Breve introdução ao DNS
Uma abordagem prática
(aka crash course on DNS :))

Prof. Rossano Pablo Pinto

Novembro/2012-v0.3

Abril/2013-v0.5

(em construção)

Agenda

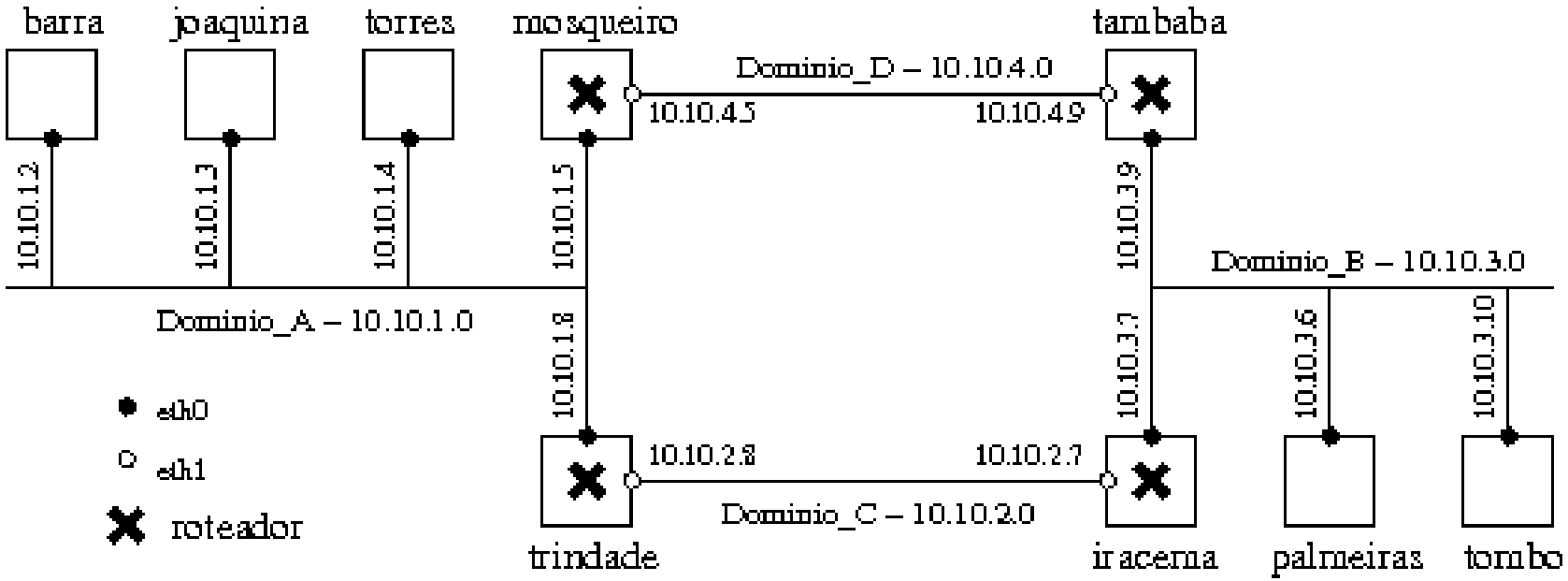
- Introdução
- DNS
- Domínios
- Name servers
- Resolução
- Registros
- Configuração de servidor
- Testes

Introdução

- Como endereçar máquinas em uma rede IP?
  - Endereços IP (IPv4 ou IPv6)
  - Números são difíceis de memorizar
    - É mais natural memorizar nomes
  - Solução: utilizar nomes para referenciar máquinas
  - Problema: o protocolo IP precisa de números para referenciar máquinas.
    - Solução: criar uma tabela que associe NOMES em IP
- Onde fica esta tabela?
  - Originalmente no arquivo texto **`/etc/hosts`**

Introdução

- Dada uma rede assim:



Introdução

- O arquivo /etc/hosts ficaria assim:

```
10.10.1.2       barra
10.10.1.3       joaquina
10.10.1.4       torres
10.10.1.5       mosqueiro
10.10.1.8       trindade
10.10.3.9       tambaba
10.10.3.7       iracema
10.10.3.6       palmeiras
10.10.3.10      tombo
```

Introdução

- Para uma rede pequena OK!
  - No exemplo anterior, existiriam 9 arquivos: 1 em cada máquina da rede
  - Internet HOJE: possui um limite máximo teórico (que está se esgotando) de aproximadamente 4 bilhões de endereços IP (espaço de endereçamento que leva em consideração endereços de rede, multicast, locais, reservados, etc..)

Introdução

- Cada alteração no endereçamento da rede demanda a alteração de todos os arquivos /etc/hosts em cada máquina existente!!!!
- Esta solução não é escalável!!!
- **DNS surge para resolver o problema de escalabilidade.**

DNS

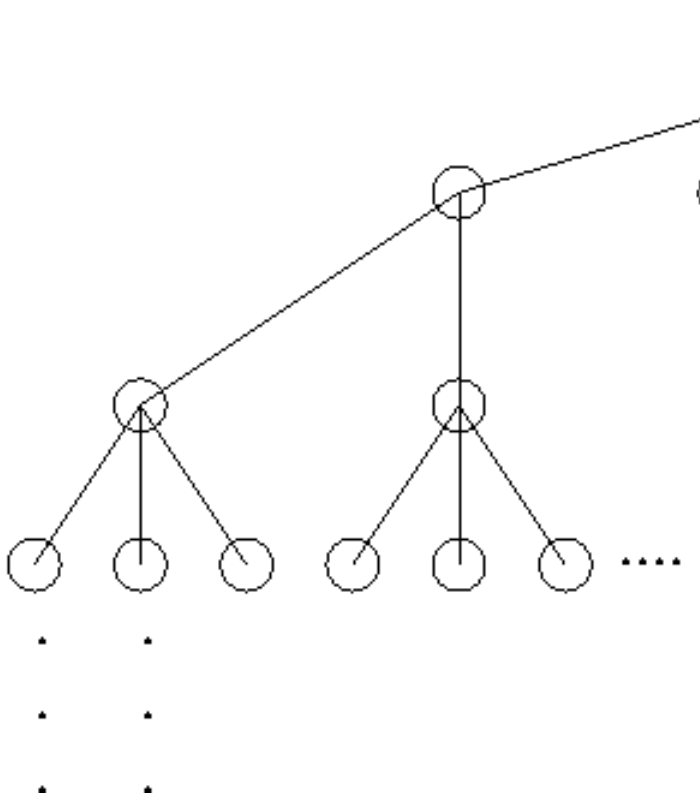
- DNS é uma base de dados distribuída
  - Principal função: resolver nomes em IP e IP em nomes
    - resolução direta: NOME -> IP
    - resolução reversa: IP -> NOME
- Existem diversas implementações do servidor DNS:
  - BIND: 80.3% dos servidores no mundo em Jul/2009
    - Autor: ISC (isc.org)

DNS

- DNS define, dentre outras coisas:
  - Um espaço de nomes hierárquico p/ hosts e endereços IP
  - Uma base de dados distribuída de nomes de hosts e informação de endereços
  - Um “resolver” para buscar dados nesta base de dados (geralmente uma função de uma biblioteca)
  - Um protocolo utilizado pelos servidores DNS para troca de informações

DNS

Funciomaneto do DNS



- Base de dados distribuída
- Formato de árvore invertida
- Nó raiz representado por nulo (ou .)
- Cada nó da árvore é representado por um nome de até 63 caracteres

DNS

- Existem **13** servidores raiz (root-servers) - e várias replicações...:

c.root-servers.net.

d.root-servers.net.

e.root-servers.net.

f.root-servers.net.

g.root-servers.net.

h.root-servers.net.

i.root-servers.net.

j.root-servers.net.

k.root-servers.net.

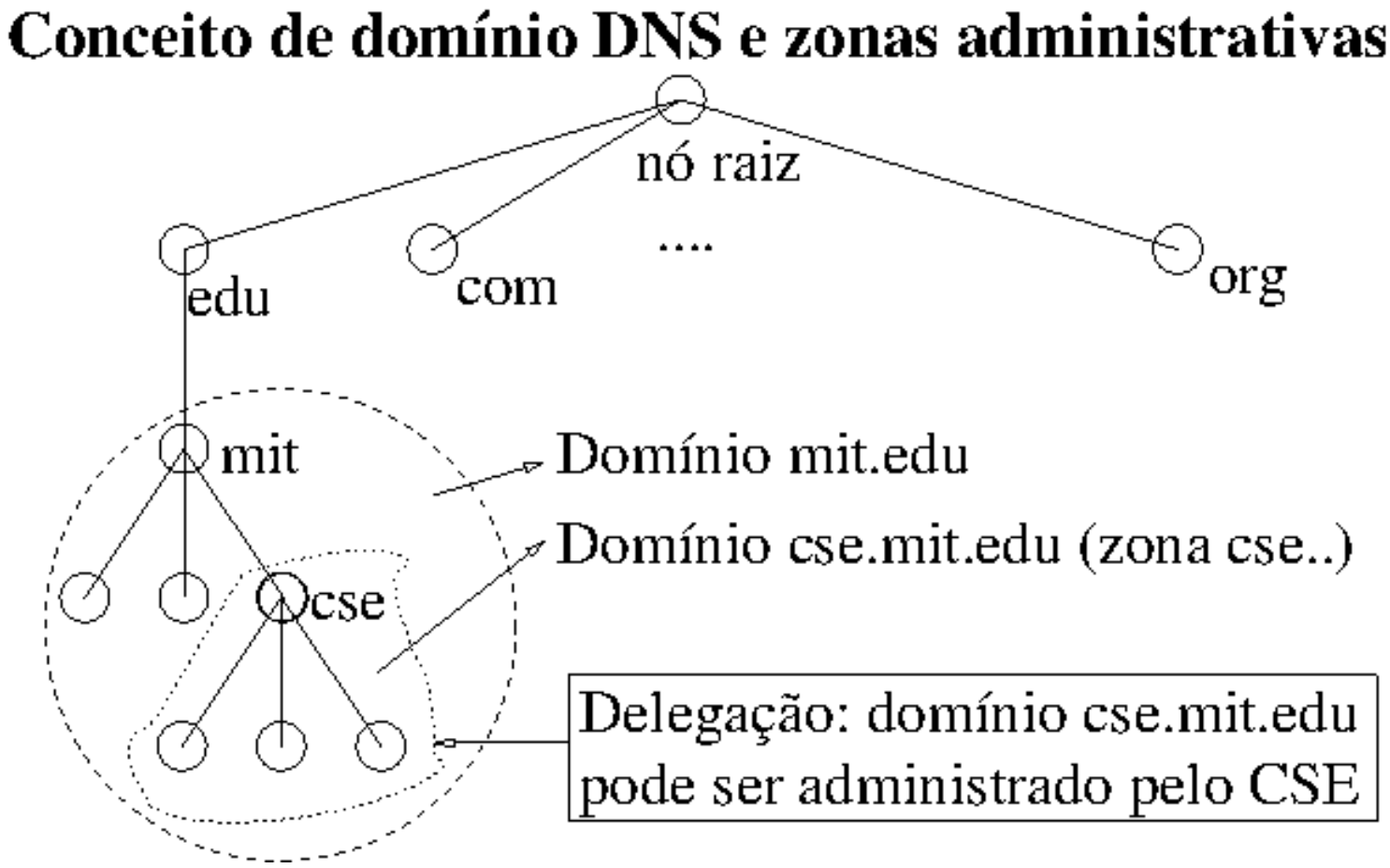
l.root-servers.net.

m.root-servers.net.

a.root-servers.net.

b.root-servers.net.

DNS - domínios



DNS - domínios

- Há cerca de 250 TLDs (Top Level Domain)
  - Top level domains (TLD). Os mais conhecidos (de 3 letras):

    .com, .edu, .org, .net, ...
  - TLDs de 2 letras (ccTLDs - Country Codes TLDs): .br, .ar, .us ....
    - Definidos na ISO 3166
    - Nomes de domínios internacionalizados foram introduzidos em 2010. Com isso é possível utilizar nomes em Árabe, Chinês, Russo, etc..

DNS - name servers

- Name servers (servidores de nome)
  - Armazenam informação de algum domínio (subdomínio)
  - Este subdomínio é conhecido por ZONA
  - O NS (name server) desta ZONA é autoritativo dela
  - Primary server (ou MASTER SERVER)
    - Informações armazenadas diretamente nele (possui os arquivos texto da zona que é autoritativo)
  - Secondary server (ou SLAVE SERVER)
    - Obtém informação do primary (serve para aliviar o número de requisições feitas ao MASTER e como redundância para o MASTER)
  - **Cada zona deve obrigatoriamente possuir pelo menos 1 MASTER e 1 SLAVE (ambos autoritativos p/ aquela zona)**

DNS - resolução

- Resolução.
  - Exemplo

    máquina **`lair.cs.colorado.edu`**

    busca pela

    máquina **`vangogh.cs.berkeley.edu`**

DNS - resolução

- Resolução (**`vangogh.cs.berkeley.edu`**)

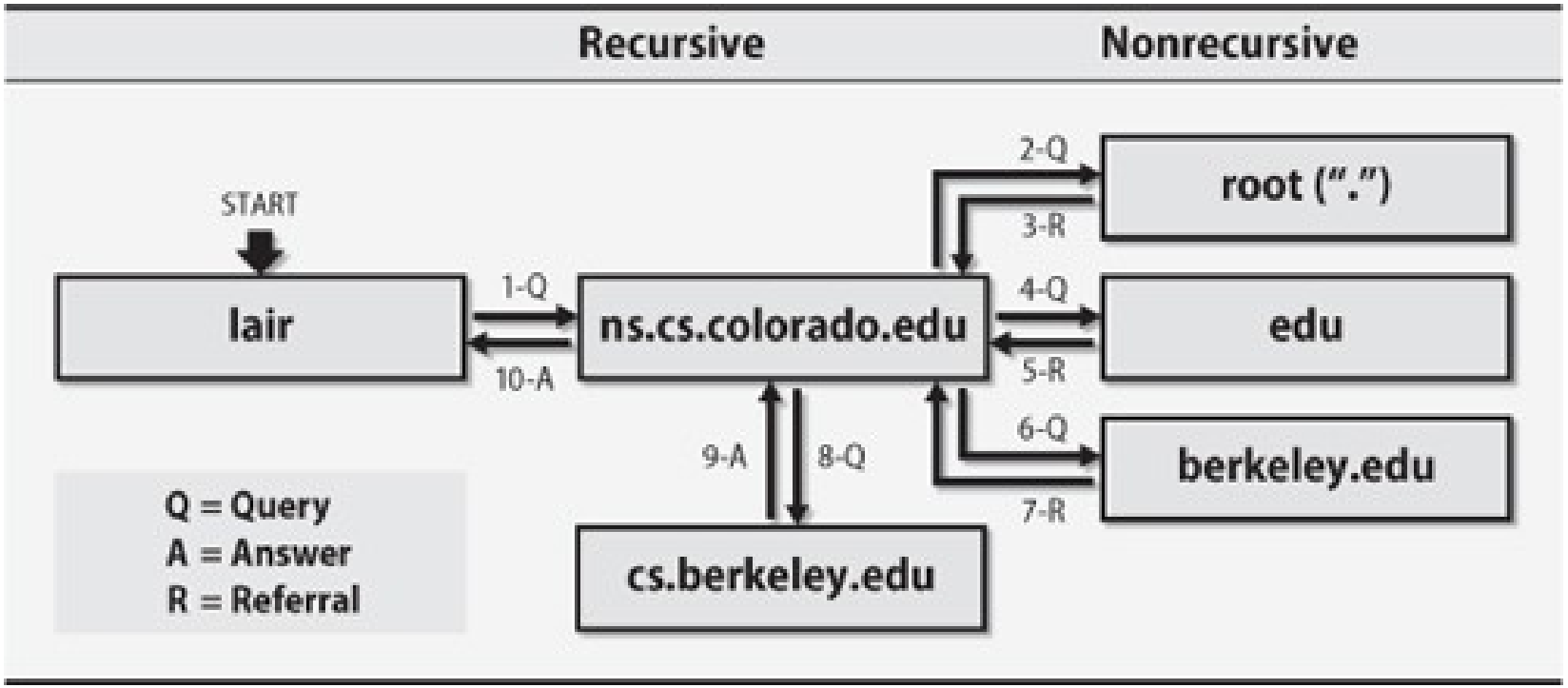


Figura do livro: UNIX and Linux Administration Handbook. 4th edition. Nemeth, Snyder, Hein, Whaley.

DNS - resolução

- Resolução (**`vangogh.cs.berkeley.edu`**)
  - Simulando o resolver com dig (*dig +trace traz tem o mesmo efeito...*)

```
dig @a.edu-servers.net vangogh.cs.berkeley.edu
dig @phloem.uoregon.edu vangogh.cs.berkeley.edu
dig @adns1.berkeley.edu vangogh.cs.berkeley.edu
```

OK, e a ANSWER SECTION é:

```
;; ANSWER SECTION:
vangogh.cs.berkeley.edu. 86400   IN A  128.32.112.208
```

DNS - resolução (resposta não autoritativa)

```
rossano@asti:~$ dig vangogh.cs.berkeley.edu

; <<>> DiG 9.7.3 <<>> vangogh.cs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42998
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vangogh.cs.berkeley.edu.       IN      A

;; ANSWER SECTION:
vangogh.cs.berkeley.edu. 86392  IN      A       128.32.112.208

;; Query time: 670 msec
;; SERVER: 192.168.200.51#53(192.168.200.51)
;; WHEN: Mon Nov 12 17:42:37 2012
;; MSG SIZE  rcvd: 57
```

DNS - resolução (resposta não autoritativa)

```
rossano@asti:~$ dig vangogh.cs.berkeley.edu

; <<>> DiG 9.7.3 <<>> vangogh.cs.berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42998
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vangogh.cs.berkeley.edu.       IN      A

;; ANSWER SECTION:
vangogh.cs.berkeley.edu. 86392  IN      A       128.32.112.208

;; Query time: 670 msec
;; SERVER: 192.168.200.51#53(192.168.200.51)
;; WHEN: Mon Nov 12 17:42:37 2012
;; MSG SIZE  rcvd: 57
```

FLAGS:

aa - authoritative
rd - recursion desired
ra - recursion available (se não aparecer em flags significa que recursão não estava disponível)
qr - não imprimir a query (omite a seção “Sending: ...” da resposta)

DNS - resolução (resposta não autoritativa. Exemplo com +qr)

```
rossano@asti:~$ dig vangogh.cs.berkeley.edu

; <<>> DiG 9.7.3 <<>> vangogh.cs.berkeley.edu

;; global options: +cmd
```

```
rossano@asti:~$ dig +qr vangogh.cs.berkeley.edu
; <<>> DiG 9.7.3 <<>> +qr vangogh.cs.berkeley.edu
;; global options: +cmd

;; Sending:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63545

;; flags: rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0


;; QUESTION SECTION:

;vangogh.cs.berkeley.edu.  IN A
```

DNS - resolução (resposta não autoritativa)

```
rossano@asti:~$ nslookup vangogh.cs.berkeley.edu

Server:         192.168.200.51

Address:        192.168.200.51#53


Non-authoritative answer:

Name:   vangogh.cs.berkeley.edu

Address: 128.32.112.208
```

DNS - resolução(resposta autoritativa)

```
rossano@asti:~$ dig hypnos.fatec.br

; <<>> DiG 9.7.3 <<>> hypnos.fatec.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24973
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;hypnos.fatec.br.               IN      A

;; ANSWER SECTION:
hypnos.fatec.br.        1200    IN      A       192.168.200.52

;; Query time: 0 msec
;; SERVER: 192.168.200.51#53(192.168.200.51)
;; WHEN: Mon Nov 12 17:49:23 2012
;; MSG SIZE  rcvd: 49
```

DNS - resolução(resposta autoritativa)

```
rossano@asti:~$ nslookup hypnos.fatec.br

Server:         192.168.200.51

Address:        192.168.200.51#53


Name:   hypnos.fatec.br

Address: 192.168.200.52
```

DNS - resolução (exemplo desde a raiz: .)

- Resolução (**`rossano.pro.br`**)
  - Simulando o resolver com dig (desde a raiz: .)
    - `dig @f.root-servers.net rossano.pro.br`
    - `dig @f.dns.br rossano.pro.br`
    - `dig @ns2.locaweb.com.br rossano.pro.br`
    - OK, e a ANSWER SECTION é:

```
;; ANSWER SECTION:
rossano.pro.br.      3600  IN A  187.45.195.63
```

DNS - Registros

- Toda a informação do serviço DNS é armazenada em **resource records**
  - Cada Resource Record possui um tipo
  - Isso permite codificar diferentes informações:
    - A, NS, CNAME, SOA, WKS, PTR, HINFO, MX, TXT

DNS - Registros

TIPO		
A	Endereço de computador	Número IP de 32 bits (4 octetos)
NS	Servidor de nomes autoritativo	Nome de domínio para servidor
CNAME	Nome canônico (alias)	Nome de domínio para alias
SOA	Marca o início dos dados da zona	Parâmetros que governam a zona
WKS	Descriçao de well-known-service	Lista de nomes de serviços e protocolos
PTR	Ponteiro de nome de domínio (reverso)	Nome de domínio
HINFO	Host information	Arquitetura de máquina e sistema operacional
MX	Mail Exchange	Lista de pares <preferência, host>
TXT	Text String	Whatever
AAAA	Endereço de computador	Número IP de 128 bits (formato hexadecimal)

DNS - Configuração SERVIDOR

- Arquivos
  - /etc/named.conf
  - /etc/dns/matrix.zone
  - /etc/dns/matrix.rev
  - /etc/dns/localhost.zone
  - /etc/dns/named.local
- Executar

```
mkdir /etc/dns

cp /var/named/caching-example/*  /etc/dns
```

DNS - Configuração SERVIDOR - /etc/named.conf (editar)

```
options {
        directory "/etc/dns";
};
zone "." IN {
        type hint;
        file "named.root";
};
zone "localhost" IN {
        type master;
        file "localhost.zone";
        #allow-update { none; };
};
```

```
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        #allow-update { none; };
};

zone "matrix.br" IN {
        type master;
        file "matrix.zone";
};

zone "10.10.in-addr.arpa" IN {
        type master;
        file "matrix.rev";
};
```

DNS - Configuração SERVIDOR - /etc/dns/matrix.zone (criar)

```
$ORIGIN matrix.br.

$TTL    86400

matrix.br. IN SOA ns.matrix.br. root.ns.matrix.br. (

        2012111301; SERIAL

        28800; REFRESH

        14400; RETRY

        3600000; EXPIRY (1000H)

        86400; default TTL

)

matrix.br.      IN      NS   ns.matrix.br.

matrix.br.      IN      MX   0 ns.matrix.br.

ns              IN      A    10.10.1.254
```

```
smith  IN     A   10.10.1.253

neo    IN     A   10.10.1.252

niobe  IN     A   10.10.1.251

zion   IN     A   10.10.1.250
```

DNS - Configuração SERVIDOR - /etc/dns/matrix.zone (criar)

- SOA
  - **Serial number** - número que indica a versão da tabela
    - Slaves sabem quando atualizar os dados
  - **Refresh** - frequencia com que SLAVES verificam se serial number do MASTER mudou (sugestão: 1 a 6 hs.)
  - **Retry** - Se MASTER não respondeu refresh, tentar em RETRY segundos (sugestão: 20 a 60 minutos)
  - **Expire** - Indica quanto tempo um SLAVE deve continuar servindo um domínio caso não consiga atualizar-se com o MASTER. (sugestão: de 1 semana a 2 meses)
  - **Minimum** (TTL) - tempo mínimo de validade da infomação no cache DNS no caso de NEGATIVE ANSWER.
    - $TTL antes de SOA indica POSITIVE ANSWER.

DNS - Configuração SERVIDOR - /etc/dns/matrix.rev (criar)

```
@ IN SOA ns.matrix.br. root.ns.matrix.br. (

        20101119; SERIAL NUMBER

        28800; REFRESH

        14400; RETRY

        3600000; EXPIRY

        86400; MINIMUM TTL

)
```

```
10.10.in-addr.arpa.   IN     NS   ns.matrix.br.
254.1   IN  PTR     ns.matrix.br.
253.1   IN  PTR     smith.matrix.br.
252.1   IN  PTR     neo.matrix.br.
251.1   IN  PTR     niobe.matrix.br.
250.1   IN  PTR     zion.matrix.br.
```

DNS - Testes

```
root@machine:~# dig zion.matrix.br

; <<>> DiG 9.4.3-P4 <<>> zion.matrix.br
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15480
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;zion.matrix.br.      IN A

;; ANSWER SECTION:
zion.matrix.br.      86400  IN A  10.10.1.250
```

```
;; AUTHORITY SECTION:
matrix.br.  86400  IN NS   ns.matrix.br.

;; ADDITIONAL SECTION:
ns.matrix.br. 86400  IN A  10.10.1.254

;; Query time: 1 msec
;; SERVER: 10.10.1.254#53(10.10.1.254)
;; WHEN: Mon Nov 19 15:12:07 2012
;; MSG SIZE  rcvd: 81
```

DNS - Testes

```
root@machine:~# dig neo.matrix.br


; <<>> DiG 9.4.3-P4 <<>> neo.matrix.br

;; global options:  printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR,
id: 19838

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1,
AUTHORITY: 1, ADDITIONAL: 1


;; QUESTION SECTION:

;neo.matrix.br.   IN     A


;; ANSWER SECTION:

neo.matrix.br.    86400       IN     A      10.10.1.252
```

```
;; AUTHORITY SECTION:

matrix.br.   86400  IN   NS   ns.matrix.br.


;; ADDITIONAL SECTION:

ns.matrix.br.    86400    IN  A     10.10.1.254


;; Query time: 1 msec

;; SERVER: 10.10.1.254#53(10.10.1.254)

;; WHEN: Mon Nov 19 15:12:22 2012

;; MSG SIZE  rcvd: 80
```

DNS - Testes

```
root@machine:~# dig ns.matrix.br

; <<>> DiG 9.4.3-P4 <<>> ns.matrix.br
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22806
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;ns.matrix.br.      IN   A

;; ANSWER SECTION:
ns.matrix.br.      86400   IN   A    10.10.1.254

;; AUTHORITY SECTION:
matrix.br.         86400      IN     NS    ns.matrix.br.

;; Query time: 1 msec
;; SERVER: 10.10.1.254#53(10.10.1.254)
;; WHEN: Mon Nov 19 15:12:30 2012
;; MSG SIZE  rcvd: 60
```

DNS - Testes

```
root@machine:~# dig  -x 10.10.1.251

; <<>> DiG 9.4.3-P4 <<>> -x 10.10.1.251
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23316
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;251.1.10.10.in-addr.arpa.  IN     PTR

;; ANSWER SECTION:
251.1.10.10.in-addr.arpa. 86400 IN     PTR  niobe.matrix.br.

;; AUTHORITY SECTION:
10.10.in-addr.arpa.    86400       IN     NS
ns.matrix.br.

;; ADDITIONAL SECTION:
ns.matrix.br.      86400       IN     A      10.10.1.254

;; Query time: 1 msec
;; SERVER: 10.10.1.254#53(10.10.1.254)
;; WHEN: Mon Nov 19 15:12:51 2012
;; MSG SIZE  rcvd: 105
```

DNS - Testes

```
root@machine:~# dig  -x 10.10.1.253

; <<>> DiG 9.4.3-P4 <<>> -x 10.10.1.253
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31511
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;253.1.10.10.in-addr.arpa.       IN      PTR

;; ANSWER SECTION:
253.1.10.10.in-addr.arpa. 86400 IN PTR  smith.matrix.br.

;; AUTHORITY SECTION:
10.10.in-addr.arpa.       86400         IN      NS      ns.matrix.br.

;; ADDITIONAL SECTION:
ns.matrix.br.       86400         IN      A       10.10.1.254

;; Query time: 1 msec
;; SERVER: 10.10.1.254#53(10.10.1.254)
;; WHEN: Mon Nov 19 15:13:03 2012
;; MSG SIZE  rcvd: 105
```

DNS - Testes

root@machine:~# nslookup zion.matrix.br

Server: 10.10.1.254

Address: 10.10.1.254#53

Name: zion.matrix.br

Address: 10.10.1.250

DNS - Testes

root@machine:~# nslookup neo.matrix.br

Server: 10.10.1.254

Address: 10.10.1.254#53

Name: neo.matrix.br

Address: 10.10.1.252

DNS - Testes

root@machine:~# nslookup ns.matrix.br

Server: 10.10.1.254

Address: 10.10.1.254#53

Name: ns.matrix.br

Address: 10.10.1.254

DNS - Testes

root@machine:~# nslookup 10.10.1.251

Server: 10.10.1.254

Address: 10.10.1.254#53

251.1.10.10.in-addr.arpa name = niobe.matrix.br.

DNS - Testes

root@machine:~# nslookup 10.10.1.250

Server: 10.10.1.254

Address: 10.10.1.254#53

250.1.10.10.in-addr.arpa name = zion.matrix.br.

DNS - Testes

root@machine:~# nslookup 10.10.1.253

Server: 10.10.1.254

Address: 10.10.1.254#53

253.1.10.10.in-addr.arpa name = smith.matrix.br.

Leitura aconselhada

- **CHAPTER 7, SECTION 7.1** – Computer Networks – Andrew S. Tanenbaum, David J. Wetherall – 5th Edition, Prentice Hall
- **CHAPTER 17** – UNIX and Linux Administration Handbook. – Nemeth, Snyder, Hein, Whaley. – 4th edition, Prentice Hall.