draft-ietf-dnsop-nsec3-iterations

Wes Hardaker

July 26, 2021

Draft Status

Primary point of the draft

- Use NSEC if you can
- NSEC3 iterations recommendation: 0
- NSEC3 salt: only use one if you're going to change it
- Validating resolvers:

	Range	Action
0	– 100	Validate
101	– 500	SHOULD Insecure
501	+	MAY SERVFAIL

Recent changes

- draft-ietf-dnsop-nsec3-iterations posted 2021-05-25
- Changes since then:
  - Minor edits
  - Clearer guidance for:
    - Zone publishers
    - Validating resolvers
    - Primary / Secondary relationships

With thanks to:

- Tony Finch
- Florian Obser

Remaining

- Discuss authoritative overhead required
- Decide if the ranges are right

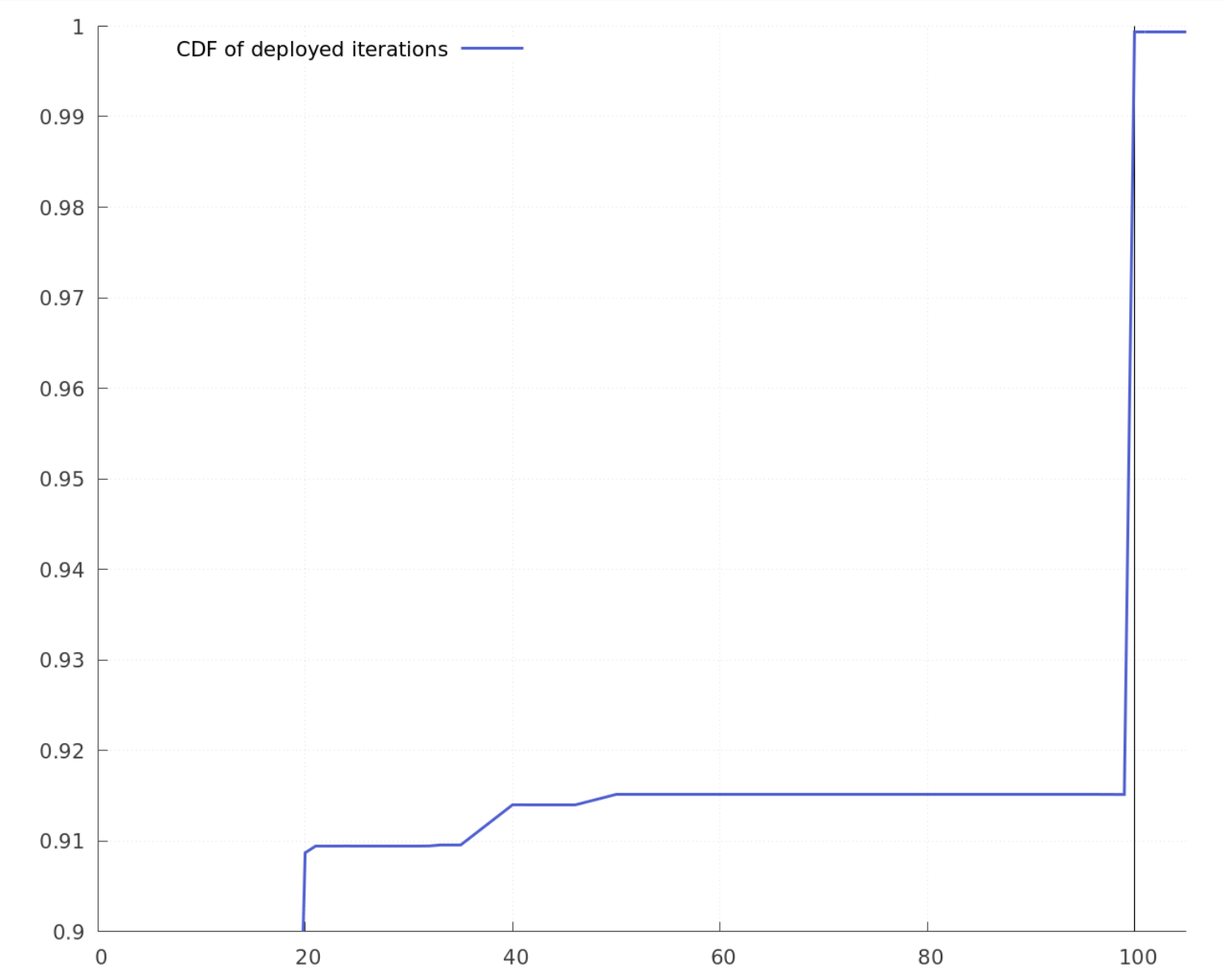
Remaining

- Discuss authoritative overhead required
- Decide if the ranges are right

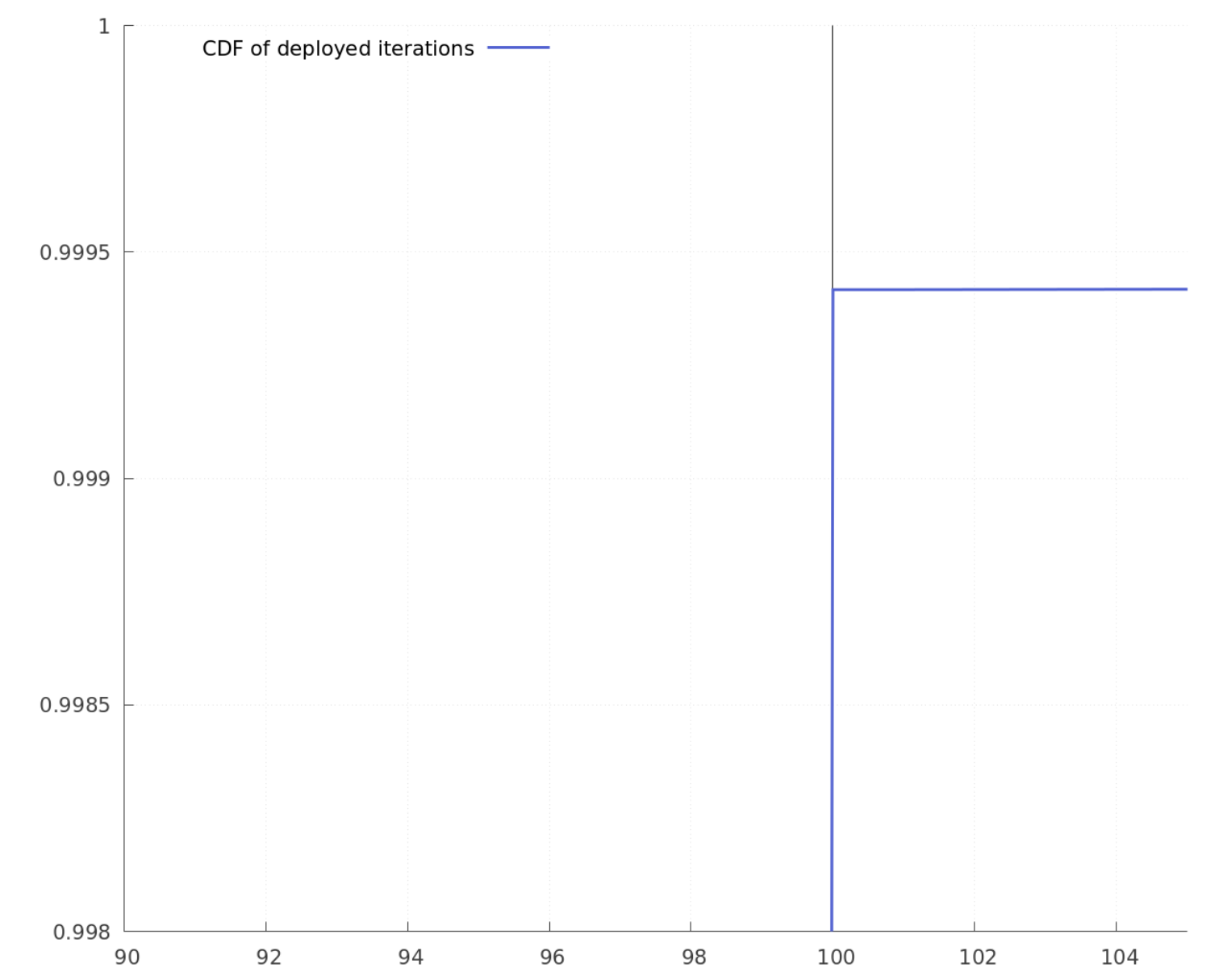
	Range	Action
0	– 100	Validate
101	– 500	SHOULD Insecure
501	+	MAY SERVFAIL

CDF of NSEC3 iterations as of 2021/07/25

CDF of NSEC3 iterations



CDF of NSEC3 iterations



Deployment figures today

- NSEC iteration deployment stats as of yesterday:

Stat	Value
Total NSEC3 measured zones	11,488,499
Fraction <= 100	0.999416633974551
Fraction <= 500	0.999996344169939

Deployment figures today

- NSEC iteration deployment stats as of yesterday:

Stat	Value
Total NSEC3 measured zones	11,488,499
Fraction <= 100	0.99941663974551
Fraction <= 500	0.99996344169939

- Given this, anyone object to:

	Range	Action	Fraction
0	– 100	Validate	
101	– 500	SHOULD Insecure	0.00057962
501	+	MAY SERVFAIL	3.8299e-06

[Thank you to Viktor for his measurements]

Backup

Iteration guidance in RFC5155

Maximum limits set in RFC5155:

Key Size	Iterations
1024	150
2048	500
4096	2,500

"This table is based on an approximation of the ratio between the cost of an SHA-1 calculation and the cost of an RSA verification for keys of size 1024 bits (150 to 1), 2048 bits (500 to 1), and 4096 bits (2500 to 1)."