

Migração para o Google Cloud Platform (GCP)

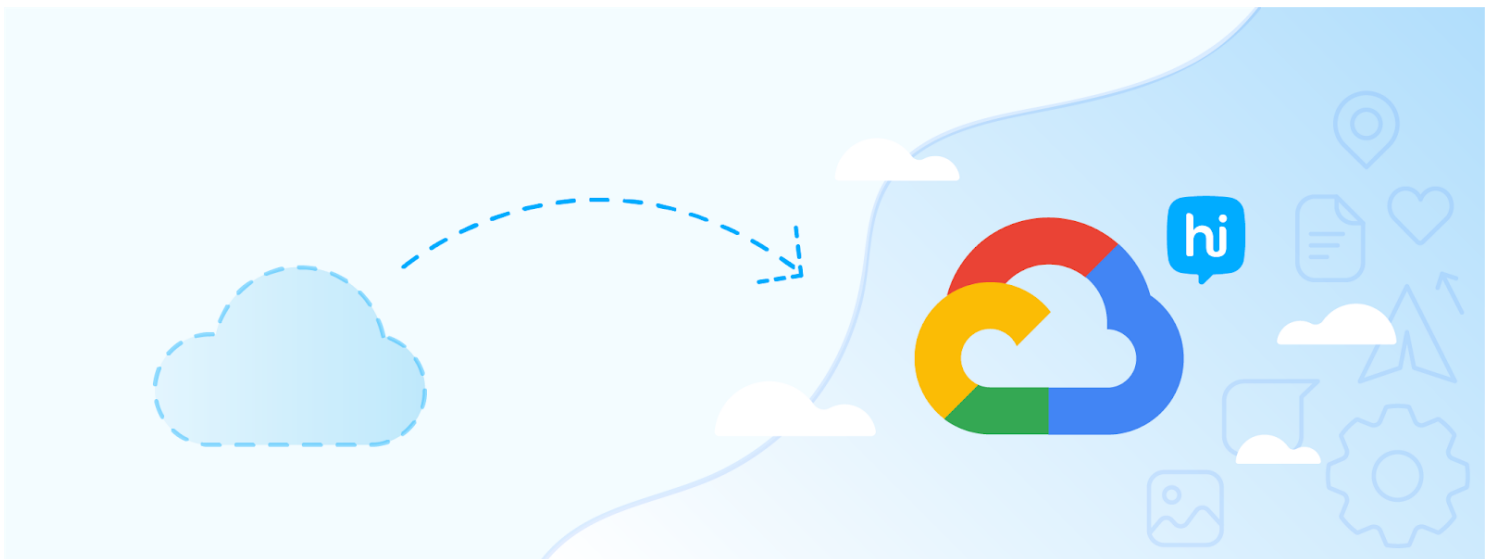
[Parte 1 de 2]

Por [Neeraj Khandelwal](#), Gerente de Engenharia Sênior - DevOps, Caminhada



Caminhada [Segue](#)

6 de setembro de 2018 · 6 minutos de leitura



Caminhada lançada em 12-12-12 com uma pequena base de usuários. Em 2016, tínhamos 100 milhões de usuários registrados e 40 bilhões de mensagens todos os meses. Mas junto com esse crescimento, começamos a enfrentar desafios relacionados ao dimensionamento de nossa infraestrutura. Para resolver esses problemas, precisávamos de uma plataforma de desempenho a um custo viável. O que criou uma urgência foi quando enfrentamos várias interrupções em 2016 e 2017 e fomos catalisados em opções de avaliação.

Nosso objetivo era escolher uma plataforma de nuvem correta que nos ajudasse a criar, testar e implantar aplicativos rapidamente em um ambiente de nuvem escalonável e confiável. Embora todas as plataformas de nuvem de grande porte possam parecer semelhantes de

várias maneiras, há várias diferenças fundamentais em plataformas de nuvem de grande escala.

Vamos dividir este post em duas partes:

1. Por que escolhemos mudar para o GCP
2. Migrando para o GCP sem nenhum tempo de inatividade

Prova de conceito

Começamos o processo com um POC no qual consideramos as incompatibilidades de execução existentes com os serviços oferecidos pelo Google Cloud Platform e também planejamos elementos em nosso roteiro futuro.

Principais áreas cobertas no POC :

- ✦ Balanceador de carga
- ✦ Compute Engine
- ✦ Rede e firewalls
- ✦ Segurança
- ✦ Acessibilidade aos recursos da nuvem
- ✦ Big Data
- ✦ Faturamento

O POC incluiu testes e verificação de serviços de VMs / Rede / Balanceador de carga, Estabilidade, Escalabilidade, Segurança, Monitoramento, Faturamento, Big Data e ML. Em junho de 2017, tomamos a grande decisão de migrar toda a pilha de infraestrutura para o Google Cloud Platform.

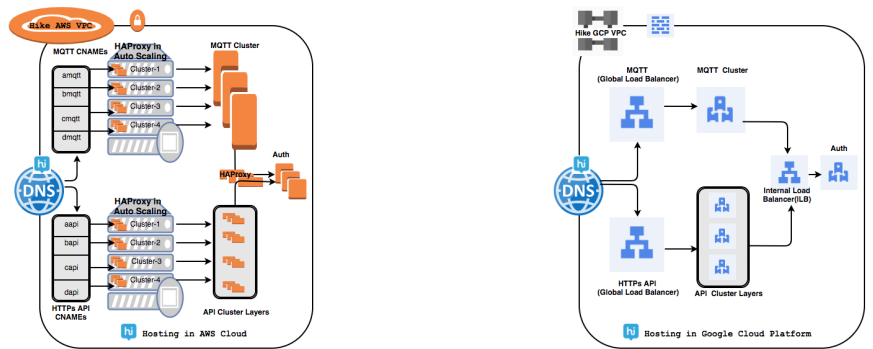
Queríamos optar por uma plataforma de nuvem em que a nuvem cuidasse dos inúmeros desafios que enfrentávamos:

✦ Balanceador de carga :

enfrentamos muitos desafios ao gerenciar clusters **internos** HAProxy para lidar com algumas dezenas de milhões de conexões de base de usuários ativos diariamente. O Global Load Balancer (GLB) resolveu nossos muitos desafios.

#	Self Managed HAProxy (Challenges)	GLB Solution
1	In auto scaled HAProxy cluster we were using lifecycle hook for scale down VMs to move in pending wait state before termination. This was needed to keep running VMs till connections drained completely.	Fully managed service with realtime scaling pattern
2	Connections throttling on VMs due to network limitation in cloud VPC. To handle more concurrent connection we needed to provisioned more HAProxy VMs into auto scaled group even VMs resource were not utilised.	
3	In cloud we didn't know how many VMs laying on same underlying H/W. We had faced many times more than 2+ VMs went down due to failure of underlying H/W. Such incidents caused reconnection for those % of users.	
4	We had faced DNS service outage for couple of hours in that new auto scale up HAProxy VMs were added into DNS but not propagated for DNS lookup.	Single Anycast IP from GLB
5	Management of static IPs in client to handle DNS failure issues on wifi connection.	
6	Used dual DNS structure where limited no. of user facing DNS records points to another CNAME records having multiple IPs for DNS resolution. Dual DNS structure was to handle cases where Hike were not working on wifi as more front IPs in DNS record were resulting for bigger packet size that small routers (which act like DNS server of wifi) unable to handle.	

Usando o balanceamento de carga global do GCP, um único IP de anycast pode encaminhar até 1 milhão de solicitações por segundo para vários back ends do GCP, como MIG (Grupo de instâncias gerenciadas) e não exige pré-aquecimento. Nosso tempo de resposta geral melhorou para 1.7–2x, já que o GLB utiliza uma implementação de pool que permite que o tráfego seja distribuído para várias origens.



✦ **Compute Engine :**
não havia grandes desafios em mecanismos de computação, mas precisávamos de uma plataforma de **alto** desempenho a um custo viável. A taxa de transferência geral das VMs da nuvem do Google melhorou para 1,3 a 1,5 vezes, o que nos ajuda a reduzir o número total de instâncias de VM em execução.

Os testes de benchmark Redis foram executados em um cluster de 6 instâncias (8 núcleos, 30 GB cada). Com base nos resultados abaixo, concluímos que o GCP fornece até 48% de melhor desempenho (em média) para a maioria das operações do REDIS e até 77% de melhor desempenho para operações específicas do REDIS.

```
redis-benchmark -h <nome do host> -p 6379 -d 2048 -r 15 -q -n
10000000 -c 100
```

REDIS Command	AWS(avg rps)	GCP(avg rps)	% improvement over AWS
PING_INLINE	55699.76	82950.38	48.92
PING_BULK	55592.93	83336.11	49.9
SET	50214.67	63391.85	26.24
GET	51831.2	81124.71	56.52
INCR	50924.02	81998.8	61.02
LPUSH	49333.26	63530.79	28.77
LPOP	46406.73	82555.93	77.89
SADD	52822.02	81618.66	54.52
SPOP	51930.25	82645.31	59.15
LPUSH	53031.55	61998.59	16.91

Os serviços do Google Compute Engine (GCE) adicionaram mais valores ao nosso gerenciamento de infraestrutura usando:

- **MIG (Grupo de instâncias gerenciadas):** MIGs nos ajudam a continuar executando nossos serviços de aplicativos em um ambiente robusto com recursos de várias zonas, em vez de provisionar recursos por zona. O MIG identifica e recria automaticamente instâncias não íntegras em um grupo para garantir que todas as instâncias estejam sendo executadas de maneira ideal.

- **Migração ao vivo :** a migração ao vivo nos ajuda a manter nossas instâncias de VM em execução mesmo quando ocorre um evento de desligamento do sistema host, como uma atualização de software ou hardware. Com nosso parceiro de nuvem anterior, recebíamos uma notificação de eventos de agendamento para manutenção que nos obrigava a interromper e iniciar a VM para passar a VM saudável.

- **VMs personalizadas:** nos GCPs, podemos criar VMs personalizadas com a quantidade ideal de CPU e memória para as cargas de trabalho necessárias.

✚ Redes e Firewalls: A

capacidade de gerenciamento de várias redes e regras de firewall não é fácil, pois isso pode levar a riscos. A VPC da rede do GCP é global por padrão e permite a comunicação entre regiões sem nenhuma configuração extra e nenhuma alteração no rendimento da rede. As regras de firewall nos dão flexibilidade dentro da VPC para projetos usando o nome da regra de tag.

Para redes de baixa latência e maior taxa de transferência, tivemos que escolher instâncias caras com capacidade para 10G e ativamos a rede aprimorada nessas instâncias.

Network VPC & Firewall	Services / Feature	Google Cloud	AWS Cloud
	VPC	Global	Regional
	Subnets	Regional	Regional
	VPN throughput	Excellent	Good
	VPC Peering	Yes	Yes
	Firewall Rule	Global	Regional

✦ Segurança: A

segurança é o aspecto mais importante para qualquer provedor de nuvem. Em nossas experiências passadas, a segurança não estava disponível ou era opcional para a maioria dos serviços.

Os serviços do Google Cloud são criptografados por padrão. O GCP usa várias camadas de criptografia para proteger os dados. O uso de várias camadas de criptografia adiciona proteção de dados redundante e nos permite selecionar a melhor abordagem com base nos requisitos da aplicação. como Identity-Aware Proxy e criptografia em repouso por padrão.

A maneira como o GCP lidou com as recentes vulnerabilidades catastróficas de execução especulativa na grande maioria das CPUs modernas (Meltdown, Specter) também é instrutiva. O Google desenvolveu uma nova técnica de modificação binária chamada Retpoline, que evita o problema e aplica a mudança de forma transparente na infraestrutura em execução, sem que os usuários percebam.

✦ Acessibilidade

do recurso de nuvem : a acessibilidade de recursos do GCP difere de outros provedores de nuvem, como na maioria dos recursos do GCP, incluindo o painel de controle, que são zonais ou regionais. Tivemos que gerenciar várias VPCs para projetos separados de contas separadas que precisavam de peering VPC ou conexão VPN para conectividade privada. Também tivemos que manter a réplica de imagem em uma conta separada também.

No Google Cloud, a maioria dos recursos é global ou regional. Isso inclui coisas como o painel de controle (onde podemos ver todas as

VMs do nosso projeto em uma única tela), imagens de disco, compartimentos de armazenamento (multi-região dentro de um continente), VPC (mas sub-redes individuais são regionais), Global Load Balancing, Pub / Sub etc.

Global and Regional	Services / Feature	Google Cloud	AWS Cloud
	Control Panel	Global	Regional
	Disk images	Global	Regional
	Storage buckets	multi-region within a continent	Regional
	Pub/Sub	Global	Regional
	Instance templates	Global	Regional

✚ Big Data:

Passamos de um monolítico, difícil de gerenciar a configuração de análise para uma configuração gerenciada completa com BQ e resultou em três áreas principais de melhoria:

- até 50x consultas mais rápidas
- Sistemas de dados totalmente gerenciados e com escalonamento automático
- Processamento de dados para até 15 m de horas anteriores.

✚ Faturamento:

foi difícil comparar diferentes provedores de nuvem, já que muitos serviços não eram semelhantes ou comparáveis, eram diferentes para diferentes casos de uso e dependiam de casos de uso exclusivos.

As vantagens do GCP foram:

- **Descontos para uso sustentado:** sustentados São aplicados ao uso incremental da VM quando atingem determinados limites de uso. Podemos obter automaticamente até 30% de desconto para cargas de trabalho que são executadas em uma parte significativa do mês de faturamento.
- **Faturamento por minuto:** o GCE tem uma taxa mínima de 10 minutos após o faturamento por minuto do uso real da VM. Isso proporciona uma redução de custo significativa, pois não temos que pagar pela hora inteira, mesmo quando uma instância é executada por menos de uma hora.

- **Hardware superior, menos instâncias:** para quase todas as camadas e aplicativos, descobrimos que era possível executar a mesma carga de trabalho com o mesmo desempenho com menos instâncias equivalentes no GCP.
- **Compromisso versus reserva:** um fator adicional é a avaliação do GCP sobre o preço da instância de VM. Com a AWS, a principal maneira de reduzir os custos das instâncias de VM é comprar instâncias reservadas para períodos de 1 a 3 anos. Se a carga de trabalho exigisse uma alteração na configuração da VM ou não precisássemos da instância, teríamos que vender a instância no mercado de instâncias reservadas com uma taxa mais barata. Com o GCPs, "Desconto de uso confirmado", que é feito para reserva de CPU e memória, não importa o tipo de instâncias de VM que estamos executando.

Resumo: com

base na avaliação detalhada, decidimos migrar para o GCP e começamos a trabalhar na estrutura de migração e nas listas de verificação. Fique atento ao nosso próximo post, pois compartilhamos alguns de nossos aprendizados durante a execução deste projeto.

