DNS Catalog Zones

draft-ietf-dnsop-dns-catalog-zones-04

Peter van Dijk
Libor Peltan
Ondřej Surý
Willem Toorop
Leo Vandewoestijne
Peter Thomassen

Abstract

… a method for automatic DNS zone provisioning among DNS primary and secondary nameservers by storing and transferring the catalog of zones to be provisioned as one or more regular DNS zones.

DNS Catalog Zones

draft-ietf-dnsop-dns-catalog-zones-04

```
$ORIGIN catzone.
@                       IN  SOA ( . . 1552507036
                              86400 14400 86400 0 )

@                       IN  NS  invalid.
version                 IN  TXT "2"
<unique-id-1>.zones     IN  PTR example.com.
<unique-id-2>.zones     IN  PTR example.net.
<unique-id-3>.zones     IN  PTR example.org.
```
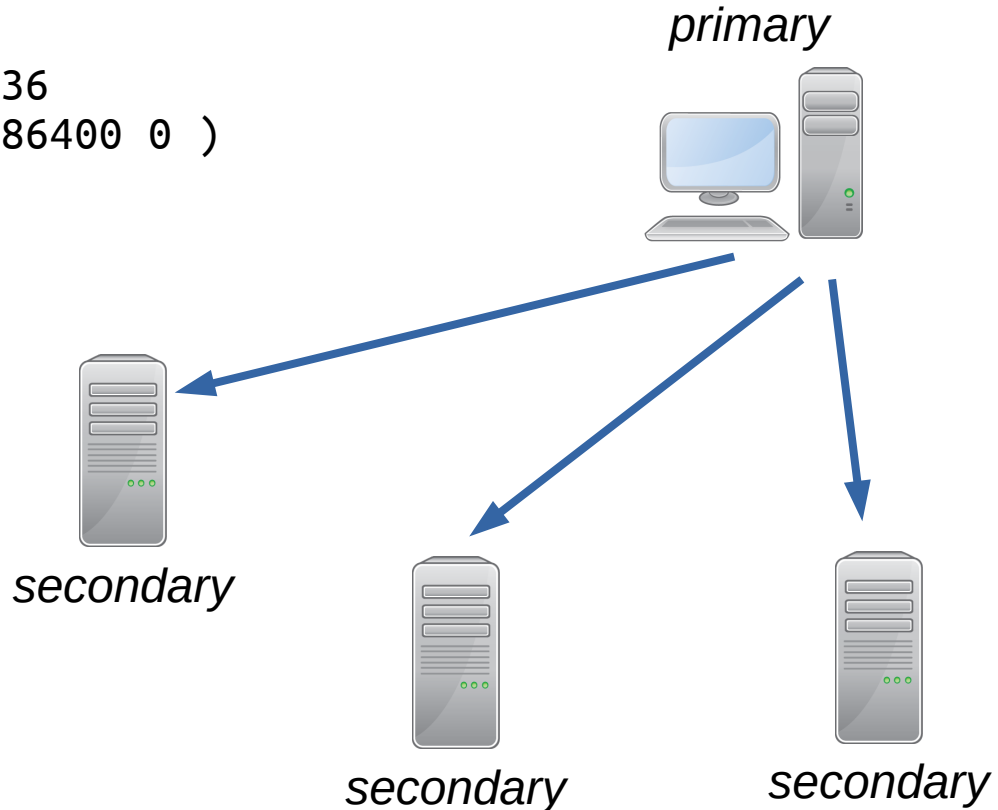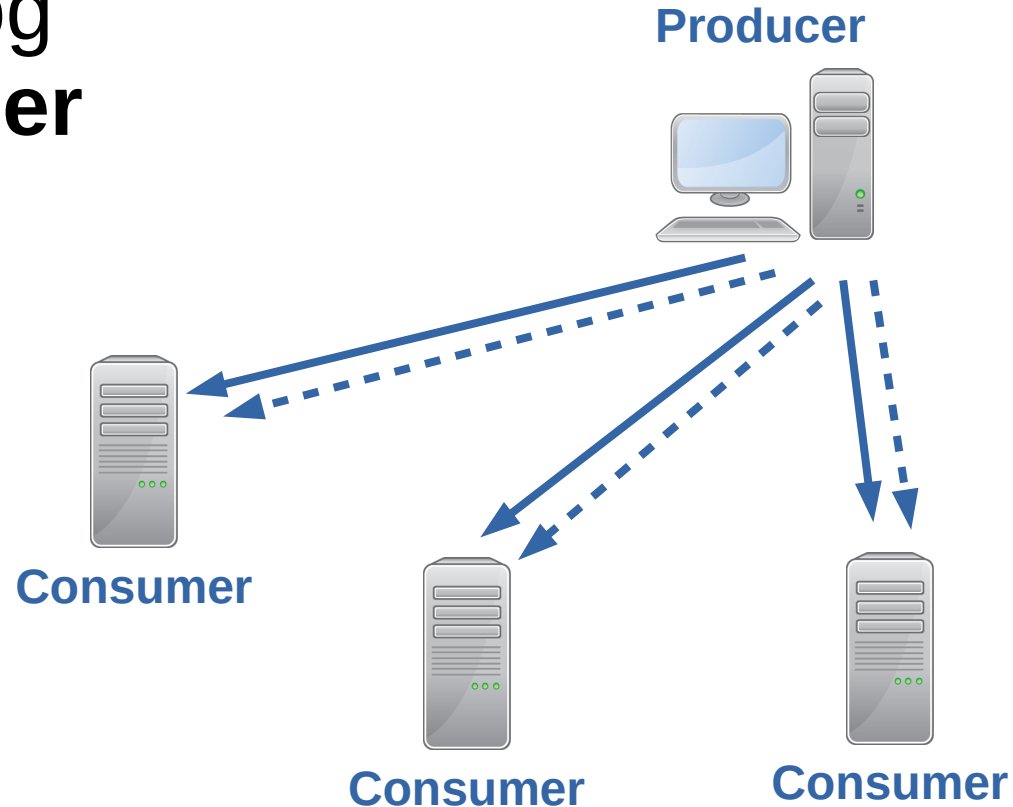
primary

secondary

secondary   *secondary*

DNS Catalog Zones

New in `draft-ietf-dnsop-dns-catalog-zones-04` since `-02`

- Introduced terms Catalog **Producer** and **Consumer**

Producer

Consumer

Consumer   **Consumer**

DNS Catalog Zones

New in `draft-ietf-dnsop-dns-catalog-zones-04` since `-02`

- Introduced terms Catalog **Producer** and **Consumer**

primary

Producer
Producer

Consumer
Consumer

Consumer
Consumer
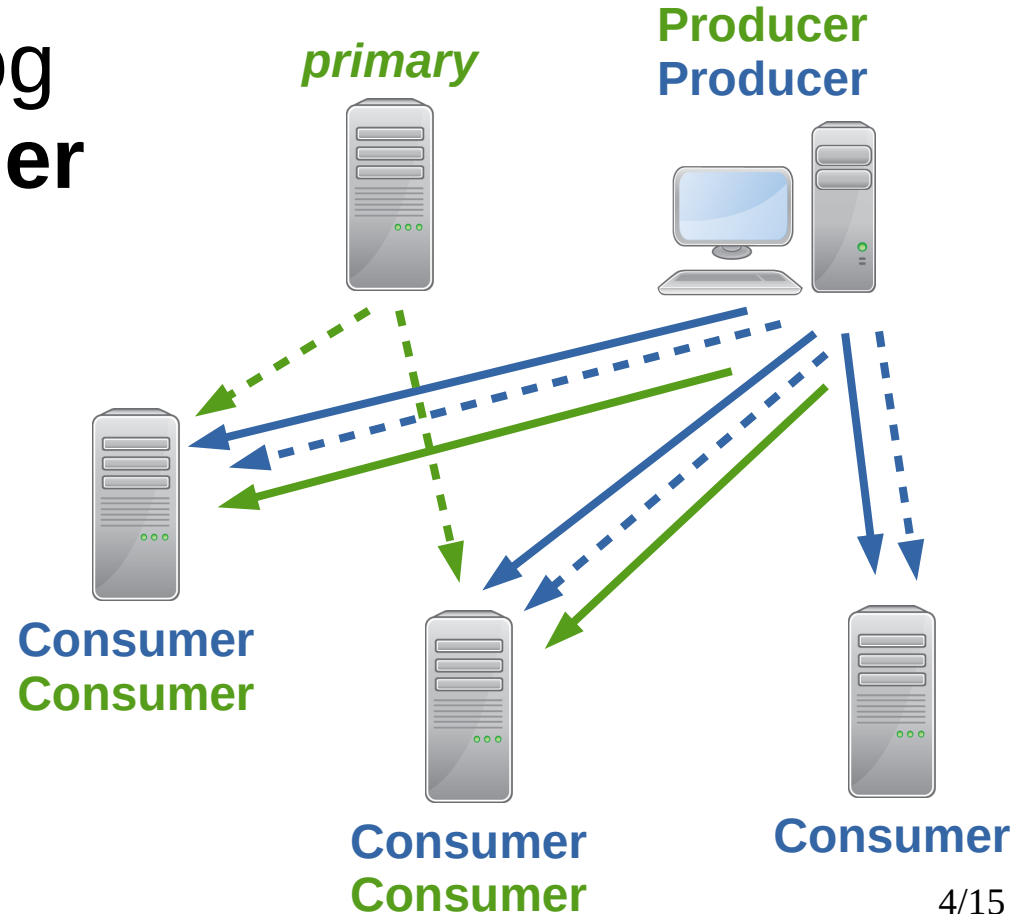
Consumer

DNS Catalog Zones

New in `draft-ietf-dnsop-dns-catalog-zones-04` since `-02`

- Introduced terms Catalog **Producer** and **Consumer**

- Make the least assumptions on implementation
  - predictability of owner names left out of consideration *(got rid of the epoch property)*

DNS Catalog Zones

New in `draft-ietf-dnsop-dns-catalog-zones-04` since `-02`

- Introduced terms Catalog
  Producer and **Consumer**

- Make the least assumptions on implementation
  - predictability of owner names left out of consideration

- Focus on basic operations
  - Adding member zones
  - Remove member zones
  - Migration of member zones
  - Zone state reset
  - Member name clashes
  - Member node name change

DNS Catalog Zones

New in draft-ietf-dnsop-dns-catalog-zones-04 since -02

- ## Members can have 'properties'

  - Properties from std documents are 1 label below zone member name

    ```
    <unique-id-1>.zones          IN  PTR     example.com.
    coo.<unique-id-1>.zones      IN  PTR     some-other-catalog-zone.
    <unique-id-2>.zones          IN  PTR     example.net.
    group.<unique-id-2>.zones    IN  TXT     sign-with-nsec3
    <unique-id-3>.zones          IN  PTR     example.org.
    serial.<unique-id-3>.zones   IN  SERIAL  1634730530
    ```

  - All properties in the draft (coo, group, serial) are optional

  - Custom properties below label ext

    ```
    <unique-id-4>.zones          IN  PTR     example.com.
    <name>.ext.<unique-id-4>.zones  IN  TXT/PTR/…   <value>
    ```

DNS Catalog Zones
draft-ietf-dnsop-dns-catalog-zones-04

- ## The Change Of Ownership (COO) property

  - Controlled migration of a member zone from one catalog to another

  - A Change Of Ownership is signaled by the current "owner"
    ```
    <unique-id-A>.zones.catzone.       IN  PTR     example.com.
    coo.<unique-id-A>.zones.catzone.   IN  PTR     other-catzone.
    ```

  - `<unique-id-A>` is associated with `example.com.`

  - Zone is not migrated yet, only after `other-catzone` is updated with:
    ```
    <unique-id-B>.zones.other-catzone. IN  PTR     example.com.
    ```

  - Zone associated state (zone data, DNSSEC keys etc.)
    is reset when `<unique-id-A>` ≠ `<unique-id-B>`

DNS Catalog Zones

draft-ietf-dnsop-dns-catalog-zones-04

- ## The group property

  - Associate with a different set of configurations within a catalog

    ```
    <unique-1>.zones.catzone.        IN  PTR example.com.
    group.<unique-1>.zones.catzone.   IN  TXT sign-with-nsec3
    <unique-2>.zones.catzone.        IN  PTR example.net.
    group.<unique-2>.zones.catzone.   IN  TXT nodnssec
    ```

  - Atomic change of config

  - Fits well with Knot templates and NSD patterns

DNS Catalog Zones
draft-ietf-dnsop-dns-catalog-zones-04

- The serial property
  - Increase reliability of zone update signalling
    - Notifies may be lost
    - Secondaries may be down
  - Reducing NOTIFY and SOA query traffic
    - With lots of secondaries and lots of zones

DNS Catalog Zones
draft-ietf-dnsop-dns-catalog-zones-04

- ## The serial property

  - ```
    <unique-1>.zones.catzone.          IN  PTR     example.com.
    serial.<unique-1>.zones.catzone.   IN  SERIAL  3
    <unique-2>.zones.catzone.          IN  PTR     example.net.
    serial.<unique-2>.zones.catzone.   IN  SERIAL  1634730530
    <unique-3>.zones.catzone.          IN  PTR     example.org.
    serial.<unique-3>.zones.catzone.   IN  SERIAL  2020112405
    ```

  - the serial number of the member zone's SOA record

  - Transfer on change – no NOTIFY needed

  - Clear refresh timer of member zone when catalog is fresh

- ## An optimization build upon catalog zones not dealing with the catalog itself

DNS Catalog Zones

New in `draft-ietf-dnsop-dns-catalog-zones-04` since `-02`

- Extended Security section
    - Administrative control over what zones are served from the configured name servers shifts completely from the server operator (consumer) to the "owner" (producer) of the catalog zone content.

- Added author: Peter Thomassen

DNS Catalog Zones

`draft-ietf-dnsop-dns-catalog-zones-04`

- This version of the draft is the result of thorough review and discussion with the goal of getting it in shape for publication as RFC.

- This version of the draft has catalog zones specified to the best of our ability and we request you to review it thoroughly with the documents readiness for WGLC in mind.

DNS Catalog Zones

draft-ietf-dnsop-dns-catalog-zones-04

- This version of the draft is the result of thorough review and discussion with the goal of getting it in shape for publication as RFC.

- This version of the draft has catalog zones specified to the best of our ability and we request you to review it thoroughly with the documents readiness for WGLC in mind.

DNS Catalog Zones

draft-...es-04

- This version of the draft is the result of thorough study and discussion with the goal of shaping it into shape for publication as RFC.

- This version of the draft is ... specific ... the best of our ab... to review it thoroughly with the documents re... GLC in mind.

MISSION

ACCOMPLISHED