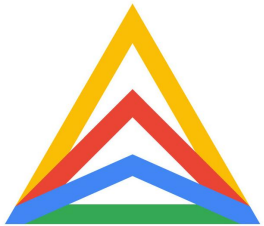
今日から始める
限定公開クラスタ

2020.01.30 Anthos Day

https://inthecloud.withgoogle.com/anthos-day-2001/register.html



アジェンダと注意点

話すこと

- 限定公開クラスタについて

話さないこと

- GCP の説明
- Kubernetes および GKE の説明

Self introduction

Hello ;)

自己紹介

person:

name: “Toru Igarashi”

twitter: “@iganari_”

position:

company: “Cloud Ace Inc.”

role: “SRE”

skills: [Terraform, Ansible, Kubernetes]

favorites: “Infrastructure as Code”

blood-donation:

count: 111

description: “I can donate blood a little”

Security in operating GKE

GKE のセキュリティどうしてますか?

GKE のセキュリティどうしてますか?

GKE のインフラストラクチャのセキュリティ

- Kubernetes のバージョンを最新の状態に保つ
  - 最新のセキュリティパッチを適用するため必須
  - マスターノードは自動的にアップデートが行われている
    - ノードのアップデートも自動設定が可能

GKE のセキュリティどうしてますか?

ネットワークのセキュリティ

- Node には、Internal IP と External IPがある
  - 外部のインターネットとルーティング可能な経路がある。ということ
    - Firewall rules の設定などで接続が出来てしまう
  - ネットワークレベルでのセキュリティを考えるべき

GKE のセキュリティどうしてますか?

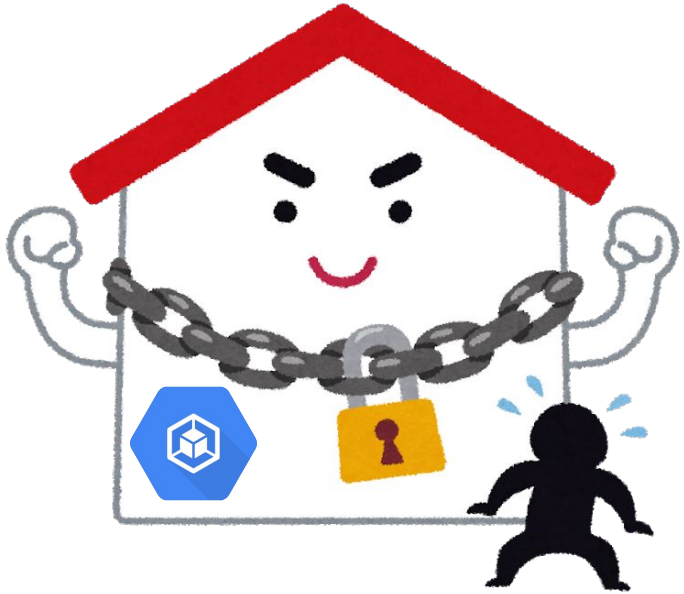
ネットワークのセキュリティ

- Node には、Internal IP と External IPがある
  - 外部のインターネットとルーティング可能な経路がある。ということ
    - Firewall rules の設定などで接続が出来てしまう
  - ネットワークレベルでのセキュリティを考えるべき

限定公開クラスタ
(private cluster)

What is Private clusters

限定公開クラスタとは

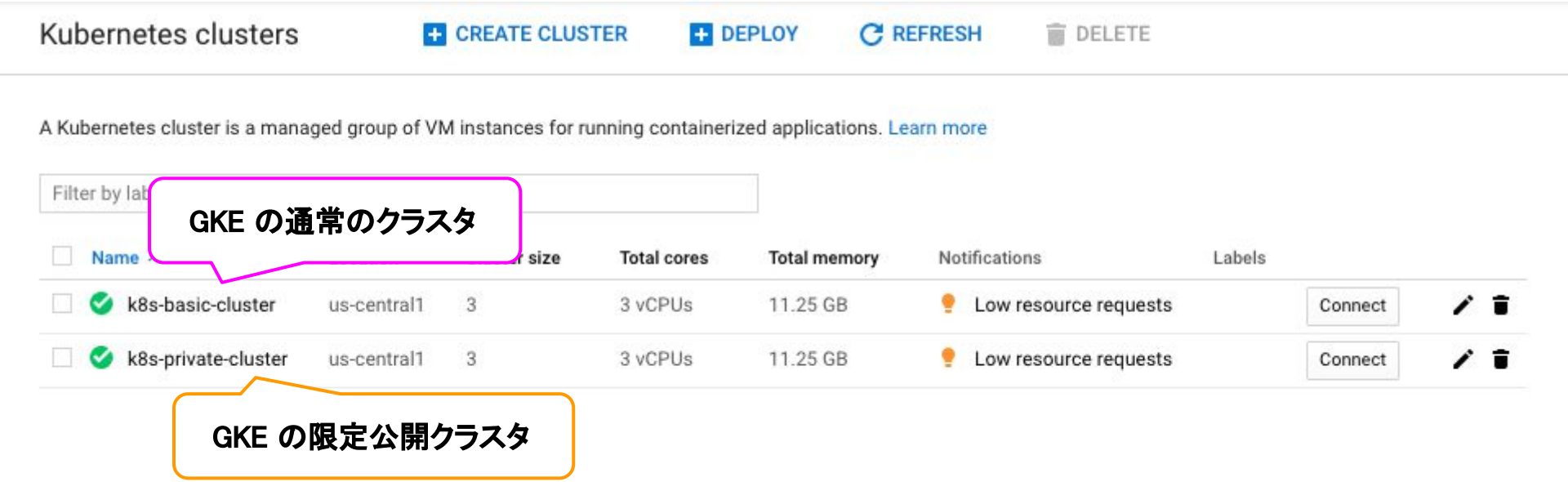


限定公開クラスタの特徴

- GKE のクラスタの種類
- Node は RFC 1918 の内部 IP アドレスしか持たない
- Master と Node 間の通信は VPC Network Peering にて行われる

ref. https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept

GKE Clusters



Cluster Nodes

GKE の通常のクラスタ

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
gke-k8s-basic-cluster-default-pool-228f4200-hjlf	us-central1-f		gke-k8s-basic-cluster-default-pool-228f4200-grp	172.16.0.5 (nic0)	35.232.198.52	SSH
gke-k8s-basic-cluster-default-pool-b754d635-s6mb	us-central1-b		gke-k8s-basic-cluster-default-pool-b754d635-grp	172.16.0.7 (nic0)	104.198.140.181	SSH
gke-k8s-basic-cluster-default-pool-e9ee236a-rwk8	us-central1-c		gke-k8s-basic-cluster-default-pool-e9ee236a-grp	172.16.0.8 (nic0)	34.66.215.103	SSH
gke-k8s-private-cluster-default-pool-49a6a3b6-r30t	us-central1-c		gke-k8s-private-cluster-default-pool-49a6a3b6-grp	192.168.0.4 (nic0)	None	SSH
gke-k8s-private-cluster-default-pool-778df18e-5pw0	us-central1-a		gke-k8s-private-cluster-default-pool-778df18e-grp	192.168.0.2 (nic0)	None	SSH
gke-k8s-private-cluster-default-pool-979e2802-mvd7	us-central1-b		gke-k8s-private-cluster-default-pool-979e2802-grp	192.168.0.3 (nic0)	None	SSH

GKE の限定公開クラスタ

Cluster Nodes

GKE の通常のクラスタ

Name	Zone	Recommendation	In use by	Internal IP	External IP	Connect
gke-k8s-basic-cluster-default-pool-228f4200-hjlf	us-central1-f		gke-k8s-basic-cluster-default-pool-228f4200-grp	172.16.0.5 (nic0)	35.232.198.52	SSH
gke-k8s-basic-cluster-default-pool-b754d635-s6mb	us-central1-b		gke-k8s-basic-cluster-default-pool-b754d635-grp	172.16.0.7 (nic0)	104.198.140.181	SSH
gke-k8s-basic-cluster-default-pool-e9ee236a-rwk8	us-central1-c		gke-k8s-basic-cluster-default-pool-e9ee236a-grp	172.16.0.8 (nic0)	34.66.215.103	SSH
gke-k8s-private-cluster-default-pool-49a6a3b6-r30t	us-central1-c		gke-k8s-private-cluster-default-pool-49a6a3b6-grp	192.168.0.4 (nic0)	None	SSH
gke-k8s-private-cluster-default-pool-778df18e-5pw0	us-central1-a		gke-k8s-private-cluster-default-pool-778df18e-grp	192.168.0.2 (nic0)	None	SSH
gke-k8s-private-cluster-default-pool-979e2802-mvd7	us-central1-b		gke-k8s-private-cluster-default-pool-979e2802-grp	192.168.0.3 (nic0)	None	SSH

GKE の限定公開クラスタ

限定公開クラスタは External IP が無い

GKE クラスタに外部からアクセスするには

パブリックエンドポイントへのアクセスを有効化

- マスターの外部 IP アドレス
- kubectl などは、通常 このエンドポイントにて通信を行っている

マスター承認済みネットワークを適宜設定

- HTTPS を使って、マスターへの通信を許可する仕組み
- 特定の CIDR 範囲をホワイトリスト登録(外部 IP アドレスも可能)

ref. https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept#overview

ノードから外部にアクセスするには

- Cloud NAT を設定する
  - https://cloud.google.com/nat/docs/overview#NATwithGKE
- NAT gateway を設定する
  - https://cloud.google.com/vpc/docs/special-configurations#multiple-natgateways

ref.
https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#granting_private_nodes_outbound_internet_access

アプリを外部に公開するには

- LoadBalancer (LB) の Service を作成することで、外部に対して LB 経由でサービスを公開することが可能
  - https://cloud.google.com/kubernetes-engine/docs/concepts/service#types_of_services
- NodePort の Service を作成してから Ingress を作成することで、GKE にてその情報を元に HTTP(S) load balancer を設定することでアプリを公開することが可能
  - https://cloud.google.com/kubernetes-engine/docs/concepts/ingress

ref. https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept

様々な制約と制限

- 制約 (restrictions)
  - 既にある非限定クラスタを限定公開クラスタへ変換することは出来ない
  - マスター承認済みネットワークに上限値がある
- 制限 (limitations)
  - 限定公開クラスタはクラスタ毎に VPC ネットワーク ピアリングが必要
    - VPC ネットワーク自体は最大 25 個の他のVPC ネットワークとピアリング可能

※ その他にも制約と制限があるので、下記を参照して下さい

ref. https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#req_res_lim

セキュリティ以外のメリット

コストに関して

2020 年 1 月より、VM に割り当ててた Static IP address や Ephemeral IP addresses も有料化 (※ 期限付きで免除)

- Standard VM Instances の場合
  - $0.004/時間 (≒ $2.88/月)
- Preemptible VM Instances の場合
  - $0.002/時間 (≒ $1.44/月)

ref. https://cloud.google.com/compute/network-pricing#ipaddress

まとめ

限定公開クラスタがどのようなものか

- 内部 IP アドレスしか持たない Node から構成される GKE クラスタ
- 外部のインターネットから環境をネットワークのレイヤーで隔離することが出来るため、ネットワークの信頼性を高めることが出来る

どのように使っていけばいいか

- アプリを公開したい場合は通常と変わらない
- オペレーションにて注意が必要

Enjoy GKE !! ;)

ここからはおまけ

LT するにあたって、先に提出したもの

タイトル

- 今日から始める限定公開クラスタ

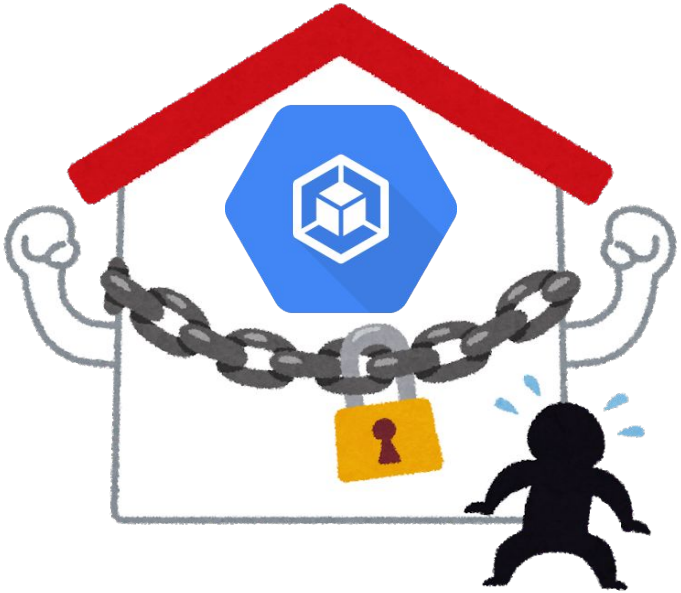
概要

Google Cloud Platform が提供する Google Kubernetes Engine を用いることで、私達は Kubernetes を容易に使い始めることが出来るようになりました。

一方で、ネットワークの作り方によってはセキュリティリスクが残ってしまう可能性があります。

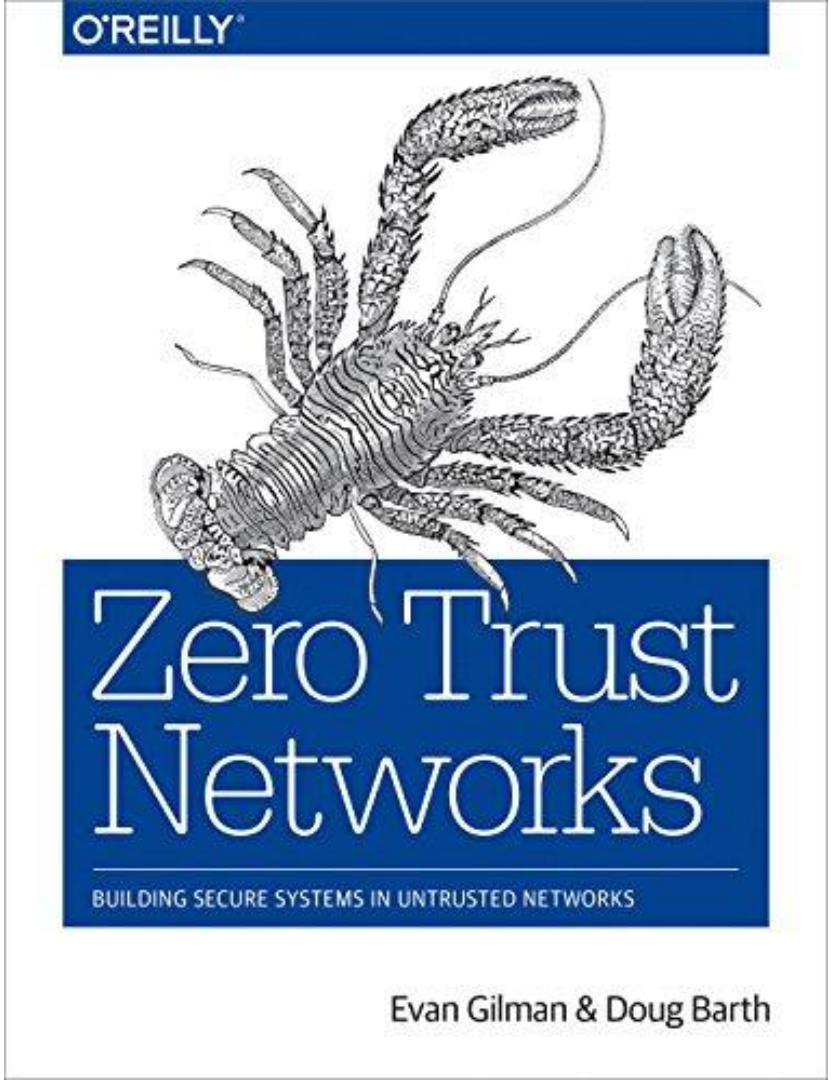
そこで、ネットワークの信頼性を高めるための対策の一つとして、限定公開クラスタをご紹介します。

ボツ絵



≒

理由: とあるキャラクターを想起させるため



いつか使いたい…けど、ちょい役で使うには、オーバーキルなイメージ

ちゃんと、内容を分解して話せる持ち時間がある時に…