Google Cloud

Google Cloud
UPDATES

Google Cloud のエンジニアによる
最新アップデートまとめ

2023 年 Q2 : Compute / DB 編
2023-01-16 ~ 2023-03-31

Google Cloud UPDATES について

https://cloudonair.withgoogle.com/events/gc-updates

- このイベントでは、Google Cloud に関する四半期分のアップデートの振り返りを行っていきます
- 既存ユーザ様を主な対象としているため、基本的には、プロダクトの概要レベルの説明は行いません
- 出入りは自由ですが、退出時にアンケートにご協力下さい
- 質問は、Chat か、こちらのフォームをご活用下さい
- 今回は、**2023-01-16 ~ 2023-03-31 の Compute / AppMod / DB / Security 系**のプロダクトのアップデートの振り返りを行っていきます

本日のスピーカー

Naoki Tochizawa

Infrastructure,
Security

Naoya Kumagai

Application
Modernization

Taka Sato

Database

Yuma Shoji

Network, その他

01

Infrastructure

GA 2023-01-25

Red Hat Enterprise Linux（RHEL）の確約利用割引

Red Hat Enterprise Linux（RHEL）イメージを利用する GCE インスタンス でライセンスのコミットメントを購入することが可能

OS イメージ	vCPU 数	1 年間の CUD 率	3 年間の CUD 率
SLES	1 ～ 2	77%	79%
SLES	3 ～ 4	54%	59%
SLES	5 年以上	45%	50%
SLES for SAP	任意	59%	63%
RHEL	任意	20%	24%
RHEL for SAP	任意	20%	24%

GA 2023-02-14

Tau T2A VM が セキュア ブート をサポート

スケールアウト最適化 : Tau T2A

- 2022 年 10 月 5 日 GA
    - 日本リージョンはまだ未対応
- はじめての ARM アーキテクチャ ベースのマシン
- 最大 48 vCPU をサポート
- 最大帯域 32 Gbps をサポート

参照 : Tau T2A VM

ワークロード タイプ					
汎用のワークロード			最適化されたワークロード		
コスト最適化	バランス	スケールアウト最適化	メモリ最適化	コンピューティング最適化	アクセラレータ最適化
E2	N2、N2D、N1	Tau T2D、Tau T2A	M3、M2、M1	C2、C2D	A2
低コストで日々のコンピューティングを実現	幅広いマシンタイプにわたるバランスの取れた価格とパフォーマンス	スケールアウト ワークロードに最適なパフォーマンスと費用	超高メモリ ワークロード	超高パフォーマンスでコンピューティング負荷の高いワークロードを実現	ハイ パフォーマンス コンピューティング ワークロード向けに最適化
• ウェブサービス • アプリの配信 • バックオフィス アプリ • 小規模データベース • マイクロサービス • 仮想デスクトップ • 開発環境	• ウェブサービス • アプリの配信 • バックオフィス アプリ • 中規模データベース • キャッシュ • メディア / ストリーミング	• スケールアウト ワークロード • ウェブサービス • コンテナ化されたマイクロサービス • メディアのコード変換 • 大規模 Java アプリケーション	• 中規模 OLAP およびインメモリ データベース（SAP HANA など） • インメモリ データベースとインメモリ分析 • Microsoft SQL Server などのデータベース • ゲノム モデリング • 電子設計自動化	• 計算依存型ワークロード • 高パフォーマンスのウェブサービス • ゲーム（AAA ゲーム サーバー） • 広告配信 • ハイ パフォーマンス コンピューティング（HPC） • メディアのコード変換 • AI / ML	• CUDA 対応の ML トレーニングと推論 • HPC • 超並列コンピューティング

オブザーバビリティ タブ

リソースを最も消費している 5 つのインスタンスを Google Cloud コンソール からダッシュボード形式で表示

- VM のパフォーマンス関連の障害の切り分け等に活用可能

Preview 2023-01-16

MIG 修復時の更新インスタンス構成の適用

マネージド インスタンス グループ（MIG）の自動修復時に最新のインスタンス テンプレートを適用

参照：修復中に構成の更新を適用する

Preview 2023-02-09

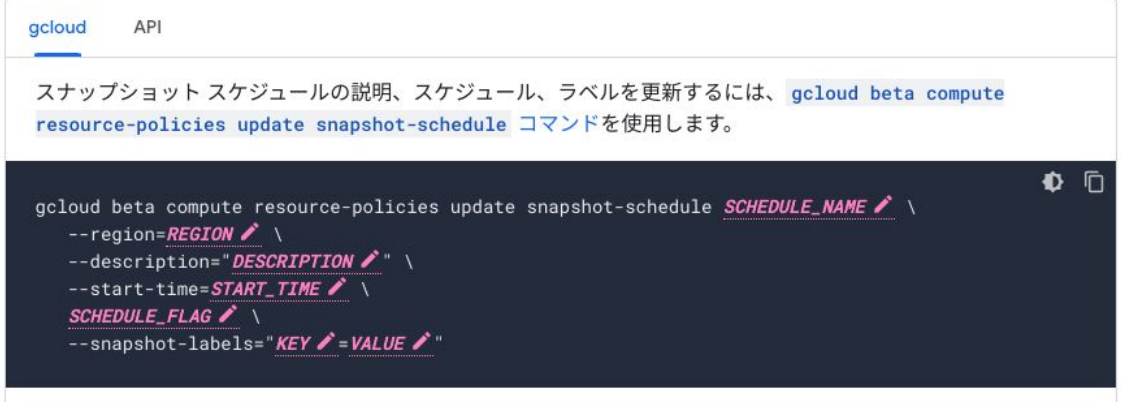
スナップショット スケジュールの変更

スナップショット スケジュールの変更機能が実装

- スナップショット スケジュールの説明
- スケジュール頻度
- ラベル

  Google Cloud CLI または API のみ

参照 スナップショット スケジュールの変更 を参照してください。



Preview
GA

永続ディスクの機能拡張

- **Persistent Disk Asynchronous Replication（PD Async Replication）** Preview 2023-03-30
  - 2 つのリージョン間でデータの非同期レプリケーションを提供
  - リージョン障害時に、セカンダリー リージョンにフェールオーバしてワークロードを再開
    - 手動でのフェールオーバーが必要

  参照：「永続ディスクの非同期レプリケーションについて」を参照してください。

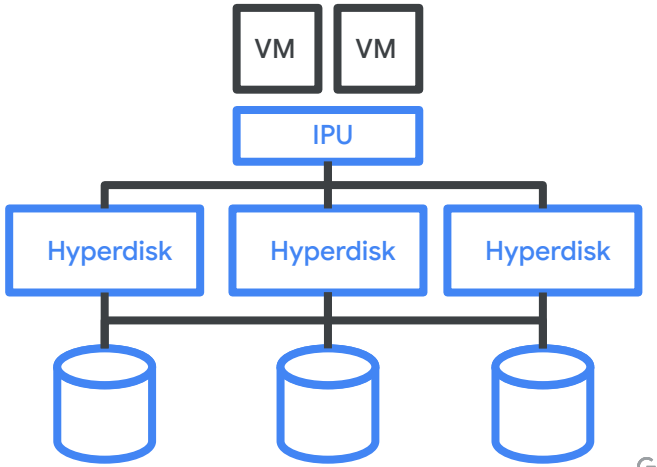
- Cloud Monitoring によって リージョン永続ディスク の Replica State が確認可能 GA 2023-03-31
  - Replica State では、2 ゾーンに存在する 永続ディスク のデータが同期されているかなどが確認可能

GA 2023-03-13

Hyperdisk リリース

ハイエンドのメモリ集約型ワークロード向けブロック ストレージ

- 永続ディスクと同様に VM がアクセスできる耐久性のあるネットワーク ストレージ デバイス
- IPU を活用した次世代のブロックストレージ
- ディスクの容量と性能を別々、かつ動的に構成が可能（永続ディスクとの違い）
  - OS Boot Disk としての設定は不可
- GA 段階では、Hyperdisk Extreme（Extreme PD 相当）のみがリリース
  - 東京、大阪リージョン利用可能
  - 64 vCPU 以上のマシンで利用可能



参照：ハイパーディスクについて

GA 2023-1-18

gcloud storage リリース 1.2

- バケットおよびオブジェクト レベルで IAM および ACL を使用してアクセスを管理
- Autoclass
- ターボ レプリケーション 機能の管理

gcloud storage とは？

- 2022 年 Q3 にリリース
- gsutil コマンドライン ツールと比較して、アップロードとダウンロードのパフォーマンスが高速

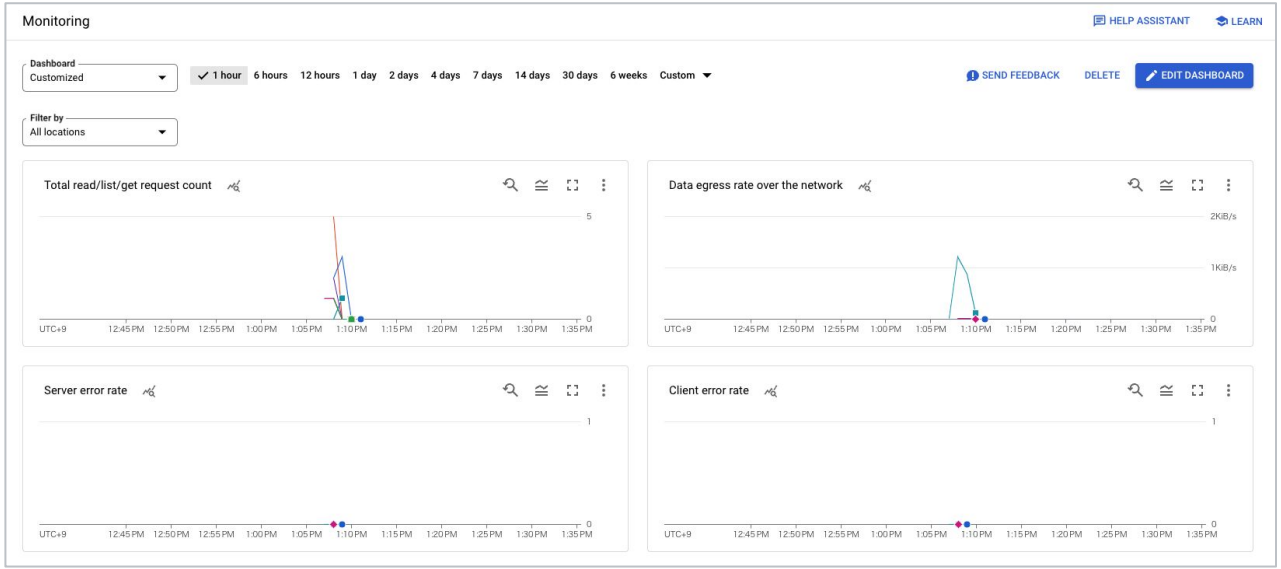
参考 : New gcloud storage CLI for your data transfers

GA 2023-03-17

Cloud Storage モニタリング ダッシュボード拡張

モニタリング ダッシュボードの拡張

サーバー エラー率
クライアント エラー率
読み取りエラー数
書き込みエラー数
Read / List / Get リクエスト数
書き込みリクエストの合計
ネットワークの上り（内向き）データレート
ネットワークの下り（外向き）データレート



GA 2023-03-23

Cloud Storage Autoclass 128 KiB 未満のオブジェクトの扱い

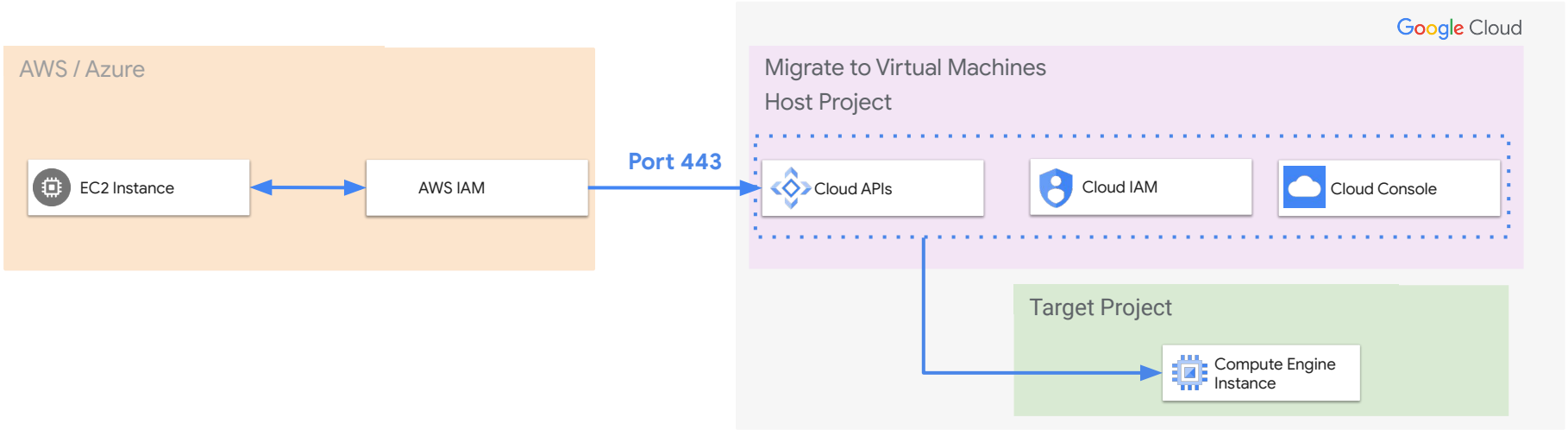
Autoclass が有効になっているバケットに格納されている 128 KiB 未満のオブジェクトは、
スタンダード クラスに静的に設定（3 / 23）

- 現在別のストレージ クラスに格納されている Autoclass バケット内のオブジェクトは、自動的に無料で スタンダード クラスに移行

Preview
GA

Migrate to Virtual Machines 他クラウドからの移行

- AWS EC2 インスタンスを Compute Engine に移行可能 — GA 2023-01-16
- Azure Virtual Machines インスタンスを Compute Engine に移行可能 — Preview 2023-02-20



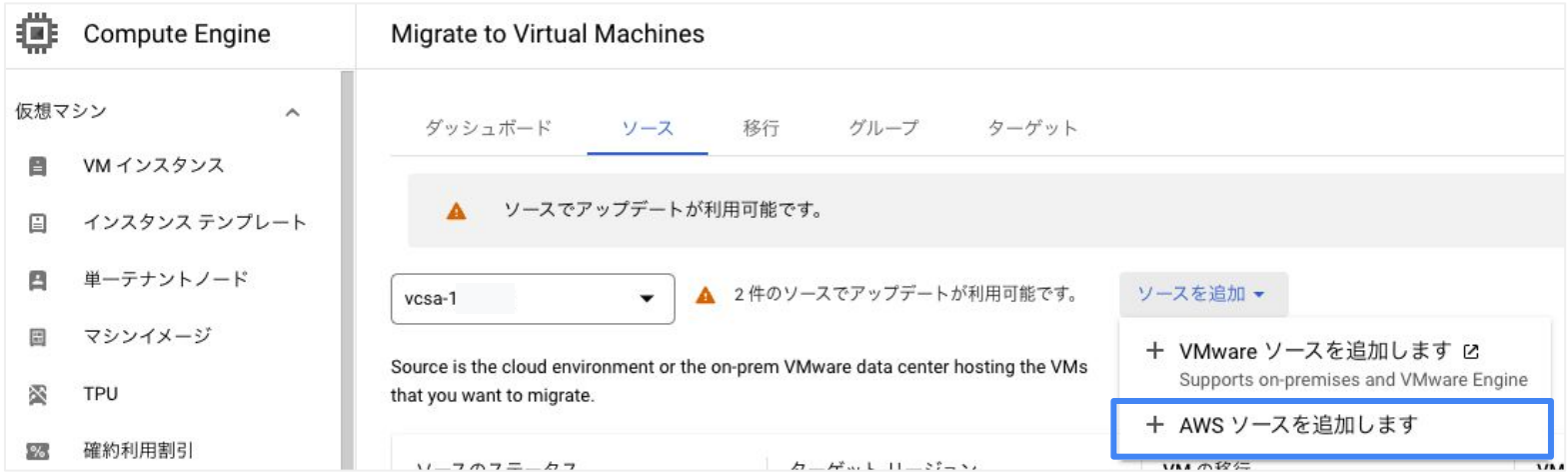
移行元の各クラウドサービス側で Migrate to Virtual Machines（M2VM）がアクセスするための権限を付与して、移行処理を行う

Migrate to Virtual Machines

左からの流れで設定を行っていく

	バージョン 5.0
移行元環境	vSphere、AWS、Azure（Preview）
サービス提供リージョン	一部リージョン
移行管理	Google Cloud Console に統合
移行時のストレージデータの転送	スナップショットのレプリケーション技術を活用（移行開始時の VM 停止）
サポート OS	サポート OS

Migrate to Virtual Machines



Azure を利用する場合には、現時点ではプレビューでの利用リクエストが必要となります

参照 : [AWS を移行元とする Migrate to Virtual Machines]
[Azure を移行元とする Migrate to Virtual Machines]

GA

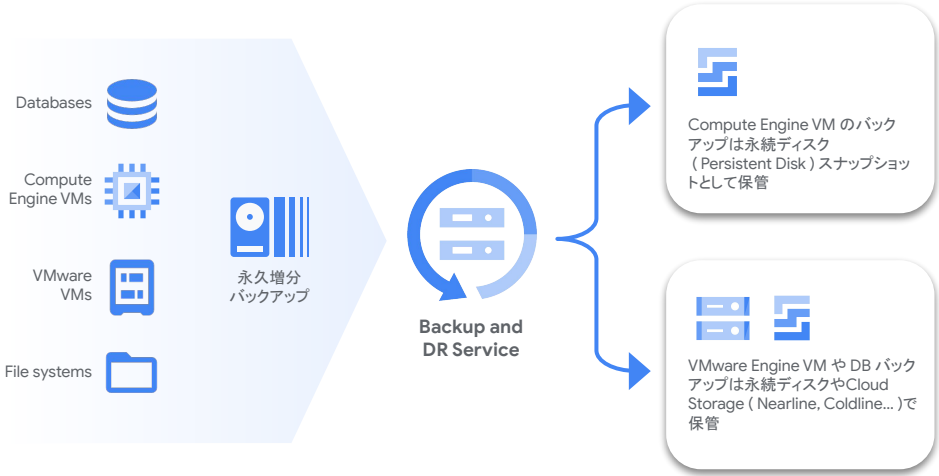
Backup & DR 各種機能拡張

- デプロイプロセスの簡素化 2023-01-03
- Cloud Logging と Cloud Monitoring のサポート 2023-03-06
  - バックアップ イベントのログ
  - カスタム フィルタによる バックアップ イベントの表示
  - Cloud Monitoring で、バックアップ イベントの アラートを構成 可能
- Hyperdisk Extreme 対応 2023-03-17
- アプライアンスのバックアップ、リカバリ機能の拡充 2023-03-24
- Compute Engine インスタンス バックアップのアーカイブ スナップショットをサポート 2023-03-24

Backup & DR 機能概要

永久増分バックアップによるコスト効率の向上や RPO を直近としながら RTO を最小化

- 増分バックアップ取得によって定期的なフルバックアップ取得の必要性をなくし、総所有コスト(TCO) を削減
- 本番環境への性能影響を最小限に抑えつつ高頻度なバックアップにより RPO を直近とすることが可能※
- コストパフォーマンスを意識した柔軟なストレージのオプションから最適な種類を選択
- ネイティブの API を利用してアプリ整合性を担保するバックアップ取得方法
    - Persistent Disk Snapshot API
    - VMware vStorage for Data Protection (VADP) API
    - SAP HANA savepoint API / backint API
    - Oracle Recovery Manager (RMAN) API
    - Microsoft VSS snapshot
    - Other database APIs



※ Compute Engine の場合は 10 分、データベースの場合は 15 分、VMware VM やファイルシステムの場合は 1 時間程度です。

02

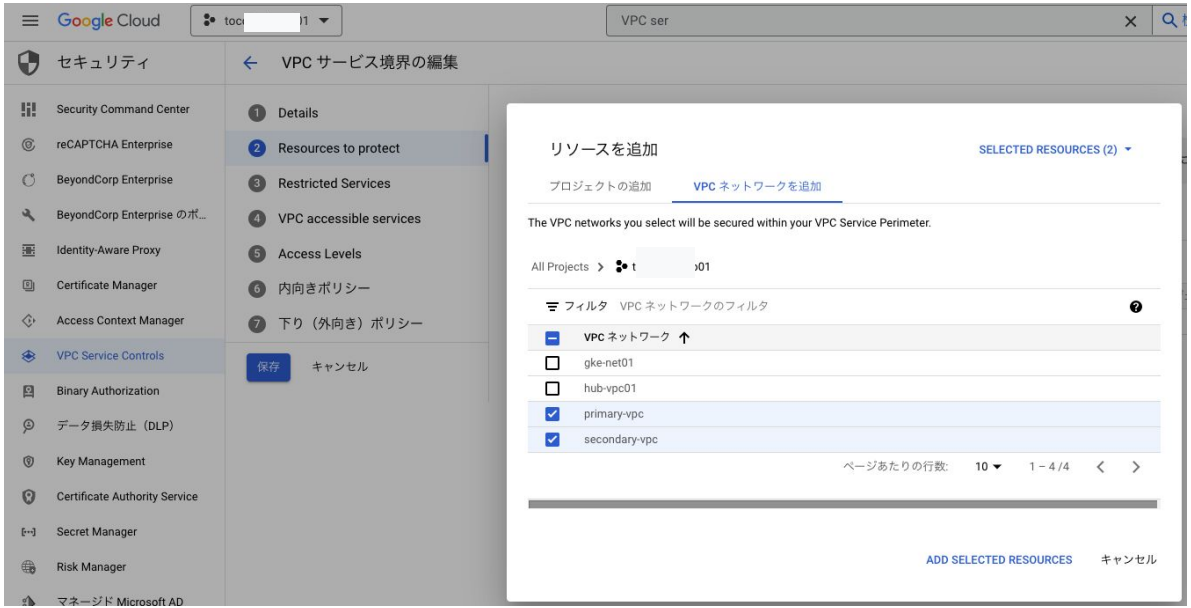
Security

GA　2023-02-17

個々の VPC ネットワークを選択してセキュリティ境界に追加

- 個々の VPC ネットワークを境界のメンバーとして追加
- 個々の VPC ネットワークが境界にアクセスすることを承認する上りルールを作成

（以前は、ホスト プロジェクト内のすべての VPC ネットワークが境界に追加されていました。）



GA 2023-01-30

Security Command Center のプロジェクト レベルのアクティブ化

個々のプロジェクトレベルで Security Command Center を有効にできるようになりました。
Security Command Center をプロジェクト レベルで有効にする場合、プレミアム 料金は
プロジェクト内の特定の Google Cloud サービスの使用量に基づいて計算されます。

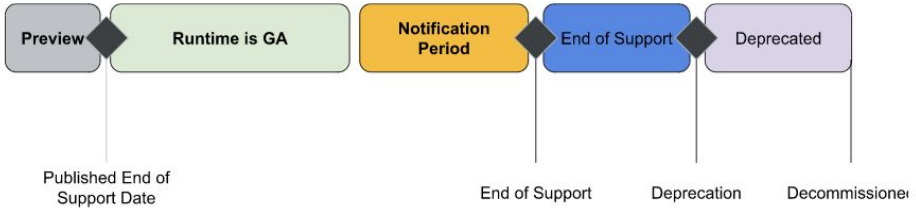
参照 : プロジェクト レベルの有効化の概要

03

Application Modernization

App Engine 第 1 世代の EoS について

2024 年 Q1 に App Engine Standard Generation 1 Runtimes が End of Support となり、当該ランタイムに対するパッチ・Bug fix 等の提供停止、また当該ランタイムに関するサポートを受けることができなくなります。



デプロイされたアプリケーションは引き続き動作し、止まることはありません（トラフィックは流れ続けます）

	一般提供レベルのサポート	サポートの終了	非推奨	廃止
作成と再デプロイ	あり	いいえ[1]	いいえ	いいえ
プロジェクト構成の更新	あり	はい	いいえ	いいえ
既存のワークロードの実行	あり	はい	はい	いいえ
UI と CLI の警告	あり	はい	いいえ	いいえ
言語パッチ	自動	自動更新なし	自動更新なし	自動更新なし
API と SDK のパッチ適用	自動	自動更新なし	自動更新なし	自動更新なし
OS へのパッチ適用	自動	自動更新なし	自動更新なし	自動更新なし
カスタマー サポート	一般提供レベルのサポート	ランタイム サポートなし	ランタイム サポートなし	ランタイム サポートなし

移行先

- Cloud Run
- App Engine 第 2 世代

詳細: https://cloud.google.com/appengine/docs/standard/lifecycle/runtime-lifecycle

バックエンド サービス ベースの外部ネットワーク ロードバランサが一般提供

既存のターゲットプールベースのロードバランサと比べ多くの機能を提供

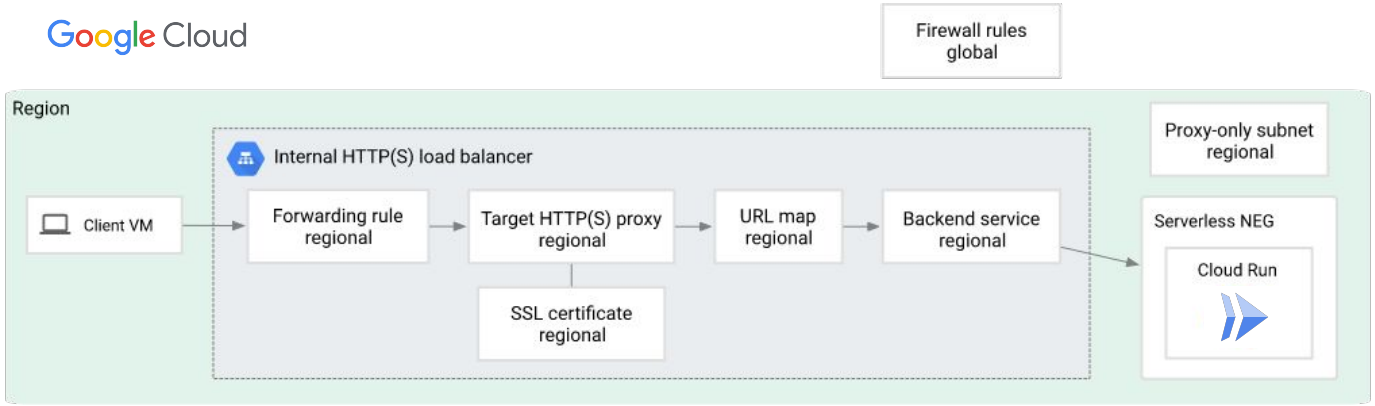
- IPv6 接続のサポート
- 複数のプロトコルのサポート（TCP、UDP、ESP、GRE、ICMP、および ICMPv6）
- きめ細かいトラフィック分散制御（セッション アフィニティ、接続トラッキング モード、重み付き負荷分散）
- Google Cloud Armor の統合
- ヘルスチェック（TCP、SSL、HTTP、HTTPS、または HTTP/2）

```
apiVersion: v1
kind: Service
metadata:
  name: store-v1-lb-svc
  annotations:
    cloud.google.com/l4-rbs: "enabled"
spec:
  type: LoadBalancer
  externalTrafficPolicy: Cluster
  selector:
    app: store
  ports:
  - name: tcp-port
    protocol: TCP
    port: 8080
    targetPort: 8080
```

詳細: https://cloud.google.com/kubernetes-engine/docs/how-to/external-svc-lb-rbs

内部 HTTP(S) ロードバランサーで Cloud Run をバックエンドとして設定可能

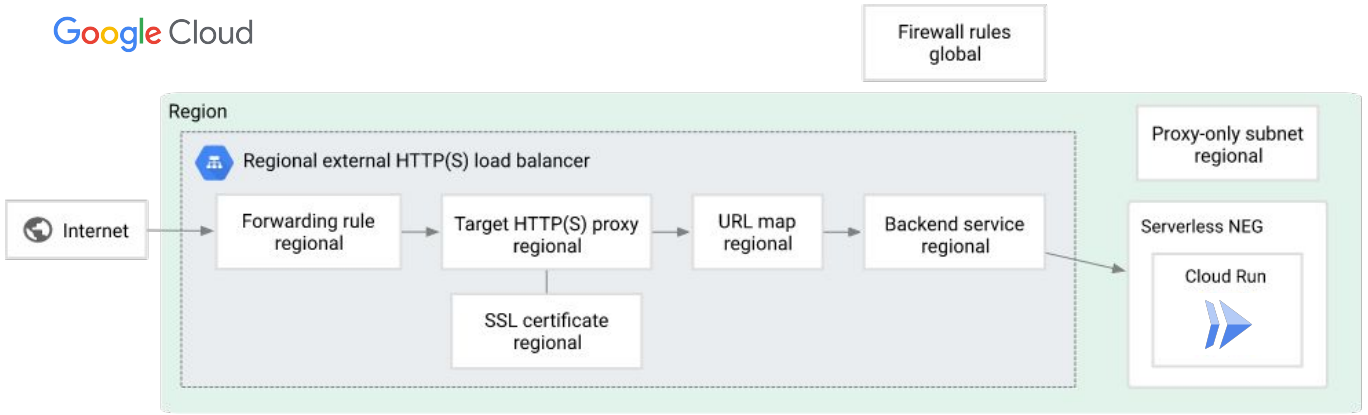
- サーバレス NEG を使用して 内部 HTTP(S) ロードバランサーのバックエンドにCloud Run を指定可能
- VPC 内のトラフィックの負荷分散に利用可能



詳細: https://cloud.google.com/load-balancing/docs/l7-internal/setting-up-l7-internal-serverless

外部リージョン HTTP(S) ロードバランサーで Cloud Run をバックエンドとして設定可能

- サーバレス NEG を使用して 外部リージョン HTTP(S) ロードバランサーのバックエンドに Cloud Run を指定可能
- 単一のリージョンでCloud Run サービスを公開する際に利用可能

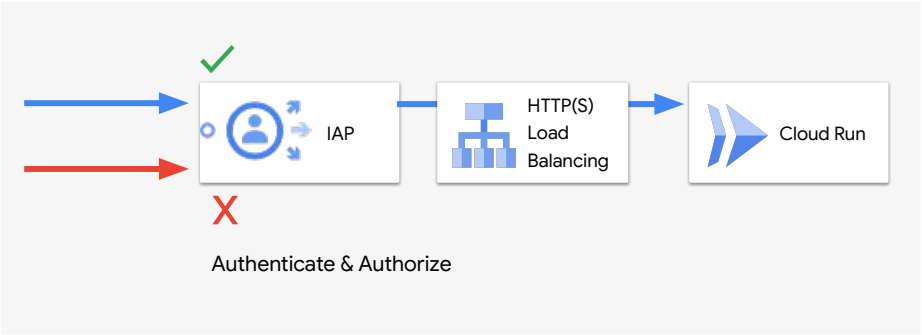


詳細: https://cloud.google.com/load-balancing/docs/https/setting-up-reg-ext-https-serverless

Cloud Run での Identity-aware Proxy のサポートが一般提供

Cloud Run へのアプリケーションレベルでのアクセス制御を実現

- サーバレス NEG により HTTP(S) Load balancing と連携することで、Cloud Run と Identity Aware Proxy が連携可能に
- ユーザー認証をアプリから切り離すことが可能
- IAM Conditions を組み合わせて、詳細な条件を付与することもできる



詳細: https://cloud.google.com/iap/docs/enabling-cloud-run

Preview

Cloud Functions 第 2 世代 の主なアップデート

vCPU と Concurrency が直接指定可能に

2023-01-18

- 同時実行数（Concurrency）と vCPU を指定して、第 2 世代の Function を構成する機能がプレビュー

CMEK (顧客管理の暗号化キー) のサポート

2023-02-27

- CMEK により以下のようなリソースが暗号化される
  - デプロイ用にアップロードされた関数のソースコード
  - 次のような関数のビルドプロセスの結果
    - 関数のソースコードからビルドされたコンテナイメージ
    - デプロイされている関数の各インスタンス

詳細: https://cloud.google.com/functions/docs/configuring/concurrency
https://cloud.google.com/functions/docs/securing/cmek

Preview 2023-01-18

Cloud Build 第 2 世代が Preview で提供開始

リポジトリ接続をプログラムで作成および管理

- gcloud コマンドや API を介してリポジトリの接続と管理が可能
- 現在は GitHub と GitHub Enterprise のみ対応
- Preview 段階ということもあり、現状第 1 世代で利用できていた多くの機能が第 2 世代では利用できない

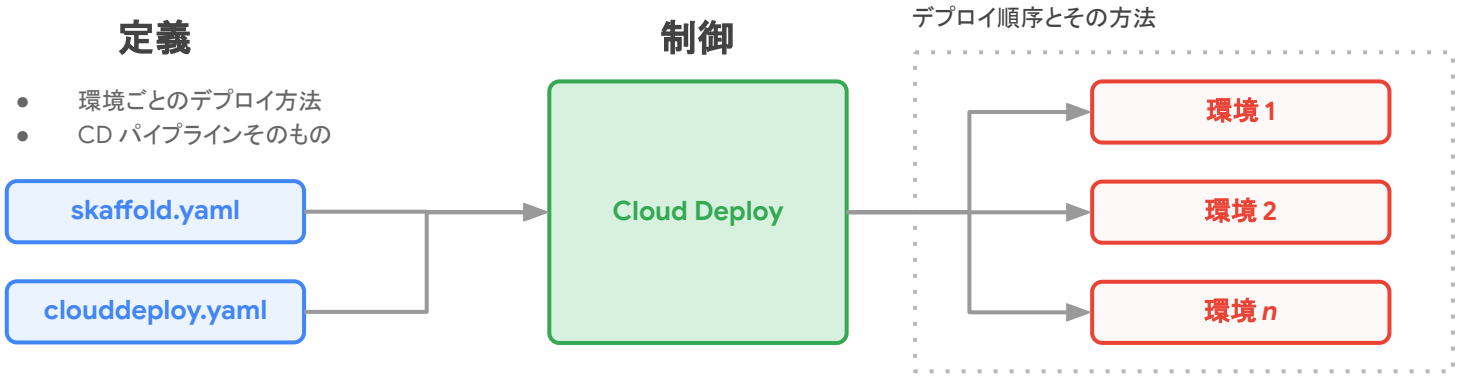
機能	Cloud Build リポジトリ（第 1 世代）	Cloud Build リポジトリ（第 2 世代）
ブランチ push、タグの push、pull リクエスト イベントに対応してビルドできます。	あり	あり
手動トリガーを作成できます	あり	いいえ
Pub/Sub トリガーを作成できます	あり	いいえ
Webhook トリガーを作成できます	あり	いいえ
リポジトリに対して単一の接続を作成し、その接続の認証を使用して、追加の接続を設定できます。	いいえ	あり
GitHub と GitHub Enterprise からリポジトリを接続できます	あり	あり
GitLab Enterprise Edition からリポジトリを接続できます	あり	いいえ
Bitbucket データセンターと Bitbucket サーバーからリポジトリを接続できます	あり	いいえ
Cloud Source Repositories からリポジトリを接続できます	あり	いいえ
ホスト接続を作成せずにリポジトリをリンクできます	あり	いいえ
gcloud を使用してリポジトリ接続を作成できます	いいえ	あり
Terraform を使用してリポジトリ接続を作成および自動化できます	いいえ	あり
ホスト接続とリンク リポジトリが特定のリージョンに存在する必要があります	いいえ	はい

詳細: https://cloud.google.com/build/docs/repositories?hl=ja#repositories_2nd_gen

Cloud Deploy で Cloud Run のサポートが一般提供

コンテナベースのワークロードを任意の Cloud Run サービスにデプロイ

- リリース作成時に Skaffold バージョン 2.0 以降を指定する必要がある
  (指定しない場合は互換性のあるデフォルトバージョンを自動選択)



詳細: https://cloud.google.com/run/docs/deploying

GA 2023-02-27

デプロイ検証が一般提供

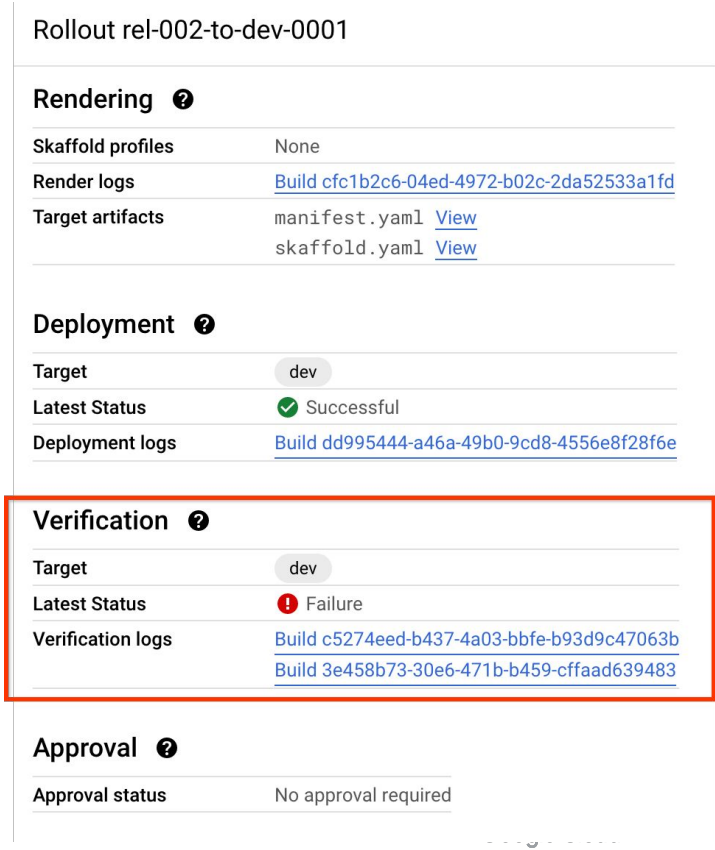
Cloud Deploy でデプロイしたアプリケーションが正常に動作しているか検証

- 検証は独自のテストイメージで行われる

デプロイ検証の仕組み

1. 検証のために Skaffold を構成
2. デリバリーパイプラインでターゲットを構成
3. デプロイされると skaffold verify を自動実行
4. skaffold.yaml の設定に基づき検証
5. テストに失敗した場合は検証失敗で扱われる
6. 再試行ができる

詳細: https://cloud.google.com/deploy/docs/verify-deployment

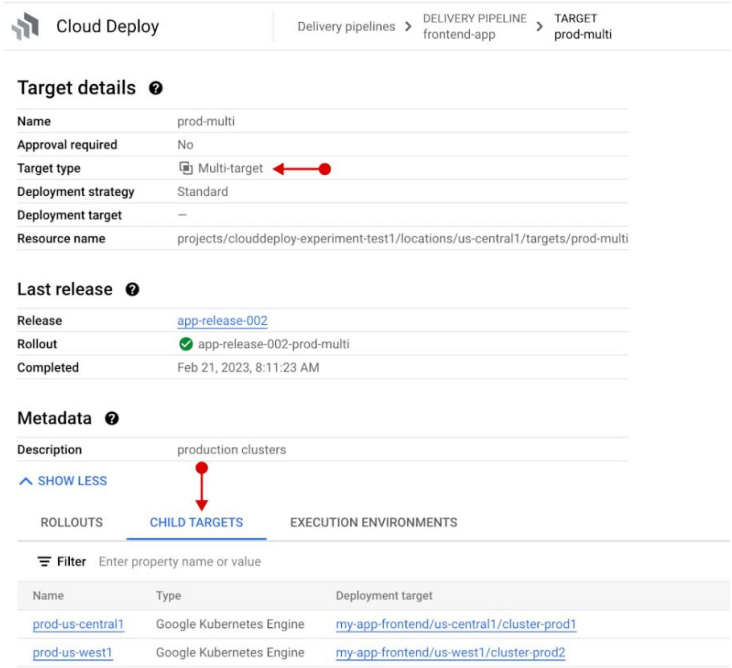


Preview 2023-03-06

Cloud Deploy での複数ターゲットへのデプロイ

複数のターゲット（GKE or Anthos Cluster / Cloud Run）に対して、一つのパイプライン上で同時にデプロイすることが可能となった

```
apiVersion: deploy.cloud.google.com/v1
kind: Target
metadata:
 name: TARGET_NAME
description: TARGET_DESCRIPTION
multiTarget:
 targetIds: [ CHILD_TARGET1, CHILD_TARGET2, CHILD_TARGETn ]
```



詳細: https://cloud.google.coma/deploy/docs/parallel

Preview 2023-03-26

SEARCH 関数の利用

Logging で Built-in の SEARCH 関数を利用可能に

- 文字列の検索に効果的
- 大文字小文字の区別なく検索可能
- フィールドまたは全体にクエリをかける

```
SEARCH([query])
SEARCH([field], [query])
```

詳細: https://cloud.google.com/logging/docs/view/logging-query-language#search-functions

04

Database

アンダー プロビジョニングの推奨事項を提供

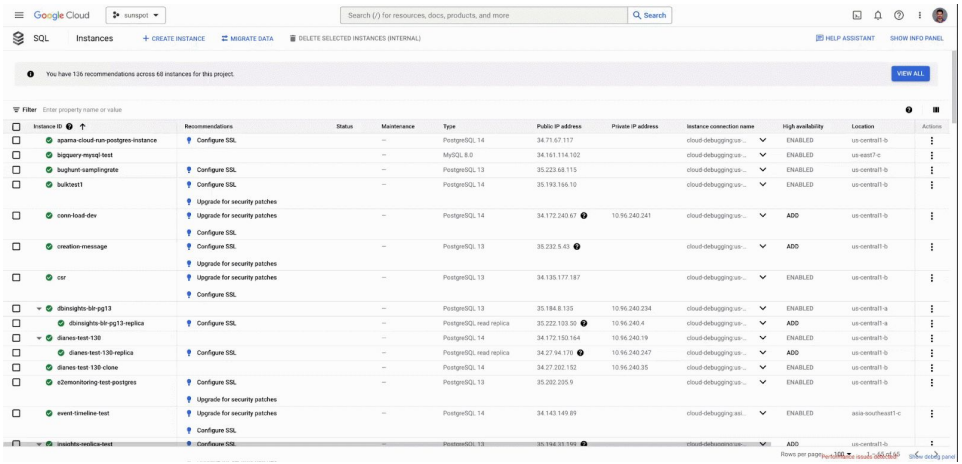
機械学習に基づくプロアクティブな推奨事項の提供により性能低下やシステム停止を予防

Cloud SQL では、利用状況に応じた推奨事項（Recommender）を提供している。ユーザーはこれらをシステムの最適化やコストの軽減などに役立てることができる。

これまであった、ディスク容量、アイドル状況、オーバー プロビジョニング、トランザクション ID の使用率（PostgreSQL）などの推奨事項に加え、アンダー プロビジョニングの推奨事項をプレビューとして提供。

アンダー プロビジョニング状態のインスタンスを特定

CPU 使用率やメモリ使用率が高いインスタンスを検出し、インスタンスを最適化する方法に関する推奨事項を表示する。

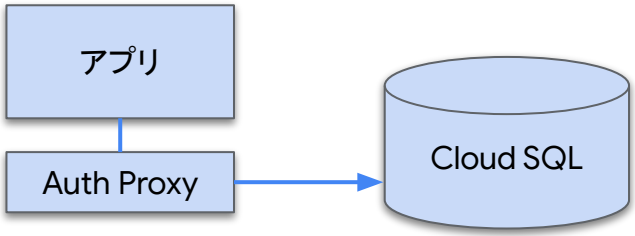


詳細: [アンダープロビジョニング状態のCloud SQL インスタンスを最適化する](https://cloud.google.com/sql/docs/postgres/recommender-underprovisioned?hl=ja)
https://cloud.google.com/sql/docs/postgres/recommender-underprovisioned?hl=ja

Cloud SQL Auth Proxy v2 がリリース

Cloud SQL Auth Proxy とは？

アプリケーションから Cloud SQL に接続する際に、セキュアな接続を提供するツールである。IAM による認証や TLS による通信路の暗号化などを、アプリが自前で管理することなく簡単に利用することができる。



パフォーマンス、安定性、オブザーバビリティが改善した v2

- Cloud Monitoring と Cloud Trace との連携
- Prometheus サポート
- HTTP ヘルスチェック
- サービスアカウントの権限借用（ impersonation）
- 環境変数にる構成
- POSIX 準拠のフラグ

v1 から移行するには？

- 引数やフラグの書式が変更になった部分の修正が必要
- GitHub の cloud-sql-proxy/migration-guide を参考に書式を修正

詳細: https://github.com/GoogleCloudPlatform/cloud-sql-proxy#readme
移行ガイド: https://github.com/GoogleCloudPlatform/cloud-sql-proxy/blob/main/migration-guide.md

Cloud SQL Proxy Operator が Public Preview

Kubernetes 用の Cloud SQL Proxy オペレータの提供

GKE などから Cloud SQL for MySQL / PostgreSQL / SQL Server に接続するための、Auth Proxy を管理する k8s 用 Operator を Public Preview として提供。

これを利用することで容易にAuth Proxy のコンテナを追加利用することが可能。

```
# Kubernetes クラスタに Cloud SQL Proxy Operator をインストール
kubectl apply -f
https://storage.googleapis.com/cloud-sql-connectors/cloud-sql-proxy-operator/v0.3.0/cloud-sql-proxy-operator.yaml

# Cloud SQL Proxy Operator の起動
kubectl rollout status deployment -n cloud-sql-proxy-operator-system cloud-sql-proxy-operator-controller-manager
--timeout=90s
```

詳細: Cloud SQL Proxy オペレータを使用して接続する
https://cloud.google.com/sql/docs/mysql/connect-proxy-operator

GitHub: GoogleCloudPlatform/cloud-sql-proxy-operator
https://github.com/GoogleCloudPlatform/cloud-sql-proxy-operator

リードレプリカへのメンテナンス制御が GA に

メンテナンスの時間枠（ウィンドウ）がレプリカにも有効に

- プライマリ インスタンスで設定した時間枠がレプリカでも有効になる

リードレプリカへのメンテナンスの挙動

- プライマリに先立ちレプリカのメンテナンスが実施
- レプリカが複数台起動している場合、レプリカは一定単位で同時にメンテナンスが実施される
- プライマリ インスタンスにメンテナンス関連の設定がされている場合、それに従ってレプリカのメンテナンスを制御
  - メンテナンス時間枠
  - メンテナンス不要期間
  - メンテナンスの再スケジュール

プライマリ インスタンスでメンテナンス ウィンドウを設定する例。
リードレプリカもこの設定に従ってコントロールされる。

詳細：Cloud SQL インスタンスでのメンテナンスについて| Cloud SQL for PostgreSQL | Google Cloud
https://cloud.google.com/sql/docs/postgres/maintenance#read-replicas

Cloud SQL for SQL Server での追加機能

SqlPackage と bcp ユーティリティに対応 2023-03-30

- Cloud SQL for SQL Server で SqlPackage を利用したデータの import / export に対応
- Cloud SQL for SQL Server で bcp ユーティリティ を利用したデータの import / export に対応

Active Directory 診断ツールの提供 2023-03-27

- Cloud SQL 用の Active Directory (AD) 診断ツールは、オンプレミスの AD ドメインを使用して、Cloud SQL for SQL Server インスタンスでの AS セットアップで起こる可能性がある問題のトラブルシューティングに役立つ

リンクサーバー(Linked Servers) に対応 2023-03-27

- Cloud SQL for SQL Server でリンクサーバーに対応
- 現在の制限として、SQL Server 以外のデータソースと Active Directory Authentication には非対応

詳細: Active Directory Diagnosis tool for Cloud SQL
https://cloud.google.com/sql/docs/sqlserver/ad-diagnosis-tool

詳細: About linked servers | Cloud SQL for SQL Server | Google Cloud
https://cloud.google.com/sql/docs/sqlserver/linked-servers

詳細: Importing and exporting data | Cloud SQL for SQL Server | Google Cloud
https://cloud.google.com/sql/docs/sqlserver/import-export#use-sqlpackage

Preview 2023-02-27

継続的バックアップ リカバリがプレビューとして提供

過去 35 日間の任意の時点を復元可能に

オンデマンド バックアップ、自動バックアップに加え、**継続的バックアップ (Continuous Backup)** が追加された。

Preview 期間中の考慮点

- 現在デフォルトではオフ
- gcloud コマンドで有効にする
- 復元も gcloud コマンドから行う
- Preview 期間中は、この機能によって作成されたファイルは、ストレージのコストにカウントされない

```
# 継続的バックアップの有効化
gcloud beta alloydb clusters update CLUSTER_ID \
    --enable-continuous-backup \
    --continuous-backup-recovery-window-days=WINDOW_LENGTH \
    --region=REGION_ID \
    --project=PROJECT_ID
```

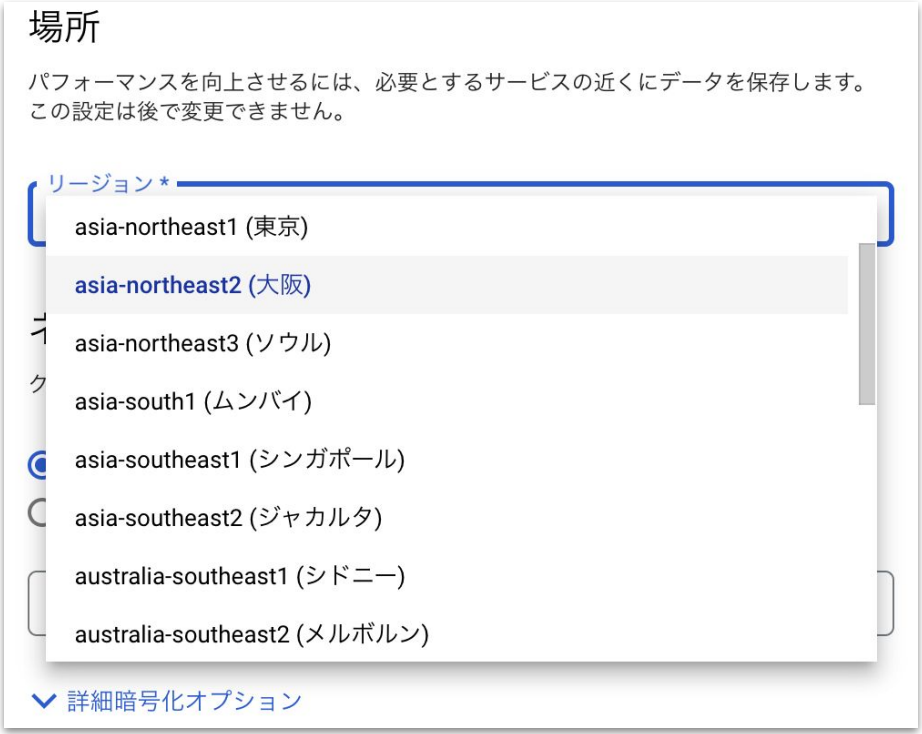
```
# 任意の時点でのリカバリ
gcloud beta alloydb clusters restore CLUSTER_ID \
    --source-cluster=SOURCE_CLUSTER \
    --point-in-time=TIMESTAMP \
    --region=REGION_ID
```

詳細: About backups | AlloyDB for PostgreSQL | Google Cloud
https://cloud.google.com/alloydb/docs/backup/overview#continuous

AlloyDB for PostgreSQL が新たなリージョンに対応

新たに追加されたリージョン一覧

- asia-east1 (台湾)
- asia-east2 (香港)
- **asia-northeast2 (大阪)**
- asia-northeast3 (ソウル)
- asia-south1 (ムンバイ)
- asia-southeast2 (ジャカルタ)
- Australia-southeast2 (シドニー)
- australia-southeast2 (メルボルン)
- europe-central2 (ワルシャワ)
- europe-north1 (フィンランド)
- europe-west2 (ロンドン)
- europe-west6 (チューリッヒ)
- us-east1 (サウスカロライナ州)
- us-east4 (バージニア北部)
- us-west1 (オレゴン州)
- us-west3 (ソルトレイクシティ)



詳細: AlloyDB locations | AlloyDB for PostgreSQL | Google Cloud
https://cloud.google.com/alloydb/docs/locations

AlloyDB Omni がテクニカル プレビューとして提供

ダウンロードできるAlloyDB

AlloyDB Omni とは、AlloyDB をローカルの環境で動作できるようにしたもの。**AlloyDB for PostgreSQL のエンジンをコンテナ化したもので、ダウンロードして手元で使うことができる** 。

AlloyDB と AlloyDB Omni の違い

AlloyDB Omni は AlloyDB のコンピューティング エンジン部分をローカルで動かすものなので、**AlloyDB のストレージ エンジン部分など、Google Cloud に依存したコンポーネントは利用できない**

開発環境としてのAlloyDB

AlloyDB Omni 現在はテクニカル プレビュー版としての提供でフィードバックを集めている最中で、まだ本番利用は想定されていない。まずはローカルでの開発環境などとして使うことができる。

詳細: [AlloyDB Omni を使い始めるには](https://cloud.google.com/blog/ja/products/databases/get-started-with-alloydb-omni?hl=ja)
https://cloud.google.com/blog/ja/products/databases/get-started-with-alloydb-omni?hl=ja

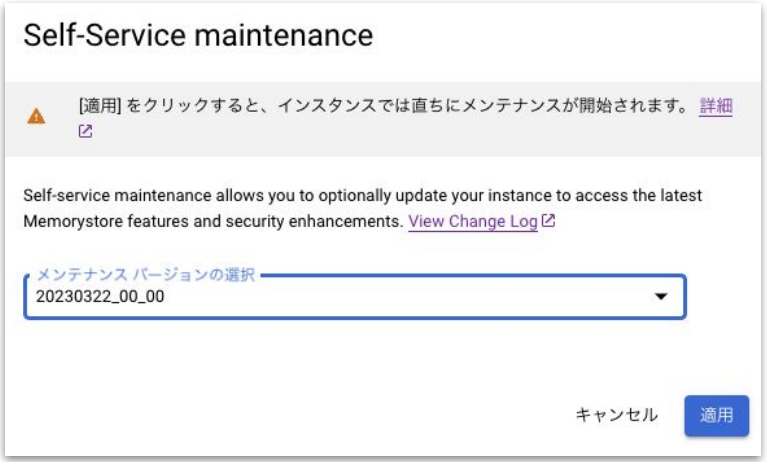
セルフサービス メンテナンスが GA

Memorystore for Redis のメンテナンス

Memorystore では Cloud SQL 同様定期メンテナンスで、各種セキュリティパッチや、エンジンのマイナーバージョンアップを行ってきた。

しかし特にセキュリティ パッチなど、より細かい頻度で追従したいといった要望に答えるため、提供されたメンテナンス バージョンを、ユーザーが任意のタイミングで（セルフサービスで）適用できるようになった。

セルフサービス メンテナンスを行わない場合、累積された更新は、次回の定期メンテナンスで実施される。



詳細: Self-service maintenance | Memorystore for Redis | Google Cloud
https://cloud.google.com/memorystore/docs/redis/self-service-maintenance

Google 標準 SQL の関数において Lambda 式をサポート

Lambda 式と配列関数の追加

Google 標準 SQL の関数呼び出しにおいて、Lambda 式が新たに追加された。また配列関数に新たなものが追加された。

- Lambda 式
  - (arg[, ...]) -> body_expression
  - arg -> body_expression
- 今回追加された配列関数
  - ARRAY_FILTER
  - ARRAY_TRANSFORM
  - ARRAY_INCLUDES_ALL
  - ARRAY_INCLUDES_ANY
  - ARRAY_MIN
  - ARRAY_MAX

Lambda 式を引数にとる関数

ARRAY_FILTER、ARRAY_TRANSFORM、ARRAY_INCLUDES といった関数は引数に Lambda 式をとることができる。そのため、複雑なフィルターや変換処理を行うことができるようになった。

```
spanner> SELECT
      ->   ARRAY_TRANSFORM([1, 2, 3], e -> e + 1) AS a1,
      ->   ARRAY_TRANSFORM([1, 2, 3], (e, i) -> e + i) AS a2;

+-----------+-----------+
| a1        | a2        |
+-----------+-----------+
| [2, 3, 4] | [1, 3, 5] |
+-----------+-----------+
```

例）a1 は配列の値 e に +1 した配列を返し、a2 は配列の値 e に配列の添字 i を足した結果の配列を返す。

詳細: [Array functions in GoogleSQL | Cloud Spanner](https://cloudoogle.com/spanner/docs/reference/standard-sql/array_functions#array_transform)
https://cloudoogle.com/spanner/docs/reference/standard-sql/array_functions#array_transform

FGAC - テーブルや列レベルのアクセス制御の提供

Fine-grained access control (FGAC)

プレビュー提供されていた FGAC が GA。RDBMS で一般に用いられる DB 内のロールと、**GRANT / REVOKE** SQL ステートメントを使用し、詳細なアクセス制御を実現。またロールと IAM プリンシパルの紐付けも可能。

FGAC で制御できる権限

- **SELECT / INSERT / UPDATE** について、実行可能なテーブル及び列の制限が可能
- **DELETE** については実行可能なテーブルの制限が可能

```
GRANT SELECT ON TABLE employees TO ROLE hr_director;

GRANT SELECT ON TABLE customers, orders, items TO ROLE account_mgr;

GRANT SELECT(name, level, cost_center, location, manager) ON TABLE employees TO ROLE hr_manager;

GRANT SELECT(name, address, phone) ON TABLE employees, contractors TO ROLE hr_rep;
```

FGAC を用いてSELECT 可能なテーブルや列の制限をかけている例

IAM プリンシパルとロールの紐付け

詳細:[きめ細かいアクセス制御について| Cloud Spanner](https://cloud.google.com/spanner/docs/fgac-about)
https://cloud.google.com/spanner/docs/fgac-about

Cloud Spanner インスタンスにタグの付与が可能に

タグを条件としたアクセス制御

Cloud Spanner がタグに対応し、インスタンスに付与されたタグに応じた IAM の設定などが可能になった。

例えば env:test タグの付与を条件として Spanner 管理者権限をユーザーに与える。この例では、該当プリンシパルは、テスト環境（test-instance）にはアクセス可能だが開発環境（dev-instance）にはアクセス不可となる。

名前	ID	処理ユニット	ストレージの利用率	タグ
dev-instance	dev-instance	1,000	552.2 GB / 4 TB	env : dev
test-instance	test-instance	200	4.1 MB / 819 GB	env : test

詳細: Google Cloud タグでリソースを整理する| Cloud Spanner
https://cloud.google.com/spanner/docs/tags?hl=ja

Preview 2023-03-31

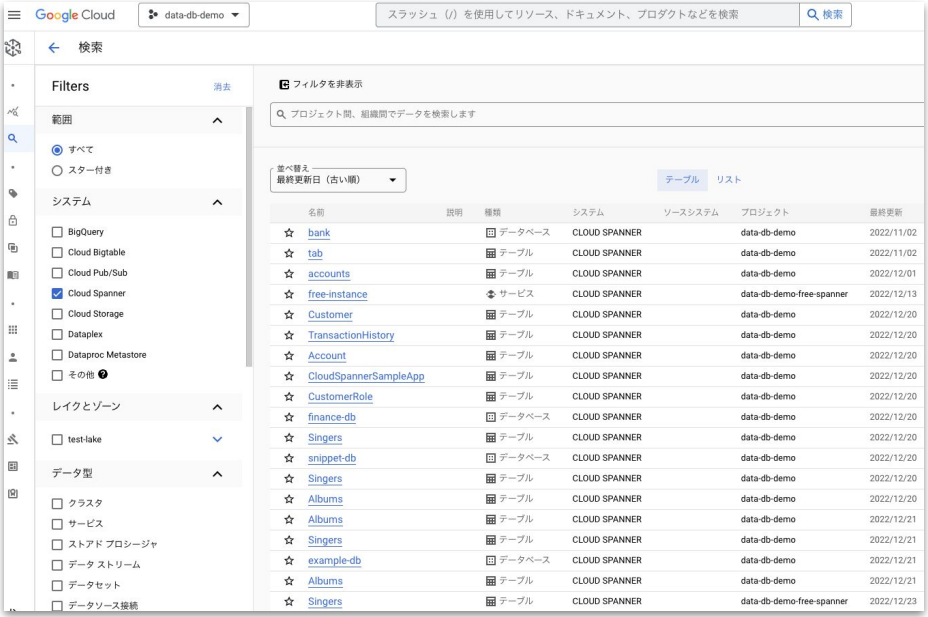
Data Catalog 連携がプレビュー提供

Data Catalog で Cloud Spanner テーブルを管理

Dataplex にてメタデータ管理を行う Data Catalog と Cloud Spanner が統合。Cloud Spanner インスタンス、データベース、テーブル、カラム、ビューなどのメタデータを、カタログとして自動管理。

自動カタログ対象

- 名前と FQDN
- ロケーション（リージョン）
- 作成日と最終更新日
- スキーマ（テーブルとビュー）
- 説明



詳細: Data Catalog を使用してリソースを管理する| Cloud Spanner
https://cloud.google.com/spanner/docs/dc-integration?hl=ja

Oracle DB から Cloud SQL for PostgreSQL への移行に対応

DMS 初の異種 DB 間の移行サポート

Oracle から Cloud SQL for PostgreSQL への移行機能が、DMS 最初の異種 DB 間マイグレーションとして、プレビュー提供。ora2pg を利用したスキーマ変換をサポートしている。

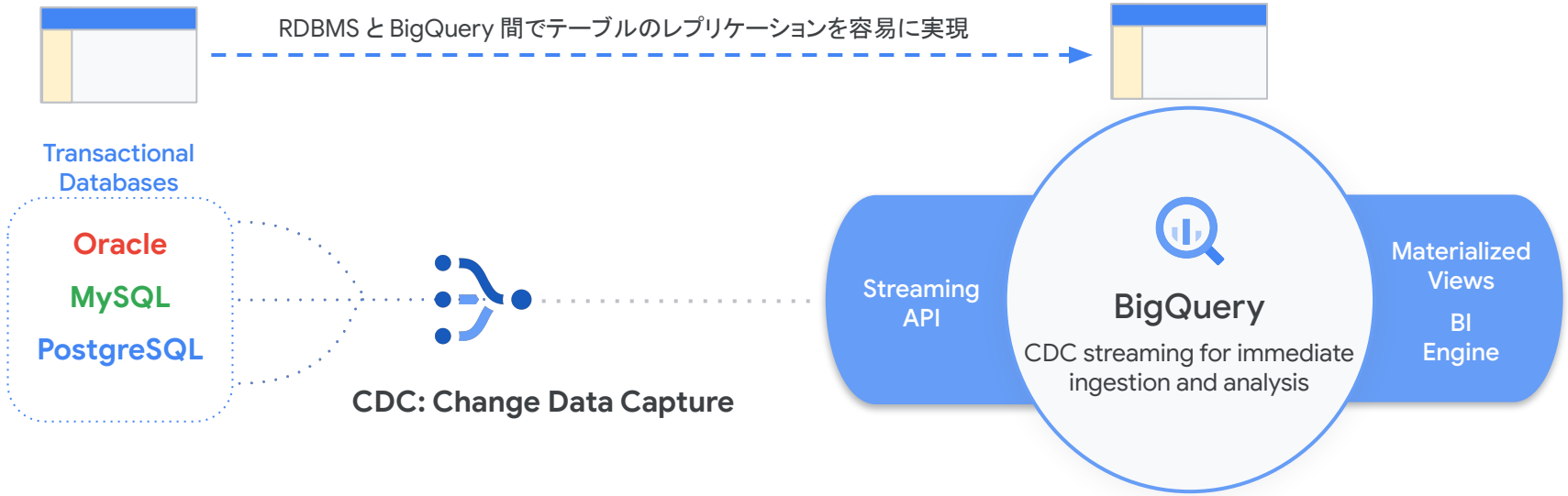
詳細: Migrate Oracle workloads into Cloud SQL for PostgreSQL by using Database Migration Service | Google Cloud
https://cloud.google.com/database-migration/docs/oracle-to-postgresql/quickstart

2023-04-04

Datastream for BigQuery 及び PostgreSQL ソースが GA

ビジネス イベントを鮮度あるリアルタイムで分析
トランザクション データを BigQuery に連続的に複製する
ことにより、いち早く示唆を得られるように

自動化されたデータ結合
中間テーブルやデータ結合のための作業が不要



詳細: Datastream for BigQuery | Google Cloud
https://cloud.google.com/datastream-for-bigquery?hl=ja

05

Networking

Preview 2023-01-26

ポリシーベースのルーティングが Preview

パケットの宛先 IP アドレス以外の条件も使用して、ネクストホップを選択出来るように

- 送信元 IP アドレス、プロトコルを指定してルートを作成し、内部 TCP / UDP ロードバランサにリダイレクト
- Cloud Interconnect 接続を介してオンプレミスネットワークから VPC ネットワークに送信されるトラフィックにもポリシーベースのルートを作成可能

```
# ポリシーベースのルート作成
gcloud network-connectivity policy-based-routes create
ROUTE_NAME \
    --source-range=IP_RANGE_A \
    --destination-range=IP_RANGE_B \
    --ip-protocol=IP_PROTOCOL \
    --network="projects/PROJECT_ID/global/networks/NETWORK" \
    --tags=NETWORK_TAGS \
    --next-hop-ilb-ip=LOAD_BALANCER_IP \
    --description=DESCRIPTION \
    --priority=PRIORITY
```

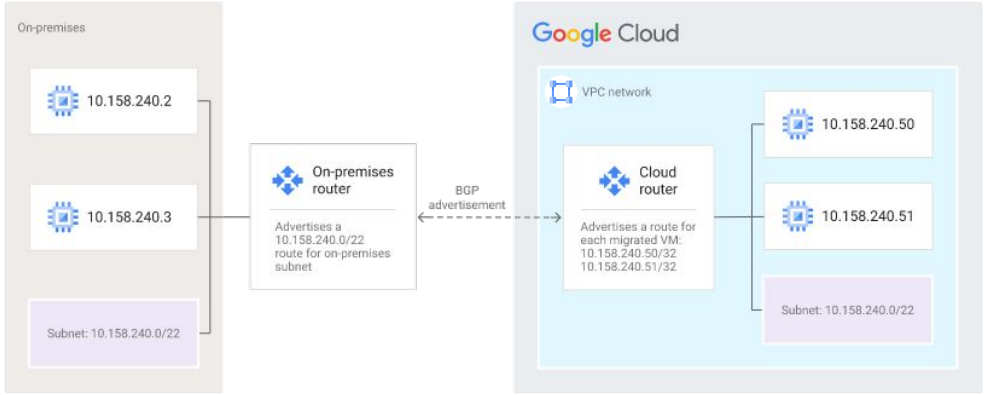
詳細 : https://cloud.google.com/vpc/docs/policy-based-routes?hl=ja

Preview 2023-03-14

オンプレミスとのハイブリットサブネットが Preview

オンプレミスサブネットと VPC サブネットを1つの論理サブネットとして統合

- IP アドレスを変更しなくても、個々のワークロードの移行がよりスムーズに実施可能
- オンプレミスサブネットと VPC サブネットのプライマリ IPv4 アドレス範囲を一致させて作成
- Cloud Router の BGP セッションのカスタムルートアドバタイズを利用して、VM の /32 IP アドレスをアドバタイズして接続



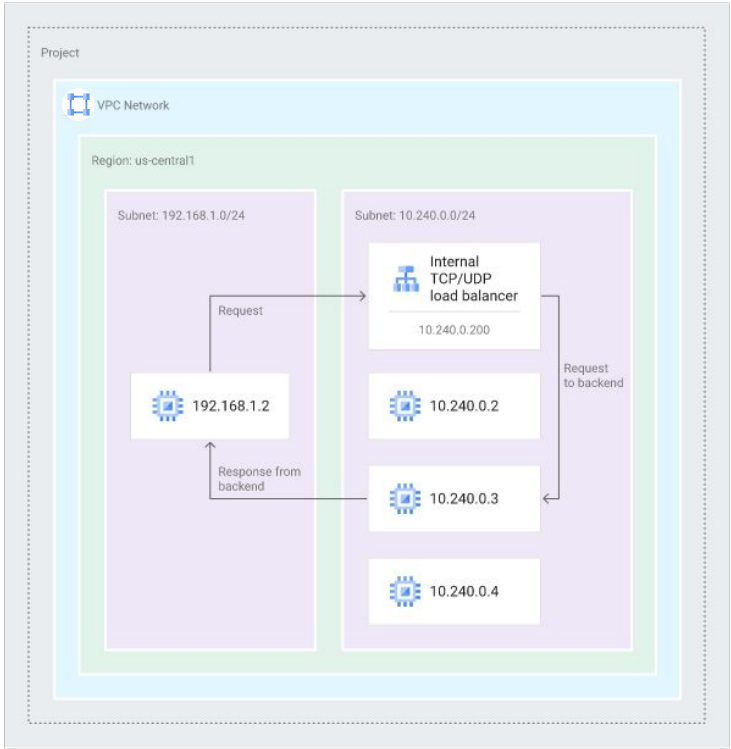
詳細 : https://cloud.google.com/vpc/docs/hybrid-subnets?hl=ja

ネットワークロードバランサと内部 TCP / UDP ロードバランサのロギングが GA

L4 のロードバランサでもロギングが可能に

- 各接続がサービスを提供するバックエンドにどのようにルーティングされるかについての分析情報が取得可能
- ログを有効にしても、ロードバランサのパフォーマンスに影響はありません

```
# ログの形式例
connection.clientIp: 192.168.1.2
connection.serverIp: 10.240.0.200
bytesSent: 1256
bytesReceived: 4521
```



詳細 : https://cloud.google.com/load-balancing/docs/internal/internal-logging-monitoring?hl=ja#ilblb-logging
https://cloud.google.com/load-balancing/docs/network/networklb-monitoring?hl=ja#netlb-logging

Preview 2023-01-31

柔軟なパターンマッチングを使用した高度なトラフィック管理が Preview

pathMatcher の任意の場所でのワイルドカード適用が可能に

- 柔軟なパターン マッチング演算子を使用すると、単純なワイルドカード構文を使用して、URL パスの複数の部分（部分的な URL や接尾辞、ファイル拡張子）を照合可能
- パス コンポーネントを名前付き変数に関連付けて、URL を書き換える際にそれらの変数を参照することも
- 書き換えられたリクエストは、書き換えられた URL パス を使用して cart-backend に送信

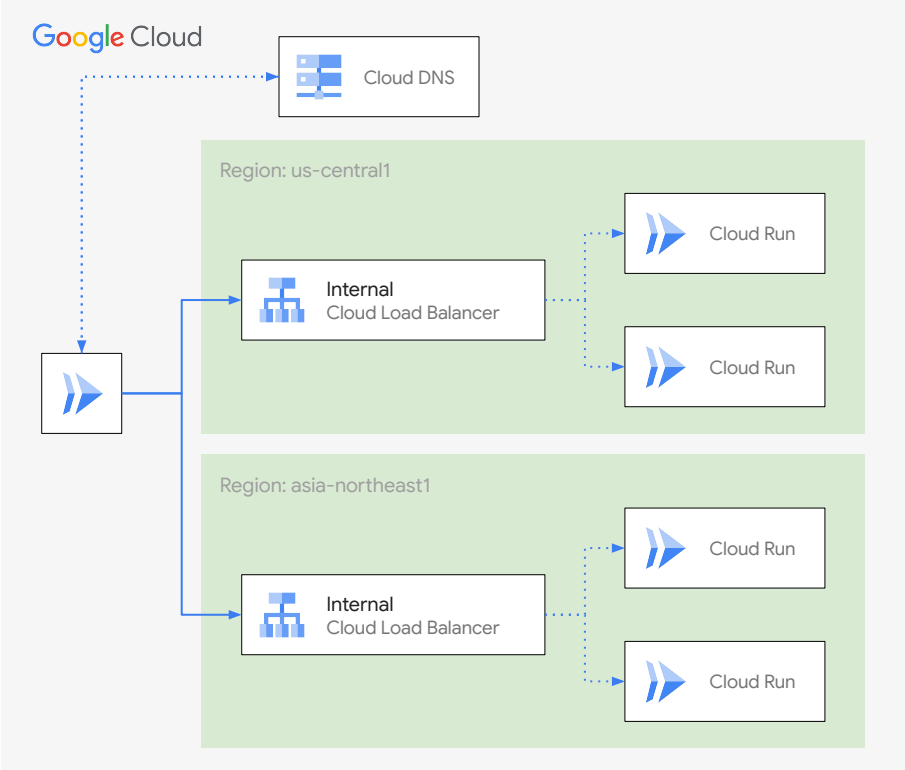
```
# パターンマッチの形式例
 pathMatchers:
    - name: Cart-Matcher
      routeRules:
        - description: CartService
          matchRules:
            - pathTemplateMatch:
'/xyzwebservices/v2/xyz/users/{username=*}/carts/{cartid=**}'
          service: cart-backend
          priority: 1
          routeAction:
            urlRewrite:
              pathTemplateRewrite: '/{username}-{cartid}/'
    - name: User-Matcher
      routeRules:
        - description: UserService
          matchRules:
            - pathTemplateMatch:
'/xyzwebservices/v2/xyz/users/*/accountinfo/*'
          service: user-backend
          priority: 1
```

詳細 : https://cloud.google.com/load-balancing/docs/url-map-concepts?hl=ja#wildcards-regx-dynamic-route

Cloud DNS の内部ロードバランサのヘルスチェックと自動フェイルオーバーが GA

複数の内部ロードバランサを持つ構成などに対するフェイルオーバーが容易に

- 各リージョン毎に同様の構成を構築し、内部ロードバランサにてルーティングされているケースなどに有用
- 内部ロードバランサに対するヘルスチェックと自動フェイルオーバーを構築可能

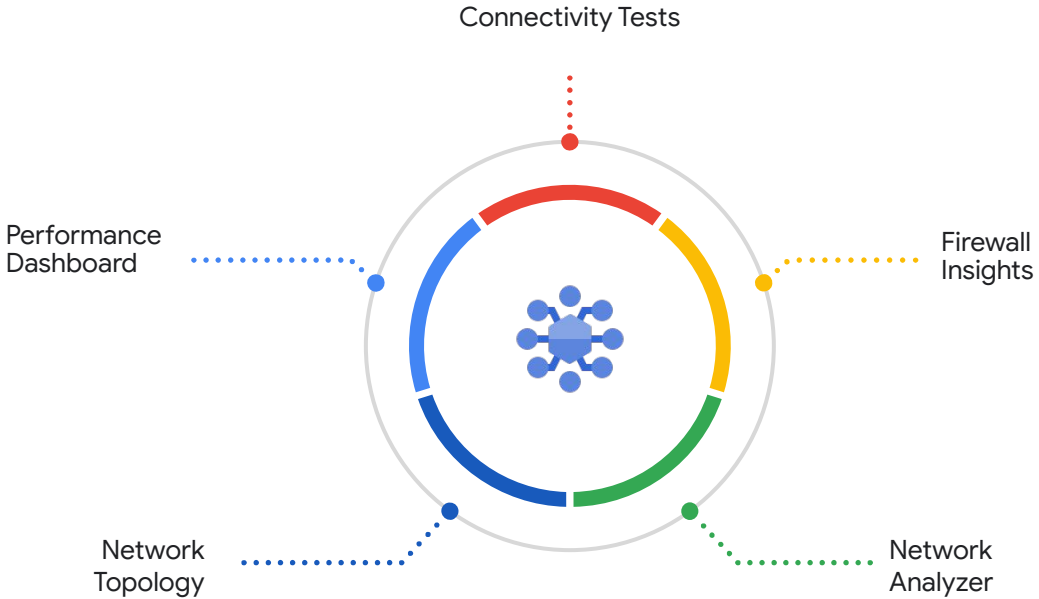


詳細 : https://cloud.google.com/dns/docs/policies-overview?hl=ja#health_checking_for_internal_load_balancers

Network Intelligence Center (NIC) のご紹介

NIC が有する 5 つの機能

- **Network Topology**
  実際のトラフィックに基づくGoogle Cloud での構成と外部への通信の可視化
- **Performance Dashboard**
  Google Cloud 全体と、プロジェクトリソースのネットワークパフォーマンス指標を可視化
- **Connectivity Test**
  接続の問題をトラブルシューティングするためのテストとトレースパスを提供
- **Firewall Insights**
  ファイアーウォールをよりセキュアに運用するための分析を提供
- **Network Analyzer**
  ネットワーク構成ミスや最適でない構成を検出し、障害を特定



GA

Network Intelligence Center のご紹介

Connectivity Test の送信元エンドポイントの対象が拡大

- 複数のネットワークインターフェースを持つインスタンスを含む、IPv4 と IPv6 の両方のアドレスを持つデュアル スタック インスタンス
- Cloud Run リビジョン
- App Engine スタンダード環境

詳細 :
https://cloud.google.com/network-intelligence-center/docs/connectivity-tests/how-to/running-connectivity-tests?hl=ja#running-conn-test

Network Intelligence Center のご紹介

Firewall Insights の機能がアップデート

- 使用パターンと傾向に基づいて、アクティブでなくなった allow ルールを確認できるように
  過去 6 週間の平均ヒット数と最近のヒット数の傾向を考慮した機械学習分析によって生成
- シャドウルール (実質的に設定が無効なルール) の検出対象にファイアーウォールポリシーも対象に

詳細 : https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/insights-categories-states?hl=ja#no-hits-trend-analysis
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/insights-categories-states?hl=ja#shadowed-firewall-rules

Appendix

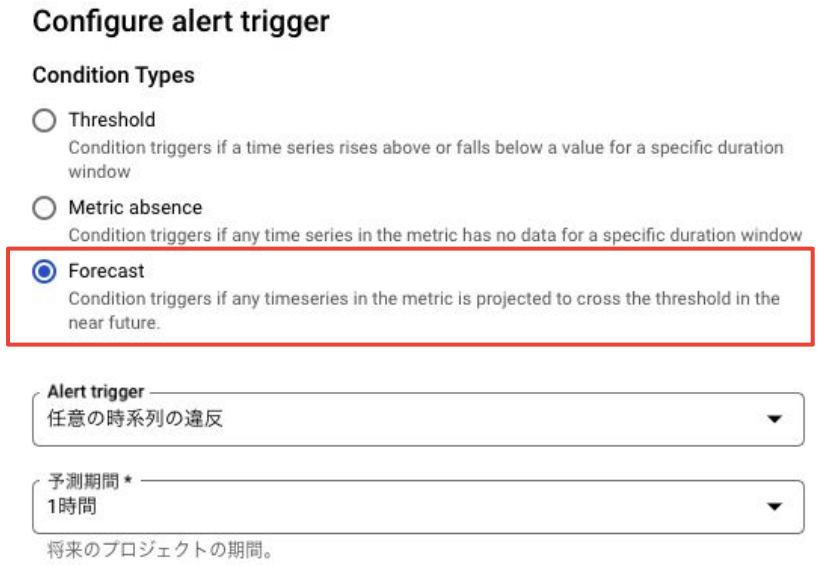
その他のアップデート

Preview 2023-01-25

しきい値に違反することを予測可能に (Preview)

制約のあるリソースの管理がより柔軟に

- クォータ（割り当て）、ディスク容量、メモリ使用量など制約のあるリソースのモニタリングに、実測値ではなく予測によりアラート
- 予測ウインドウは 1 時間～ 7 日間で指定
- 初期トレーニングは予測ウィンドウの長さの 2 倍
- 各決定アルゴリズムは、予測ウィンドウの最大 6 倍までの長さのデータで継続的にトレーニング



詳細 : https://cloud.google.com/monitoring/alerts/types-of-conditions?hl=ja#forecast

Google Cloud

Google Cloud
UPDATES

次回予告

Data Analytics / ML 編
2023 年 7 月 24 日 (月) 15:00 ~ 16:30
カレンダーに追加はこちらから

Compute / DB 編
2023 年 7 月 31 日 (月) 15:00 ~ 16:30
カレンダーに追加はこちらから

Google Cloud

Google Cloud Day ’23 Tour

TOKYO Online 5.23 - 25

OSAKA Hybrid 6.2

NAGOYA Hybrid 6.22

FUKUOKA Hybrid 6.30

企業の DX を加速する、そのヒントを 4 都市からお届けします。今すぐ登録 goo.gle/gcd23_1p