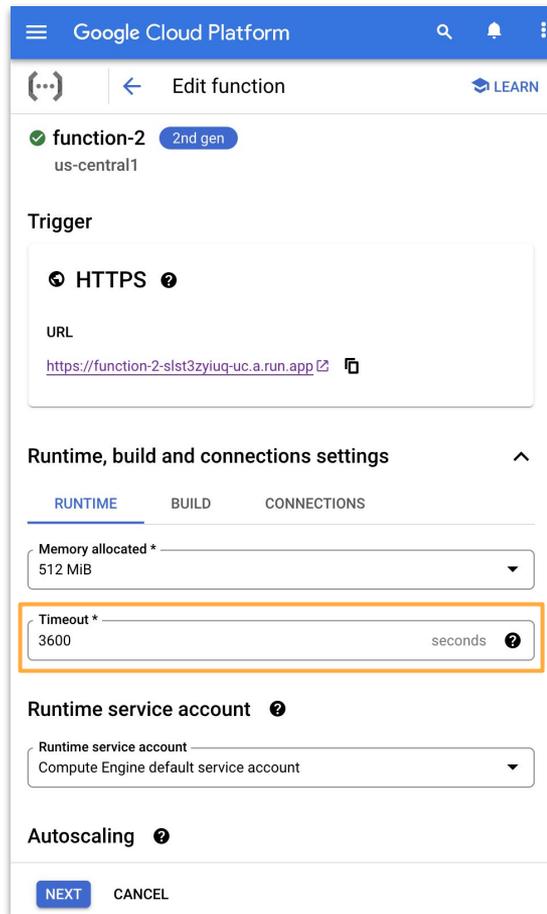
より多くの CPU やメモリ割り当てが必要なワークロードもサポート



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



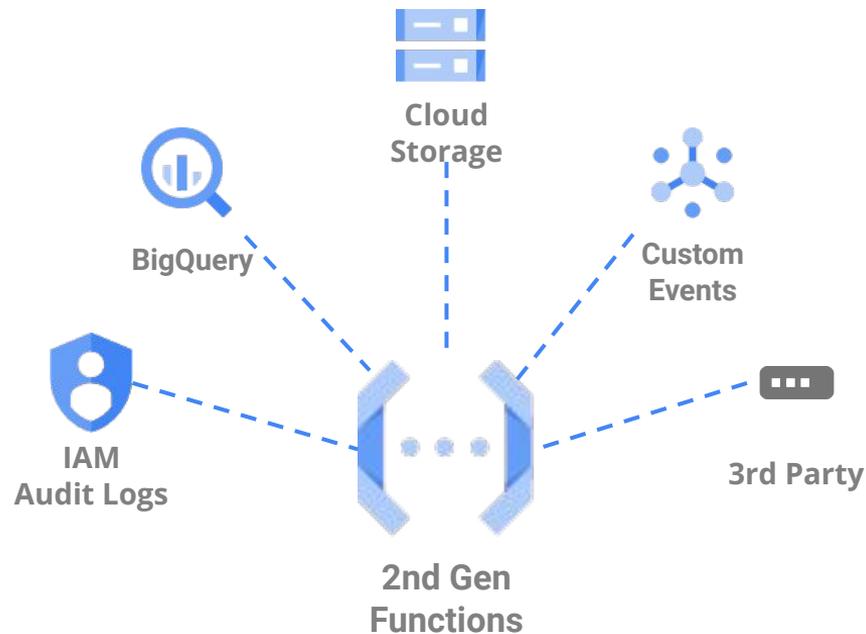
10 倍のイベントソース

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

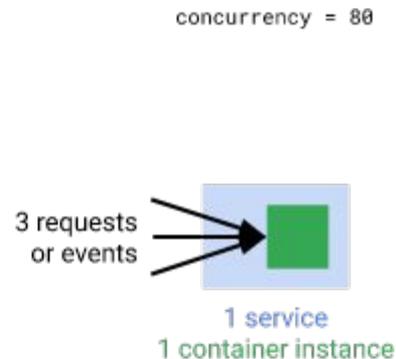
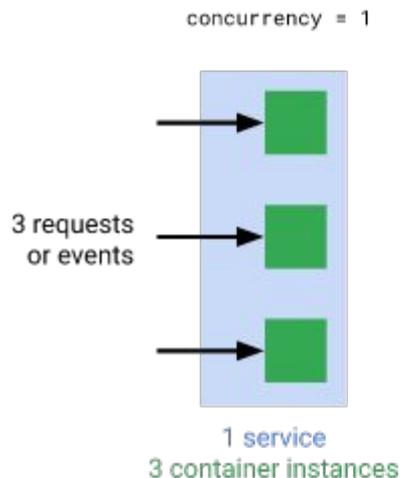
```
CREATE FUNCTION `project`.`table`.`bq-function-name`(  
    input INT  
  ) RETURNS BOOL  
  REMOTE WITH CONNECTION 'your-connection'  
  OPTIONS (endpoint =  
    'https://your-cloud-function-url');
```

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

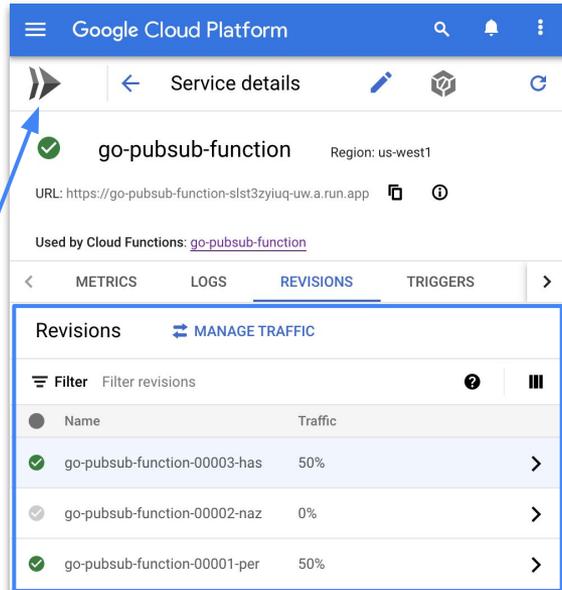
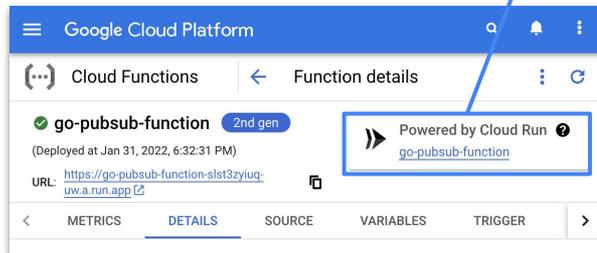
CPU やメモリリソースを複数の呼び出しで共有することにより、コストの削減にも繋がる



簡単なロールバック

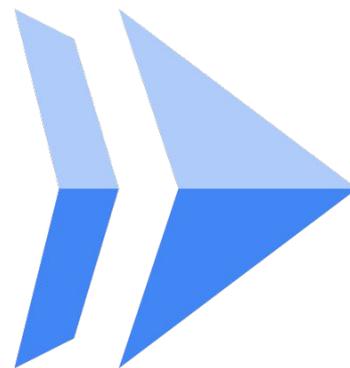
デプロイメント毎に新しいリビジョンが自動的に作られており、簡単に以前のリビジョンにロールバックすることができる

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



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

Google Cloud stereen-serverless Search

Cloud Run ← Create job **PREVIEW**

A Cloud Run job executes containers to completion. Job name and region cannot be changed later.

Container image URL SELECT

[TEST WITH A SAMPLE CONTAINER](#)
[How to build a container?](#)

Job name *

Region * ▼
[How to pick a region?](#)

Number of tasks *

The number of times to run the container. All tasks must succeed in order for a job to succeed.

Container, Variables & Secrets, Connections, Security ▼

Execute job immediately

CREATE **CANCEL**

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:

- データベースとの接続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

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

CPU Boost 無効

Startup



Serving



CPU Boost 有効

Startup



Serving



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

Move password to Secret Manager



Refreshed: Aug 15, 2022, 12:14:45 AM

Insight



An environment variable in service test-security-recommendations (us-central1) might contain a password.

Service	test-security-recommendations
Region	us-central1
Last observed	1 day ago

Recommendation



Storing a password in the value of an environment variable prevents you from easily changing it and makes it visible to many in your organization (anyone with Project Viewer or Cloud Run Developer IAM role). Moving this password into a secret stored in Secret Manager and exposing it as an environment variable better protects the password.

How to: [Use secrets](#)

EDIT SERVICE

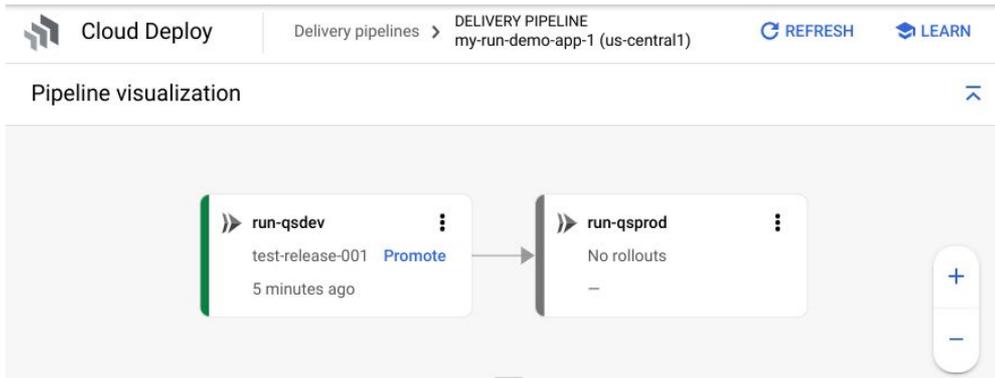
DISMISS

CANCEL

Cloud Deploy サポート

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
```

Integrations

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

The screenshot shows the Google Cloud console interface for a Cloud Run service named 'hello'. The page is titled 'Service details' and includes a search bar and navigation options. The 'Integrations' tab is selected, showing a list of integrated services. Two services are listed: 'Redis' and 'Custom Domains'. The 'Redis' service is active, while 'Custom Domains' is pending.

Integrations	
Redis	
Name	redis-kqva
Status	Active
Capacity (GB)	1
VIEW DETAILS	
Custom Domains	
Name	custom-domains
Status	Pending
Domain	cats-xor-dogs.com
VIEW DETAILS	

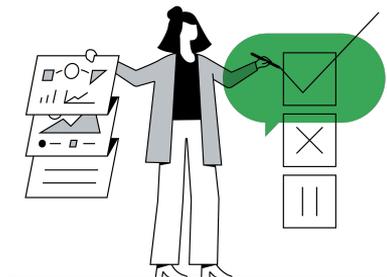
04

Google Kubernetes Engine (GKE)



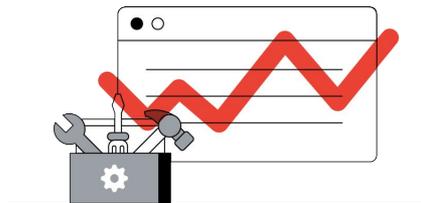
GKE Security Posture Management

GKE Security Posture Management



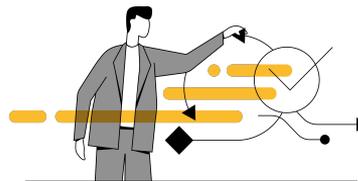
セキュリティ ガイダンス

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



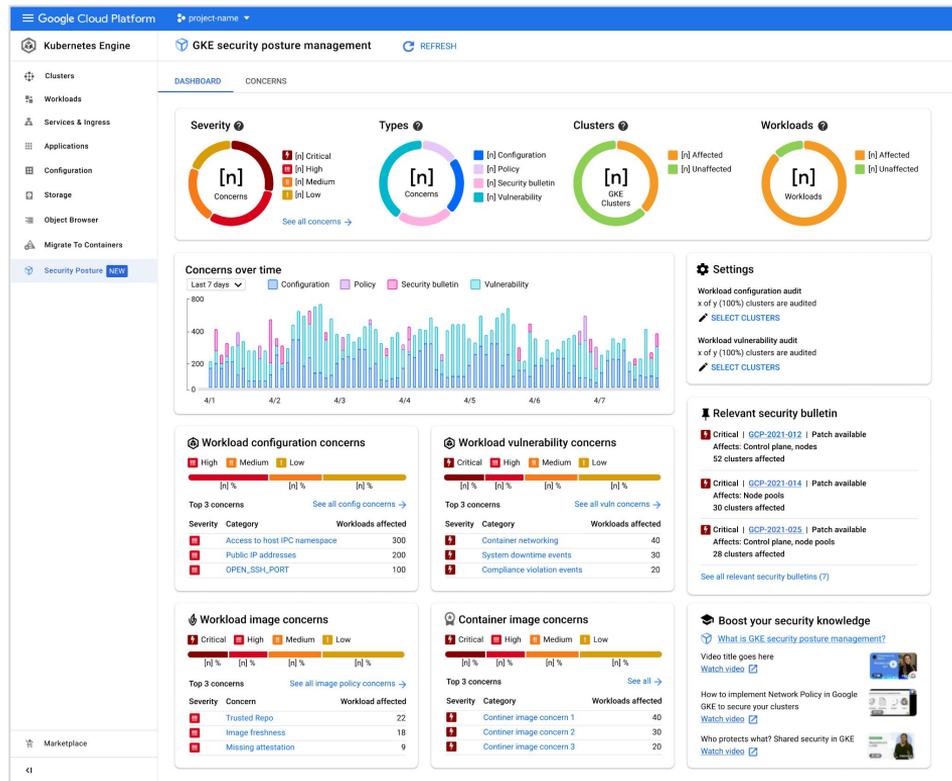
GKE 機能の一部

GKE に含まれている機能なので、追加費用なしで利用可能

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



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

The screenshot displays the Google Cloud Platform console interface for GKE security posture management. The main dashboard shows two donut charts: 'Severity Concerns' and 'Clusters GKE', both indicating zero issues. Below these are two bar charts for 'Configuration concerns by severity' and 'Vulnerability concerns by severity', both showing zero concerns. A 'Concerns over time' bar chart shows zero concerns from 4/1 to 4/6. On the right, the 'Workload vulnerability audit settings' panel is open, showing a table of clusters with their audit status. A tooltip indicates that workload vulnerability auditing is only available in Kubernetes Engine version 1.22 and later.

Workload vulnerability audit settings

AUDIT OFF | AUDIT ON

When you enable auditing on a cluster, its workloads are audited for workload vulnerability. [Learn more](#)

2 clusters listed below can't be audited because Protect for GKE auditing is only available in Kubernetes Engine version 1.22 and later.

TURN ON AUDIT

Filter Enter property name or value

Status	Cluster	Configuration audit	Location
<input type="checkbox"/>	cluster-01	Disabled	us-central1-c
<input checked="" type="checkbox"/>	cluster-02	Disabled	us-central1-c
<input checked="" type="checkbox"/>	cluster-03	Disabled	us-central1-c
<input checked="" type="checkbox"/>	cluster-04	Disabled	us-central1
<input checked="" type="checkbox"/>	cluster-05	Disabled	us-central1
<input checked="" type="checkbox"/>	cluster-06	Disabled	us-central1
<input type="checkbox"/>	cluster-07	Disabled	us-central1
<input checked="" type="checkbox"/>	cluster-08	Disabled	us-central1

Workload vulnerability auditing is only available in Kubernetes Engine version 1.22 and later. This cluster has version 1.21.6-gke-1503.

CLOSE

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

Google Cloud Platform project-name

GKE security posture management REFRESH

DASHBOARD CONCERNS

Filter concerns CLEAR ALL |<

Severity

- Critical
- High
- Medium
- Low

Concern type

- Configuration
- Vulnerability

Locations

- us-central-1
- us-central-2

Clusters

- cluster-a
- cluster-b
- cluster-c
- cluster-d
- cluster-e
- cluster-f
- cluster-g
- cluster-h
- cluster-i
- cluster-j

[n] concerns

View by: Concern Namespace Workload Page refreshed: 5 minutes ago

Filter Filter table Is system object: False

Severity ↓	Type	Concern	Workloads affected	Cluster affected
High	Vulnerability	CVE-123456 for package-a (Debian)	200	40
High	Vulnerability	Container networking	200	40
High	Vulnerability	PUBLIC_IP_ADDRESS	200	40
High	Security bulletin	GCP-2022-012	200	40
High	Security bulletin	GCP-2022-014	200	40
High	Security bulletin	GCP-2022-015	200	40
High	Vulnerability	CVE-2021-25741	200	40
High	Vulnerability	CVE-2021-25737	200	40
High	Vulnerability	CVE-2020-8565	200	40
High	Vulnerability	CVE-2020-8565	200	40
High	Vulnerability	Privileged containers	200	40
High	Vulnerability	CVE-2018-20119	200	40
High	Vulnerability	CVE-2020-11245	200	40
High	Vulnerability	CVE-2020-1028	200	40
High	Vulnerability	CVE-2020-3325	200	40
High	Vulnerability	CVE-2020-3328	200	40
High	Vulnerability	CVE-2020-3398	200	40
High	Vulnerability	CVE-2020-5210	200	40

Rows per page: 100 1-100 of [n]



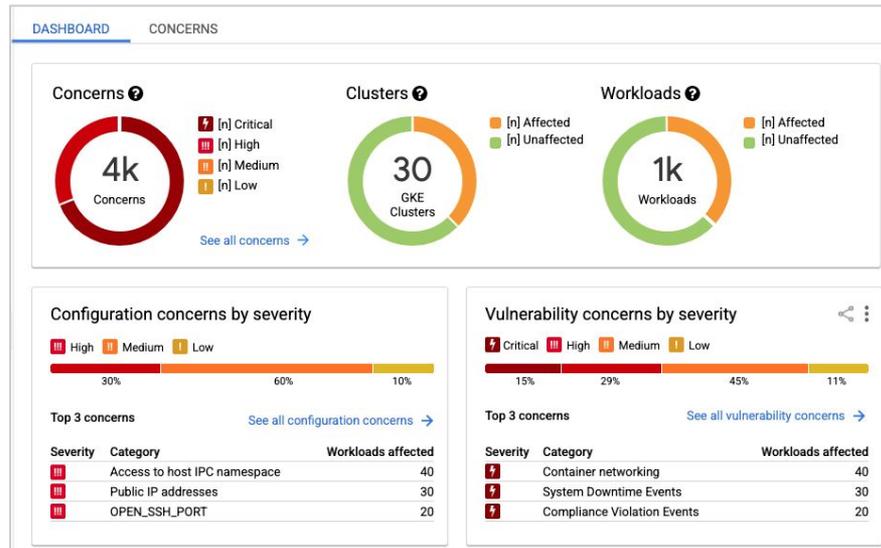
ワークロード構成スキャン

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)

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 Cloud My Project 5514

Kubernetes Engine Backup for GKE **PREVIEW** + CREATE A BACKUP PLAN + CREATE A RESTORE PLAN

Configure backup and restore operations to protect workloads in your Kubernetes clusters. [Learn more](#)

BACKUP PLANS RESTORE PLANS BACKUPS RESTORES

Use backup plans to configure and administer backups.

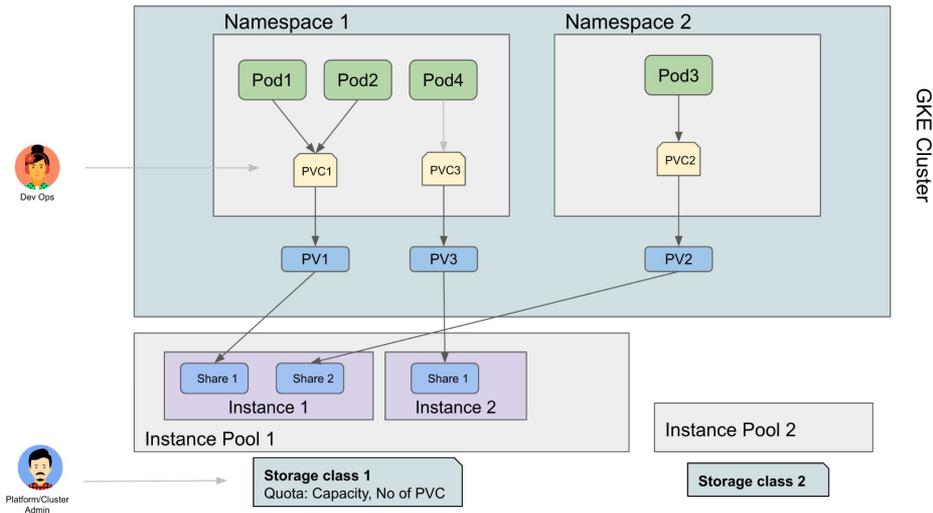
Cluster / Backup plan	Total backup plans	Restore plans	Total backups	Location	Backup scope
cluster-1	1		1	us-central1-c	
my-stateful-backup		0	1	us-central1	All namespaces

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 1TB)

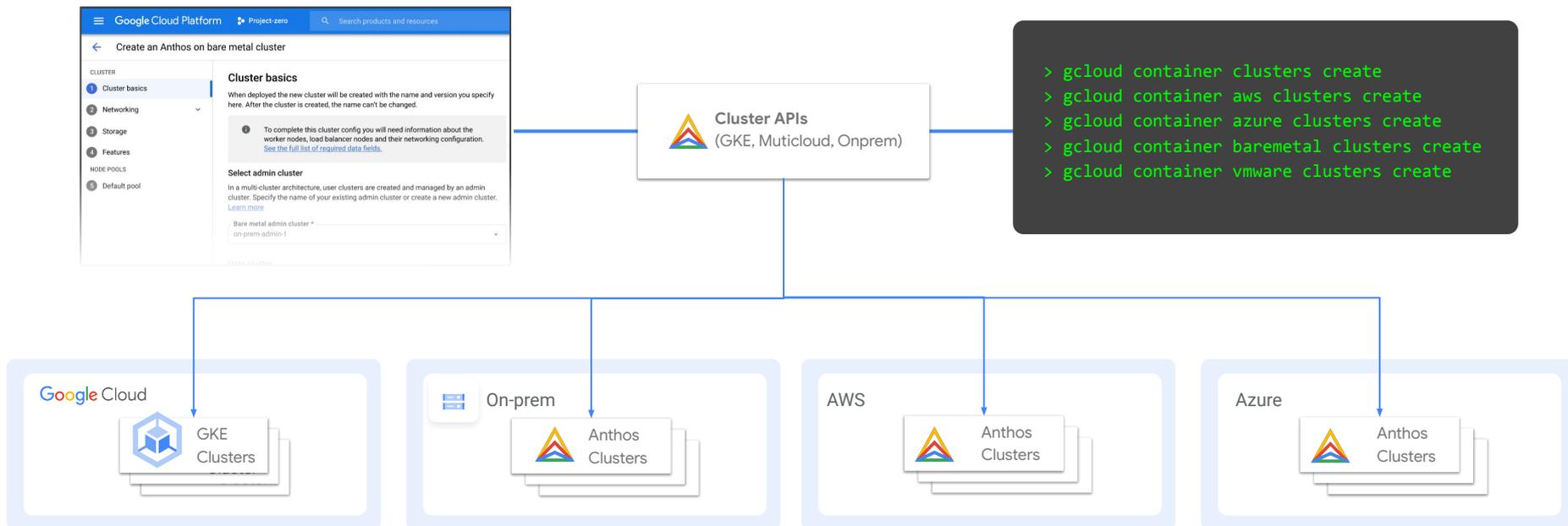


05

Anthos

コンソールや API によるクラスタ ライフサイクル管理

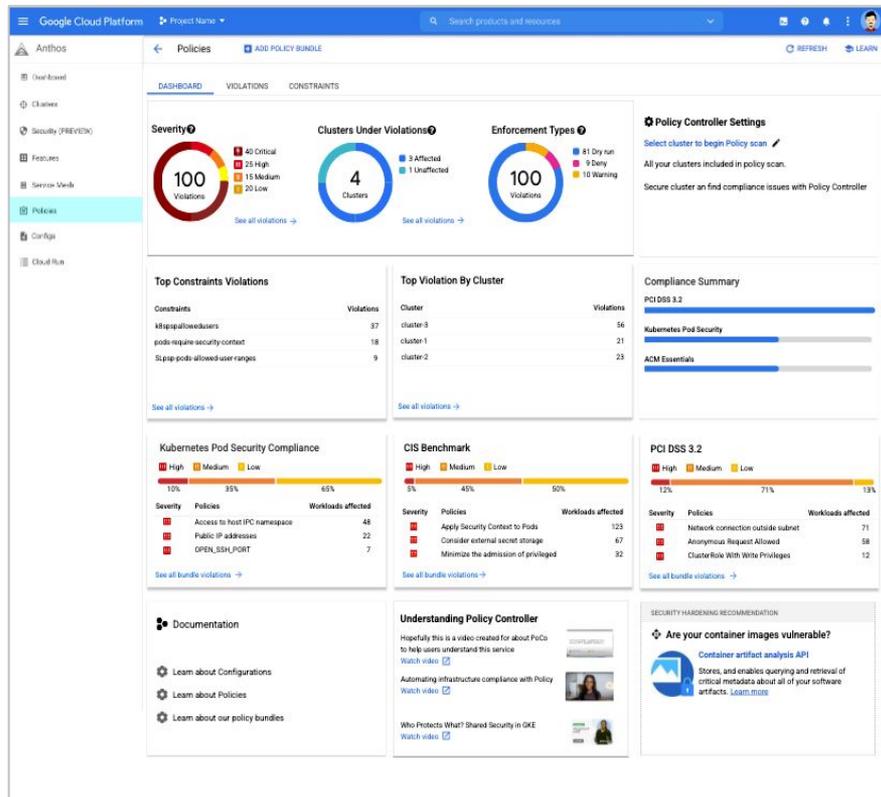
Anthos clusters のライフサイクル (構築 / アップグレード等) を gcloud コマンドや Google Cloud コンソールから管理



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.