



Catalog zones version 2: BIND and beyond

Petr Špaček

2022-05-19

<https://www.isc.org>

The Problem

- Manage zone list on secondaries
 - ... all of them!
- Server-specific
 - Text configuration
 - APIs

The Problem

```
zone "example1.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

The Problem

```
zone "example1.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
  
zone "example2.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

The Problem

```
zone "example1.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
  
zone "example2.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
  
zone "example3.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```



The Problem

```
zone "example1.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

```
zone "example3.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

```
zone "example2.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

```
zone "example4.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```



The Problem

```
zone "example1.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
zone "example2.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
zone "example3.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
zone "example4.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};  
zone "example5.com" {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

The Problem

```
zone "example1.com" {
    type secondary;
    primaries { 192.0.2.1; };
};

zone "example2.com" {
    type secondary;
    primaries { 192.0.2.1; };
};

zone "example3.com" {
    type secondary;
    primaries { 192.0.2.1; };
};

zone "example4.com" {
    type secondary;
    primaries { 192.0.2.1; };
};

zone "example5.com" {
    type secondary;
    primaries { 192.0.2.1; };
};

zone "example6.com" {
    type secondary;
    primaries { 192.0.2.1; };
};
```


The Pr

zone "exa

type se

primary:

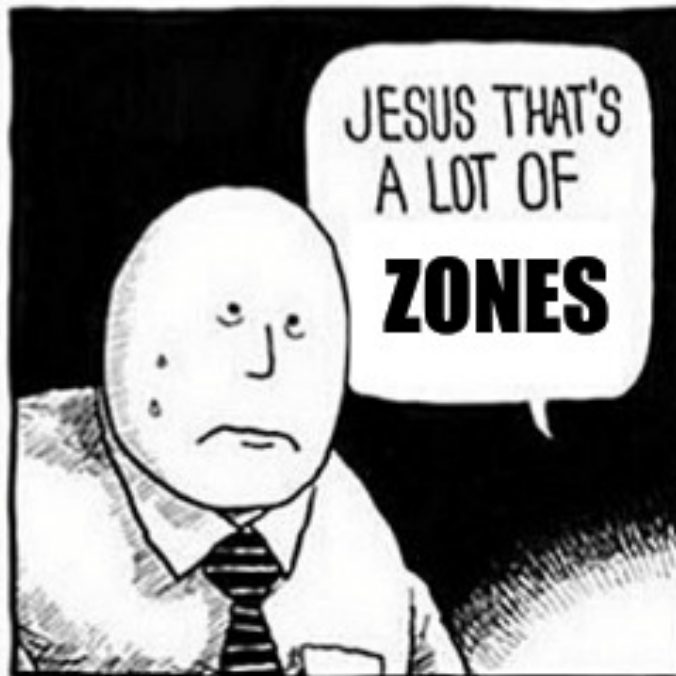
}; zon

zone "examp

type secc

primaryes

};



```
n" {
```

```
: 0.2.1; };
```

```
com" {
```

```
y; 1; };
```

```
92.0.2.1; };
```

```
com" {
```

```
y;
```

```
92.0.2.1; };
```

Home-grown solutions

- Ansible, Puppet, Chef, ... you name it
 - Custom development
 - Often for a single DNS implementation
 - "It works!"
- Not interoperable
 - Cross-organization or multi-vendor secondaries



An observation

- DNS lacks provisioning, but ...
- Lots of zones
 - Groups with the same parameters
- Essentially a list of zones
 - Repetition ad absurdum



Solution for DNS purists

- When you have a hammer, everything looks like a nail
- When you have zone transfers, everything looks like a DNS zone
- => Catalog Zones



Catalog Zones: principle

- List of DNS zones
 - ... in form of a DNS zone!
 - Zone-transferable
 - "Meta-zone" – not to be queried by resolvers
 - Only for secondary servers

ONE ZONE



TO RULE THEM ALL

Catalog Zones

- Version 1
 - BIND 9.11+ (a hack exists for PowerDNS)
- **Version 2** – joint work – Willem, Peter, Libor, Peter, Aram,
 - BIND 9.18.3+
 - Knot DNS 3.0+
 - NSD "coming soon"
 - PowerDNS ?



Catalog Zones aka CATZ

- Version 1
 - BIND 9.11+ (a hack exists for PowerDNS)
- **Version 2** – joint work – Willem, Peter, Liikla
 - BIND 9.18.3+
 - Knot DNS 3.0+
 - NSD "coming soon"
 - PowerDNS ?



Catalog Zones: format

\$ORIGIN catalog.example.

Name of this catalog zone
– arbitrary, not to be queried

; pretend this is a regular zone

@ SOA . . 1234 900 600 3600 1

Serial and transfer timers
(as usual)

@ NS invalid.

Unused but mandatory

; don't forget the version number

!! version TXT "2"

Zone name

to be provisioned on secondaries
("catalog-member zone")

5960700569b6a05c.zones PTR domain.example.

Random zone ID

8rff9what88dunno.zones PTR domain2.example.

BIND primary

```
zone "catalog.example." {  
    type primary;  
    file "catalog.db";  
};  
zone "domain.example." {  
    type primary;  
    file "domain.db";  
};
```

Normal zones on the primary!
All usual mechanisms work – AXFR, IXFR, NOTIFY, ...

BIND secondary

```
zone "catalog.example." {  
    type secondary;  
    primaries { 192.0.2.1; };  
};
```

The catalog zone
– a secondary zone as usual

```
options {  
    catalog-zones {  
        zone "catalog.example."
```



Enable special interpretation
– automatic setup of *other*
secondary zones

Multiple catalog
zones can be specified

```
        default-primaries { 192.0.2.1; };  
    };
```

Primary to transfer
"catalog-member zones" from



BIND secondary logs

- 1 client 192.0.2.1#45137: received notify for zone 'domain.example': not authoritative
- 2 client 192.0.2.1#53718: received notify for zone 'catalog.example'
- 3 **zone catalog.example/IN: Transfer started.**
- 4 catz: updating catalog zone 'catalog.example' with serial 1234
- 5 zone catalog.example/IN: transferred serial 1234
- 6 catz: adding zone 'domain.example' from catalog 'catalog.example' - success
- 7 **zone domain.example/IN: Transfer started.**
- 8 zone domain.example/IN: transferred serial 1

Knot DNS secondary

template:

- id: member_template
master: *master_list*

Primary to transfer
"catalog-member zones" from
(list of IP addresses)

zone:

- domain: catalog.example.
master: *master_list*
catalog-role: interpret

Enable special interpretation
– automatic setup of *other*
secondary zones



catalog-template: member_template

Configuration template for
"member zones"



Knot DNS secondary logs

- 1 [catalog.example.] notify, incoming, remote
192.0.2.1@58736, serial 1234
- 2 [catalog.example.] AXFR, incoming, remote
192.0.2.1@53, finished
- 3 [catalog.example.] catalog reloaded, 1 updates
- 4 **[domain.example.] zone added from catalog**
- 5 [domain.example.] zone will be bootstrapped
- 6 [domain.example.] AXFR, incoming, remote
192.0.2.1@53, started
- 7 [domain.example.] AXFR, incoming, remote
192.0.2.1@53, finished
- 8 **[domain.example.] zone file updated, serial 1**



Closing words

- Catalog zones version 2
 - Interoperable provisioning of zones to secondary servers
 - BIND 9.18.3, Knot DNS 3.0
- Support for other servers coming
- Read the [specification](#)
- [Chat](#) with spec authors and implementors

Thank you!

- Main website: <https://www.isc.org>
- Software downloads:
<https://www.isc.org/download> or
<https://downloads.isc.org>
- Presentations:
<https://www.isc.org/presentations>
- Main GitLab: <https://gitlab.isc.org>