KubeCon | CloudNativeCon

North America 2018

Intro: CoreDNS

Yong Tang, Cricket Liu

Speakers

- ## Cricket Liu
  - EVP Engineering and Chief DNS Architect, Infoblox
  - Co-author of *DNS and BIND, 5th Edition*
  - Co-author of all of O'Reilly Media's books on DNS

- ## Yong Tang
  - Director of Engineering, *MobileIron*
  - Maintainer, *CoreDNS*
  - Maintainer, *Docker (Moby)*
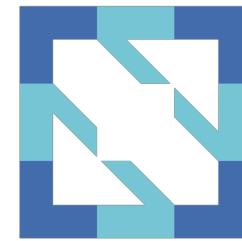 - Maintainer and SIG I/O Lead, *TensorFlow*

Agenda

- Introduction
- Status update
- Future roadmap
- Service discovery
- Corefile and plugins

CoreDNS

CoreDNS: Introduction

- Flexible DNS server written in Go

- Plugin based architecture, easily extended

- Supports DNS, DNS over TLS, DNS over gRPC

- Started and led by Miek Gieben

- Originally a fork of Caddy HTTP server ("Caddy DNS")

CoreDNS

CoreDNS: Introduction

- Focus on service discovery
- Native support with Kubernetes, contributions from Infoblox
- Integration with etcd and cloud vendors (e.g., route53)
- Support for Prometheus metrics
- Proxy/forward to recursive name server

CoreDNS

CoreDNS: Plugins

- *auto*: enables serving zone data from an RFC 1035-style master file, which is automatically picked up from disk.
- *autopath*: allows for server-side search path completion.
- *bind*: overrides the host to which the server should bind.
- *cache*: enables a frontend cache.
- *chaos*: allows for responding to TXT queries in the CH class.
- *debug*: disables the automatic recovery upon a crash so that you'll get a nice stack trace.
- *dnssec*: enables on-the-fly DNSSEC signing of served data.
- *dnstap*: enable logging to dnstap.
- *erratic*: a plugin useful for testing client behavior.
- *errors*: enables error logging.
- *etcd*: enables reading zone data from an etcd version 3 instance.
- *federation*: enables federated queries to be resolved via the kubernetes plugin.
- *file*: enables serving zone data from an RFC 1035-style master file.
- *forward*: facilitates proxying DNS messages to upstream resolvers.
- *health*: enables a health check endpoint.
- *hosts*: enables serving zone data from a `/etc/hosts` style file.
- *kubernetes*: enables the reading zone data from a Kubernetes cluster.

CoreDNS: Plugins

- *loadbalance*: randomizes the order of A, AAAA and MX records.
- *log*: enables query logging to standard output.
- *loop*: detects simple forwarding loops and halts the server.
- *metadata*: enables a meta data collector.
- *prometheus*: enables [Prometheus](#) metrics.
- *pprof*: publishes runtime profiling data at endpoints under `/debug/pprof`.
- *proxy*: facilitates both a basic reverse proxy and a robust load balancer.
- *reverse*: allows for dynamic responses to PTR and the related A/AAAA requests.
- *reload*: allows automatic reload of a changed Corefile.
- *rewrite*: performs internal message rewriting.
- *root*: simply specifies the root of where to find (zone) files.
- *route53*: enables serving zone data from AWS Route 53.
- *secondary*: enables serving a zone retrieved from a primary server.
- *template*: allows for dynamic responses based on the incoming query.
- *tls*: allows you to configure the server certificates for the TLS and gRPC servers.
- *trace*: enables OpenTracing-based tracing of DNS requests as they go through the plugin chain.
- *whoami*: returns your resolver's local IP address, port and transport.

CoreDNS: Project Status

- Release 1.2.6 (11/14/2018)

- Incubating project in CNCF
  - Inception in 2017, incubating in 2018
  - Plan on graduation now

- Growing community
  - 113 contributors (Big Thanks!)
  - 16 maintainers
  - 29+ public adopters
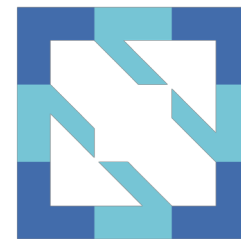 - 3000+ stars

CoreDNS: Project Status

- Google Summer of Code 2018
  - Thanks **Jiacheng Xu** (GitHub: **jiachengxu**)
  - Student in École Polytechnique Fédérale de Lausanne (Switzerland)
  - Distributed server setup with CoreDNS (idetcd)
- Second year in a row of CoreDNS in GSoC

CoreDNS: Project Status

- Each plugin is now backed by a number of OWNERs

- New plugin (loop) for DNS loop detection

- Kubernetes plugin:
  - General availability (GA) in Kubernetes 1.11
  - Didn't go default in Kubernetes 1.12 (increased memory usage)
    - Improvement: Increased speed and decreased memory usage
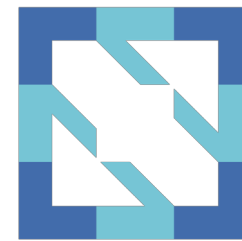 - Now default in Kubernetes 1.13

CoreDNS: Project Status

- Security review from Cure53
  - Sponsored by CNCF (first project in CNCF for security review)
  - Cache spoofing fixed 1.1.1
  - Two other minor bugs fixed
  - Written in Go (advantageous over C/C++ DNS implementations)

CoreDNS: Roadmap

- Core:
  - Relatively stable with enhancements

- Plugin
  - kubernetes: now default in 1.13
  - log: additional features and enhancements
  - cache: performance improvements
  - resolver: lots of interest
  - cloud integration: contribution welcome

- CNCF graduation (?)

CoreDNS: Corefile Configurations

- An authoritative DNS server

  ```
  coredns.io {
      file coredns.io {
          transfer to * 185.49.140.62
      }
      errors
      log
  }
  ```

- A recursive DNS server

  ```
  . {
      proxy . 8.8.8.8
      cache
      errors
      log
  }
  ```

CoreDNS: Service Discovery

- `.:53 {`
-     `kubernetes cluster.local 10.96.0.0/12 {`**`<- k8s integration`**
-       `pods insecure`
-     `}`
-     `route53 example.com.:Z1Z2Z3Z4DZ5Z6Z7`   **`<- route53 aws cloud data sync up`**
-     `hosts example.hosts example.org {`   **`<- additional records, added (inline)`**
-       `192.0.0.100 www.example.org`
-     `}`
-     `health`   **`<- healthcheck`**
-     `prometheus`   **`<- metrics`**
-     `cache 30`   **`<- cache & performance`**
-     `forward . 1.1.1.1:53`   **`<- forward to 1.1.1.1 (Cloudflare)`**
-     `errors`
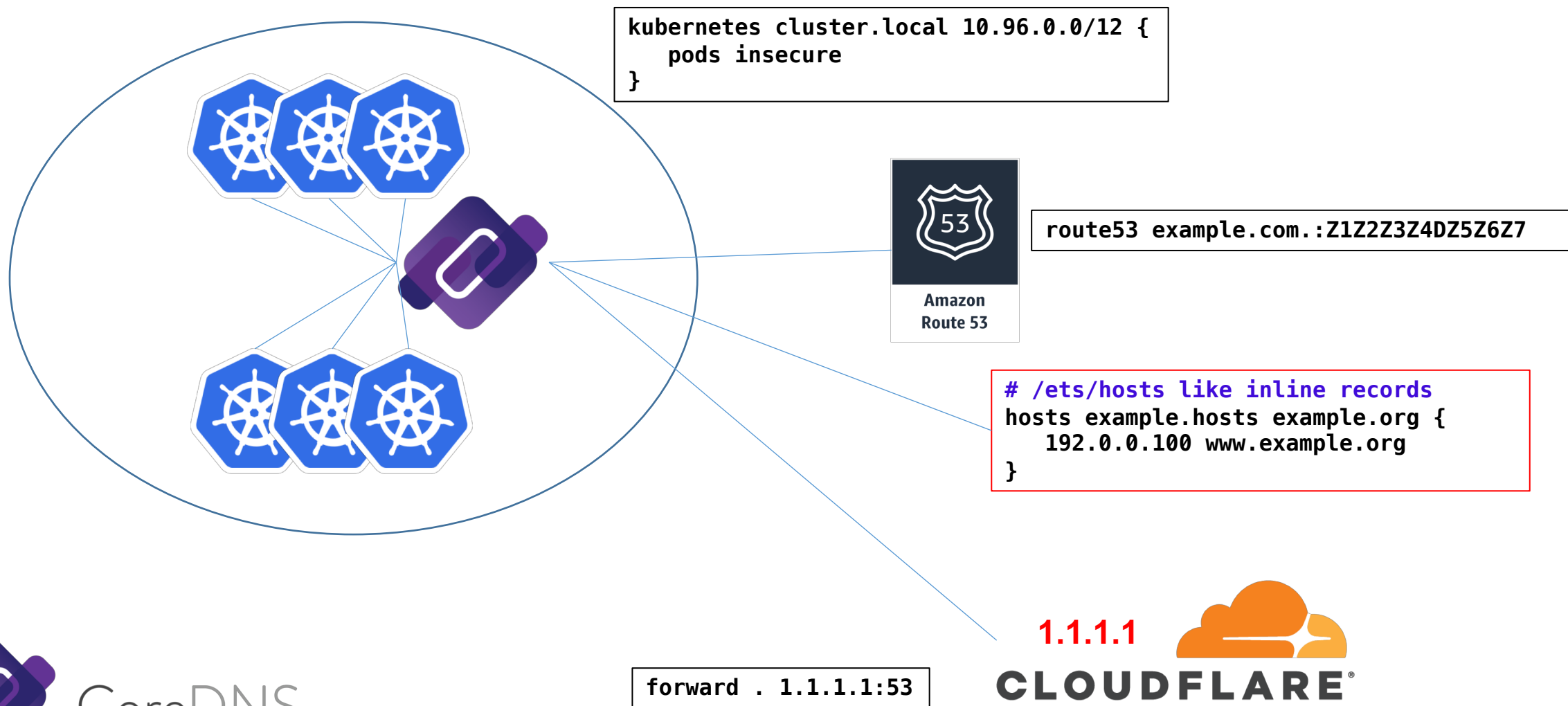- `}`

CoreDNS: Service Discovery


```
kubernetes cluster.local 10.96.0.0/12 {
    pods insecure
}
```

```
route53 example.com.:Z1Z2Z3Z4DZ5Z6Z7
```

Amazon
Route 53

```
# /ets/hosts like inline records
hosts example.hosts example.org {
    192.0.0.100 www.example.org
}
```

```
forward . 1.1.1.1:53
```

1.1.1.1
CLOUDFLARE®

CoreDNS: Service Discovery

api servers
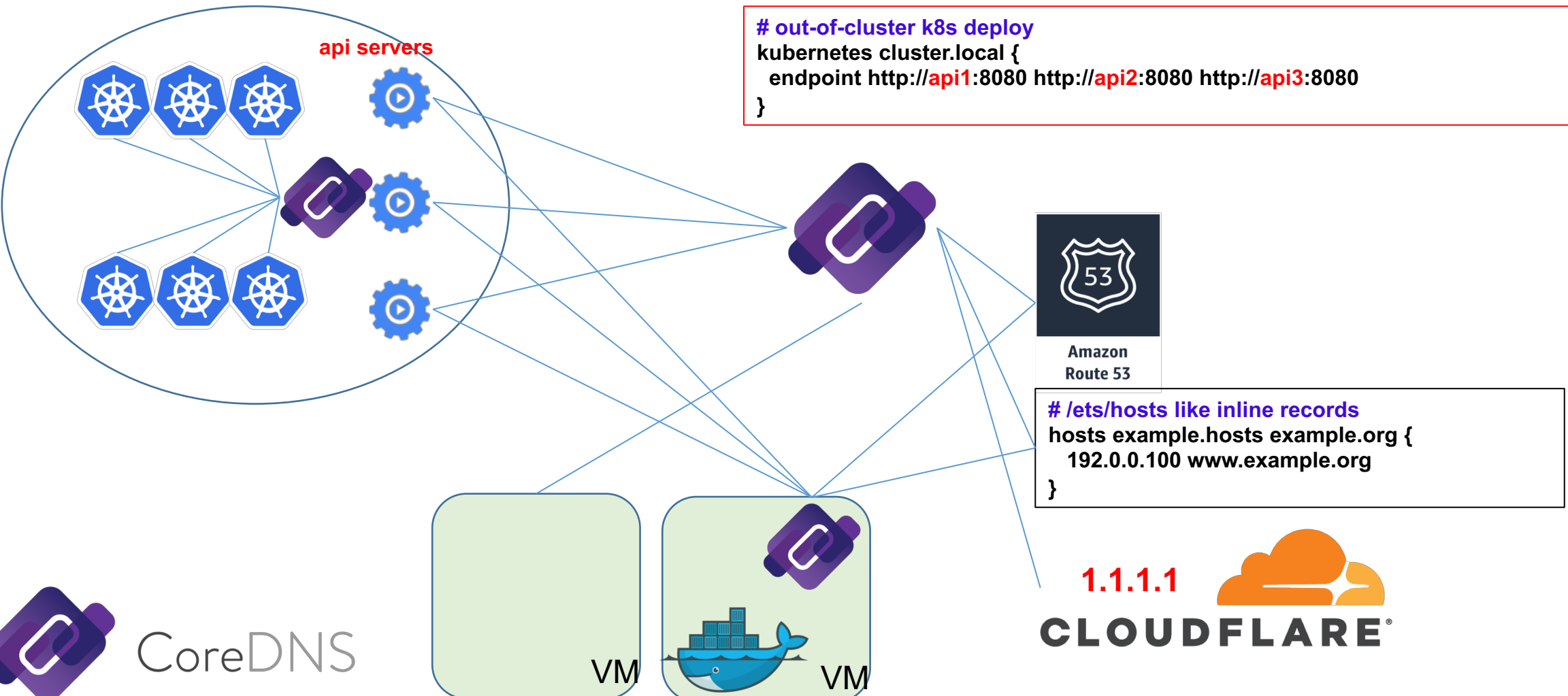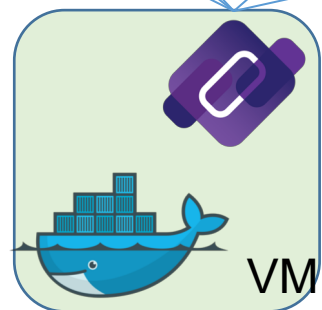
# out-of-cluster k8s deploy
kubernetes cluster.local {
    endpoint http://api1:8080 http://api2:8080 http://api3:8080
}

Amazon
Route 53

# /ets/hosts like inline records
hosts example.hosts example.org {
    192.0.0.100 www.example.org
}

VM

VM

1.1.1.1

CLOUDFLARE®

CoreDNS

CoreDNS: Community

- Most active:
  - GitHub: https://github.com/coredns/coredns
  - Slack: #coredns on https://slack.cncf.io

- More resources:
  - Web: https://coredns.io
  - Blog: https://blog.coredns.io
  - Twitter: @corednsio
  - Mailing list/group (not very active):
    - coredns-discuss@googlegroups.com

CoreDNS: Contributions Welcome

- Star CoreDNS in GitHub:
  - https://github.com/coredns/coredns
- Add the name to ADOPTERS.md
- Create a PR to become a contributor
- Become a maintainer
  - One significant pull request
  - Sponsored by one current maintainer