

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

DNS – hogyan és hogyan ne

Lajber Zoltán
ISZT Nonprofit Kft.
lajber@nic.hu

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritativ
szerverek

Rekurziv
szerverek

Összefoglalás

- Autoritativ szerverek
 - DNSSEC
 - NSEC és NSEC3
 - Biztonságos zóna transzfer
 - Zóna integritás
 - Autoritativ és rekurziv szerver legyen külön
 - Monitorozás szükséges
- Rekurziv szerverek
- Összefoglalás

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

Autoritatív szerverek

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ UDP 53 és **TCP 53** portok legyenek nyitva
- ▶ DNSSEC: zóna legyen aláírva
- ▶ kulcs kezelésénél ragaszkodjunk a "best practice"-okhoz (RFC 6841)
 - ▶ privát kulcs megfelelő kezelése - esetleg hidden masters
 - ▶ monitorozás: kulcsok lejáratra, időben csere
- ▶ automatizálás - minden mai DNS szoftver támogatja
- ▶ DNSSEC nélkül egy zóna "örök életű", DNSSEC esetén nem - kivéve automatizálással
- ▶ egyszerű domain-nél CSK is szóba jöhet KSK és ZSK helyett (RFC 6781 "DNSSEC Operational Practices")

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

Tulajdonság	NSEC	NSEC3
Nem létező rekordok kezelése	Nyíltan felsorolja a következő létező rekordot, így felfedheti a zóna teljes tartalmát.	Hash-elt formában tárolja a rekordokat, így nehezebb visszafejteni a zóna tartalmát.
Zóna feltérképezés elleni védelem	Nincs védelem – könnyen lekérdezhető a teljes zóna.	Védelmet nyújt a zóna feltérképezése ellen.
Használat	Egyszerűbb, kisebb számítási igény.	Komplexebb, hash-elést igényel

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ zóna transzfer csak limitált klienseknek
- ▶ ACL - megadott IP címek és/vagy kulcsok (TSIG)
- ▶ TSIG - Transaction SIGnature: hitelesítés és integritás biztosítása szimmentrikus kulcsokkal
- ▶ TSIG zónatranszfernél, és ha esetleg van, akkor dinamikus zóna update-nél is használható
- ▶ legjobb, ha **ACL és TSIG egyszerre**

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ Generáláskor mindig ellenőrizzük a zóna integritást
- ▶ véletlen módosítás vagy hiba is okozhat gondot
- ▶ támadás hatását hamar észleljük
 - ▶ változás mértéke - pl. 10% -nál nagyobb változás
 - ▶ bizonyos fix rekordok (golden records) megléte
 - ▶ ZONEMD (Zone Message Digest) egy DNS rekord típus, amely egy kriptográfiai hash értéket (digest) tartalmaz az egész zónára vonatkozóan.
- ▶ az egész zóna generálási és aláírási folyamat részletes monitorozása

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ a két eltérő DNS funkció ne legyen egy DNS szerveren
- ▶ legalább két szerver szolgálja ki a zónát
 - ▶ ne legyenek azonos subnet-en
 - ▶ ne legyenek azonos fizikai helyen (rack, UPS, gépterem, város, ország, AS)
 - ▶ esetleg eltérő szoftvert használjanak



Autoritatív szerverek

Monitorozás szükséges

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ zóna generálás, aláírás folyamata
- ▶ aláírások élettartama - tartalék!
- ▶ szolgáltatások
- ▶ szerverek
- ▶ hálózat
- ▶ környezet

NS prod

All dashboards / NS prod

Hosts	HU zone date	HU zone serial	HU zone serial age	HU zone serial date
a.hu	2025-09-27T09:31:33	1758958246	5	2025-09-27T09:30:46
b.hu	2025-09-27T09:31:33	1758958246	4	2025-09-27T09:30:46
c.hu	2025-09-27T09:31:33	1758958246	5	2025-09-27T09:30:46
d.hu	2025-09-27T09:31:33	1758958246	4	2025-09-27T09:30:46
Kpuff DP	2025-09-27 09:30:06	1758957105	23	2025-09-27T09:11:45
Kpuff VH	2025-09-27 09:30:06	1758958246	4	2025-09-27T09:30:46

kpuff-dp domain count

882126

2025-09-27

09:35:46 AM

Budapest

kpuff-vh domain count

882126

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

Rekurzív szerverek

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ DNSSEC
- ▶ ACL - ki használhatja, ha nem **publikus** szolgáltatás
- ▶ QNAME minimization-t kapcsoljuk be
- ▶ spórolhatunk a gyöker névszerverekkel való állandó kommunikáción: pl. Unbound-nál ezt az 'auth-zone' lehetővé teszi
- ▶ **autoritatív és rekurzív szerver legyen külön**
- ▶ legalább két különböző szerver szolgálja ki a funkciót
- ▶ ha lehet, különböző DNS szoftverek is legyenek
- ▶ monitorozás: szolgáltatások, szerverek, hálózat
- ▶ opcionális: DoQ (DNS over QUIC), DoT (DNS-over-TLS) vagy DoH (DNS-over-HTTPS) használata
- ▶ publikus DNS rezolvereken adatmegőrzés (napló, stb) csak a szükséges ideig

DNS – hogyan
és hogyan ne

Lajber Zoltán
ISZT
Nonprofit Kft.
lajber@nic.hu

Miről lesz szó?

Autoritatív
szerverek

Rekurzív
szerverek

Összefoglalás

- ▶ DNSSEC resolvereken is
- ▶ DNSSEC automatizálás
- ▶ DNSSEC monitorozás kiemelten fontos
- ▶ Autoritativ és rekurzív szerver legyen külön
- ▶ Autoritativ szerverek külön fizikai elhelyezése
- ▶ Rezolvereken is DNSSEC, redundancia és log kezelés
- ▶ publikus rezolver külön megfontolást érdemel

KINDNS.ORG