

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



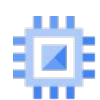
Taka Sato
Database



Yuma Shoji
Network, その他

01

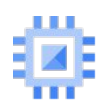
Infrastructure



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%



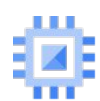
Tau T2A VM がセキュアブートをサポート

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](#)

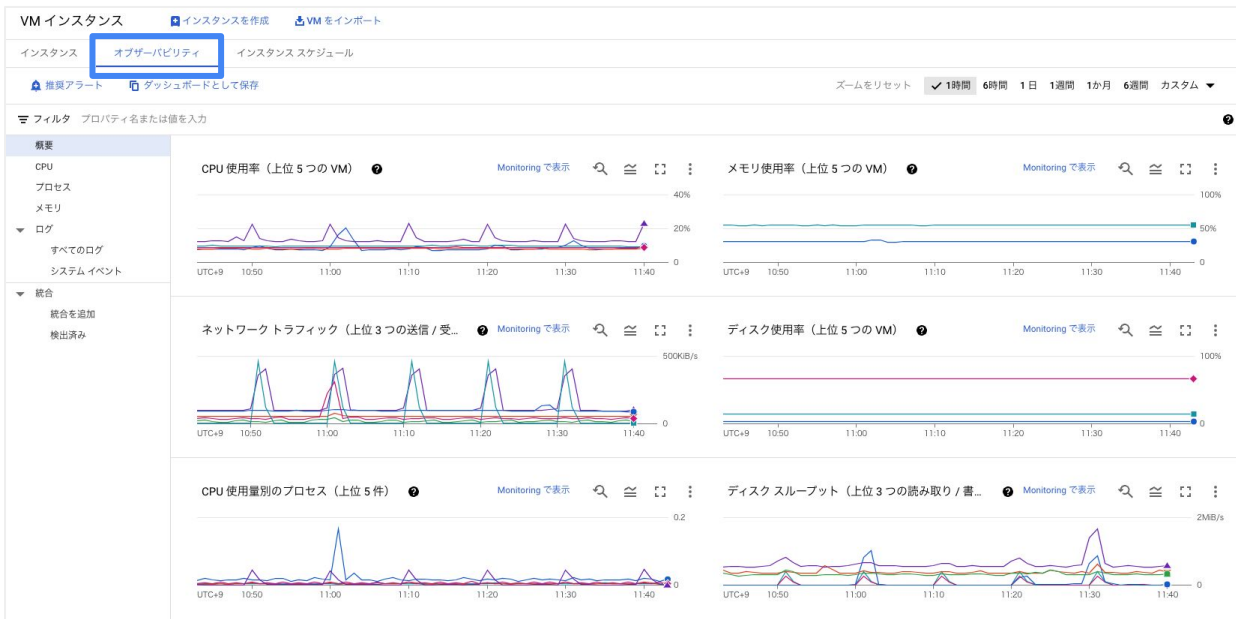
ワークロードタイプ					
汎用のワークロード			最適化されたワークロード		
コスト最適化	バランス	スケールアウト最適化	メモリ最適化	コンピューティング最適化	アクセラレータ最適化
E2	N2, N2D, N1	Tau T2D, Tau T2A	M3, M2, M1	C2, C2D	A2
低コストで日々のコンピューティングを実現	幅広いマシンタイプにわたるバランスの取れた価格とパフォーマンス	スケールアウトワークロードに最適なパフォーマンスと費用	超高メモリワークロード	超高パフォーマンスでコンピューティング負荷の高いワークロードを実現	ハイパフォーマンスコンピューティングワークロード向けに最適化
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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

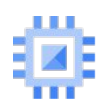


オブザーバビリティタブ

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





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](#)

Compute Engine

td-demo-hello-world-mig の編集 [ステートフルにする](#)

インスタンス グループ

- インスタンス グループ
- ヘルスチェック

VM Manager

- OS Patch Management
- OS 構成管理

Bare Metal Solution

- サーバー
- ネットワーク
- ボリューム
- NFS 共有

設定

- メタデータ

VM インスタンスのライフサイクル

VM が作成、修復、削除された場合の動作を構成します

VM インスタンス修復中の更新

- インスタンス構成を維持
VM を再作成するときに、元のインスタンス テンプレートと作成時に使用されたインスタンスごとの構成を使用します
- インスタンス構成を更新
VM を再作成するときに、最新のインスタンス テンプレートとインスタンスごとの構成を適用します

自動修復

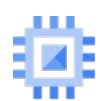
Autohealing recreates VM instances if your application cannot be reached by the health check. [Learn more](#)

ヘルスチェック
td-test-health-check1 (HTTP)

ポート: 80、タイムアウト: 5 秒、チェック間隔: 5 秒、異常しきい値: 2 回の試行

初期遅延*
300 秒

i 自動修復を使用するには、ファイアウォール ルールを構成します。これにより、グループ内の VM インスタンスにヘルスチェックを接続できます。 [How to configure firewall rules to allow health checking](#)



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

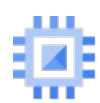
Google Cloud CLI または API のみ

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。

gcloud API

スナップショット スケジュールの説明、スケジュール、ラベルを更新するには、`gcloud beta compute resource-policies update snapshot-schedule` コマンドを使用します。

```
gcloud beta compute resource-policies update snapshot-schedule SCHEDULE_NAME \
  --region=REGION \
  --description="DESCRIPTION" \
  --start-time=START_TIME \
  SCHEDULE_FLAG \
  --snapshot-labels="KEY=VALUE"
```



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ー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

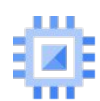
参照:「永続ディスクの非同期レプリケーションについて」を参照してください。

- 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

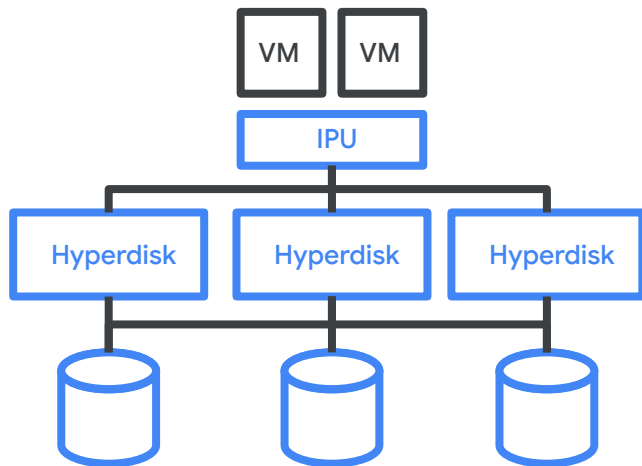
- Replica State では、2ゾーンに存在する永続ディスクのデータが同期されているかなどが確認可能



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](#)

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？

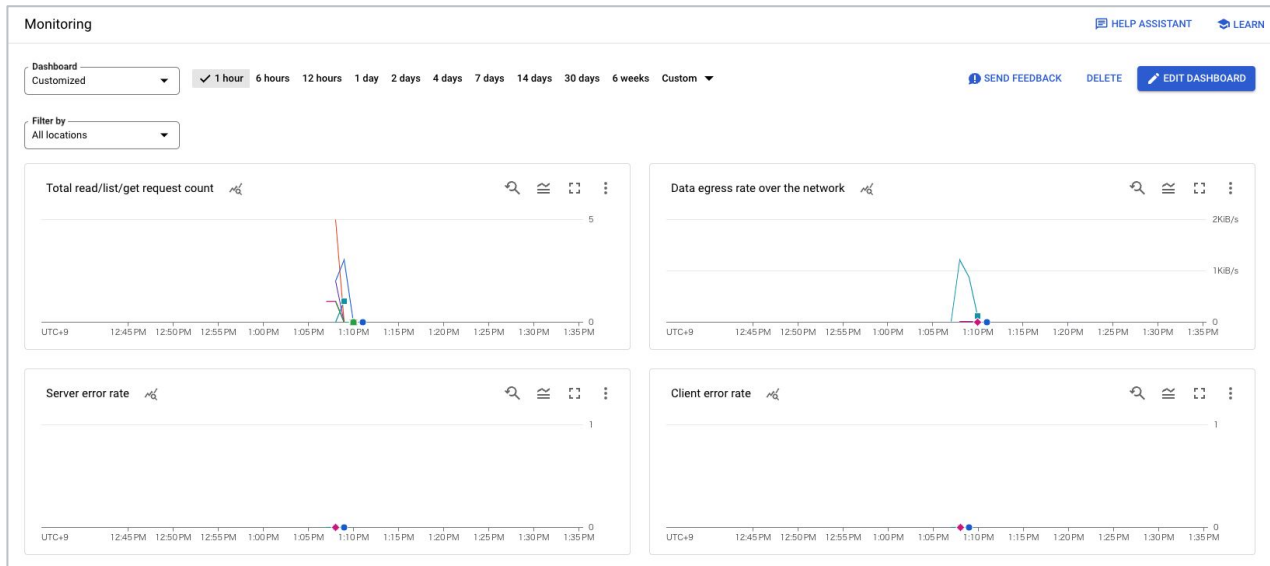
- 2022 年 Q3 にリリース
- gsutil コマンドライン ツールと比較して、アップロードとダウンロードのパフォーマンスが高速

参考: [New gcloud storage CLI for your data transfers](#)

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



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



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

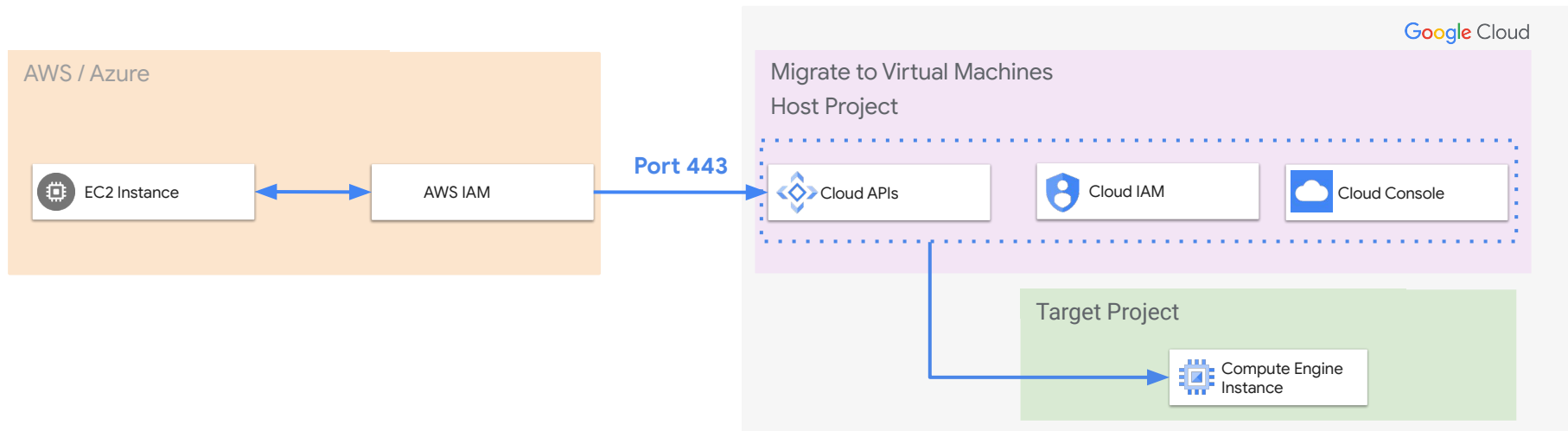
- AWS EC2 インスタンスを Compute Engine に移行可能
- Azure Virtual Machines インスタンスを Compute Engine に移行可能

GA

2023-01-16

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

ダッシュボード ソース 移行 グループ ターゲット

Migrate to Virtual Machines へようこそ 非表示

✓ ソースの追加
移行元を接続します。
[ソースを管理](#)

✓ ターゲットを追加する
Add GCP projects as targets for migrated VMs.
[ターゲットを管理](#)

✓ 移行を追加
ソースから Google Cloud に移行する VM を選択します。
[移行を追加](#)

✓ グループの作成
グループとして VM を整理して移行します。
[グループを管理](#)

	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

Compute Engine

Migrate to Virtual Machines

ダッシュボード ソース 移行 グループ ターゲット

仮想マシン

- VM インスタンス
- インスタンス テンプレート
- 単一テナントノード
- マシンイメージ
- TPU
- 確約利用割引

ソースでアップデートが利用可能です。

vcsa-1 ▲ 2件のソースでアップデートが利用可能です。

ソースを追加 ▼

- + VMware ソースを追加します ☒
Supports on-premises and VMware Engine
- + AWS ソースを追加します

Source is the cloud environment or the on-prem VMware data center hosting the VMs that you want to migrate.

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](#)



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

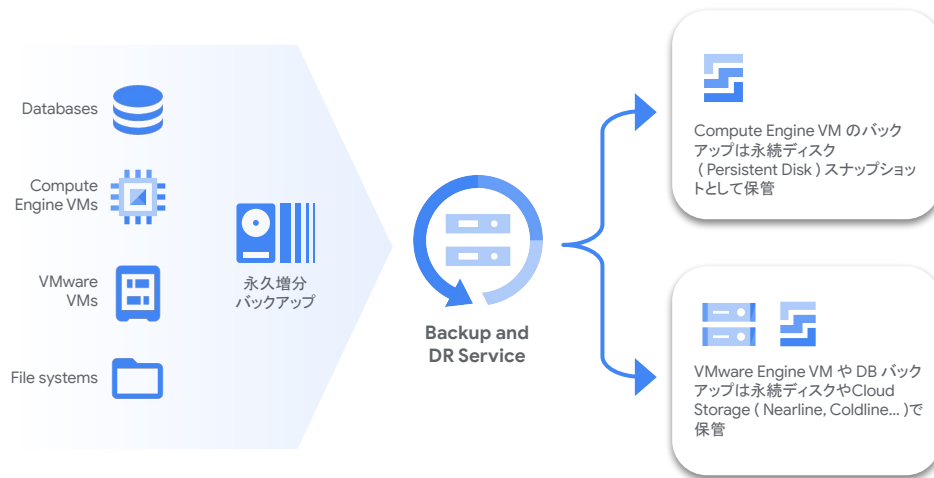


Backup & DR 機能概要

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



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。)

The screenshot shows the Google Cloud console interface for configuring VPC Service Controls. The left sidebar contains navigation options like Security Command Center, reCAPTCHA Enterprise, and VPC Service Controls. The main area is titled 'VPC サービス境界の編集' (Edit VPC Service Perimeter). A dialog box titled 'リソースを追加' (Add Resources) is open, showing a list of VPC networks to be added to the perimeter. The selected resources are 'primary-vpc' and 'secondary-vpc'. The dialog also includes a search filter and pagination controls.



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



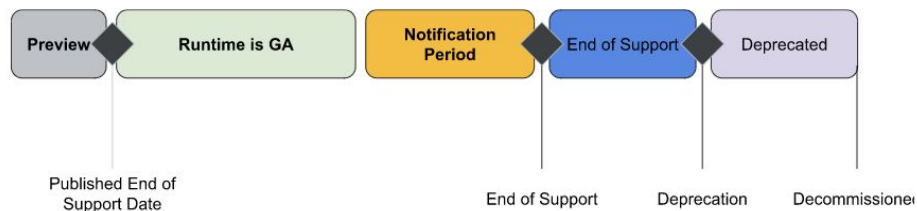
App Engine 第 1 世代の EoS について

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)

移行先

- Cloud Run
- App Engine 第 2 世代



	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



バックエンド サービス ベースの外部ネットワーク ロードバランサーが一般提供

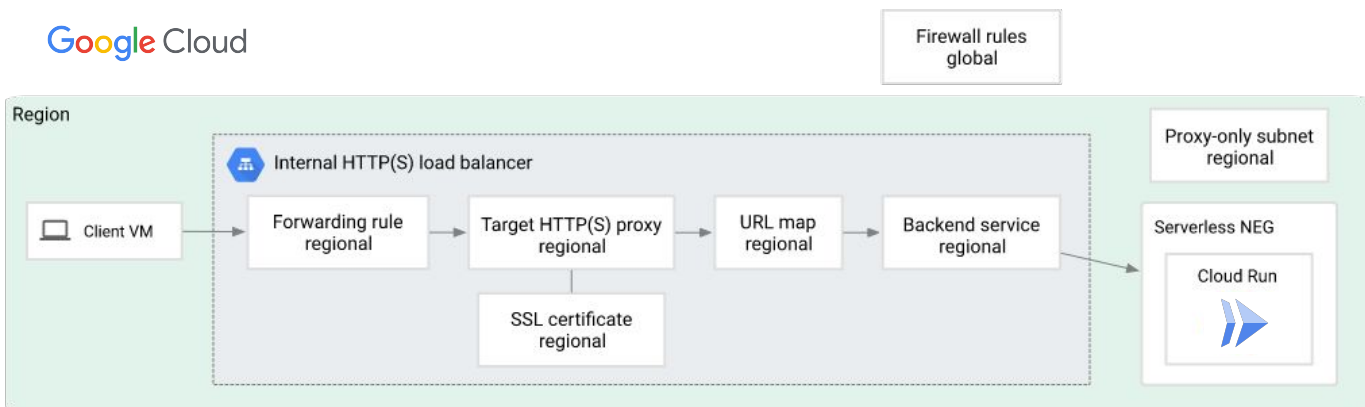
既存のターゲットプールベースのロードバランサーと比べ多くの機能を提供

- 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
```

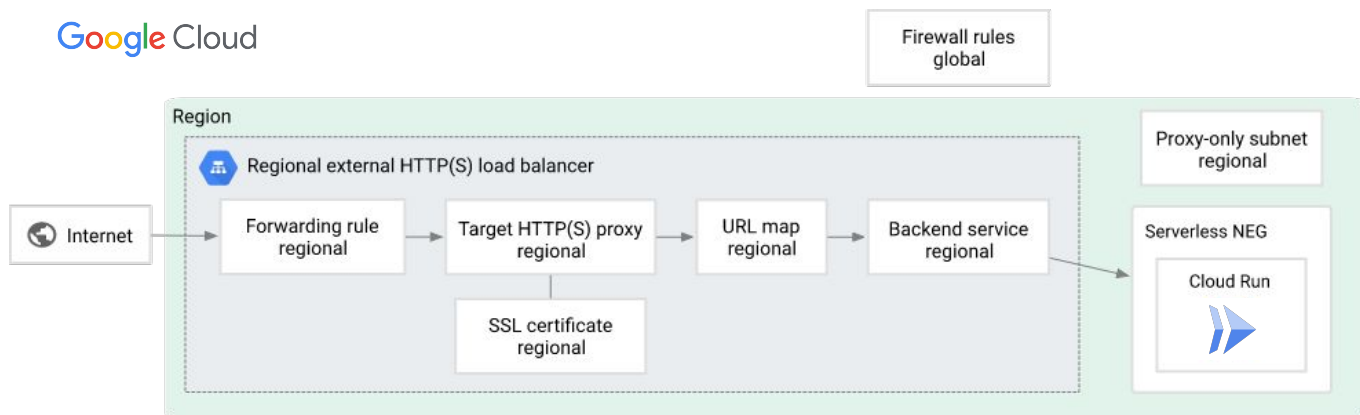
内部 HTTP(S) ロードバランサーで Cloud Run をバックエンドとして設定可能

- 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



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

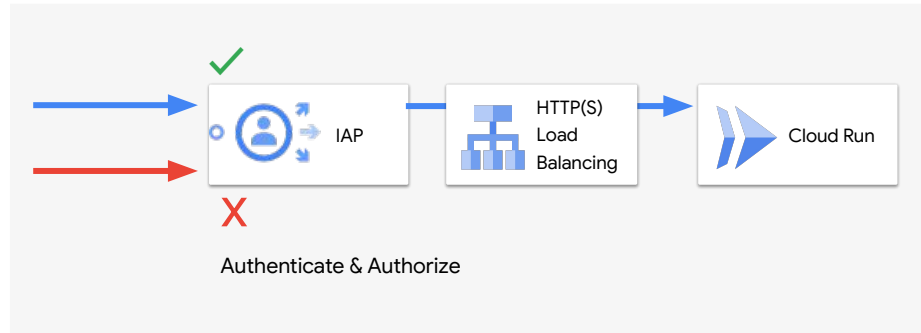
- サーバレス NEG を使用して外部リージョン HTTP(S) ロードバランサーのバックエンドに Cloud Run を指定可能
- 単一のリージョンで Cloud Run サービスを公開する際に利用可能



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





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

ランタイム、ビルド、接続、セキュリティの設定 ↑

< **ランタイム** ビルド 接続 セキュリティとイメージ >

割り当てられるメモリ* ▼
2 GiB

CPU (preview)* ▼
1

タイムアウト* 秒 ?
60

同時実行 **プレビュー**

インスタンスあたりの最大同時リクエスト数 ?
100

暗号化 ?

- Google が管理する暗号鍵
構成は不要です
- 顧客管理の暗号鍵 (CMEK) **プレビュー**
[Google Cloud Key Management Service](#) で管理します

顧客管理の暗号鍵を選択*

キーが表示されない場合は、権限を確認してください。 [詳細](#)注: CMEK 暗号化を選択する場合は、暗号化された Artifact Registry を選択する必要があります。イメージ リポジトリで選択内容を確認してください。 [詳細](#)



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

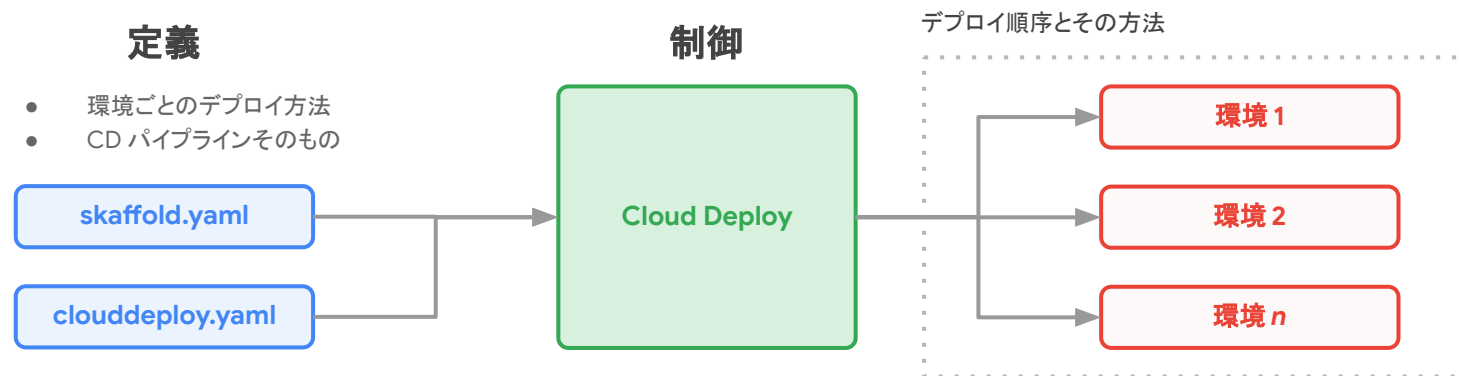
機能	Cloud Build リポジトリ (第 1 世代)	Cloud Build リポジトリ (第 2 世代)
ブランチ push、タグの push、pull リクエスト イベントに対応してビルドできます。	あり	あり
手動トリガーを作成できます	あり	いいえ
Pub/Sub トリガーを作成できます	あり	いいえ
Webhook トリガーを作成できます	あり	いいえ
リポジトリに対して単一の接続を作成し、その接続の認証を使用して、追加の接続を設定できます。	いいえ	あり
GitHub と GitHub Enterprise からリポジトリを接続できます	あり	あり
GitLab Enterprise 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
<code>gcloud</code> 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



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)





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

Rollout rel-002-to-dev-0001

Rendering

Scaffold profiles	None
Render logs	Build cfc1b2c6-04ed-4972-b02c-2da52533a1fd
Target artifacts	manifest.yaml View skaffold.yaml View

Deployment

Target	dev
Latest Status	Successful
Deployment logs	Build dd995444-a46a-49b0-9cd8-4556e8f28f6e

Verification

Target	dev
Latest Status	Failure
Verification logs	Build c5274eed-b437-4a03-bbfe-b93d9c47063b Build 3e458b73-30e6-471b-b459-cffaad639483

Approval

Approval status	No approval required
-----------------	----------------------



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 ]
```

The screenshot shows the Cloud Deploy console interface. At the top, the breadcrumb navigation is: Cloud Deploy > Delivery pipelines > DELIVERY PIPELINE frontend-app > TARGET prod-multi. The 'Target details' section shows: Name: prod-multi, Approval required: No, Target type: Multi-target (indicated by a red arrow), Deployment strategy: Standard, and Resource name: projects/clouddeploy-experiment-test1/locations/us-central1/targets/prod-multi. The 'Last release' section shows: Release: app-release-002, Rollout: app-release-002-prod-multi (with a green checkmark), and Completed: Feb 21, 2023, 8:11:23 AM. The 'Metadata' section shows: Description: production clusters. Below this, there are tabs for ROLLOUTS, CHILD TARGETS (selected), and EXECUTION ENVIRONMENTS. A filter bar is present with the text 'Filter Enter property name or value'. The table below lists the child targets:

Name	Type	Deployment target
prod-us-central1	Google Kubernetes Engine	my-app-frontend/us-central1/cluster-prod1
prod-us-west1	Google Kubernetes Engine	my-app-frontend/us-west1/cluster-prod2



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])
```

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。

The screenshot shows the Google Cloud console interface for Cloud SQL instances. At the top, there's a search bar and navigation options. Below that, a notification states: "You have 135 recommendations across 68 instances for this project." A table lists various instances with columns for Instance ID, Recommendations, Status, Maintenance, Type, Public IP address, Private IP address, Instance connection name, High availability, and Location. Recommendations include "Configure SSL", "Upgrade for security patches", and "Configure SSL".

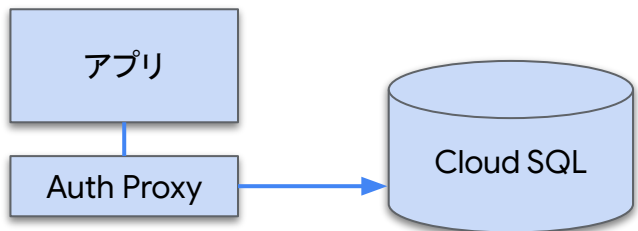
Instance ID	Recommendations	Status	Maintenance	Type	Public IP address	Private IP address	Instance connection name	High availability	Location
apana-cloud-run-postgres-instance	Configure SSL	—	—	PostgreSQL_14	34.71.67.117	—	cloud-debugging-us-central1-a	ENABLED	us-central1-a
bigquery-mysql-test	Configure SSL	—	—	MySQL_8.0	34.161.114.102	—	cloud-debugging-us-central1-a	ENABLED	us-central1-c
bigquery-sampling-rate	Configure SSL	—	—	PostgreSQL_13	35.223.68.115	—	cloud-debugging-us-central1-a	ENABLED	us-central1-b
bulktest1	Configure SSL	—	—	PostgreSQL_14	35.193.166.10	—	cloud-debugging-us-central1-a	ENABLED	us-central1-a
conn-load-dev	Upgrade for security patches	—	—	PostgreSQL_14	34.172.243.67	10.96.240.241	cloud-debugging-us-central1-a	ADD	us-central1-b
creation-message	Configure SSL	—	—	PostgreSQL_13	35.232.5.43	—	cloud-debugging-us-central1-a	ADD	us-central1-b
csr	Upgrade for security patches	—	—	PostgreSQL_13	34.135.177.187	—	cloud-debugging-us-central1-a	ENABLED	us-central1-b
diagnostics-bq-pg13	Configure SSL	—	—	PostgreSQL_13	35.184.8.135	10.96.240.234	cloud-debugging-us-central1-a	ENABLED	us-central1-a
diagnostics-bq-pg13-replica	Configure SSL	—	—	PostgreSQL_read-replica	35.222.193.50	10.96.240.4	cloud-debugging-us-central1-a	ADD	us-central1-a
diagnostics-test-120	Configure SSL	—	—	PostgreSQL_14	34.172.193.164	10.96.240.19	cloud-debugging-us-central1-a	ENABLED	us-central1-a
diagnostics-test-130-replica	Configure SSL	—	—	PostgreSQL_read-replica	34.21.94.198	10.96.240.247	cloud-debugging-us-central1-a	ADD	us-central1-b
diagnostics-test-130-client	Configure SSL	—	—	PostgreSQL_14	34.27.202.152	10.96.240.35	cloud-debugging-us-central1-a	ENABLED	us-central1-b
edmonstrating-test-postgres	Configure SSL	—	—	PostgreSQL_13	35.202.205.9	—	cloud-debugging-us-central1-a	ENABLED	us-central1-b
event-timeline-test	Upgrade for security patches	—	—	PostgreSQL_14	34.143.149.89	—	cloud-debugging-us-central1-a	ENABLED	asia-southeast1-c
multi-replica-test	Configure SSL	—	—	PostgreSQL_13	35.198.93.790	—	cloud-debugging-us-central1-a	ADD	us-central1-b



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)
- 環境変数による構成
- 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](https://github.com/GoogleCloudPlatform/cloud-sql-proxy/migration-guide) を参考に書式を修正



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)

<https://cloud.google.com/sql/docs/mysql/connect-proxy-operator>

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

メンテナンス

メンテナンスは通常、数か月に一度の頻度で行われます。更新が行われている間にインスタンスを再起動する必要があるため、サービスが短期間中断します

メンテナンスの時間枠

このインスタンスの定期メンテナンスを行うのに最適な日時枠を選択します。

日曜日

2:00 - 3:00

時刻は、ユーザーの地域のタイムゾーン (UTC+9) で表示されます。

更新の順序

このリージョンの他のインスタンスと関連します

後で

メンテナンス不要期間

メンテナンス不要期間 (最大 90 日間) を作成して、予定されているメンテナンスを拒否できます。一度に有効にできるメンテナンス不要期間は 1 つだけです。[詳細](#)

開始日 2022/10/01

終了日 2022/12/30

メンテナンスは午前 12 時 (GMT+9) から拒否されます

メンテナンスは午前 12 時 (GMT+9) に再開されます

消去

繰り返し: 1 年サイクル

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。



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)
<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)
<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)
<https://cloud.google.com/sql/docs/sqlserver/import-export#use-sqlpackage>



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
```

バックアップ [バックアップの作成](#) [更新](#)

バックアップはデータ保護の中心となるもので、クラスタを復元して、失われたデータの復元やエラーの修正を行うことができます。AlloyDB では、バックアップはプロジェクトレベルのリソースであり、そのためソースクラスタとは独立して存在します。

▼ フィルタ バックアップのフィルタ

ソースクラスタ	場所	名前	作成日	種類	サイズ	
dev-cluster	asia-northeast1	contin-bkp-20230309-10-add6449e-26c4-4c50-94e4-ef633efc9d04	2023/03/09 18:46:35	自動	51.69 MB	復元
dev-cluster	asia-northeast1	automated-bkp-20230309-08-af941476-a073-4b24-aae9-f7e76dda5ba	2023/03/09 16:46:09	自動	51.68 MB	復元
dev-cluster	asia-northeast1	contin-bkp-20230308-10-471a29db-8ef9-4346-9d6d-2ad4386e90c4	2023/03/08 18:46:11	自動	51.63 MB	復元
dev-cluster	asia-northeast1	automated-bkp-20230308-08-51282605-0cda-40f4-9ed2-f1e3c2f3e7f5	2023/03/08 16:46:55	自動	51.61 MB	復元
dev-cluster	asia-northeast1	initial-backup	2023/03/08 13:54:57	オンデマンド	44.15 MB	復元



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)

場所

パフォーマンスを向上させるには、必要とするサービスの近くにデータを保存します。
この設定は後で変更できません。

リージョン *

asia-northeast1 (東京)

asia-northeast2 (大阪)

asia-northeast3 (ソウル)

asia-south1 (ムンバイ)

asia-southeast1 (シンガポール)

asia-southeast2 (ジャカルタ)

australia-southeast1 (シドニー)

australia-southeast2 (メルボルン)

▼ 詳細暗号化オプション



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。

```
To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with Docker Hub:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/

rrhea@smurf-rhea-02:~$ gcloud auth configure-docker
Adding credentials for all GCR repositories.
WARNING: A long list of credential helpers may cause a slow 'docker build'. We recommend passing the registry name to configure only the registry.
After update, the following will be written to your Docker config file located at [/home/rrhea/.docker/config.json]:
{
  "credHelpers": {
    "gcr.io": "gcloud",
    "us.gcr.io": "gcloud",
    "eu.gcr.io": "gcloud",
    "asia.gcr.io": "gcloud",
    "staging-k8s.gcr.io": "gcloud",
    "marketplace.gcr.io": "gcloud"
  }
}

Do you want to continue (Y/n)? y

Docker configuration file updated.
rrhea@smurf-rhea-02:~$
```

1. Install Docker

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。

メンテナンス

優先ウィンドウ

Friday, 5:00 - 6:00 (UTC+9)

近日中のイベント

まだメンテナンスがスケジュールされていません。

セルフサービス メンテナンス ⓘ

Update available [VIEW AND APPLY](#)

Self-Service maintenance

[適用] をクリックすると、インスタンスでは直ちにメンテナンスが開始されます。 [詳細](#)

Self-service maintenance allows you to optionally update your instance to access the latest Memorystore features and security enhancements. [View Change Log](#)

メンテナンス バージョンの選択

20230322_00_00

キャンセル

適用



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。



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

プリンシパルの追加

プリンシパルは、ユーザー、グループ、ドメイン、またはサービス アカウントです。

[IAM のプリンシパルの詳細](#)

新しいプリンシパル

user01@takasato.altostrat.com

ロールを割り当てる

ロールは一連の権限で構成され、プリンシパルがこのリソース で実行できることを決定します。[詳細](#)

ロール *

Cloud Spanner のきめ細かいアク...

IAM の条件 (省略可)

+ IAM の条件を追加

Spanner のきめ細かいアクセス制御フレームワークを使用する権限を付与します。特定のデータベース ロールへのアクセス権を付与するには、Cloud Spanner データベース ロール ユーザーの IAM ロールと必要な条件も追加します。

ロール

Cloud Spanner データベース ロール..

IAM の条件 (省略可)

+ IAM の条件を追加

Cloud Spanner のきめ細かいアクセス制御ユーザーの IAM ロールと組み合わせて、個々の Spanner データベース ロールに権限を付与します。必要な Spanner データベース ロールごとに条件 (リソースタイプ

「spanner.googleapis.com/DatabaseRole」、
「/<自分の Spanner データベース ロール>」
で終わるリソース名など) を追加します。

保存

キャンセル

IAM プリンシパルとロールの紐付け



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。

条件を追加 削除

プリンシパル user02@takasato.altostrat.com プロジェクト data-db-demo

タイトル* Spanner Tester

説明

条件ビルダー 条件エディタ

条件タイプ タグ 演算子 値がある 値のパス* takasato.altostrat.com/env/test

追加

条件として env:test タグを設定

env:dev はアクセス不可

env:test はアクセス可

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



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

The screenshot shows the Google Cloud Data Catalog interface for a project named 'data-db-demo'. The left sidebar contains filters for '範囲' (Scope), 'システム' (System), 'レイクとゾーン' (Lake and Zone), and 'データ型' (Data Type). The main area displays a table of resources with columns for Name, Description, Type, System, Source System, Project, and Last Updated. The table lists various tables and views, including 'bank', 'tab', 'accounts', 'free-instance', 'Customer', 'TransactionHistory', 'Account', 'CloudSpannerSampleApp', 'CustomerRole', 'finance-db', 'Singers', 'snippet-db', 'Albums', and 'example-db'.

名前	説明	種類	システム	ソースシステム	プロジェクト	最終更新
★ bank	データベース	データベース	CLOUD SPANNER		data-db-demo	2022/11/02
★ tab	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/11/02
★ accounts	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/01
★ free-instance	サービス	サービス	CLOUD SPANNER		data-db-demo-free-spanner	2022/12/13
★ Customer	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ TransactionHistory	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ Account	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ CloudSpannerSampleApp	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ CustomerRole	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ finance-db	データベース	データベース	CLOUD SPANNER		data-db-demo	2022/12/20
★ Singers	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ snippet-db	データベース	データベース	CLOUD SPANNER		data-db-demo	2022/12/20
★ Singers	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ Albums	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/20
★ Albums	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/21
★ Singers	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/21
★ example-db	データベース	データベース	CLOUD SPANNER		data-db-demo	2022/12/21
★ Albums	テーブル	テーブル	CLOUD SPANNER		data-db-demo	2022/12/21
★ Singers	テーブル	テーブル	CLOUD SPANNER		data-db-demo-free-spanner	2022/12/23



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

The screenshot shows the Google Cloud Database Migration Service interface. The main content area is titled 'コンバージョン ワークスペース プレビュー' (Conversion Workspace Preview). It includes a sidebar with navigation options like 'データベースの移行' (Database Migration), '移行ジョブ' (Migration Jobs), 'コンバージョン ワークスペース...' (Conversion Workspaces), '接続プロファイル' (Connection Profiles), and 'プライベート接続' (Private Connections). The main area contains a table of conversion workspaces. One workspace is selected, showing its details in a table below.

コンバージョン ワークスペース名	コンバージョン ワークスペース ID	最新バージョンの ID	コンバージョンの状態	作業内容	ソース / 宛先	リージョン	作成日
oracle11g-migration-poc	oracle11g-migration-poc	e698a1cd	コンバージョン...	...	Oracle / ...	asia-southeast1	2023/02/09

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。

構成ファイルの選択

Oracle データベース用に生成したすべての Ora2Pg 構成ファイルを選択します。ファイルを置換する必要がある場合は、閉じるアイコン (X) をクリックしてフィールドをクリアします。注: [保存して閉じる] をクリックすると、Ora2Pg 構成ファイルは保存されません。

Ora2Pg 構成ファイル 1 *

参照

ファイルの中身は有効な Ora2Pg 構成ファイルにしてください

+ ファイルを追加

構成の変換

ソースに接続し、移行ジョブで使用できるマッピングに構成ファイルを変換します。

PULL スキーマと変換



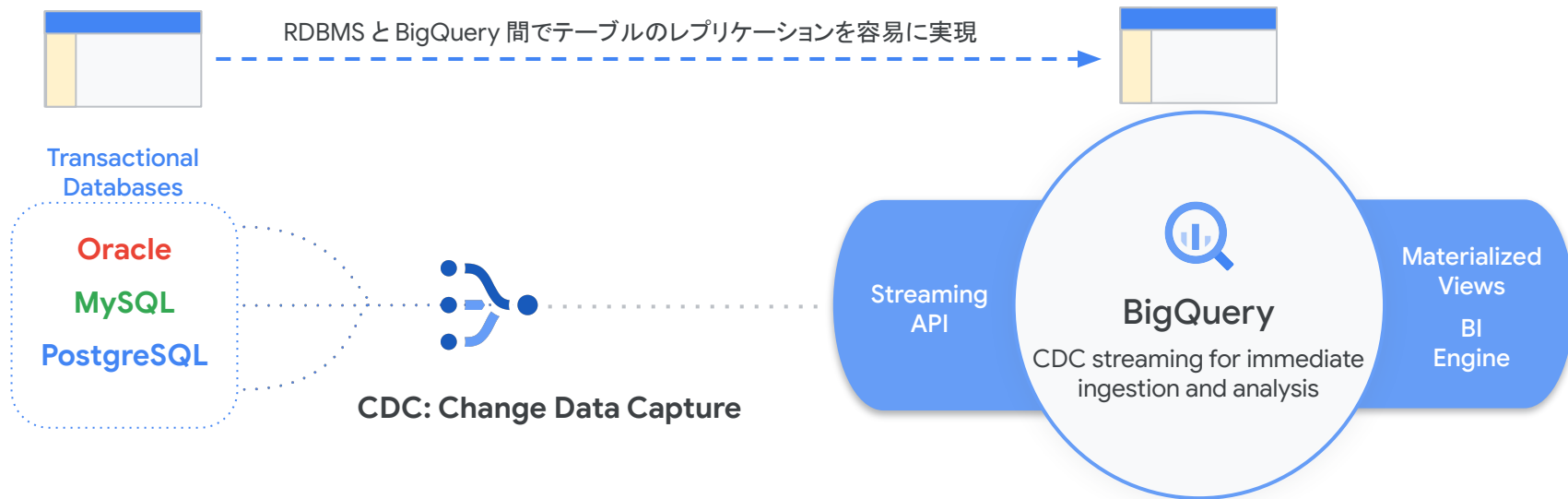
Datastream for BigQuery 及び PostgreSQL ソースが GA

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



05

Networking



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

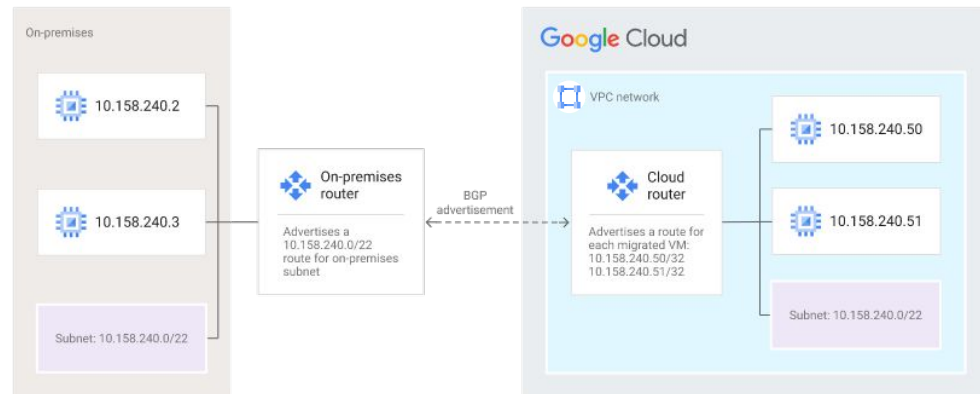
- 送信元 IP アドレス、プロトコルを指定してルートを作成し、内部 TCP / UDP ロードバランサにリダイレクト
- Cloud Interconnect 接続を介してオンプレミスネットワークから VPC ネットワークに送信されるトラフィックにもポリシーベースのルートを作成可能

```
# 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
```

オンプレミスとのハイブリッドサブネットが 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





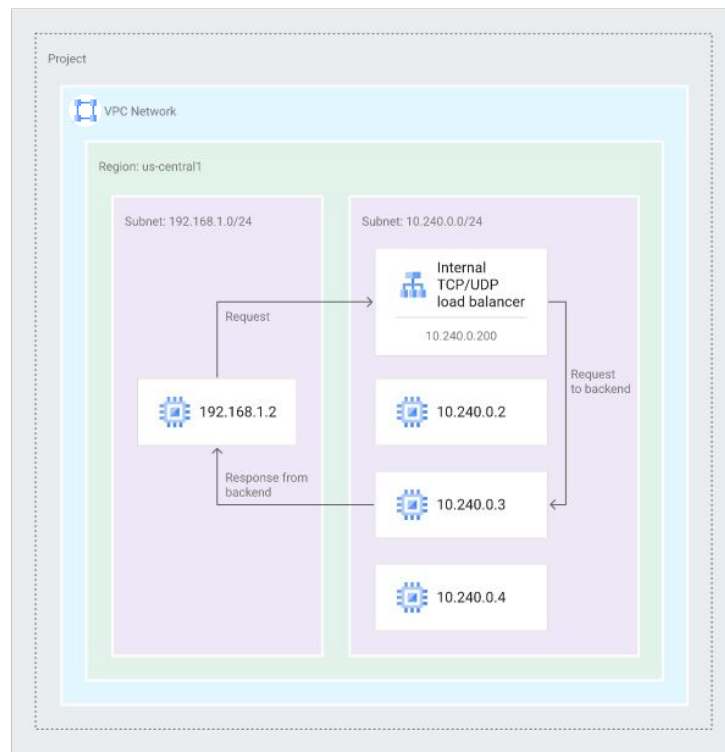
ネットワークロードバランサと内部 TCP / UDP ロードバランサのログिंगが GA

L4 のロードバランサでもログिंग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
```





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

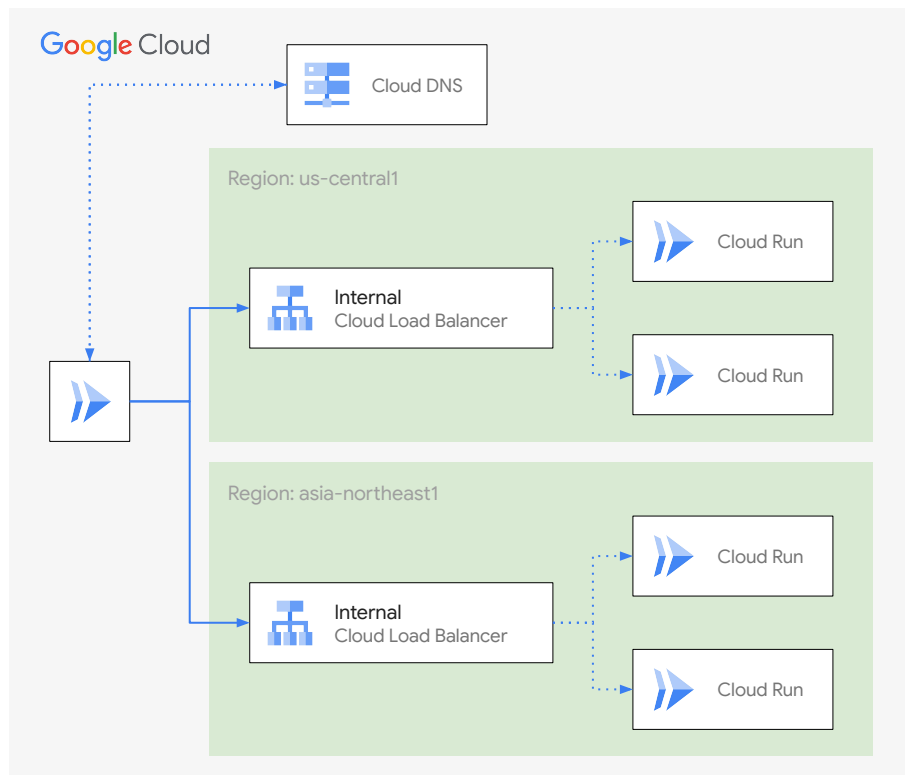
```
# パターンマッチの形式例
pathMatchers:
  - name: Cart-Matcher
    routeRules:
      - description: CartService
        matchRules:
          - pathTemplateMatch:
              '/xyzwebservices/v2/xyz/users/{username=*/carts/{cartid=**}'
            service: cart-backend
            priority: 1
            routeAction: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



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

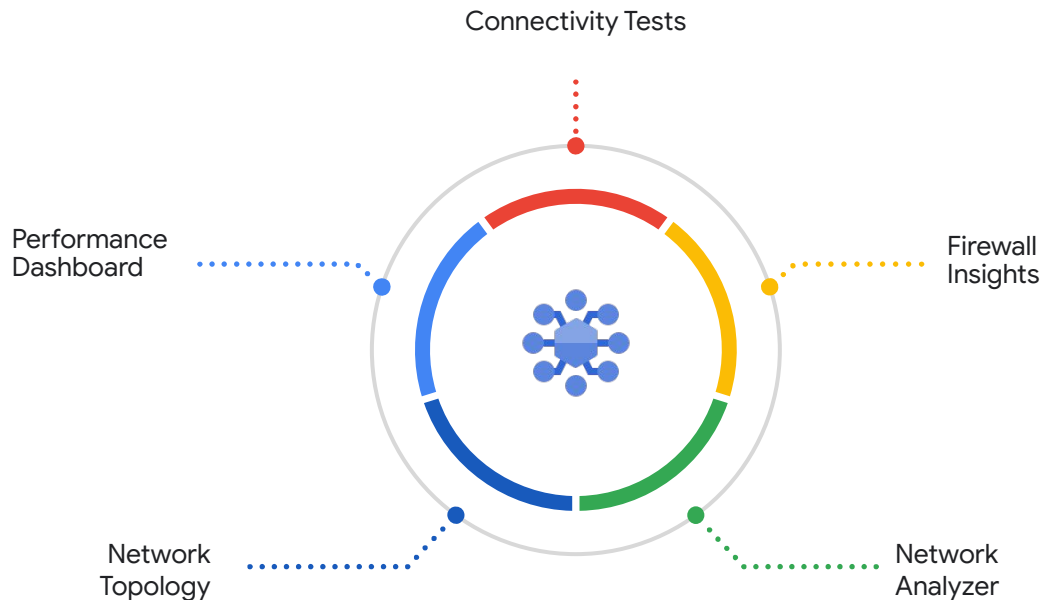




Network Intelligence Center (NIC) のご紹介

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





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

← 接続テストの作成

テスト名 *

小文字、数字、ハイフンのみ使用できます

プロトコル
tcp

ソース

送信元エンドポイント

VM インスタンス

IP アドレス

App Engine

Cloud Functions 第 1 世代

Cloud Run

Cloud SQL インスタンス

GKE クラスタ コントロール プレーン

送信元 IP アドレス *

プロジェクトの選択

例: 192.0.2.1

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

ファイアウォールのインサイト

≡ フィルタ ネットワークのフィルタ

🔍 シャドウルール
分析情報の数: 0
観察期間: 該当なし

ネットワーク ↑	分析情報の数	最終更新時間
default-network	0	—

→ 完全なリストを表示

🔍 ヒットが含まれる拒否ルール
分析情報の数: 0
観察期間: 1 日
最終更新日時: 該当なし

ネットワーク ↑	分析情報の数	最終更新時間
default-network	0	4月9日 14:46

→ 完全なリストを表示

構成

観察期間 有効化

次の分析情報を有効または無効にできません。有効にすると、ファイアウォール インサイトの使用に対して課金が発生します。 [ファイアウォール インサイトの料金の詳細については、こちらをご覧ください。](#)

シャドウルールの分析情報

これらの分析情報は、他のルールによって隠されているルールを検出します。有効にすると、これらの分析情報を生成するスケジュールを設定できます。

 有効

分析情報の生成スケジュール

開始日: *
2000/01/01

次の間隔で繰り返す: *
日

制限が緩すぎるルールの分析情報

これらの分析情報で未使用の許可ルールが検出され、未使用の属性を持つルールや、属性が広範囲に定義されている可能性があるルールを許可できるようになります。有効にすると、これらの分析情報が毎日生成されます。

 有効

Appendix

その他のアップデート



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
- 予測ウィンドウは 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

Configure alert trigger

Condition Types

- Threshold
Condition triggers if a time series rises above or falls below a value for a specific duration window
- Metric absence
Condition triggers if any time series in the metric has no data for a specific duration window
- Forecast
Condition triggers if any timeseries in the metric is projected to cross the threshold in the near future.

Alert trigger

任意の時系列の違反

予測期間 *

1時間

将来のプロジェクトの期間。

Google Cloud UPDATES

次回予告

Data Analytics / ML 編

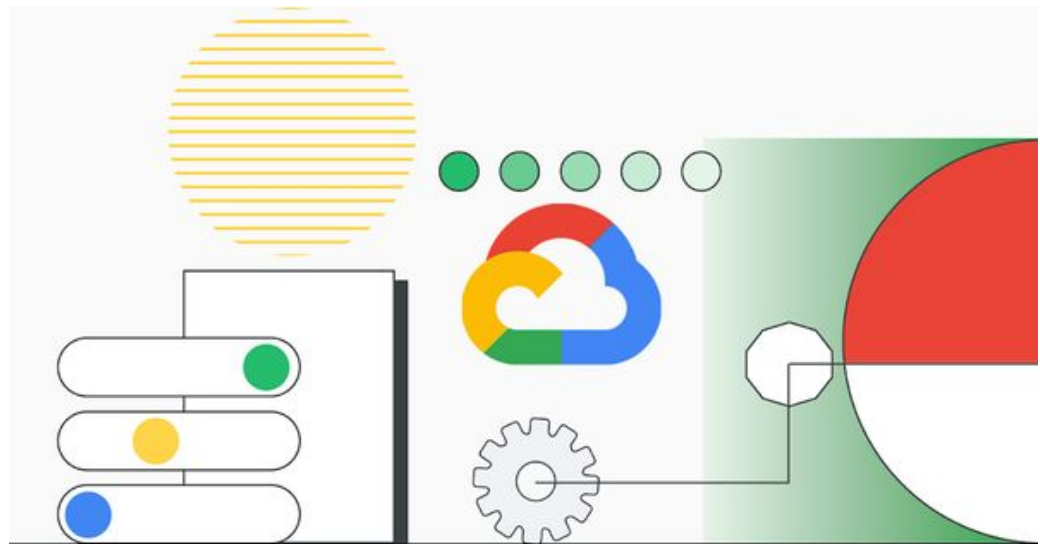
2023年7月24日(月) 15:00 ~ 16:30

[カレンダーに追加はこちらから](#)

Compute / DB 編

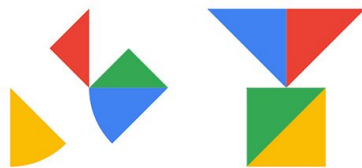
2023年7月31日(月) 15:00 ~ 16:30

[カレンダーに追加はこちらから](#)



Google Cloud

Google Cloud Day '23 Tour

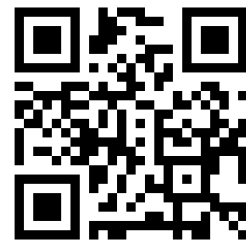


TOKYO Online 5.23 - 25

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