POWERDNS

LIGHTNING STREAM REPLIKATION

PowerDNS Authoritative + LMDB + Lightning Stream

Adminstammtisch 10/2026

Norbert Auler

POWERDNS

AGENDA

1. DNS?
2. Was ist Lightning Stream?
3. Architektur & Theorie
4. Installation & Setup
5. Zone & DNSSEC Setup
6. Lightning Stream Konfiguration
7. Live Demo
8. Deployment & Betrieb
9. Monitoring
10. Debugging & Troubleshooting
11. Performance
12. Takeaways
13. Fragen

POWERDNS

DNS

Domain Name System

- Übersichtliche 297 RFCs (ca.)
- Baumstruktur, www.example.com:
  . -> .com -> example -> www -> A Record (IP)
- Mehrere 100 Record-Typen, 8-10 im täglichen Einsatz
  (A,AAAA,MX,CNAME,TXT,SOA,NS,PTR etc.)
- Zone Transfer via AXFR/Notify
- Zone "Transfer" via Backend -> Datenbank

POWERDNS

WAS LIGHTNING STREAM LÖST?

> Lightning Stream ist ein Tool, mit dem Änderungen zwischen einer lokalen LMDB (Lightning Memory-Mapped Database) und einem S3-Bucket nahezu in Echtzeit synchronisiert werden können

- Kein (komplexes) [hidden] Primary/Secondary Model
- Keine SQL-Replikation nötig
- Lokale Datenbank pro Node
- Pull-basierte Synchronisation

POWERDNS

WIE LS ES LÖST

Lokale LMDB Datenbank + synchronisation via S3 Storage

POWERDNS

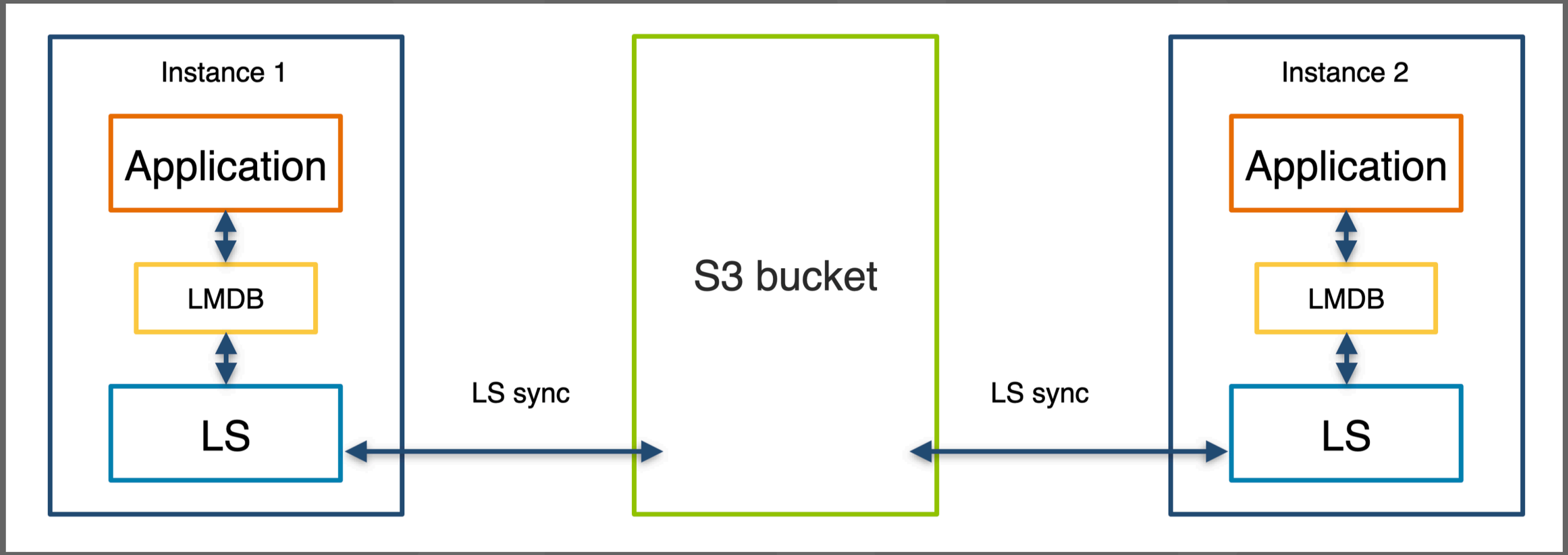
> Lokale LMDB Datenbank [...]

- Lightning Memory-Mapped Database (LMDB) is an embedded transactional database in the form of a key-value store, written in C.
- LMDB is not a relational database, it is strictly a key-value store like Berkeley DB and DBM.
- PowerDNS LMDB Backend (pdns-backend-lmdb)

More: Wikipedia

> [...] + synchronisation via S3

- LMDB Snapshots -> S3
- 2 Shards, (main und shard), Benamung nach Node & Timestamp


Instance 1
Application
LMDB
LS
LS sync
S3 bucket
LS sync
Instance 2
Application
LMDB
LS

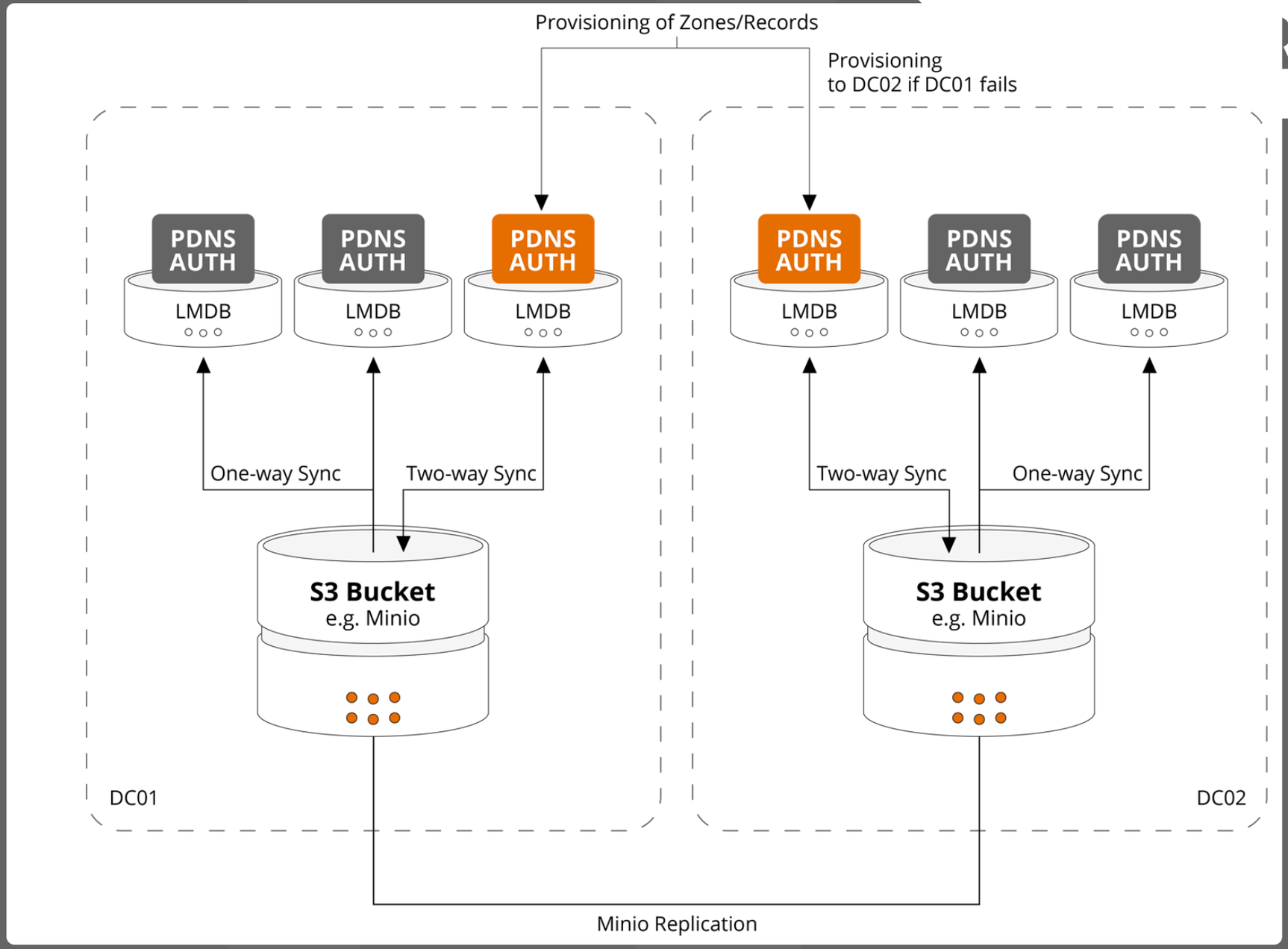
POWERDNS

1. Snapshot der LMDB Datenbank in einen S3-Bucket geschrieben
2. Nodes prüfen via poll ob ein neuer Snapshot von einer anderen Instanz im S3-Bucket geschrieben wurde
3. Download des Snapshots und auf die lokale LMDB anwenden

S3 CONTENT

```
main__ls-demo-1__20260506-151047-136497540__GX.pb.gz

shard__ls-demo-1__20260506-151047-135248438__GX.pb.gz
```


Provisioning of Zones/Records
Provisioning
to DC02 if DC01 fails
PDNS AUTH
LMDB
PDNS AUTH
LMDB
PDNS AUTH
LMDB
PDNS AUTH
LMDB
PDNS AUTH
LMDB
PDNS AUTH
LMDB
One-way Sync
Two-way Sync
Two-way Sync
One-way Sync
S3 Bucket
e.g. Minio
S3 Bucket
e.g. Minio
DC01
DC02
Minio Replication

POWERDNS

DEMO SETUP

- PowerDNS Authoritative + LMDB backend installieren
- Installation von Lightning Stream
- S3 Storage konfigurieren

DEMO SETUP

- Installieren der PowerDNS Repositories (repo.powerdns.com)
- Installieren der Packages *"pdns-server"* und *"pdns-backend-lmdb"*

PDNS.CONF

```
[..]
launch=lmdb
lmdb-filename=/var/lib/powerdns/pdns.lmdb
lmdb-lightning-stream=yes
lmdb-shards=1
[...]
```

POWERDNS

ZONE ERSTELLEN

```
ls-demo-1 $: pdnsutil zone create flarp.test
Creating empty zone 'flarp.test'

ls-demo-1 $ pdnsutil zone list flarp.test
$ORIGIN .
flarp.test.     3600    IN      SOA     a.misconfigured.dns.server.invalid. hostmaster.flarp.test. 0 10800 3600 6

ls-demo-1 $ pdnsutil rrset add flarp.test foo.flarp.test. A 3600 1.2.3.4
New rrset:
foo.flarp.test. 3600 IN A 1.2.3.4

ls-demo-1 $ pdnsutil zone list flarp.test
$ORIGIN .
flarp.test.     3600    IN      SOA     a.misconfigured.dns.server.invalid. hostmaster.flarp.test. 0 10800 3600 6
foo.flarp.test. 3600    IN      A       1.2.3.4
```

POWERDNS

VERIFY

```
ls-demo-1 $ dig @127.1 foo.flarp.test +short
1.2.3.4
```

SECURE ZONE

```
ls-demo-1 $ pdnsutil zone secure flarp.test
Securing zone with default key size
Adding CSK (257) with algorithm ecdsa256
Zone flarp.test secured
Adding NSEC ordering information for zone 'flarp.test', 2 updates
```

> [...] a single ECDSA (algorithm 13, ECDSAP256SHA256) key is generated that is used as CSK

CSK? KSK? ZSK?

- **CSK (Combined Signing Key):** Ein einziger Schlüssel, der sowohl die DNS-Zonendaten als auch den DNSKEY-Datensatz signiert. Er fungiert gleichzeitig als ZSK und KSK.
- **KSK (Key Signing Key):** Ein Schlüssel, der ausschließlich zum signieren des DNSKEY-Datensatzes dient. Zum signieren von Daten ist ein separater Zone Signing Key (ZSK) erforderlich.

PowerDNS DNSSEC Dokumentation

DNSSEC ANZEIGEN

```
ls-demo-1 $ pdnsutil zone show flarp.test
This is a Native zone
Metadata items:
        SOA-EDIT-API    DEFAULT
Zone has NSEC semantics
keys:
ID = 1766299710 (CSK), flags = 257, tag = 63810, algo = 13, bits = 256    Active         Published  ( ECDSAP256SH
CSK DNSKEY = flarp.test. IN DNSKEY 257 3 13 /qAO7ZWQJ8FxJJPhogEcvLjusD34VZSG7dsrPY3oCLj8tcugIUVAhJnX1L+5FQvoXZfqR
DS = flarp.test. IN DS 63810 13 2 63edca6d6d92b327abf95877a46229d151b7cc0cfbb4b57b2e5817a597c55f57 ; ( SHA256 dig
DS = flarp.test. IN DS 63810 13 4 9e3095e5ab0e7b36ac98d7f022473f1a33e3d47e01a68a6c6ae939b9c0c06e29259b056e3b26666
```



Familienkadse*

*Präsentationen mit Katzen oder Tierbabies werden besser bewertet (vgl. "Kawaii-Effekt").

INSTALLATION LIGHTNING STREAM (VM)

Folgen der Anleitung: github.com/PowerDNS/lightningstream

```
run ./build.sh to install it in a bin/ subdirectory of this repo.
```

KONFIGURATION LIGHTNING STREAM (VM)

```
root@ls-demo-1:~# cat /etc/lightningstream.yaml
main:
  path: /var/lib/powerdns/pdns.lmdb
  schema_tracks_changes: true
  options:
    no_subdir: true
    create: false
shard:
  path: /var/lib/powerdns/pdns.lmdb-0
  schema_tracks_changes: true
    options:
      no_subdir: true
      create: true
storage:
  type: s3
  options:
    endpoint_url: http://10.50.2.39:9000
    access_key: 123
    [...]
```

POWERDNS

LIGHTNING STREAM STARTEN (VM)

- Starten im sync mode auf allen 3 Nodes
- Logs prüfen

ls-demo-2:
msg="[main] Loaded remote update" compressed_size_bytes=727 db=main extra= instance=ls-demo-2 kind=snapshot shorthash=869f4b4 snapshot_instance=ls-demo-1 time_total=1ms [...]

ls-demo-3:
msg="[main] Loaded remote update" compressed_size_bytes=727 db=main extra= instance=ls-demo-3 kind=snapshot shorthash=869f4b4 snapshot_instance=ls-demo-1 time_total=2ms [...]

POWERDNS

LIVE DEMO

POWERDNS

DEPLOYMENT

- Ansible oder anderes Konfigurationsmanagementsystem
- + GIT

POWERDNS

MONITORING/TRENDING

- Prometheus
- Alertmanager

POWERDNS

BACKUPS? RECOVERY!

- S3 Snapshots / Backups
- VMs via Konfigurationsmanagementsystem

POWERDNS

FAILURE: OBJECT STORAGE DOWN

- DNS Queries werden weiterhin beantwortet
- Keine Updates

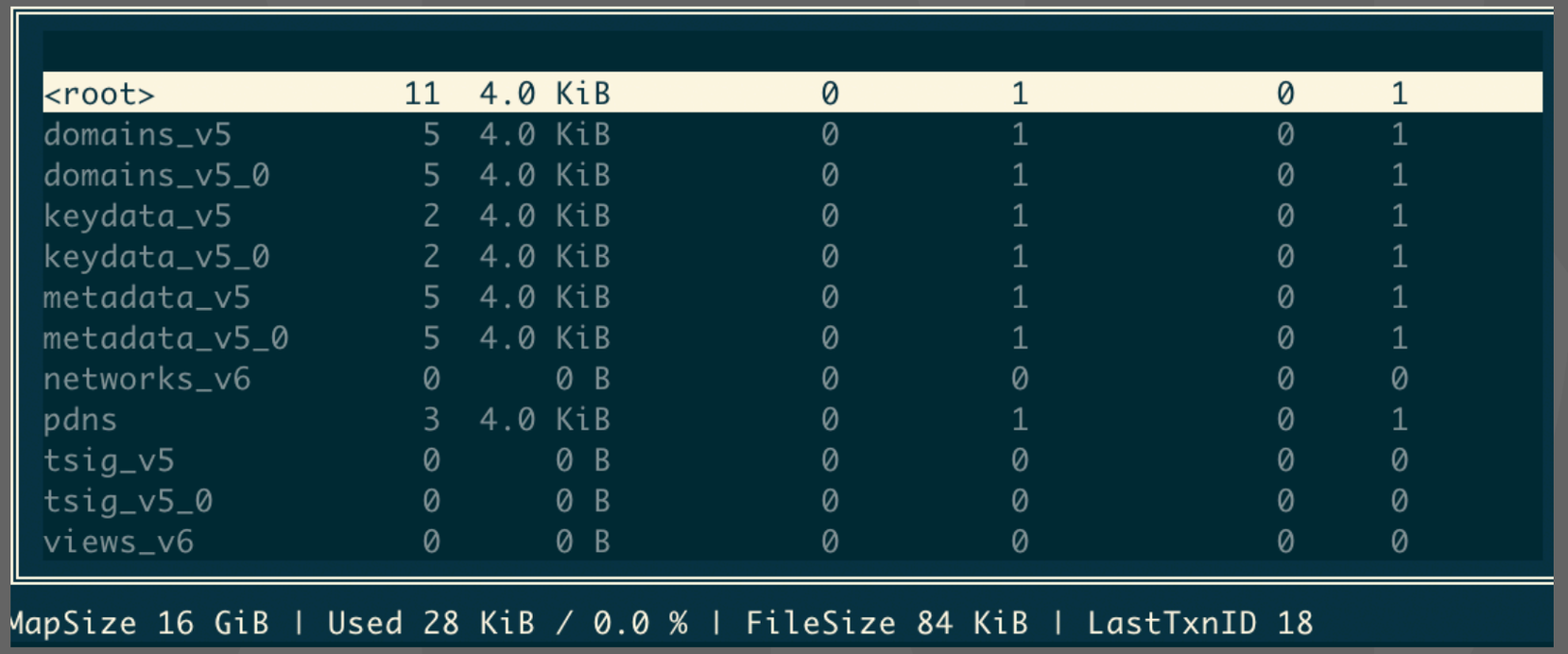
DEBUGGING

- dig
- PowerDNS Logs
- Lightning Stream Logs

LMDBNAV

POWERDNS

A terminal UI to inspect LMDB database files.



github.com/PowerDNS/lmdbnav

POWERDNS

PERFORMANCE

- Query Performance: sehr hoch (lokale LMDB)
- Latency: ms bis Sekunden (je nach Größe/Anzahl der Zones/Records)

POWERDNS

TAKEAWAYS

- Modernes DNS Replikationsmodell
- Stark für Cloud/VM Betrieb
- Wartungsarm
- Enterprise

POWERDNS

FRAGEN?

Danke für die Aufmerksamkeit

Norbert Auler

norbert.auler@powerdns.com

Lighting Stream | Github

Lighting Stream | Dokumentation

PowerDNS DNSSEC

PowerDNS Repo(s)

PowerDNS Dokumentation(en)

PowerDNS DNSdist

revealjs.com | Presentation Framework