r/kubernetes

Posted by u/cablespaghetti 2 years ago

Kubernetes cluster on AWS for as little as $3 a month

https://github.com/cablespaghetti/kubeadm-aws

A little pet project of mine to build the cheapest possible Kubernetes cluster on AWS using spot fleet, kubeadm and Terraform. It's got some pretty big limitations at the moment, but right now it has:

- Automatic backup and recovery. So if your master gets terminated, when the replacement is provisioned by AWS it will pick up where the old one left off without you doing anything.
- Completely automated provisioning through Terraform and Bash.
- Variables for many things including number of workers and EC2 instance type.
- External DNS as a cheap ELB alternative.
- Persistent Volumes using GP2 storage on EBS.

Bug reports/feature requests/pull requests are very welcome. :)

This thread is archived

New comments cannot be posted and votes cannot be cast

SORT BY **BEST**

mzehrer 2 years ago

How does the external DNS Feature work?

3 Share •••

cablespaghetti 2 years ago

I should really document this, sorry.

Basically set up a NodePort service in Kubernetes and a domain you own in Route53. Then add an annotation to

The result will be a DNS entry managed by the cluster with the IPs of all the nodes.

I plan on using it to avoid paying for an ELB and using the cluster to host websites. But there are a few shortcomings I haven't quite worked out yet, such as only being allowed to use high ports (35000+ or something) for NodePort services.

3 Share •••

mzehrer 2 years ago

Why not use a nginx-ingress instead of NodePort?

3 Share •••

b00n 2 years ago

How do you think nginx-ingress works as a service?

You can run nginx/haproxy as an ingress as a damonset with hostPort and bind it to port 80/443 on all nodes though. NodePort only allows ports in a high range.

2 Share •••

cablespaghetti 🎤 2 years ago

You can override the NodePort range with an API server flag, but I'm still experimenting with that. The Nginx option isn't something

1 Share ···

[deleted] 2 years ago

Technically ingress is going to run using NodePort anyways since he's not using a load balancer. I do think it's a good idea but is another component using resources which aren't needed for a 3$ cluster.

1 Share ···

mzehrer 2 years ago

There is a problem with the external-dns pod I think, the logs say:

```
time="2018-08-27T10:00:27Z" level=info
msg="config: {Master: KubeConfig:
RequestTimeout:30s Sources:[service ingress]
Namespace: AnnotationFilter: FQDNTemplate:
CombineFQDNAndAnnotation:false
Compatibility: PublishInternal:false
PublishHostIP:false
ConnectorSourceServer:localhost:8080
Provider:aws GoogleProject: DomainFilter:[]
ZoneIDFilter:[] AWSZoneType:public
AWSAssumeRole: AWSMaxChangeCount:4000
AWSEvaluateTargetHealth:true
AzureConfigFile:/etc/kubernetes/azure.json
AzureResourceGroup: CloudflareProxied:false
InfobloxGridHost: InfobloxWapiPort:443
InfobloxWapiVersion:2.3.1
InfobloxSSLVerify:true DynCustomerName:
DynUsername: DynPassword: DynMinTTLSeconds:0
OCIConfigFile:/etc/kubernetes/oci.yaml
InMemoryZones:[]
PDNSServer: http://localhost:8081
PDNSAPIKey: PDNSTLSEnabled:false TLSCA:
TLSClientCert: TLSClientCertKey:
Policy:upsert-only Registry:txt
TXTOwnerID:k8s TXTPrefix: Interval:1m0s
Once:false DryRun:false LogFormat:text
MetricsAddress::7979 LogLevel:info
TXTCacheInterval:0s
ExoscaleEndpoint: https://api.exoscale.ch/dns ExoscaleAPIKey: ExoscaleAPISecret:}"

time="2018-08-27T10:00:27Z" level=info
msg="Connected to cluster at
https://10.96.0.1:443 "

time="2018-08-27T10:00:30Z" level=error
msg="services is forbidden: User
\"system:serviceaccount:kube-system:external-dns\" cannot list services
at the cluster scope"
```

1 Share ···

cablespaghetti 2 years ago

Interesting. I had it working before. I'll see if it does it on my cluster.

mzehrer 2 years ago

Yes, strange the clusterrole looks okay:

```
o → kubectl --insecure-skip-tls-verify describe clusterrole external-dns

Name: external-dns

Labels: <none>

Annotations: kubectl.kubernetes.io/last-applied-configuration={"apiVersion":"rbac.authorization.k8s.io/v1beta1","kind":"ClusterRole","metadata":{"annotations":{},"name":"external-dns","namespace":""},"rules":[{"ap ...

PolicyRule:

Resources Non-Resource URLs Resource Names Verbs

--------- ----------------- -------------- -----

ingresses.extensions [] [] [get watch list]

nodes [] [] [list]

pods [] [] [get watch list]
```

2 Share ···

cablespaghetti 2 years ago

Found this. https://github.com/kubernetes-incubator/external-dns/issues/582

Going to try and add the extra permissions. Not sure why it worked before!

1 Share ···

cablespaghetti 2 years ago

Whoops. I moved it from default to kube-system and didn't update the YAML properly. I'll make a commit.

1 Share ···

mzehrer 2 years ago

Not a terraform pro... can I simply update the current cluster?

1 Share ···

cablespaghetti 2 years ago

Not easily with the way the bash actually applies the yaml.

Easiest way is to change the line in /tmp/manifests/external-

"namespace: kube-system" (you'll need to sudo for that) and then as ubuntu run "kubectl apply -n kube-system -f /tmp/manifests/external-dns.yaml"

2 Share •••

mzehrer 2 years ago

Works! I would also leave out the --policy=upsert-only to get full sync between services and the dns.

2 Share •••

mrcrassic 2 years ago

dude. yes. i was working on this myself, but recovery was the key i couldn't make work.

thank you!

3 Share •••

cablespaghetti 🎤 2 years ago

Glad it's of some use to someone. Feel free to send me pull requests. 😉

1 Share •••

mrcrassic 2 years ago

paul_h 2 years ago

Nice work.

⬆ 4 ⬇ Share •••

cablespaghetti 2 years ago

Thanks!

⬆ 1 ⬇ Share •••

cr125rider 2 years ago

That’s excellent! Nicely done!

⬆ 2 ⬇ Share •••

cablespaghetti 2 years ago

Thanks!

⬆ 1 ⬇ Share •••

ruwing 2 years ago

Great work! I'll give it a try this days

⬆ 2 ⬇ Share •••

cablespaghetti 2 years ago

Thanks!

⬆ 1 ⬇ Share •••

Awesome. I was hoping there would be a cheaper option for individuals. Thank you!

2 Share •••

richraid21 2 years ago

I would really appreciate the ability to specific a different instance type for the master and the workers. Just a little feature request!

3 Share •••

cablespaghetti 2 years ago

Good idea. I'll add that. Won't be much work.

3 Share •••

cablespaghetti 2 years ago

Done

9 Share •••

SilentLennie 2 years ago · *edited 2 years ago*

Might be important to tell people: after the initial backup of the cluster files like certificates, the backup that runs every 15 minutes only backups up the etcd database, no other data is backed up it's all ephemeral. Did I see that correctly ? So all the data you have should be part of the images that get downloaded. Everything else people do, need to be on Persistent Volumes.

4

cablespaghetti 2 years ago

That's correct. I'll put that in the README.

1 Share •••