

Google Kubernetes Engine 最新情報を徹底解説！

INSIDE Games and Apps

Google Cloud カスタマーエンジニア
TT 🦊 Tsukasa / たまるつかさ

Google Kubernetes Engine (GKE) おさらい

Google Kubernetes Engine (GKE)



- Google Cloud 上で動作する Kubernetes のマネージドサービス
- マスターノードの管理は全て Google が行う
- 自動アップグレード
- Google Cloud の各種サービスとのインテグレーション

OSS Kubernetes と GKE、そして Anthos の位置付け

マネージド
ユーザーの負担少



Anthos

Google Cloud 以外の環境で GKE を使いたい
サービスマッシュなどをマネージドで使いたい



GKE

Kubernetes の複雑性を心配せず、
スケーリングや管理を Google に任せたい

アンマネージド
ユーザーの負担多い



OSS k8s on
Google Cloud

OSS k8s
on your own

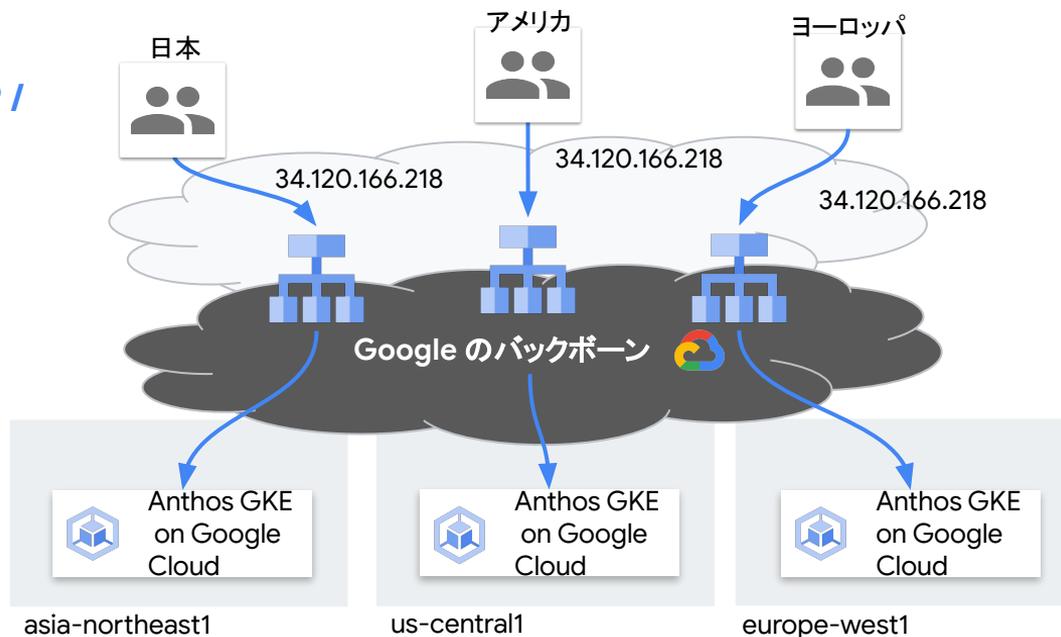
様々な設定やデプロイの管理をする
技術と時間があり、Google Cloud のサービス
とのインテグレーションや Google の SRE を
利用する必要がない

GKE 最近のアップデート



Ingress for Anthos

- リージョンを跨いだクラスタ間での HTTP / HTTPS ロードバランシングが可能
- VPC ネイティブクラスタでのみ利用可能
- バックエンドの状態に応じて、
最寄りのクラスタにトラフィックを転送
- kubemci との違い
 - CLI ツールではなく、CRD
 - 宣言型
 - Google Cloud によるサポート

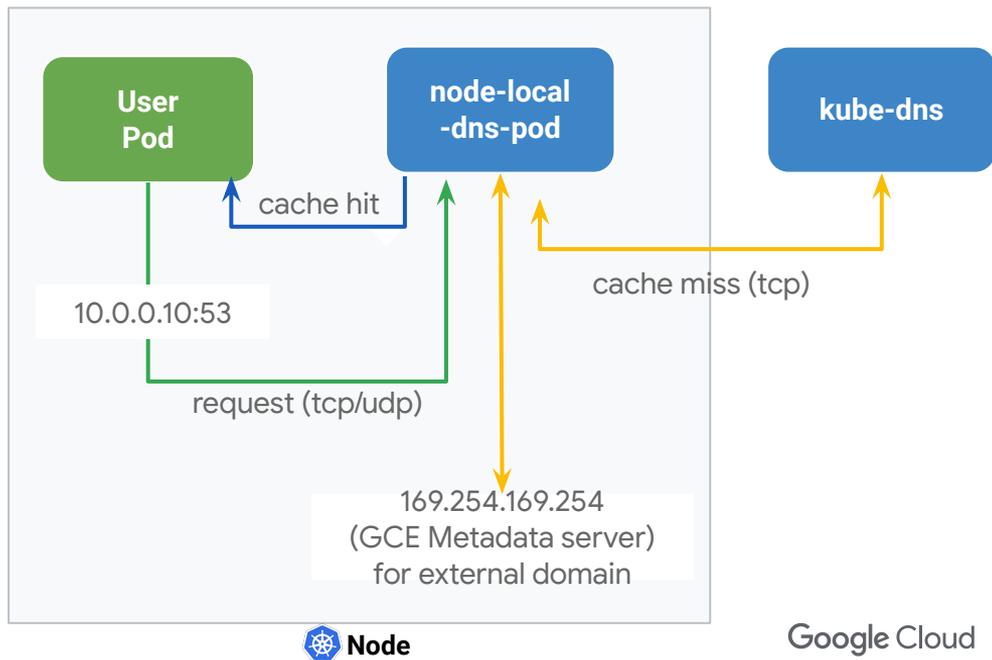


NodeLocal DNSCache

Node 毎に Daemonset で DNSCache を配置

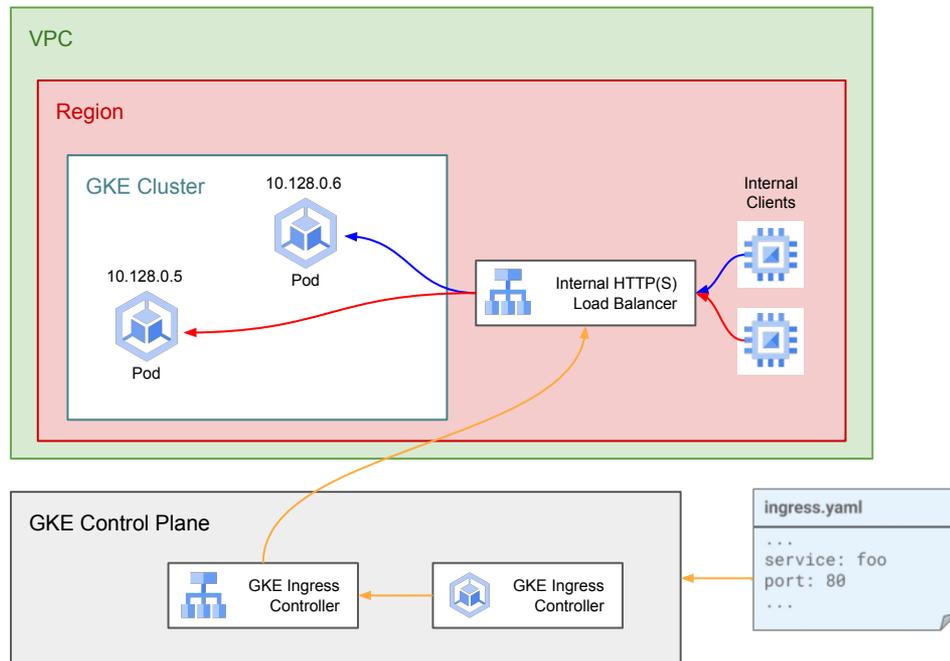
メリット

- DNS lookup time の軽減
- conntrack table のリソース消費軽減



Ingress for Internal HTTP(S) Load Balancing

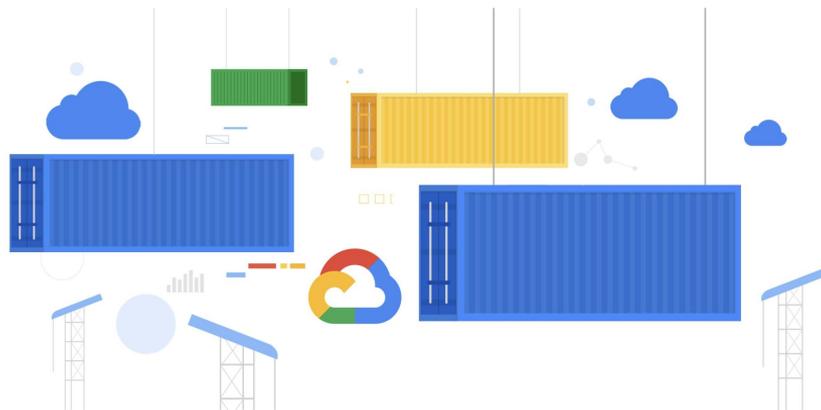
- Envoy が実体の L7 LB
- 専用サブネットが必要
(64 以上のホストIP が必要)
- NEG(Network Endpoint Group)の利
用が前提
- BackendConfig は External と比較して
未サポートのものが多い



Windows Container

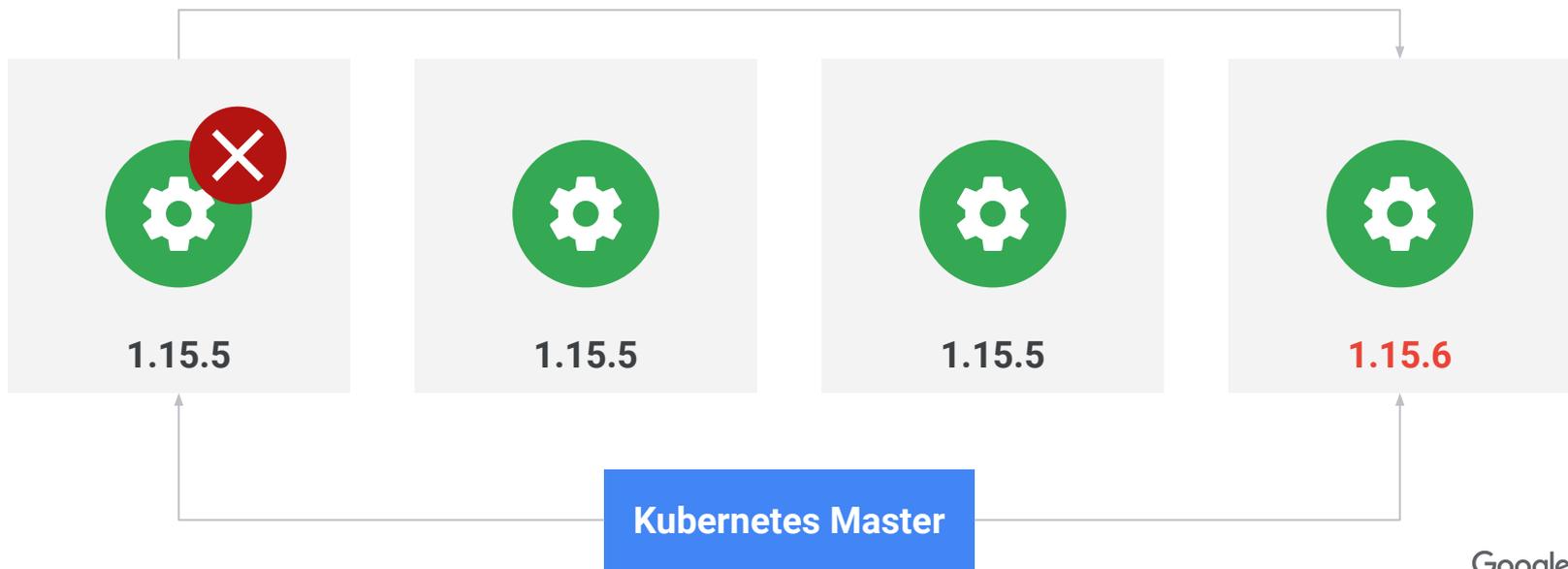
- VPC Native クラスタ必須
- **Windows Container 用の Node pool を作成する必要がある**
 - Windows Server version 2019 (LTSC)
 - Windows Server version 1909 (SAC).
- Linux Node(COS / Ubuntu)の Node Pool も並列で作成する必要あり
- **Windows ライセンス料金は Node の料金に含まれます**

Windows Server applications, welcome to Google Kubernetes Engine



Surge Upgrade

Cluster AutoScaler によって Node pool に新しいバージョンの Node を追加し、
Cordon&Drain で既存 Pod を移行していく手法
デフォルトで有効



Release channel

リリースチャンネルでは Master と Node のアップグレードを Google が行う
アップグレードの頻度とリスクのバランスをユーザー自身でコントロール可能
コンセプトは Chrome の自動更新と同じ



マスターのバージョン

新しいバージョンの準備ができたなら、リリース チャンネルを選択して GKE の自動アップグレードを取得します。将来的に手動でアップグレードする静的バージョンを選択します。 [詳細](#)

i Regular リリース チャンネルが選択されているため、このクラスタでは Anthos の機能を使用できます。

[詳細](#)

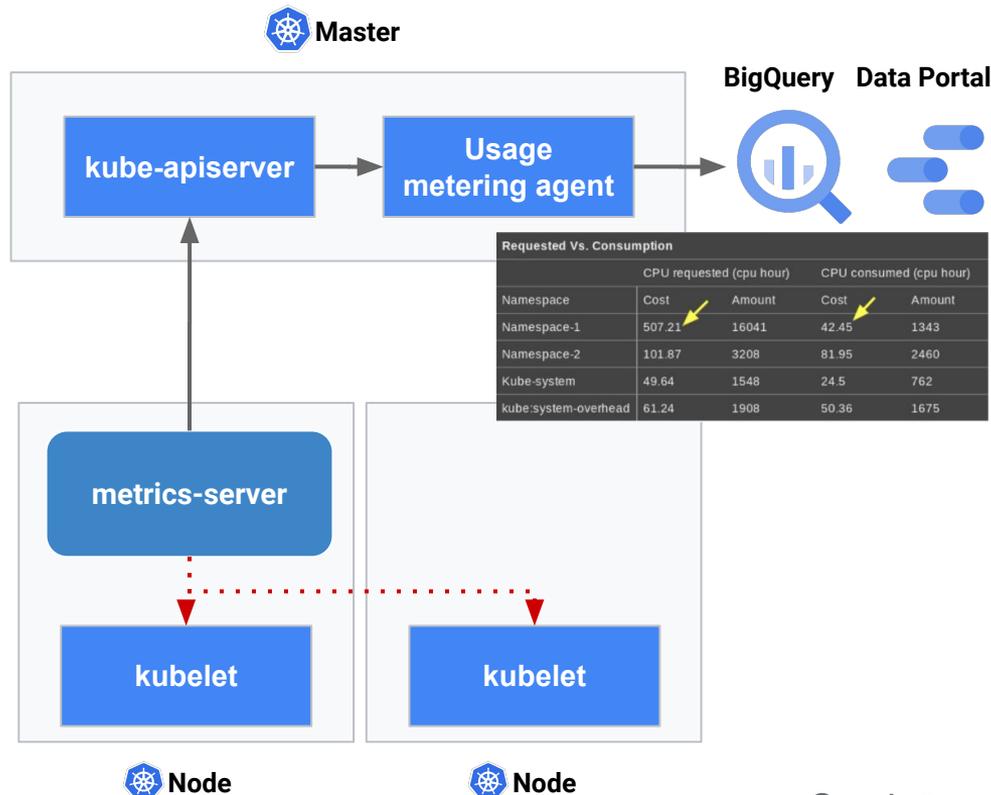
- 静的バージョン
- リリース チャンネル

リリースチャンネル

- Rapid チャンネル
- Regular チャンネル (デフォルト)**
- Stable チャンネル

GKE Usage metering

- ワークロードが使用するリソースを **namespace** やラベル単位で解析
- CPU、メモリ、GPU、PD、ネットワーク(egress)
- **Billing Export** と組み合わせる事でコストを可視化



Supports upto 15,000 nodes in GKE 1.18

CONTAINERS & KUBERNETES

Bayer Crop Science seeds the future with 15000-node GKE clusters



Shielded GKE Nodes

GCE の [Shielded VM](#) を使ったよりセキュアな Node

COS / Ubuntu のイメージで利用可能

GKE version 1.18 からデフォルトとなる

Shielded GKE Nodes を有効にすると、GKE の Control plane が以下を検証する

- クラスタの全ての Node が Google の DC 内で動作している仮想マシンであること
- 全ての Node が 当該クラスタが作成した Managed instance group の一部であること
- 各 Kubelet が 動作する Node 向けの証明書がプロビジョニングされていること

Workload Identity



Kubernetes の RBAC(GKE クラスタ内部で有効)

Kubernetes Cluster A

Namespace A

Pod

Pod

Namespace B

Pod

Pod

Namespace C

Pod

Pod

Kubernetes の
サービスアカウント

```
gcloud beta container clusters create [CLUSTER_NAME] \  
--workload-pool=[PROJECT_ID].svc.id.goog
```

Cloud IAM Policy Bind
による紐付け

Google Cloud の
サービスアカウント

ロール

Google Cloud の各
サービス



Cloud IAM(Google Cloud の RBAC)

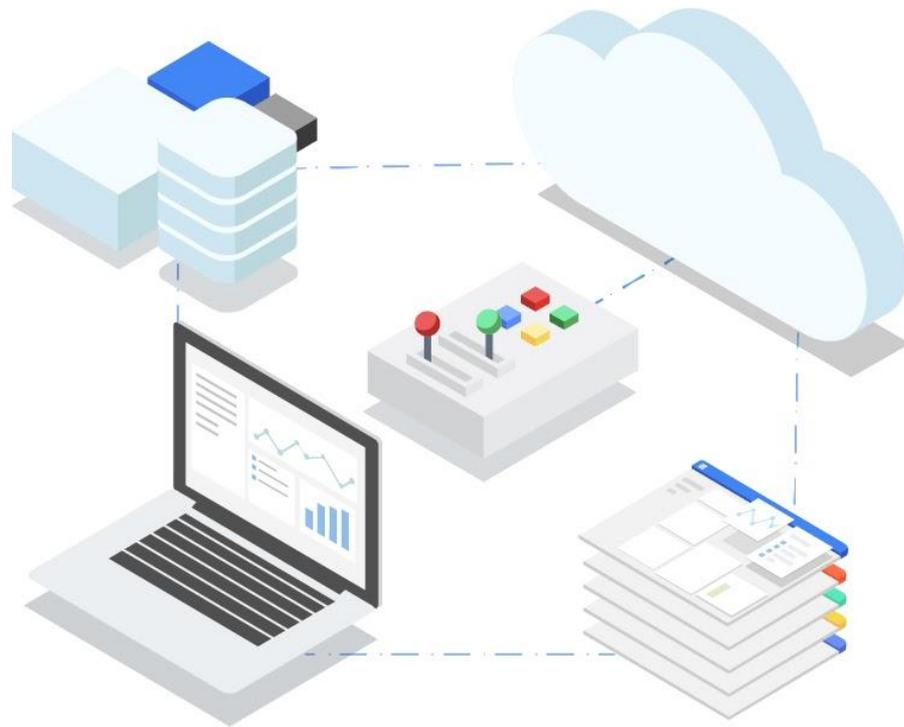
アカウント+ ロールの組み合わせで
各 Google Cloud サービスへのアクセス
を制御

Anthos Service Mesh



Google が提供する
エンタープライズグレードの
サービスメッシュ

- ✓ Istio がベース
- ✓ マルチ、ハイブリッドクラウドをサポート
- ✓ コントロールプレーンがフルマネージド
- ✓ OSS を超えたサポート
- ✓ Google の知見が組み込まれている



Price change / SLA

2020.06.06 より GKE に Cluster management fee が追加

- 1 時間 1 クラスタあたり \$0.10 の Cluster management fee が発生
- 1 Billing Account あたり 1 ゾーンクラスタ (Single or Multi) は無料
- Environ (GKE Hub) に登録した クラスタ (Anthos GKE クラスタ) は無料

併せて Master に対する SLA が設定

- ゾーンクラスタ: 99.5%
- リージョンクラスタ: 99.95%
- SLA が適用されるのは Stable channel の default version で動作するクラスタのみ

Thank you!!