

[zurück](#)

# DNS - Zonentransfer

Ein Zonentransfer ist der Prozess, bei dem ein DNS-Server eine komplette DNS-Zone an einen anderen DNS-Server überträgt.

Er wird verwendet, damit **Primary** und **Secondary Nameserver** synchron bleiben.

## Warum braucht man Zonentransfers?

- Redundanz: mehrere DNS-Server halten dieselben Daten
- Lastverteilung
- Ausfallsicherheit
- automatische Aktualisierung von Secondary-Servern

## Arten von Zonentransfers

### AXFR - Full Zone Transfer

- Überträgt **die gesamte Zone**
- langsam, aber vollständig
- wird genutzt, wenn:
  - Secondary neu gestartet wurde
  - Zone komplett geändert wurde
  - Keys geändert wurden

### IXFR - Incremental Zone Transfer

- Überträgt nur **Änderungen**
- schneller und effizienter
- basiert auf Seriennummern im SOA-Record

## SOA (Start of Authority) - wichtig für Transfers

Der SOA-Record enthält:

- Primary-Server
- Kontaktadresse
- Seriennummer (wichtig für IXFR)
- Refresh
- Retry
- Expire
- Minimum TTL

Beispiel:

```
example.com. IN SOA ns1.example.com. admin.example.com. (
    2025010101 ; Seriennummer
    3600       ; Refresh
    600        ; Retry
    604800    ; Expire
    86400     ) ; Minimum TTL
```

## Wie funktioniert ein Zonentransfer?

ASCII-Ablauf:

```
Primary DNS ----AXFR/IXFR----> Secondary DNS
```

1. Secondary fragt beim Primary die SOA-Seriennummer ab
2. Wenn Seriennummer unterschiedlich:  
→ Anfrage eines Transfers
3. Primary sendet AXFR oder IXFR
4. Secondary aktualisiert seine Zone

## Sicherheit: Zonentransfers dürfen NICHT öffentlich sein

Ein offener Zonentransfer erlaubt Angreifern:

- vollständigen Einblick in interne DNS-Strukturen
- Auflistung aller Hosts, Server, internen Systeme

Gefährlich:

```
dig AXFR example.com @ns1.example.com
```

Wenn das funktioniert → riesiges Security-Problem.

## Zonentransfer absichern

Empfehlungen:

- nur autorisierte Secondary-Server erlauben
- IP-Whitelist im Primary
- TSIG-Schlüssel verwenden

### IP-basierte Zugriffskontrolle

Beispiel (BIND):

```
allow-transfer { 192.0.2.10; };
```

### TSIG - Transaction Signatures

TSIG sorgt für:

- Authentifizierung
- Integrität
- Schutz vor Spoofing

Beispiel-Key:

```
hmac-sha256 "RANDOMBASE64KEY==";
```

## Unterschied: Transfer vs. Delegation

- **Delegation** = Parent-Zone verweist auf Child-Zone (NS-Records)
  - **Transfer** = Child-Zone wird auf Secondary kopiert

### Prüfung per dig

#### SOA prüfen

```
dig example.com SOA
```

## AXFR versuchen

```
dig AXFR example.com @ns1.example.com
```

## Seriennummer vergleichen

```
dig example.com SOA @ns1
dig example.com SOA @ns2
```

Wenn unterschiedlich → Secondary ist veraltet.

## Wann wird AXFR oder IXFR verwendet?

Situation	AXFR?	IXFR?
-----	----	----
Secondary frisch gestartet	Ja	Nein
Zonenfile komplett geändert	Ja	möglich
nur ein Record geändert	Nein	Ja
Key-Rollover	Ja	Ja

## Zusammenfassung

- Zonentransfer = Übertragung einer DNS-Zone von Primary zu Secondary
  - AXFR = vollständiger Transfer
  - \* IXFR = inkrementeller Transfer (nur Änderungen)
  - \* Seriennummer (SOA) steuert den Prozess
  - \* Zonentransfers müssen abgesichert werden (IP-ACL, TSIG)
  - \* offene AXFR sind ein massives Sicherheitsrisiko

From: <http://wiki.nctl.de/dokuwiki/> - **Veni. Vidi. sudo rm -rf / vici.**

Permanent link: <http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:grundlagen:netzwerkdienste:dns-zonentransfer&rev=1764586599>

Last update: **01.12.2025 11:56**

