Linux para Infraestrutura

Prof. André Nasserala

nasserala@gmail.com

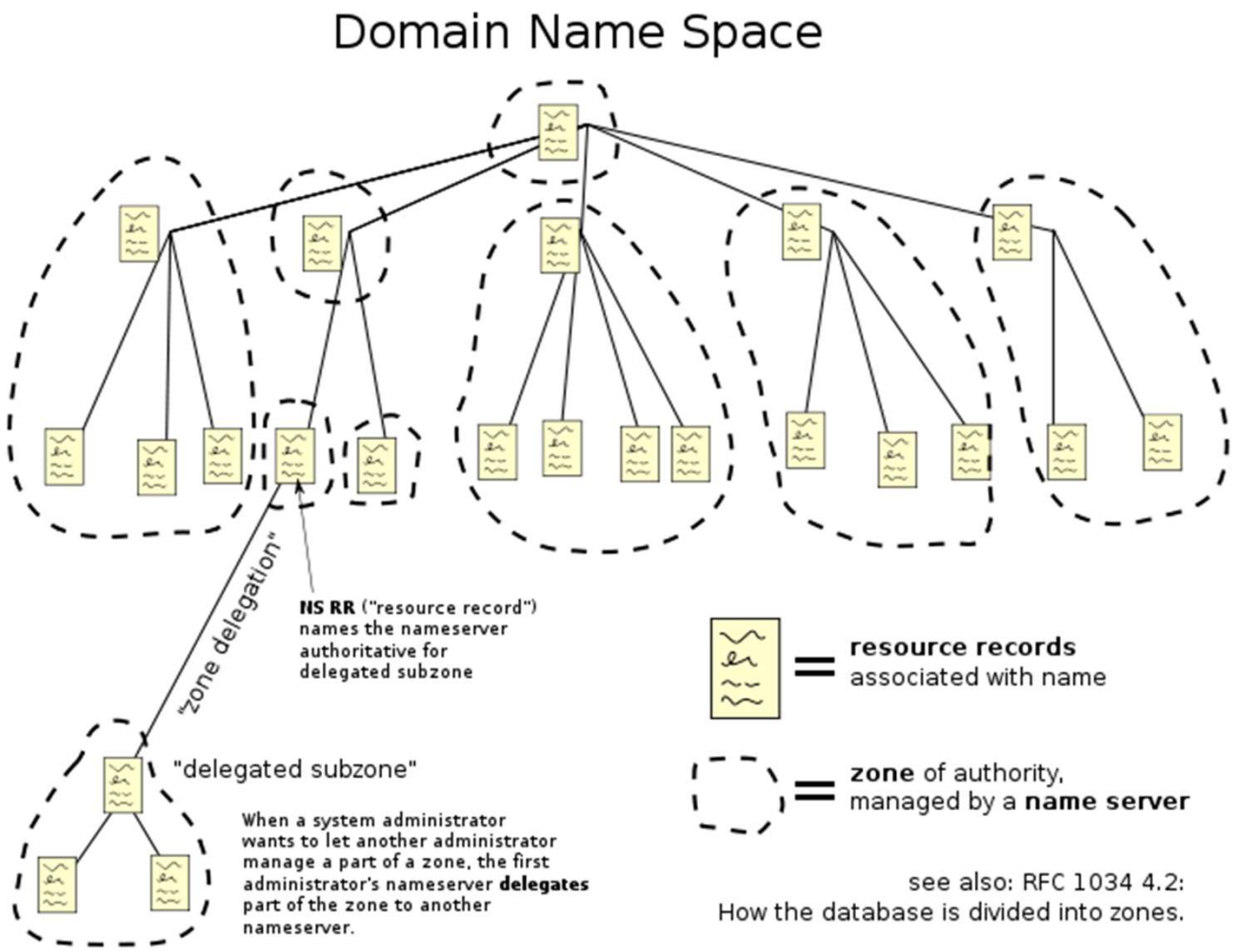
DNS

- O DNS (Domain Name System - Sistema de Nomes de Domínios) é um sistema de gerenciamento de nomes hierárquico e distribuído operando segundo duas definições:

1. Examinar e atualizar seu banco de dados.
2. Resolver nomes de servidores em endereços de rede (IPs).

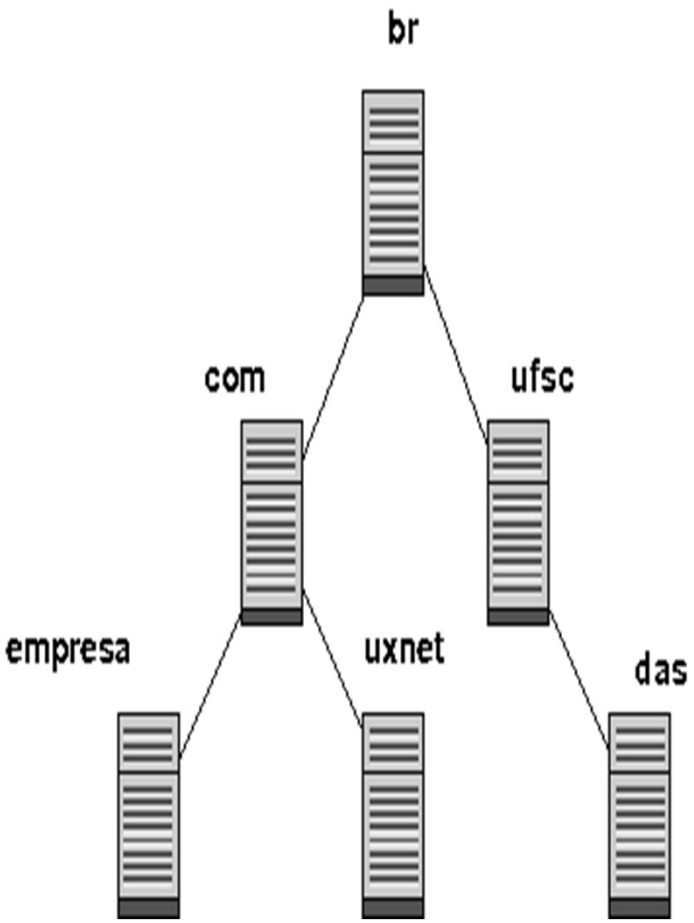
- RFC 1034, 1035, 1713
- **Servidores:**
- Bind
- DJBDNS

DNS


Domain Name Space
"zone delegation"
NS RR ("resource record") names the nameserver authoritative for delegated subzone
"delegated subzone"
When a system administrator wants to let another administrator manage a part of a zone, the first administrator's nameserver delegates part of the zone to another nameserver.
resource records associated with name
zone of authority, managed by a name server
see also: RFC 1034 4.2: How the database is divided into zones.

DNS

- Trata-se de um sistema hierárquico, onde cada servidor na árvore fica responsável por uma zona, delimitada pelo símbolo "." nos nomes.;
- Assim o domínio empresa.com.br recebeu autoridade de .com.br para operar nessa zona, assim como .com.br recebe tal autoridade de .br e .br deve esta listado nos ROOT Server de DNS;
- Quando registramos empresa.com.br recebemos autoridade de .com.br para cuidar dessa zona e assim podemos criar nomes válidos na Internet ou conceder autoridades a outro servidos abaixo dessa zona.



DNS

- **Bind**
- BIND (Berkeley Internet Name Domain ou, como chamado previamente, Berkeley Internet Name Daemon) é o servidor para o protocolo DNS mais utilizado na Internet, especialmente em sistemas do tipo Unix e Linux, onde ele pode ser considerado um padrão de fato.
- Foi criado por quatro estudantes de graduação, membros de um grupo de pesquisas em ciência da computação da Universidade de Berkeley, e foi distribuído pela primeira vez com o sistema operacional 4.3BSD.
- O programador Paul Vixie, enquanto trabalhava para a empresa DEC, foi o primeiro mantenedor do BIND.
- Atualmente o BIND é suportado e mantido pelo Internet Systems Consortium.

DNS

- **NSLOOKUP**
- O comando NSLOOKUP solicita informações para Servidores de Domínios da Internet, podendo trabalhar em dois modos.
- No modo interativo pode-se interagir com vários Servidores de Domínios e com várias máquinas.
- No modo não interativo a solicitação de informações é específica para uma determinada máquina ou um determinado Servidor de Domínio.
- O comando NSLOOKUP entra em modo interativo quando nenhum argumento de configuração é fornecido.
- O comando executa no modo não interativo quando o primeiro argumento é o endereço ou o nome de um Servidor de Domínio do qual serão mostradas as informações.

DNS

- **NSLOOKUP**
- SINTAXE DO COMANDO NSLOOKUP
- nslookup [-Optção ...] [Host] [-Nameserver]

- ARGUMENTOS DE INFORMAÇÕES
- server NOME
- Considera como default o servidor especificada pelo NOME.
- lserver NOME
- Este argumento usa o servidor inicial para procurar informações sobre o domínio especificado pelo NOME.

DNS

- [root@localhost ~]# nslookup
- > server 8.8.8.8
- Default server: 8.8.8.8
- Address: 8.8.8.8#53
- > nasserala.duckdns.org
- Server: 8.8.8.8
- Address: 8.8.8.8#53

- Non-authoritative answer:
- Name: nasserala.duckdns.org
- Address: 191.217.16.156

DNS

- A instalação:

- **# yum install bind bind-utils -y**

- O serviço de DNS faz 2 tipos básicos de trablho:

1. Resolução Direta: Transformar nome em IP;
2. Resolução Reversa: Transformar IP em nome;

- O Bind faz os 2 serviços por padrão, assim teremos basicamente 4 arquivos de configuração para editar.

DNS

- Iniciando o serviço:
- systemctl start named

- Marcando para iniciar junto com a máquina:
- systemctl enable named

- Ou

- # ntsysv

DNS

- Por padrão, o servidor BIND está atendendo apenas no host local.
- Portanto, você precisará configurá-lo para escutar em todas as interfaces de rede.
- Você pode configurá-lo editando o arquivo /etc/named.conf:

- # vi /etc/named.conf

- Comentando as seguintes linhas:
- //listen-on port 53 { 127.0.0.1; };
- //listen-on-v6 port 53 { ::1; };

DNS

- Altere a seguinte linha para permitir a consulta de sua rede local:

- allow-query { localhost;192.168.1.0/24; };

- Salve e feche o arquivo quando terminar.

- Reiniciando o serviço:
- systemctl restart named

DNS

- Criar zona de DNS direta e reversa
- Uma zona direta é usada para resolver o nome do host para o endereço IP, enquanto uma zona reversa é usada para resolver o endereço IP para o nome do host.
- Geralmente, todas as consultas DNS normais são consultas de pesquisa direta.
- Você pode definir as zonas de pesquisa direta e inversa no arquivo /etc/named.conf.
- Edite o arquivo /etc/named.conf com o seguinte comando:
- # vi /etc/named.conf

DNS

- Adicione as seguintes linhas no final do arquivo:
- zone “curso.local" IN {

- type master;
- file “curso.local.db";
- allow-update { none; };
- };
- zone "1.168.192.in-addr.arpa" IN {

- type master;
- file "192.168.1.db";
- allow-update { none; };
- };

DNS

- Em seguida, você precisará criar os arquivos de zona direta e reversa definidos na etapa anterior.
- Por padrão, todos os arquivos de pesquisa de zona estão localizados no diretório /var/named.
- Primeiro, crie um arquivo de zona de encaminhamento com o seguinte comando:

- # vi /var/named/curso.local.db

- Altere de acordo com o slide seguinte...

DNS

```
$TTL 86400
@   IN  SOA     ns1.curso.local. root.curso.local. (
                                3           ;Serial
                                3600        ;Refresh
                                1800        ;Retry
                                604800      ;Expire
                                86400       ;Minimum TTL
)
;Name Server Information
@       IN  NS      ns1.curso.local.
;IP address of Name Server
ns1       IN  A       192.168.1.100
;A - Record HostName To Ip Address
www     IN  A       192.168.1.101
;CNAME record
ftp     IN CNAME        www.curso.local.
```

DNS

- Salve e feche o arquivo e crie um arquivo de zona reversa com o seguinte comando:

- # vi /var/named/192.168.1.db

- Adicione as seguintes linhas, de acordo com o slide a seguir:

DNS

```
$TTL 86400
@   IN  SOA     ns1.curso.local. root.curso.local. (
                              3         ;Serial
                              3600      ;Refresh
                              1800      ;Retry
                              604800     ;Expire
                              86400     ;Minimum TTL
)
;Name Server Information
@         IN      NS        ns1.curso.local.
;Reverse lookup for Name Server
100       IN  PTR     ns1.curso.local.
;PTR Record IP address to HostName
101       IN  PTR     www.curso.local.
```

DNS

- Verificando a configuração de DNS
- Depois de configurar todos os arquivos de zona, você precisará verificar os arquivos de configuração.
- Primeiro, valide o arquivo de configuração principal com o seguinte comando:

- # named-checkconf /etc/named.conf

- Se tudo estiver bem, você não verá nenhum erro.

DNS

- Em seguida, verifique o arquivo de zona de encaminhamento com o seguinte comando:
- # named-checkzone curso.local /var/named/curso.local.db

- Você deve obter a seguinte saída:
- zone curso.local/IN: loaded serial 3 OK

- Em seguida, verifique o arquivo de zona reversa com o seguinte comando:
- named-checkzone 1.168.192.in-addr.arpa /var/named/192.168.1.db

DNS

- Você deve obter a seguinte saída:
- zone 1.168.192.in-addr.arpa/IN: loaded serial 3
- OK

- Por fim, reinicie o serviço BIND para aplicar as alterações:
- systemctl restart named

DNS

- Verificando servidor DNS
- Neste ponto, o servidor BIND DNS está instalado e configurado.
- É hora de verificar se está funcionando ou não.
- Primeiro, edite seu arquivo /etc/resolv.conf e adicione o IP do seu servidor DNS:

- # vi /etc/resolv.conf

DNS

- Adicione a seguinte linha no início do arquivo:
- nameserver 192.168.1.100

- Salve e feche o arquivo e verifique a pesquisa direta usando o comando dig:
- dig www.curso.local
- Ou
- dig ns1.curso.local

- Se tudo estiver bem, você deve obter a seguinte resposta:

DNS

- ; <<>> DiG 9.11.20-RedHat-9.11.20-5.el8 <<>> www.curso.local
- ;; global options: +cmd
- ;; Got answer:
- ;; WARNING: .local is reserved for Multicast DNS
- ;; You are currently testing what happens when an mDNS query is leaked to DNS
- ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52518
- ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

- ;; OPT PSEUDOSECTION:
- ; EDNS: version: 0, flags:; udp: 4096
- ; COOKIE: cd9d365f1f02621aa9c8753c5fd47154db8cae737b9ca09f (good)
- ;; QUESTION SECTION:
- ;www.curso.local. IN A

- ;; ANSWER SECTION:
- www.curso.local. 86400 IN A 192.168.1.101

- ;; AUTHORITY SECTION:
- curso.local. 86400 IN NS ns1.curso.local.

- ;; ADDITIONAL SECTION:
- ns1.curso.local. 86400 IN A 192.168.1.100

- ;; Query time: 0 msec
- ;; SERVER: 192.168.1.100#53(192.168.1.100)
- ;; WHEN: Sat Dec 12 02:29:24 EST 2020
- ;; MSG SIZE rcvd: 128

DNS

- Em seguida, verifique a pesquisa reversa com o seguinte comando:

- # dig -x 192.168.1.100

- Você deve obter a seguinte resposta:

DNS

- ; <<>> DiG 9.11.20-RedHat-9.11.20-5.el8 <<>> -x 192.168.1.100
- ;; global options: +cmd
- ;; Got answer:
- ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30878
- ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

- ;; OPT PSEUDOSECTION:
- ; EDNS: version: 0, flags:; udp: 4096
- ; COOKIE: 18a66bab478cf57219e6c17c5fd471671887a1dd983fef57 (good)
- ;; QUESTION SECTION:
- ;100.1.168.192.in-addr.arpa. IN PTR

- ;; ANSWER SECTION:
- 100.1.168.192.in-addr.arpa. 86400 IN PTR ns1.curso.local.

- ;; AUTHORITY SECTION:
- 1.168.192.in-addr.arpa. 86400 IN NS ns1.curso.local.

- ;; ADDITIONAL SECTION:
- ns1.curso.local. 86400 IN A 192.168.1.100

- ;; Query time: 0 msec
- ;; SERVER: 192.168.1.100#53(192.168.1.100)
- ;; WHEN: Sat Dec 12 02:29:43 EST 2020
- ;; MSG SIZE rcvd: 148