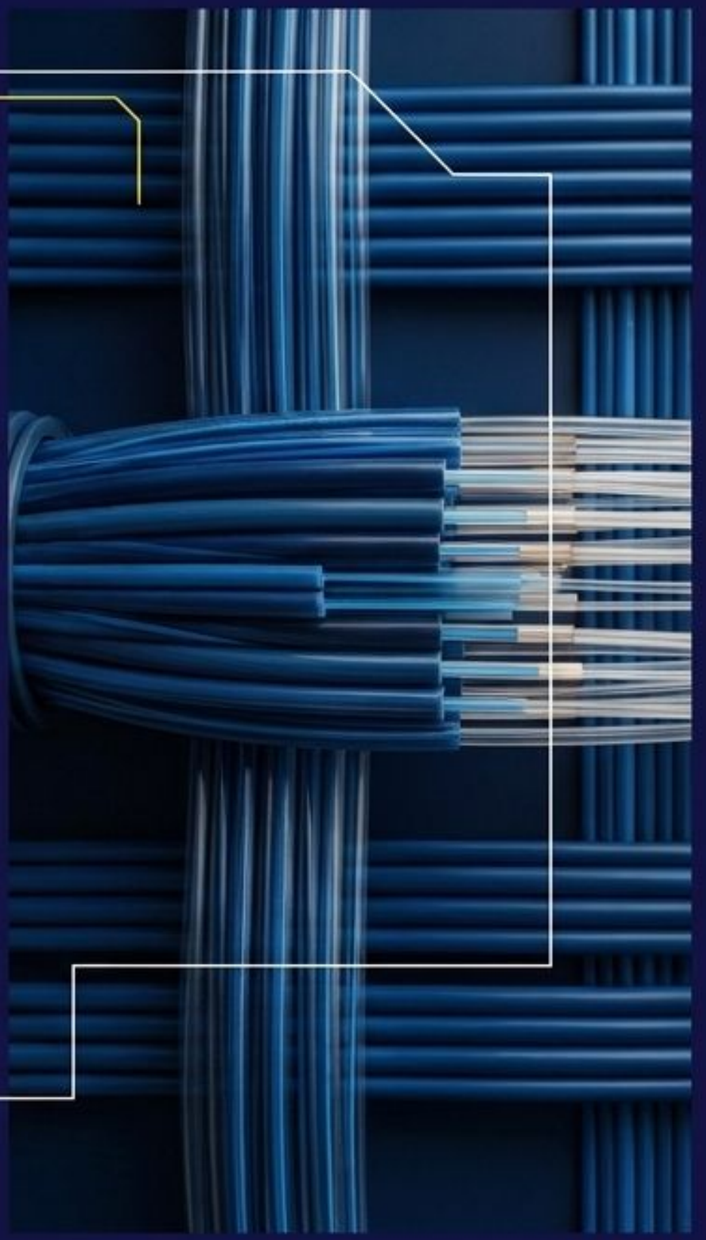
brphonia
liderança em inovaçãr

nic.br

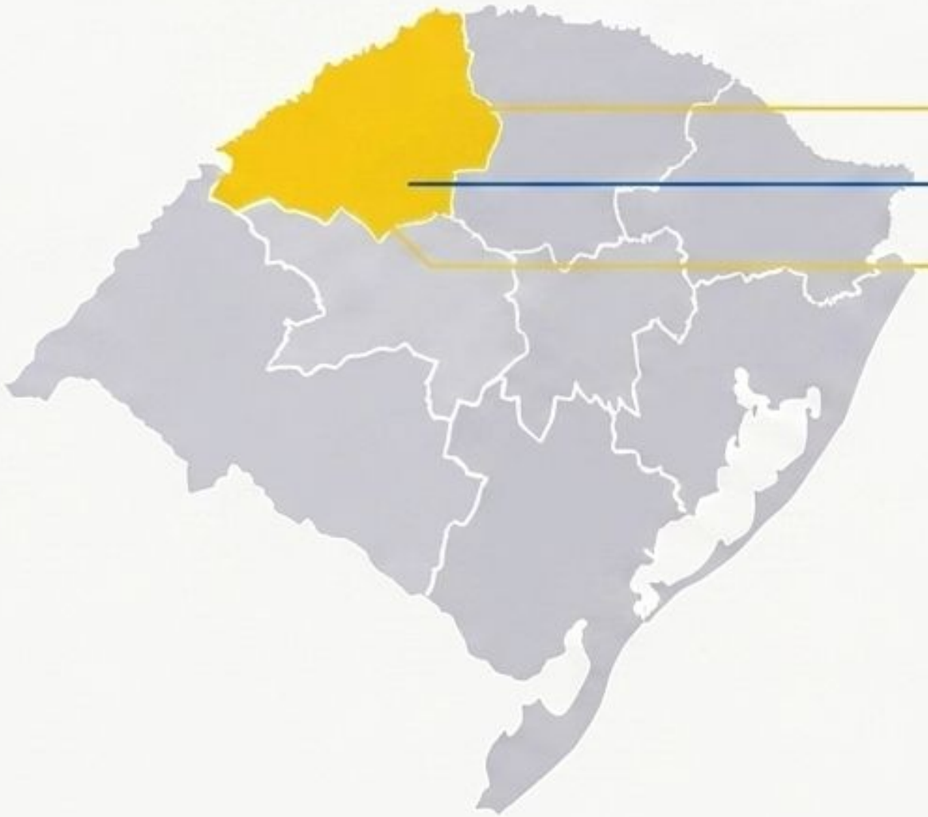
Boas Práticas de DNS e a Conquista do Selo KINDNS

Como a Brphonia elevou a resiliência
e a segurança na resolução de nomes.



AS263649 | LIVE INTRAREDE NIC.BR

A Brphonia: Protagonismo no Noroeste Gaúcho



13 Anos

De operação contínua.

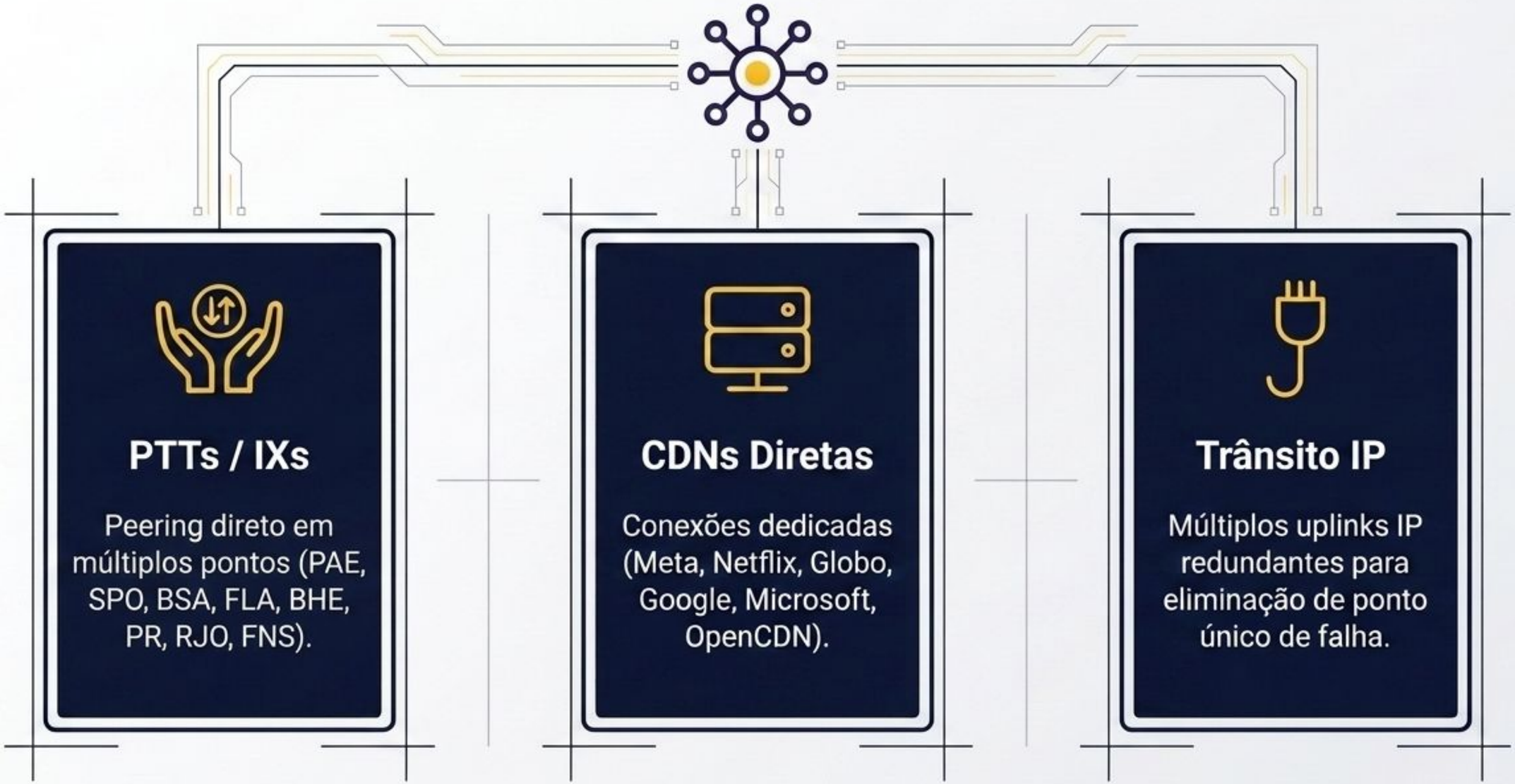
Fibra Óptica

Conectividade de ponta 100% ótica.

Protagonismo Regional

Profundo compromisso social e desenvolvimento econômico no RS.

AS263649: Topologia e Conectividade Global



PTTs / IXs

Peering direto em múltiplos pontos (PAE, SPO, BSA, FLA, BHE, PR, RJO, FNS).

CDNs Diretas

Conexões dedicadas (Meta, Netflix, Globo, Google, Microsoft, OpenCDN).

Trânsito IP

Múltiplos uplinks IP redundantes para eliminação de ponto único de falha.

Histórico de Excelência Operacional

NIC.br

2021
Certificado GPTW
(Mantido por 5 anos)

2022
Prêmio IPv6 NIC.br
e Selo TOP

2023
MANRS
(Iniciativa global de
roteamento seguro)

2024
Prêmio BCOP NIC.br
(Boas Práticas
Operacionais)

2025 / 2026
Selo KINDNS
Recebido 2026

O Desafio Global: A Iniciativa KINDNS

Projeto global da ICANN focado em normas técnicas rígidas para segurança, privacidade e resiliência de servidores DNS.

KINDNS

Categoria Certificada: Shared Private Resolvers

Resolução de nomes operada com máxima segurança, projetada e restrita exclusivamente para a base de assinantes da Brphonia.

A Matriz de Resiliência DNS

Pilar Estratégico	Ameaça Mitigada	Solução Técnica	Práticas
Segurança	Envenenamento de Cache e Amplificação DDoS	Implementação de DNSSEC e ACLs	Prática 1: Validação DNSSEC Prática 2: ACLs Rígidas
Privacidade	Espionagem e Monitoramento Passivo	Minimização de QNAME e DNS Criptografado (DoH/DoT)	Prática 3: Minimização de QNAME Prática 4: DoH e DoT
Resiliência	Falhas de Link e Quedas de Hardware	Raiz Local, Anycast e Arquitetura Segregada	Prática 5: Raiz Local & Anycast Prática 6: Segregação e Telemetria

Plano de Engenharia Fundamentado: Prática 1: Validação DNSSEC

Foco em proteção contra Envenenamento de Cache

O Unbound atua como validador iterativo, rejeitando sumariamente respostas forjadas.

Com âncoras de confiança atualizadas automaticamente, a autenticidade é garantida.

Código

```
# Unbound - Validação DNSSEC
module-config: "validator iterator"      ← Módulo de validação ativo
auto-trust-anchor-file: "/var/lib/unbound/root.key"
harden-dnssec-stripped: yes              ← Rejeita respostas sem assinatura
```

Comando de Validação (Exemplo):

```
$ dig @127.0.0.1 example.com +dnssec +multi
```

Resultado Esperado:

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54321
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; ANSWER SECTION:
example.com.     3600   IN A          93.184.216.34
example.com.     3600   IN RRSIG A    8 ... (assinatura digital) ...
```

Prática 2: Listas de Controle de Acesso (ACLs)

A primeira linha de defesa contra ataques de amplificação DDoS. Bloqueio total externo, permitindo apenas clientes internos.

```
# Unbound - Access Control Lists
access-control: 192.0.2.0/24 allow #exemplo de ip publico
access-control: 2001:db8::1/32 allow #exemplo de ip publico
access-control: 100.64.0.0/10 allow

# Bloqueio total externo
access-control: 0.0.0.0/0 deny
access-control: ::/0 deny
```

IPv4 Permitido
(Rede de clientes/CGNAT)

IPv6 Permitido
(Alocação própria)

Demais Origens
(Bloqueio total via deny explícito)

Práticas de Privacidade e Segurança DNS

Prática 3.1: Privacidade (QNAME MINIMISATION)	Prática 3.2: Criptografia(DoH e DoT)	Prática 3.3: Segurança (TLS)
Conceito: Reduz dados enviados aos servidores DNS, melhorando a privacidade.	**Conceito:** Protege consultas DNS com criptografía contra espionagem.	**Conceito:** Garante autenticidade e confiabilidade com certificados corretos.
Comando (exemplo): “qname-minimisation: yes” “minimal-response: yes”	**Comando (exemplo):** “interface: 192.168.2.1@443” “http-endpoint: /dns-query”	**Comando (exemplo):** “ssh-service-key: /etc/unbound/ssl/key.pem” “ssh-service-pem: /etc/unbound/ssl/cert.pem”

Prática 4: Local Root (RFC 8806) e Segregação

Local Root Code

Trazendo a zona raiz para "dentro de casa": latência reduzida e imunidade contra quedas de link internacional.

```
# Unbound - Local Root (RFC 8806)
auth-zone:
  name: "."
  master: "b.root-servers.net"
  master: "c.root-servers.net"
  fallback-enabled: yes
```

Diagrama de Arquitetura de Segregação

Conforme KINDNS: Segregação Rigorosa

Prática 5: Resiliência e Anycast Hyperlocal

Layer 1: Infraestrutura

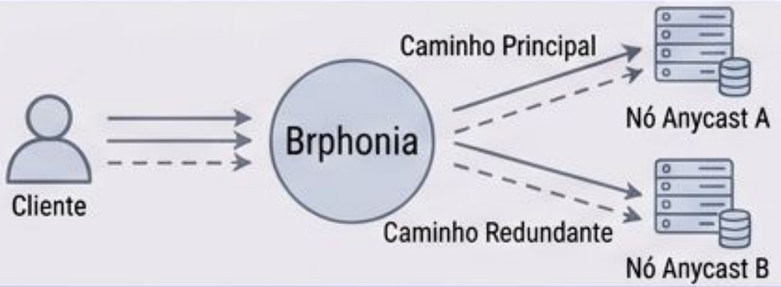
(**DNS Anycast Hyperlocal**)

Arquitetura distribuída de alta disponibilidade. O nó fisicamente mais próximo sempre responde.

Layer 2: Conectividade

(**Interfaces Dual-Stack** Dedicadas)

Operação nativa e simultânea em múltiplas interfaces (IPv4 e IPv6 dedicados).



Demonstração de Redundância

Arquitetura de rede com múltiplos caminhos de roteamento para garantir **alta disponibilidade** e **tolerância a falhas**.

Prática 6: Telemetria e Monitoramento Contínuo

Disponibilidade

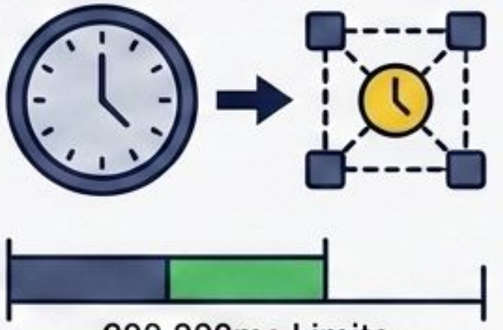
100%

Monitoramento ativo das requisições. Alertas automatizados para falhas de acessibilidade.

Validação

Validação constante da flag "ad" (Authenticated Data) para assegurar a integridade e barrar respostas forjadas.

Latência



Resoluções recursivas mantidas estritamente abaixo do limite operacional de 200 a 300 milissegundos.

DNS

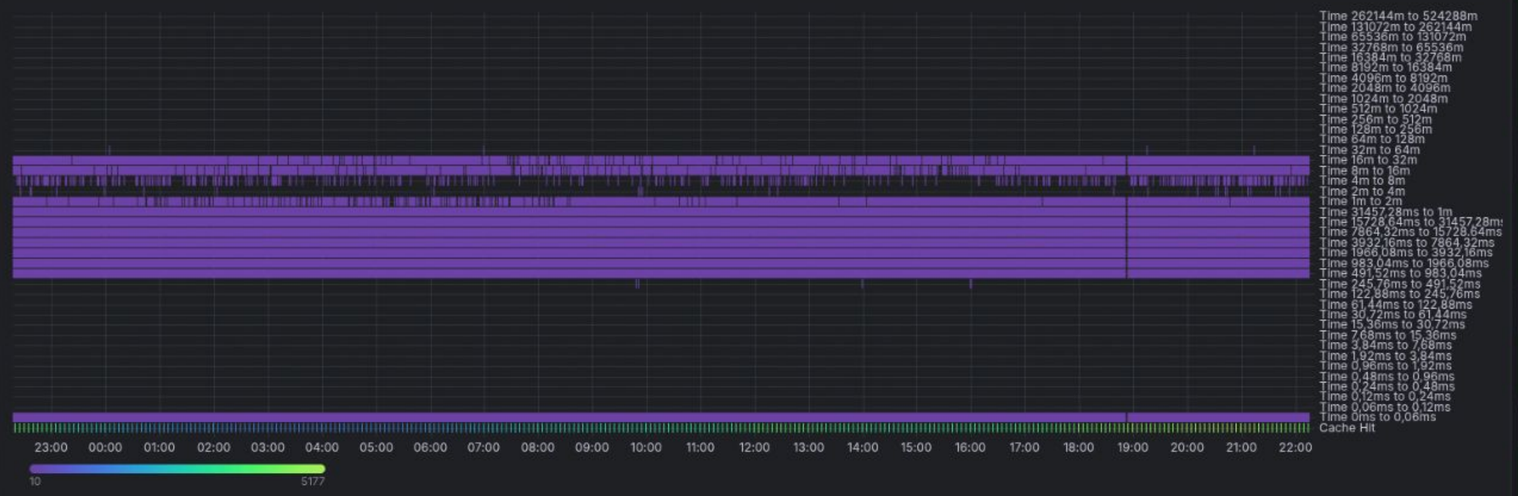
Queries Total	Recursion time AVG	Recursion time Mediana	Fila DNS	Fila DNS AVG	Fila DNS MAX	Percent HIT	Percent HIT Subnet
4939	156 ms	111 ms	1	0	0	147%	0

NOERROR	Query Subnet
4434	0

REFUSED	SERVFAIL
0	73

NXDOMAIN	SECURE
255	127

Distribuição da quantidade de consulte em relação tempo de resposta



Queries Timeout
0

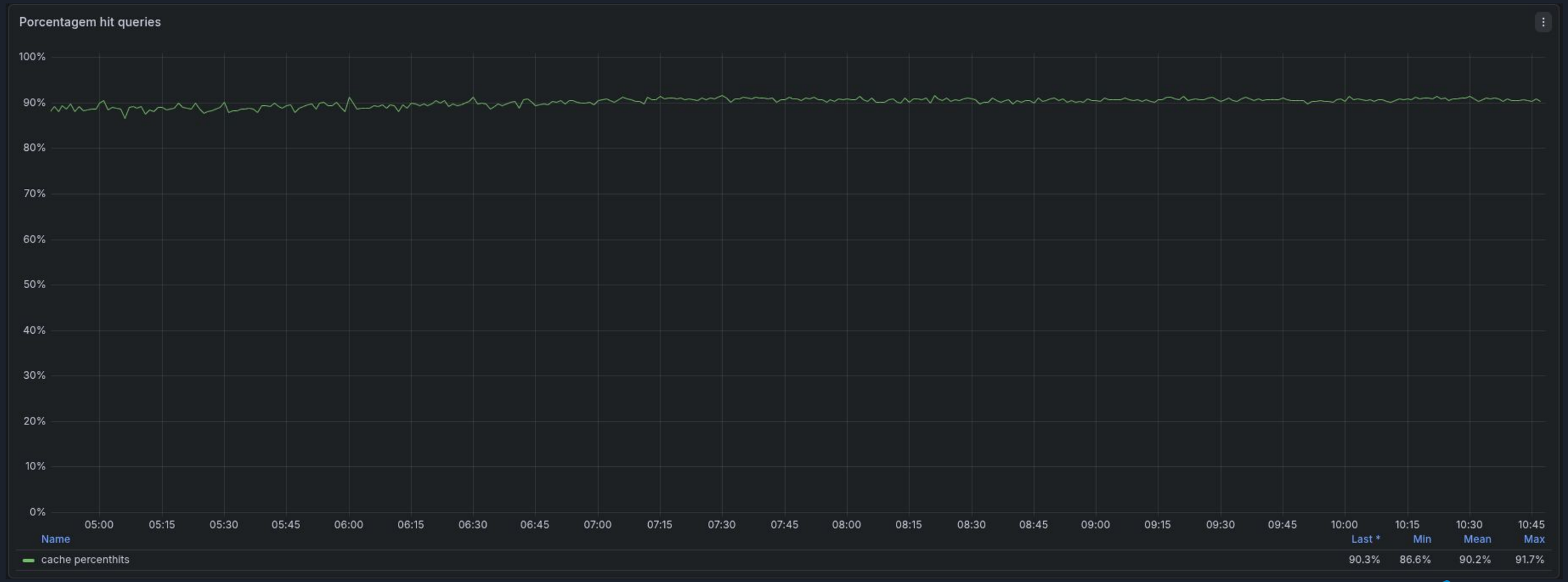
Bogus
0

Query Ratelimited
0

Query IP Ratelimited
0

Memory RRSET	Memory Message	Memory DNSSEC	Memory Interator	Memory Subnet	Memory Total	Time UP
5 GB	2 GB	705 MB	17 kB	0	8 GB	6 d 06:30:29

Queries



brphonia
liderança em inovação

Num answer

Name	Last *	Min	Mean	Max
No Data	280	118	225	342
No Error	1760	723	1404	1954
NXDOMAIN	78	42	86.6	169
Refused	0	0	0.0444	2
Secure	146	101	125	181
Servfail	19	11	17.3	29

brphonia
liderança em inovação

O Checklist de Validação

Passo 1: Teste DNSSEC Local

```
dig @ip-do-servidor nic.br +dnssec
```

- Confirme se a flag 'ad' está presente.

Passo 2: Relatório Oficial KINDNS

- Submissão de dados no painel da ICANN para confirmação externa e emissão do selo.

Passo 3: Monitoramento Contínuo NOC

- Integração das métricas ao Zabbix/Grafana (latência, taxas de validação, bloqueios ACL).

brphonia
iiderança em inovaçãr

Liderança em Inovação e Segurança

A adoção das práticas KINDNS não é apenas um selo de conformidade é a garantia de uma **internet mais rápida, segura e imune a falhas** para milhares de usuários. A Brphonia segue comprometida com a evolução da internet no Brasil.

Agradecimentos: NIC.br e ICANN pelo apoio. | AS263649 | brphonia.com.br