DDIUG 2024 - DNS Katalogzonen

Carsten Strotmann

DNS Zonen automatisch anlegen mit Katalog-Zonen

Bereitstellung neuer Zonen

- Das Hinzufügen oder Löschen neuer Zonen kann eine Herausforderung sein.
- Neben der Aktualisierung der Konfiguration auf dem Server der primären Zone muss auch jeder Server mit einer sekundären Zone geändert werden.
- Für Installationen mit vielen sekundären Zonen oder mit häufigem Hinzufügen und Löschen von Zonen ist aufwändig.
- Viele Unternehmen haben Skripte geschrieben (oder verwenden Tools wie Ansible oder SaltStack), um die sekundären DNS-Server automatisch zu konfigurieren.

Bereitstellung neuer Zonen

- Eine Katalogzone stellt normale Zonen mit Standard-DNS-Inhalten und -Kommunikation bereit.
  - Sie sind eine Entwicklung von ISC, neu in BIND 9.11 (2016), und wurden in der IETF standardisiert.
  - RFC 9432: ↪DNS-Katalog-Zonen
  - Die Katalogzone im RFC-Stil (Version 2) wird ab BIND 9.16+ unterstützt.

Unterstützung von Katalogzonen in DNS-Server-Software

- KnotDNS hat eine voll funktionsfähige Implementierung seit Version 3.0.0 (September 2020)
- PowerDNS Authoritative Server unterstützt Katalogzonen seit 4.7.0 (↪https://doc.powerdns.com/authoritative/catalog.html)
- NSD: unterstützt Katalogzonen nach RFC 9432 seit Version 4.9.0 (↪https://nsd.docs.nlnetlabs.nl/en/latest/catalog-zones.html)

Katalogzone

- Eine Katalogzone funktioniert wie eine normale DNS-Zone.
- Eine Katalogzone wird auf dem Primärserver verwaltet.
- Sie enthält Zonennamen und Konfigurations-Metadaten der DNS-Zonen, welche auf sekundären Servern vorhanden sein sollten.
- Zonen, die zur Katalogzone hinzugefügt werden, werden automatisch auf den Sekundärservern bereitgestellt.
    - Zonen in einer Katalogzone sind Mitgliedszonen (Memberzones).

Katalogzone

- Ein primärer DNS-Server, der eine Katalogzone hostet, muss keine spezielle Unterstützung für Katalogzonen bieten.
  - Dies liegt daran, dass Katalogzonen Standard-DNS-Inhalte und -Kommunikation verwenden.
  - Die sekundären Server müssen Katalog-Zonen unterstützen, damit sie den Inhalt einer Katalogzone als Bereitstellungsinformation verwenden.

Katalogzone

- Ein Sekundär-DNS-Server hat eine Katalogzone für jeden DNS-Primary-Server.
    - Angenommen, der Primary-DNS-Server hostet eine Katalog-Zone

Katalogzone: named.conf:Primary

- In der `named.conf` eines DNS-Primary ist eine Katalogzone eine ganz normale Zone.
- Es gibt keine besonderen Anforderungen an die Konfiguration oder an den Namen der Zone.
- Die Domain der Katalog-Zone muss nicht im Internet delegiert oder auflösbar sein

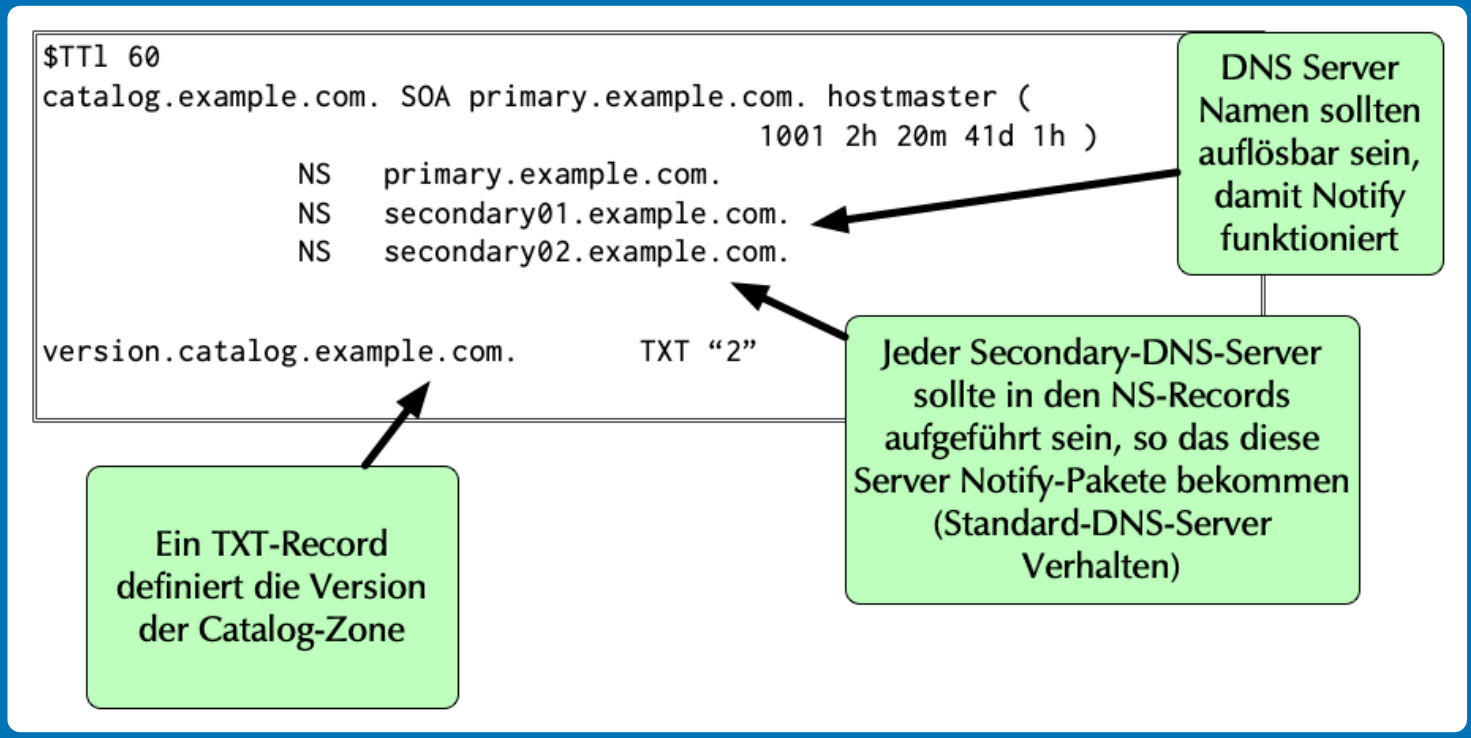
```
zone "catz.dnslab.org" {
        type primary;
        file "catz.dnslab.org";
};
```

Katalogzone: Zonendatei:Primary

- Eine Katalog-Zonendatei enthält den SOA-Record und die NS-Records für die Zone.
- Sie muss außerdem einen TXT-Eintrag mit der Versionsnummer der Implementierung des Katalogzonenprotokolls enhalten
    - Version 1: das Katalogzonenprotokoll, wie es in BIND 9.11 - BIND 9.14 implementiert wurde
    - Version 2: das Katalogzonenprotokoll, wie es im Internet RFC beschrieben und in BIND 9.16+ implementiert ist.
    - DNS-Server-Software ignoriert Katalogzonen mit einer Versionsnummer Versionsnummer, die sie nicht unterstützt (BIND 9 lädt keine Katalogzone ohne den TXT-Eintrag mit der Versionsnummer)

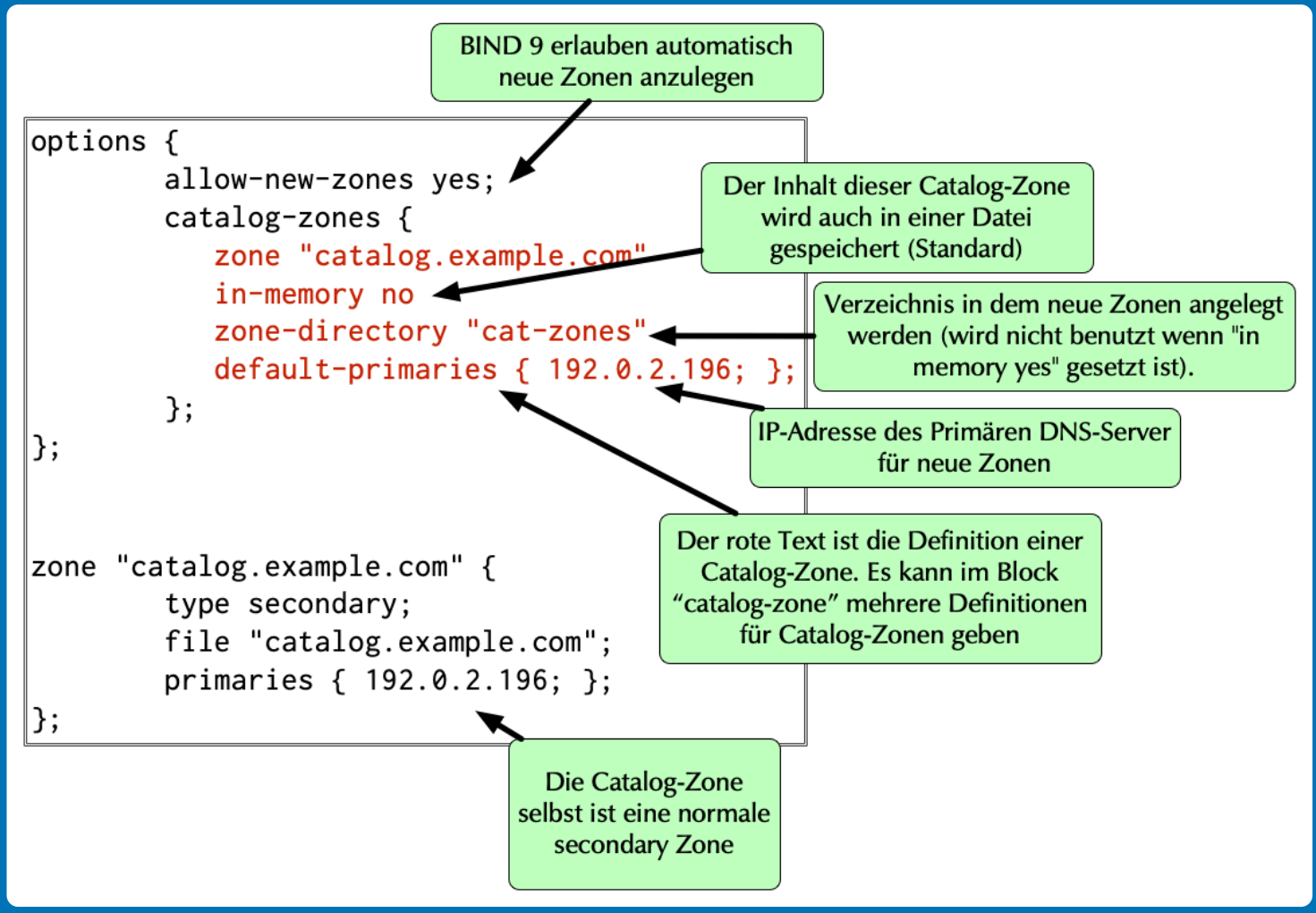
Katalogzone: Zonendatei:Primary

- Eine Katalogzone hat einen PTR RR für jede Mitgliedszone. In der gezeigten Katalog Zone sind noch keine Mitgliedszonen bereitgestellt worden. Sie ist leer. (Sie hat keine PTR RRs).



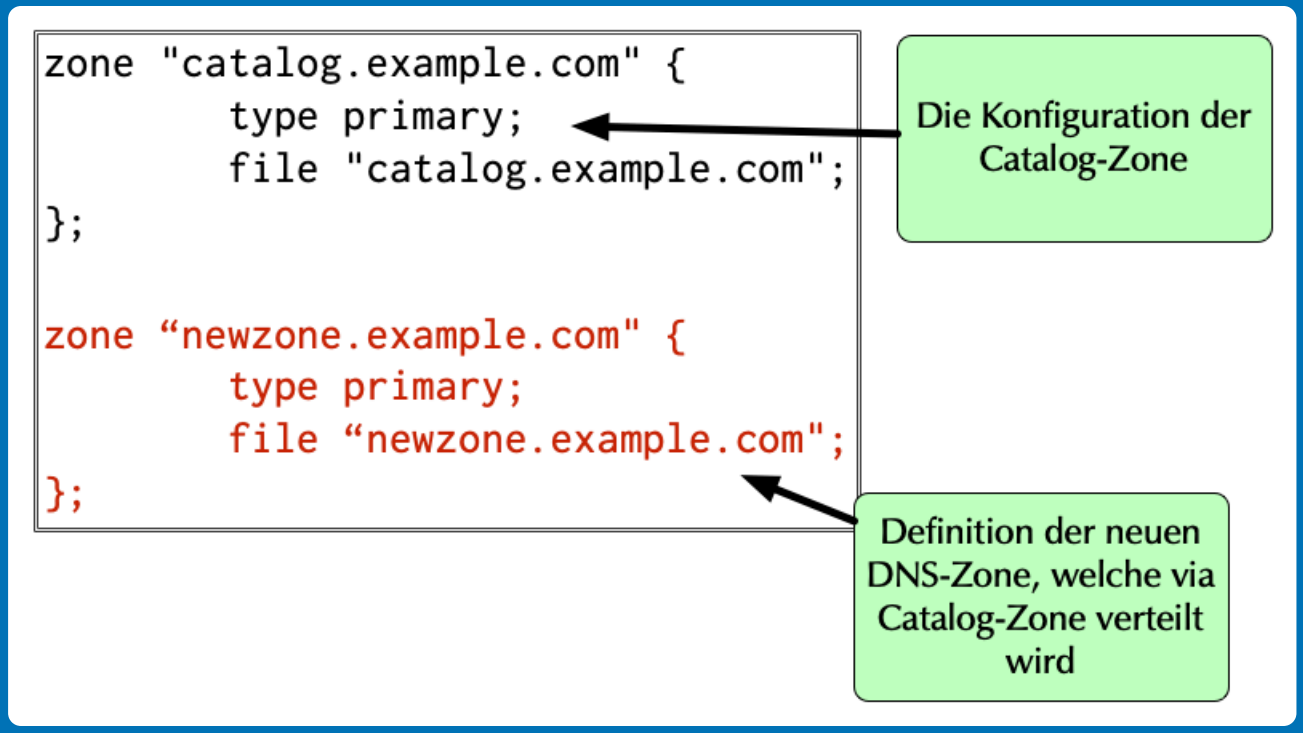
Katalogzone: named.conf:Secondary

- Die Konfiguration für Katalogzonen befindet sich auf den Secondary DNS-Servern.


BIND 9 erlauben automatisch neue Zonen anzulegen
options {
allow-new-zones yes;
catalog-zones {
zone "catalog.example.com"
in-memory no
zone-directory "cat-zones"
default-primaries { 192.0.2.196; };
};
};
zone "catalog.example.com" {
type secondary;
file "catalog.example.com";
primaries { 192.0.2.196; };
};
Der Inhalt dieser Catalog-Zone wird auch in einer Datei gespeichert (Standard)
Verzeichnis in dem neue Zonen angelegt werden (wird nicht benutzt wenn "in memory yes" gesetzt ist).
IP-Adresse des Primären DNS-Server für neue Zonen
Der rote Text ist die Definition einer Catalog-Zone. Es kann im Block “catalog-zone” mehrere Definitionen für Catalog-Zonen geben
Die Catalog-Zone selbst ist eine normale secondary Zone

Bereitgestellte Mitgliederzone

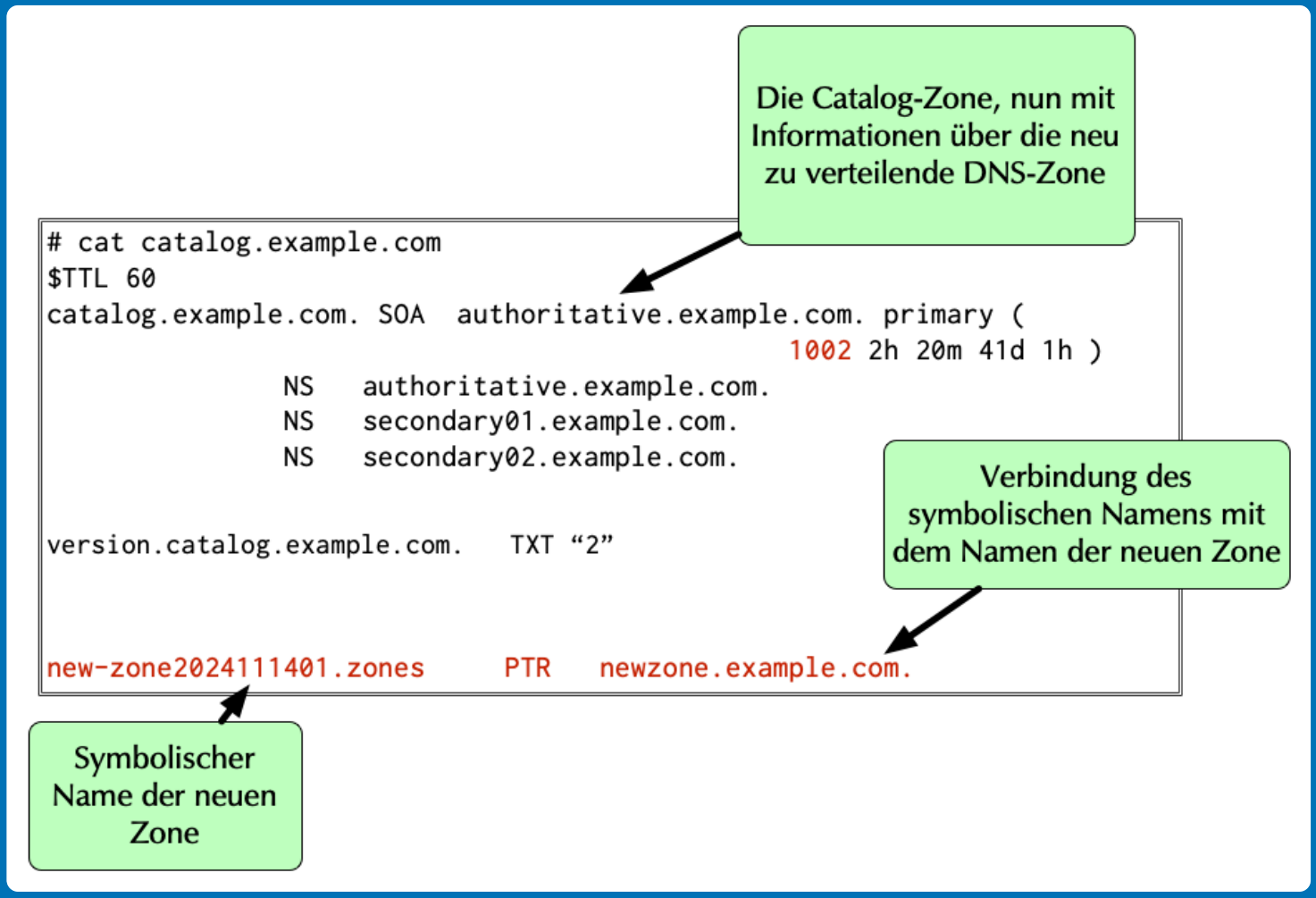
- Die Zonendatei für eine Mitgliederzone wird wie üblich auf dem Primary-DNS-Server erstellt, wie bei jeder anderen Zone auch (nicht gezeigt). Sie wird zu `named.conf` hinzugefügt.



Registrierung einer neuen Zone im Katalog

- Die neue Zone muss in der Katalogzone registriert werden.
- Die Registrierung erfolgt mit einem `PTR` (Pointer)-Record, wobei der Datenteil dieses Datensatzes der Zonenname ist (`neuezone.beispiel.com` in diesem Beispiel)
    - Der Domänenname des Datensatzes muss ein eindeutiger Name (Label) sein (zum Beispiel der SHA1-Hash des Namens der neuen Zone), das Label `zones` und der Domänenname der Katalogzone (Im Beispiel das Label `Zone2024111401.zones` in der Domain `catalog.example.com.`)

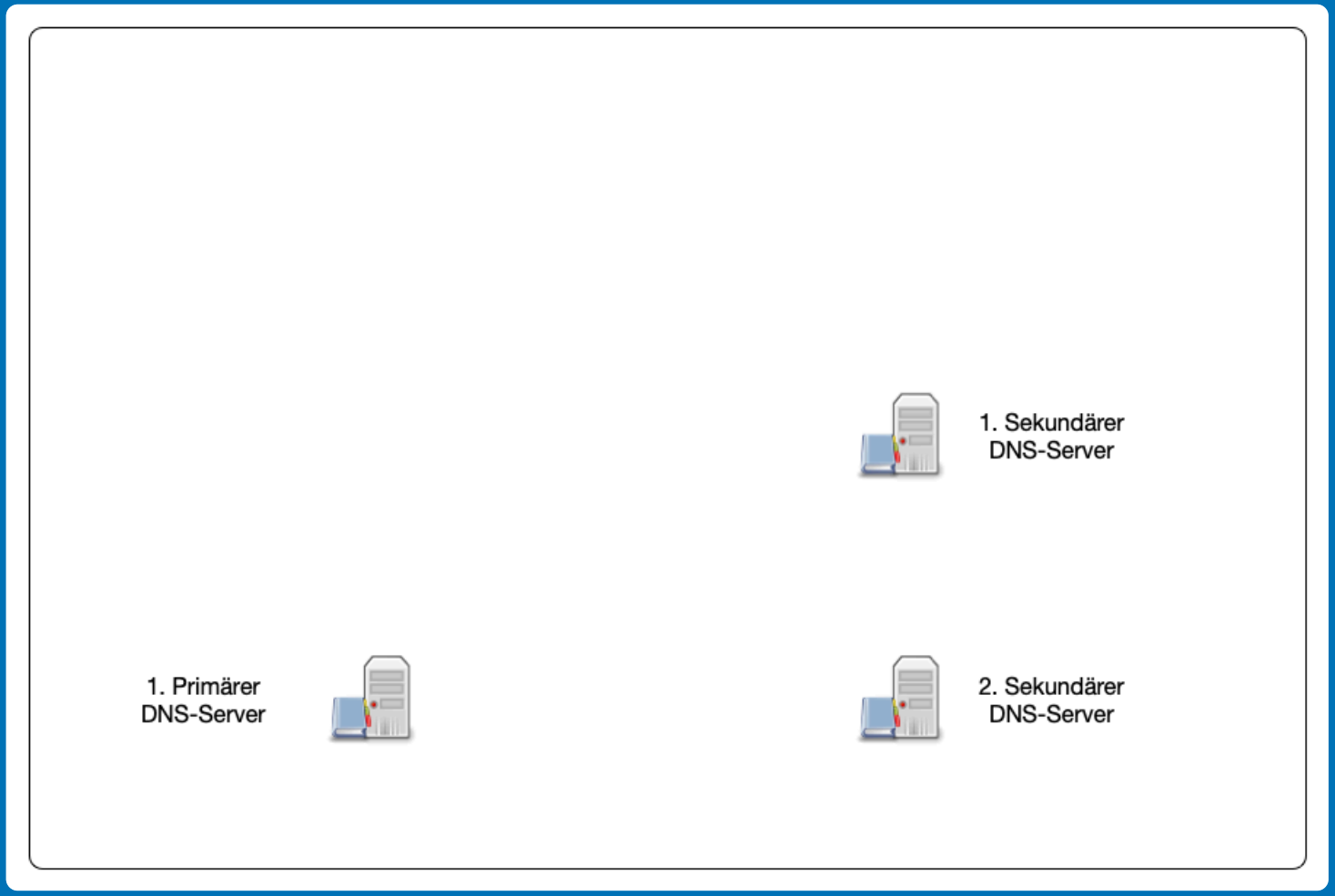
Registrierung einer neuen Zone im Katalog



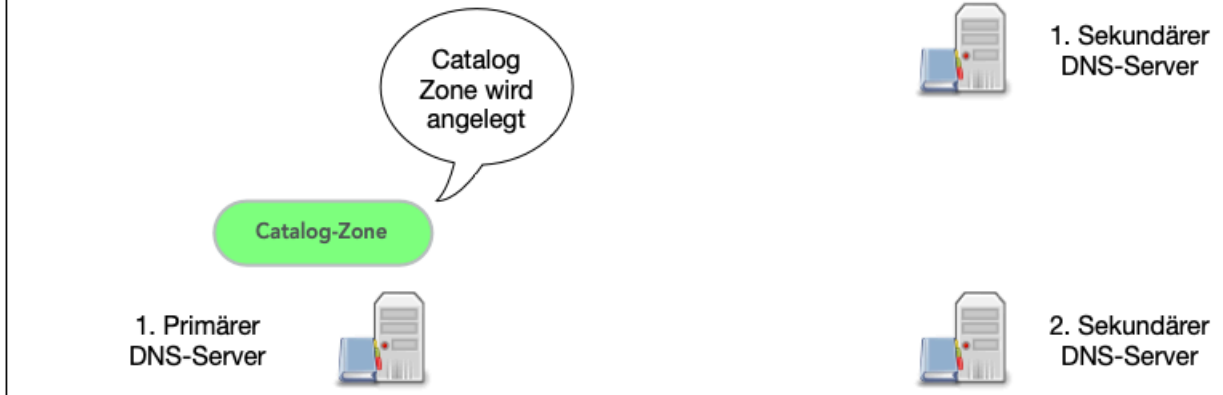
Erfolg der Provisionierung

- Der Sekundärserver lädt automatisch die neue Mitgliederzone.
- Aktualisierungen der Mitgliederzone werden automatisch an den sekundären Server übertragen.
    - Dies geschieht mit den üblichen Methoden (`NOTIFY`, `IXFR`, usw.).
- Zusätzliche Zonen, welche der Katalogzone hinzugefügt werden, werden automatisch auf den sekundären DNS-Servern bereitgestellt.
- Eine Zone, die aus der Katalogzone entfernt wird, wird von den sekundären Servern entfernt.
    - Eine Zonensicherungsdatei auf einem Sekundärserver wird gelöscht.

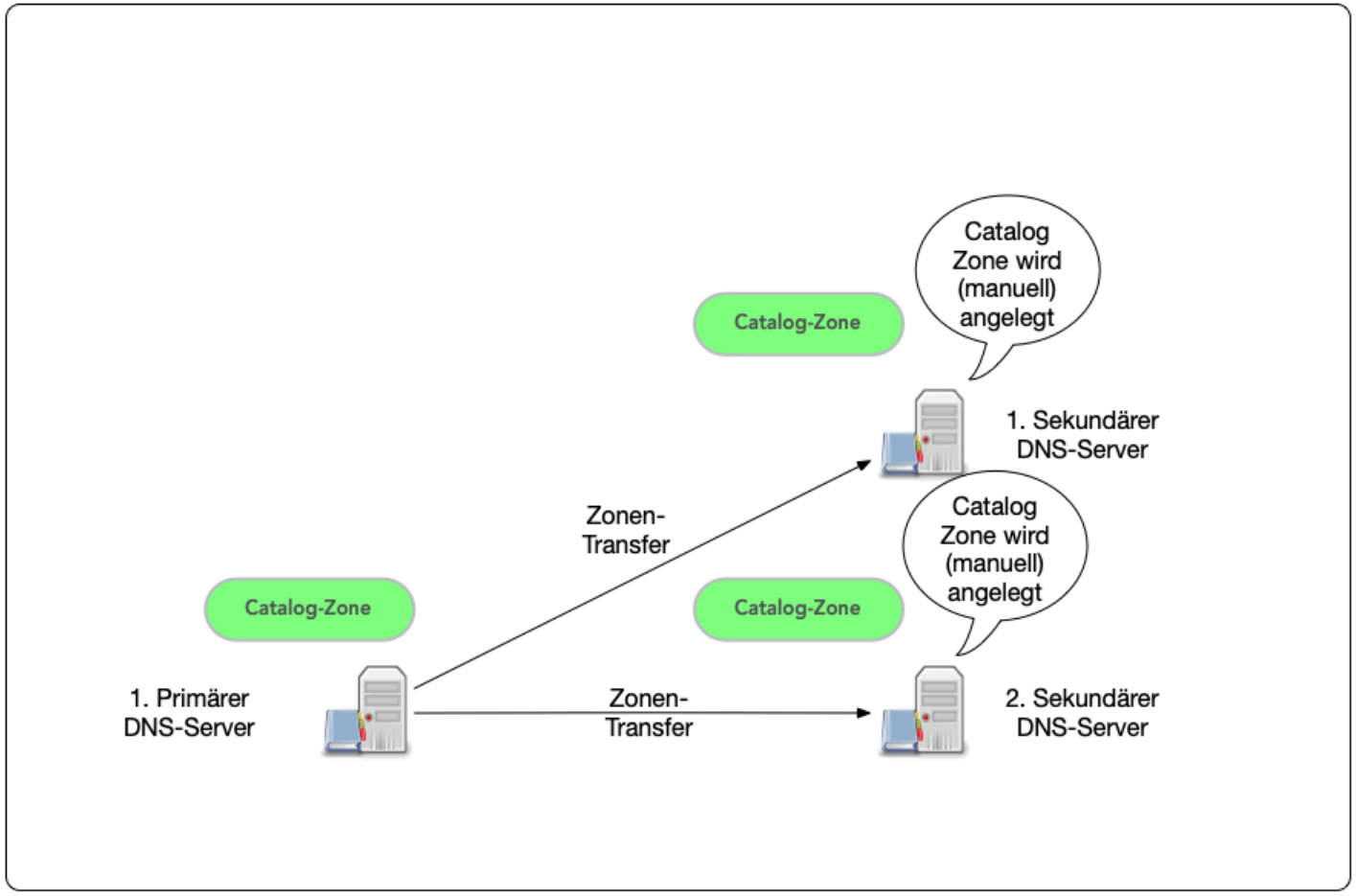
Katalogzone (1/7)



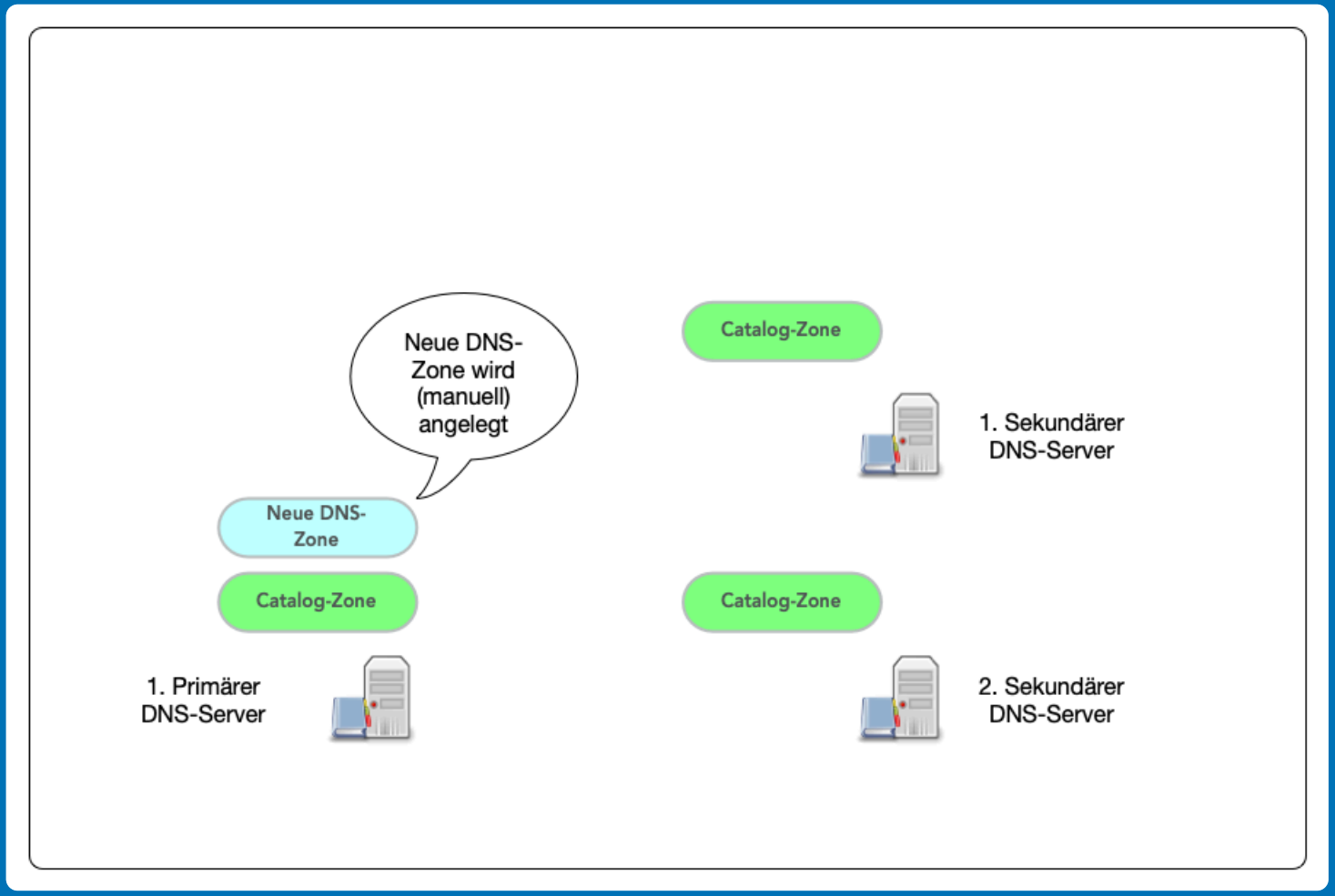
Katalogzone (2/7)



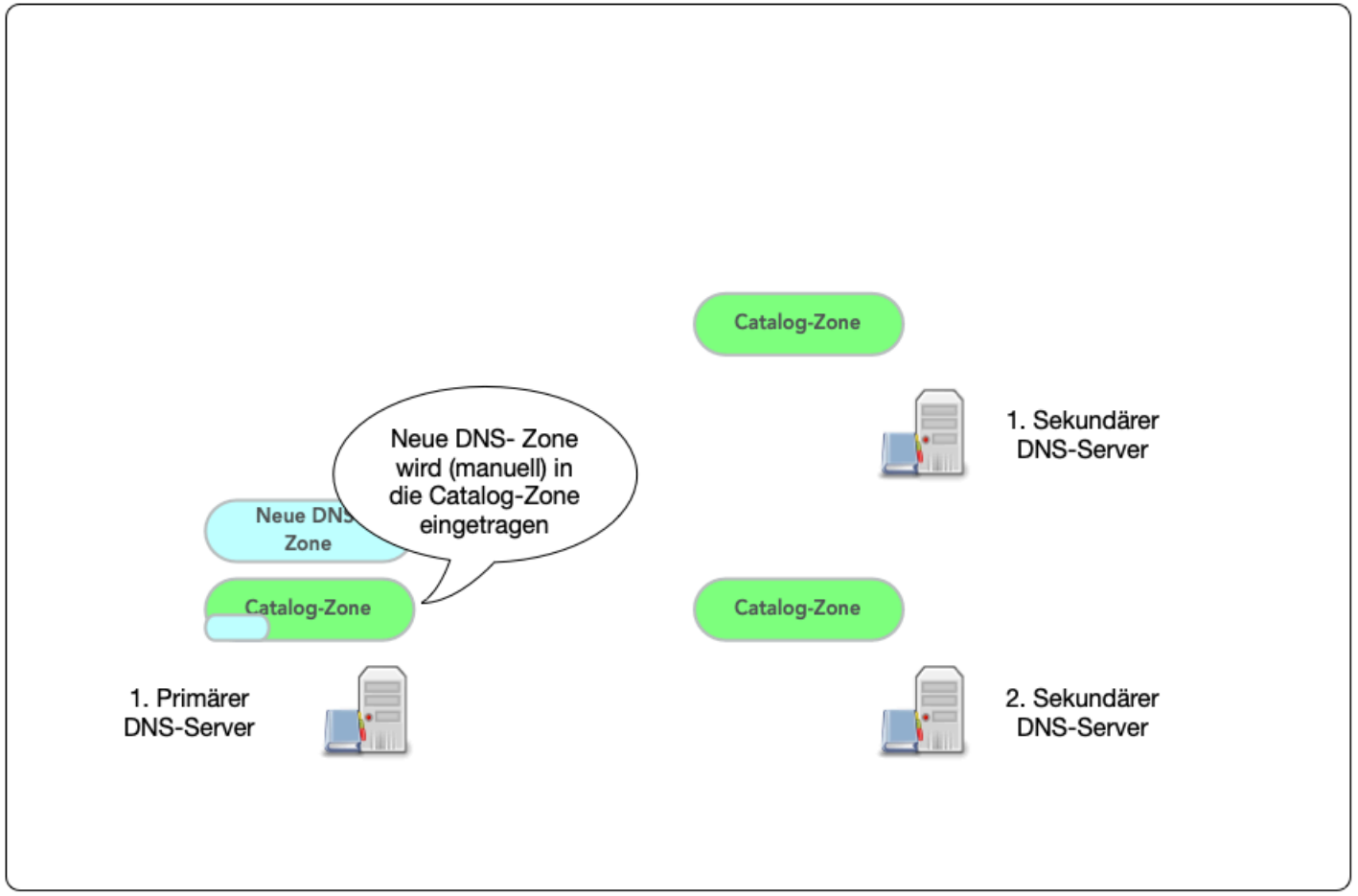
Katalogzone (3/7)



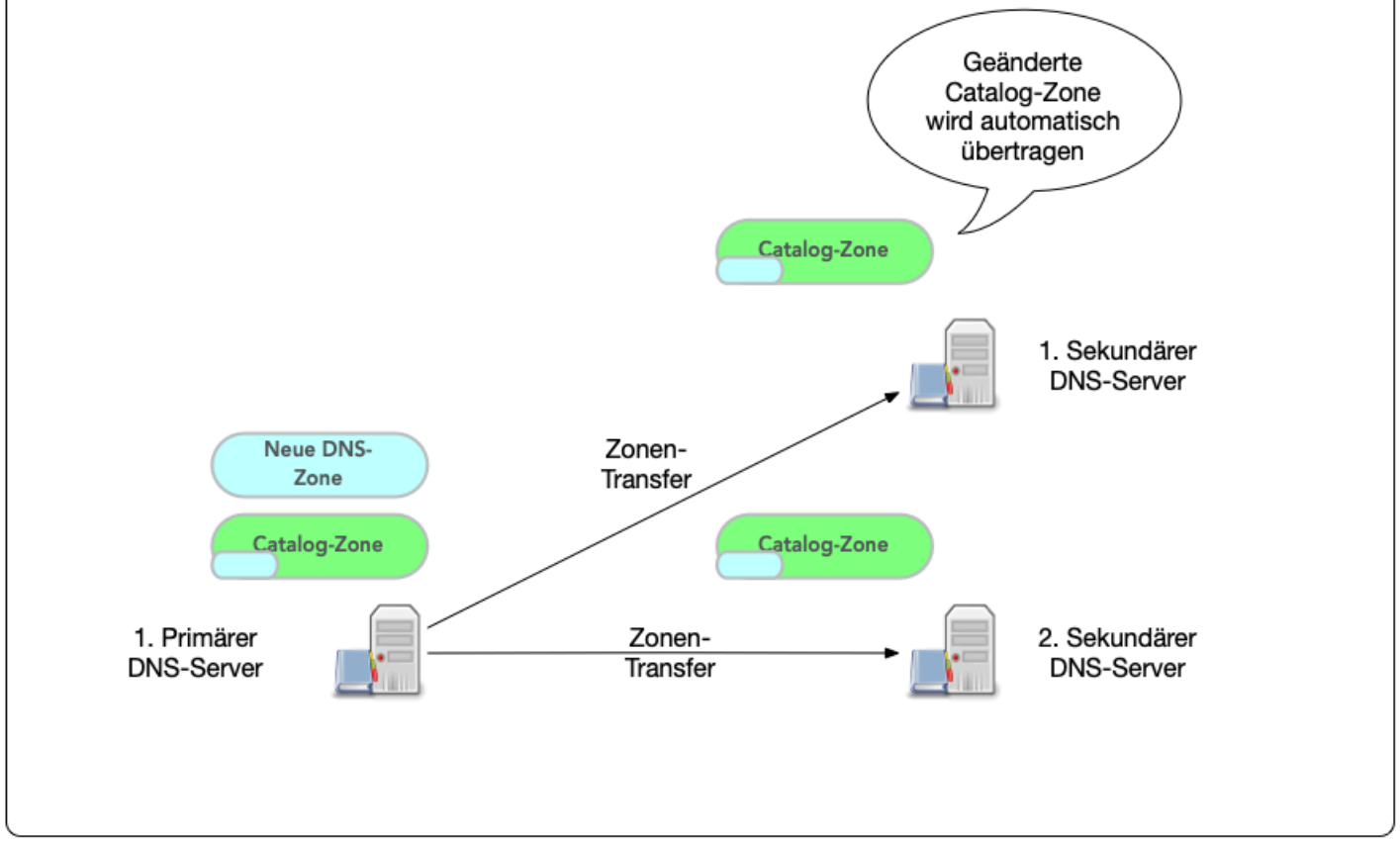
Katalogzone (4/7)



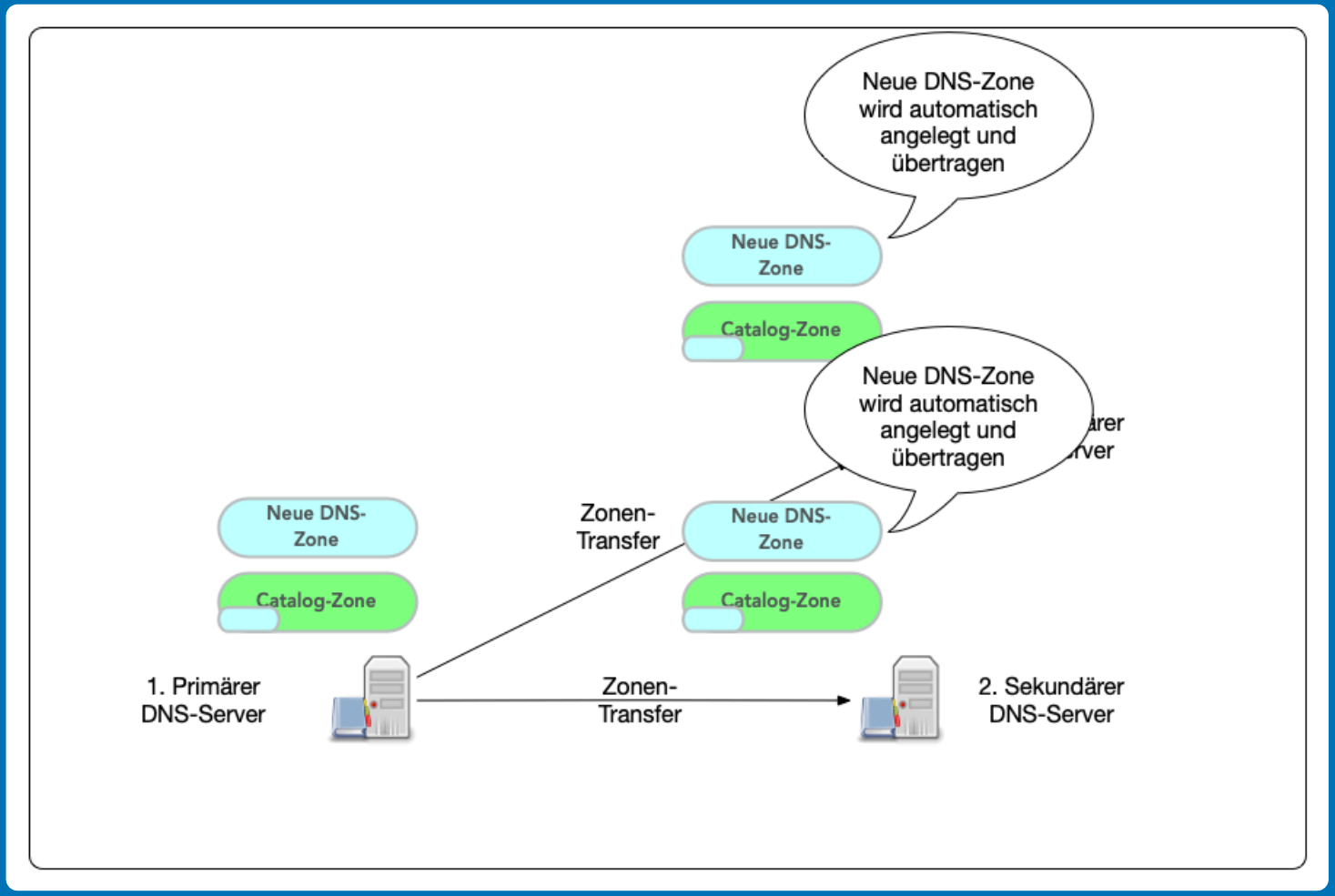
Katalogzone (5/7)



Katalogzone (6/7)



Katalogzone (7/7)



Zusätzliche Zonenblockkonfiguration

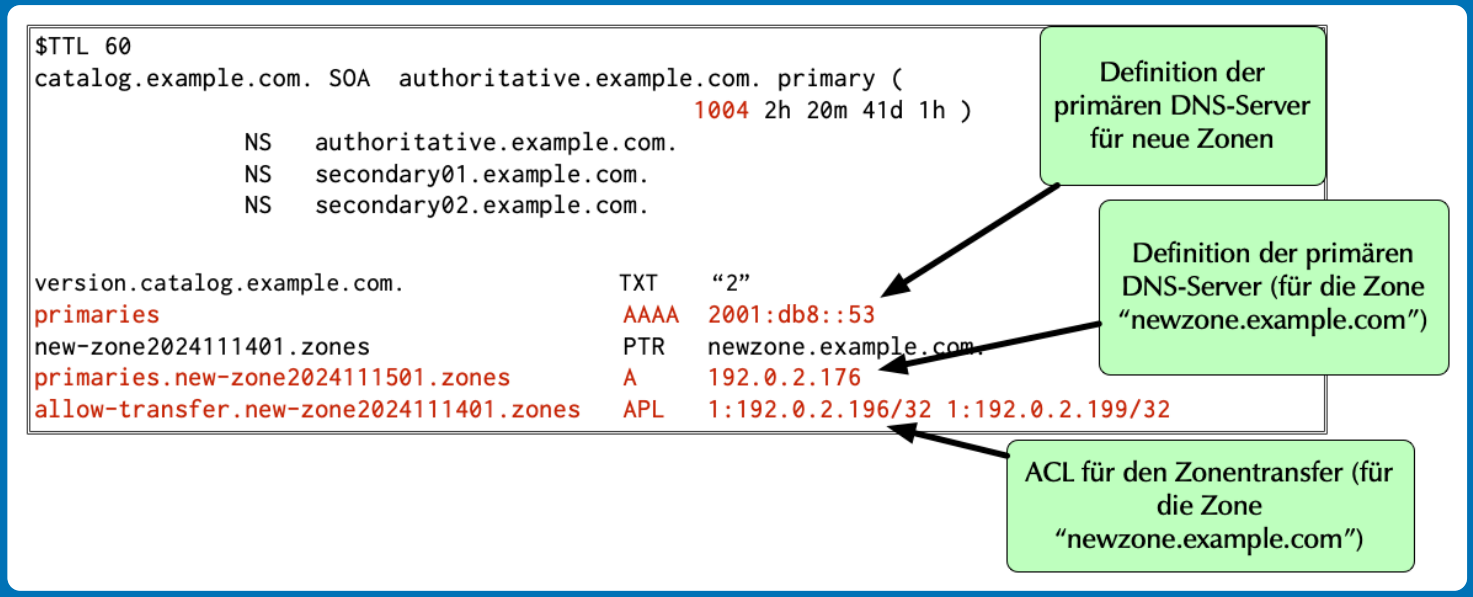
- Katalogzonen können Konfigurationsinformationen für den neuen Zonenblock enthalten (z. B. Zugriffskontrolllisten, Liste der `primaries` usw.)
- Optionen können global für die gesamte Katalogzone angegeben werden, oder spezifisch für jede in der Katalogzone aufgeführte Zone
- Details im BIND Administration Reference Manual:

  ↪https://downloads.isc.org/isc/bind9/9.16.16/doc/arm/html/advanced.html#catalog-zones

Verfügbare Katalogzonenoptionen in BIND 9.16.x

- `primaries`: Diese Option setzt einen oder mehrere primäre DNS-Server für die sekundäre Zone. Primäre Server können als IPv4 A oder IPv6 AAAA Einträge angegeben werden.
- `allow-query`: Diese Option definiert die `allow-query` ACL. Die ACLs werden mit Hilfe des `APL` Resource Records definiert (siehe ↪RFC 3123 „A DNS RR Type for Lists of Address Prefixes (APL RR)“
- `allow-transfer`: Diese Option definiert die `allow-transfer` ACL für Zonentransfers. Sie verwendet ebenfalls den APL-Eintrag.

Verfügbare Katalogzonenoptionen in BIND 9.16.x



Übersicht

- Katalogzonen vereinfachen das Verwalten von DNS-Zonen auf sekundären DNS-Servern
- Zonen können hinzugefügt und entfernt werden
- Essentielle Konfigurationsoptionen für die Zonen können in den Katalogzonen definiert werden
- Katalogzonen sind ein Internet-Standard und werden von vielen DNS-Server Produkten unterstützt

Fragen?

Kontakt: carsten@dnsworkshop.de