EXPIRE a MINIMUM definované RFC 1035 musí být stejné na všech autoritativních serverech pro danou doménu.

■ **Všechny jmenné servery musí vracet stejnou sadu NS záznamů.** Nekonzistence těchto záznamů může způsobit selhání překladu doménového jména, a tím i nedostupnost domény.

Delegace

Každá doména (vyjma root zóny) se deleguje z nadřazené zóny. Podmínky delegace jsou definovány jednak normami RFC, jednak pravidly provozovatelů jednotlivých registrů.

■ **Delegace musí obsahovat alespoň dva jmenné servery.** Pro předcházení problémům s dostupností domény by podle požadavků RFC 1034 měla být každá doména dostupná alespoň ze dvou jmenných serverů. Doménové registry běžně vyžadují alespoň dva jmenné servery, aby byla doména do zóny vložena, a stala se tak dostupnou. RFC 2182 doporučuje pro domény běžných organizací tři jmenné servery, kdy alespoň jeden by měl být umístěn jinde než zbylé dva, aby se snížila odolnost infrastruktury.

■ **Sada jmenných serverů v nadřazené zóně by měla odpovídat jmenným serverům v zóně samotné.** Podle principu algoritmu překladu doménových jmen, popsaném v RFC 1034, je jediným zdrojem seznamu jmenných serverů pro doménu pouze jeho autoritativní server. Delegace získané z nadřazené zóny jsou po kontaktování autoritativních serverů zahozeny.

V případě uplatňování principů ochrany soukromí, jako je například minimalizace DNS odpovědí, však používají rekurzivní servery údaje z delegace, a proto všechny servery z nadřazené zóny musí být autoritativní pro danou doménu.

■ **Jmenné servery by měly mít rozdílné síťové cesty.** Pro zajištění dostupnosti alespoň části jmenných serverů v případě problémů v síti by se tyto servery měly nacházet v topologicky a geograficky oddělených systémech (viz RFC 2182, sekce 3.1) a měly by být připojeny přes různé autonomní systémy (AS).

Toto pravidlo se dá nahradit dostupností serverů pomocí anycastu, kdy jsou servery dostupné z jednoho AS a adresného rozsahu, ale fakticky jsou distribuované a dostupné z různých sítí.

■ **Jmenné servery musí mít unikátní IP adresy.** Pro předcházení chybám a nedostupnosti domén musí jednotlivé jmenné servery v delegaci používat unikátní adresy. Ačkoliv je technicky možné použít více hostname pro jednu IP adresu, jde o postup ohrožující dostupnost dané domény.

■ **Všechny jmenné servery musí být autoritativní pro dané doménové jméno.** Podle RFC 2181 musí jmenný server pro doménu poskytovat autoritativní odpovědi. Jmenný server, který vrací data pro doménové jméno, ale není autoritativní, představuje známku chybné konfigurace a je příčinou problémů s dostupností domény.

■ **Glue záznamy v delegaci by měly přesně odpovídat záznamům v dané doméně.** Glue záznamy jmenných serverů v delegaci, jejichž doménové jméno je v dané doméně (tzv. in-bailiwick), by se měly shodovat s adresami jmenných serverů v doméně. Neshoda těchto záznamů značí závažnou konfigurační chybu a může způsobit nedostupnost domény.

Syntaxe

Nedodržení syntaxe v DNS způsobuje chyby při jeho zpracování a interpretaci. Je proto nutné, aby správci zóny dodrželi tato pravidla, která se v mnoha serverových implementacích vyžadují. Pokud DNS server tuto možnost podporuje, doporučuje se zapnout striktnější formu hlídání syntaxe, jež zajistí maximální interoperabilitu.

■ **NS záznam musí obsahovat validní hostname.** Hostname jmenného serveru uvedeného v NS záznamu musí být validní podle RFC 1035, RFC 1123, RFC 2181 a RFC 3696.

■ **NS záznam nesmí být alias.** Hodnota NS záznamu nesmí směřovat na záznam typu CNAME, ale může směřovat na záznamy typu A reprezentující IPv4 adresu a/nebo AAAA pro IPv6 adresu.

■ **Hodnota parametru *RNAME* v SOA záznamu nesmí obsahovat „@“.** Znak zavináče se v položce RNAME nahrazuje znakem tečky podle popisu v RFC 1034 a RFC 1123.

■ **Hodnota parametru *RNAME* v SOA záznamu musí být validní hostname.** V parametru RNAME je adresa e-mailu osoby odpovědné za správu domény, tato adresa musí být po převodu na hostname validní podle RFC 1035 a RFC 1123.

■ **Hodnota parametru *MNAME* v SOA záznamu musí být validní hostname.** V parametru MNAME je uveden master server, pro danou doménu, hostname tohoto serveru musí být validní podle RFC 1035 a RFC 1123.

DNSSEC

DNSSEC představuje rozšíření DNS, které zvyšuje jeho bezpečnost.

DNSSEC poskytuje uživatelům jistotu, že informace, jež z DNS získal, poskytl správný zdroj, jsou úplné a jejich integrita se při přenosu nenarušila. DNSSEC přidává k DNS protokolu možnost podepsat DNS data, a zajistit tak jejich autenticitu a integritu během přenosu.

Poprvé se DNSSEC představil v RFC 4033, RFC 4034 a RFC 4035, obecná doporučení, jak pracovat a nasazovat DNSSEC jsou k dispozici v RFC 6781.

Pro organizace státní správy je podle Usnesení vlády č. 982 ze dne 18. prosince 2013 zabezpečení jimi držených domén povinné.

■ **Řetězec důvěry musí být validní.** Pokud se v nadřazené zóně publikuje DS záznam, musí existovat řetězec důvěry od tohoto DS záznamu pro SOA, DNSKEY a NS záznamy v doméně. Pouze podepsaná doména s validním řetězem důvěry je opravdu zabezpečená technologií DNSSEC.

■ **Pro každý algoritmus použitý v DS záznamu by měl existovat odpovídající DNSKEY záznam.** Delegace zabezpečená pomocí technologie DNSSEC se vykoná publikováním DS záznamu v nadřazené zóně společně s NS záznamy pro delegaci. Pro každý algoritmus vyjmenovaný v DS záznamu v delegaci by měl existovat odpovídající DNSKEY záznam v doméně. Tento konzervativní přístup vychází z principu předběžné opatrnosti, kdy některé rekurzivní servery vyžadují striktní dodržení tohoto pravidla, zatímco jiným stačí jedna přímá cesta.

■ **Počet iterací u NSEC3 záznamů nesmí překročit povolenou mez.** Maximální počet přesměrování (iterací) závisí na velikosti klíče, která by podle RFC 5155 neměla překročit následující hodnoty, viz tabulku.

Velikost klíče	Počet iterací
1 024	150
2 048	500
4 096	2 500

Tento počet se nesmí překročit, jinak může dojít k vyhodnocení domény jako nevalidní.

■ **Jmenný server musí zahrnout DNSSEC podpisy (RRSIG) do všech odpovědí na DNSSEC dotazy.** Pokud je doména podepsaná, musí jmenný server na všechny dotazy indikující zájem o DNSSEC data pomocí DO bitu odpovídat včetně uvedení odpovídajících RRSIG. Při ignorování tohoto požadavku u podepsaných domén dojde na rekurzivním serveru k vyhodnocení domény jako nevalidní a doména se bude jevit jako nedostupná.

■ **Jmenný server musí přiložit NSEC/NSEC3 záznamy k odpovědím o neexistenci domény** (NXDOMAIN). Pokud je zóna podepsaná, jmenný server musí být schopen přiložit NSEC/NSEC3 záznamy jako data v sekci *additional* ke všem odpovědím na dotazy s nastaveným DO bitem, které jsou vyhodnoceny jako neexistující domény, a odpovědí je zpráva se stavem NXDOMAIN. ■

Autoři pracují ve společnosti CZ.NIC.