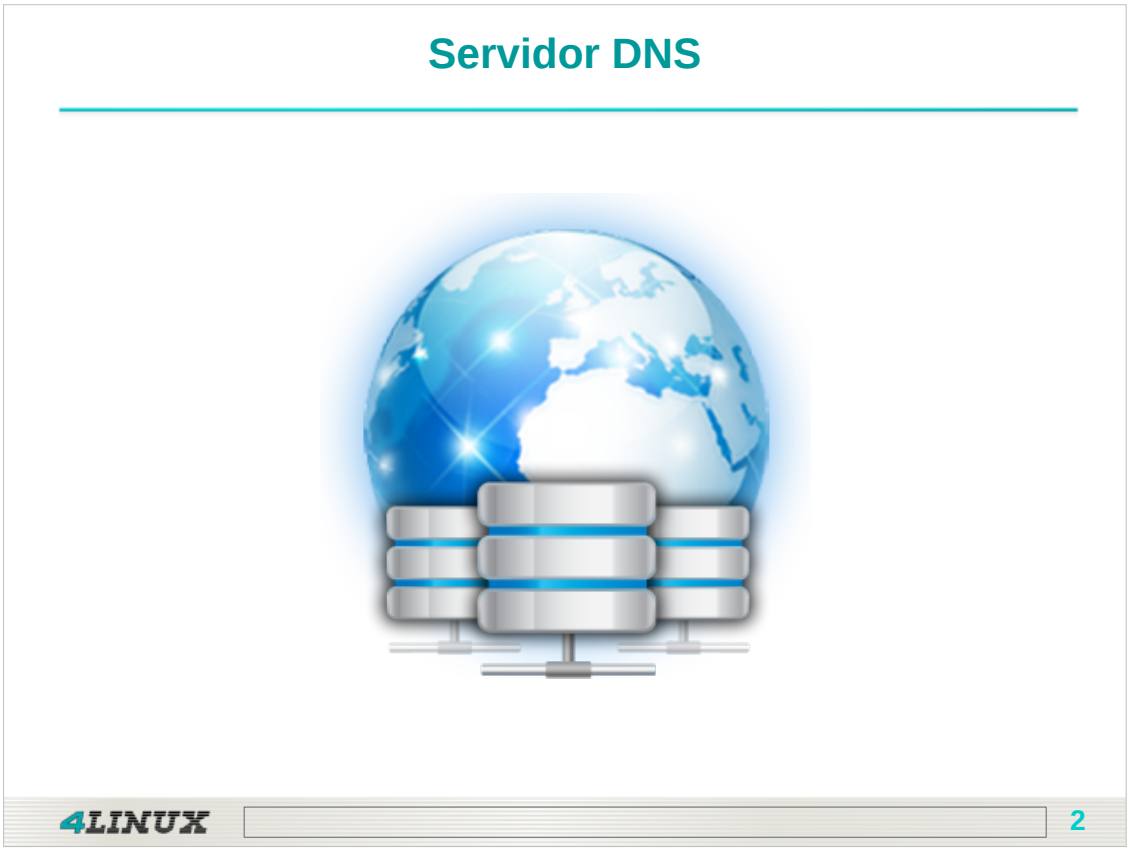
Curso 452

Linux Security Servers in Cloud

Versão 2015_3.0

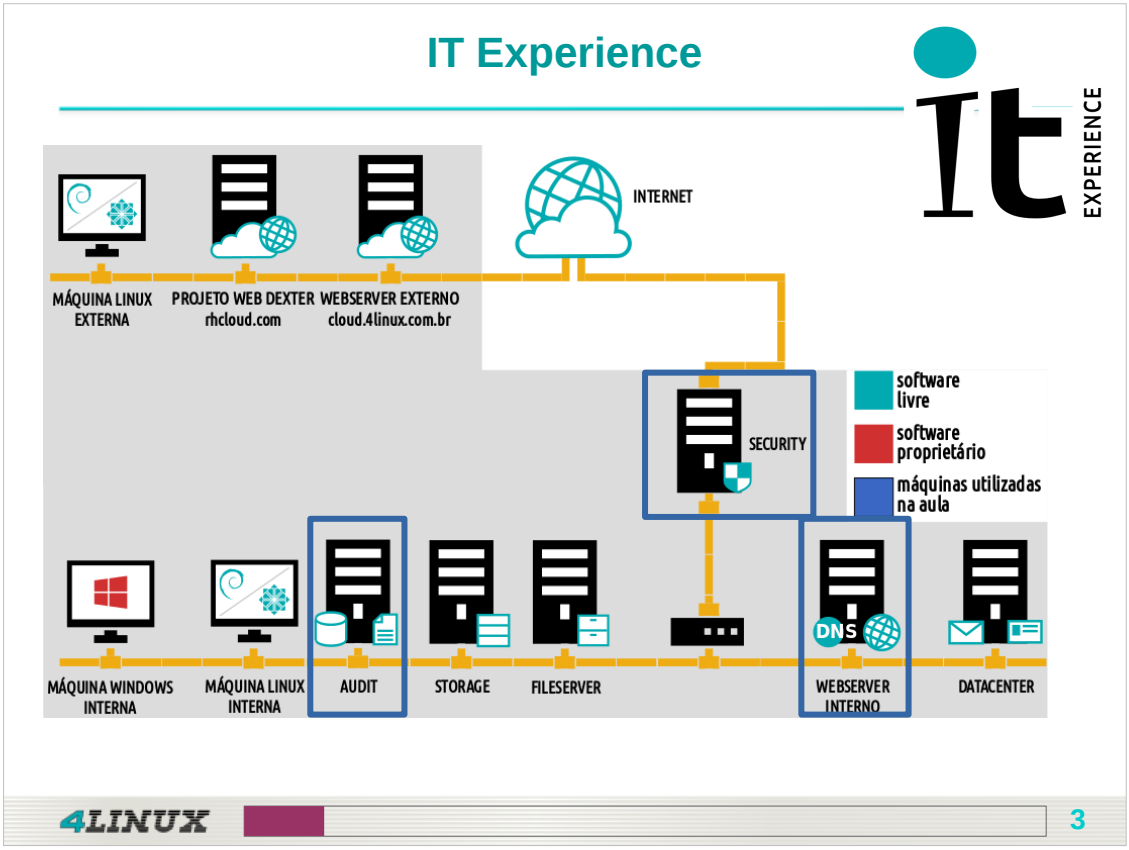


Fundamentação

Durante os anos 70, Arpanet era uma pequena comunidade de algumas centenas de hosts. Um único arquivo, HOSTS.TXT, continha toda a informação necessária sobre os hosts. Este arquivo continha nome para endereçar cada host conectado a ARPANET. O arquivo era mantido pela Network Information Center (NIC) e distribuido por um único host, Stanford Research Institute's Network Information Center (SRI-NIC).

Os administradores da ARPANET enviavam ao NIC, por e-mail, quaisquer mudanças que tivessem sido efeituadas e periodicamente SRI-NIC era atualizado, assim como o arquivo HOSTS.TXT.

As mudanças eram compiladas em um novo HOSTS.TXT uma ou
duas vezes por semana. Com o crescimento da ARPANET, entretanto, este esquema tornou-se inviável. O tamanho do arquivo HOST.TXT crescia na proporção em que crescia o número de hosts. Além disso, o tráfego gerado com o processo de atualização crescia em proporções ainda maiores uma vez que cada host que era incluído não só significava uma linha a mais no arquivo HOST.TXT, mas um outro host atualizando a partir do SRI-NIC.


IT Experience
IT EXPERIENCE
INTERNET
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER rhcloud.com
WEBSERVER EXTERNO cloud.4linux.com.br
SECURITY
software livre
software proprietário
máquinas utilizadas na aula
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
AUDIT
STORAGE
FILESERVER
DNS
WEBSERVER INTERNO
DATACENTER
4LINUX
3

Anotações:

Objetivos da Aula

Aula 02 – Servidor DNS (1/2)

- Introdução a resolução de nomes;
- Executar diagnósticos utilizando servidor DNS externo;
- Implementar na prática um servidor de cache com bind9;
- Implementar na prática um servidor primário com bind9;
- Executar diagnósticos utilizando servidor DNS interno;

Anotações:

Objetivos da Aula

Aula 02 – Servidor DNS (2/2)

- Utilizar ferramenta de gerenciamento do named;
- Implementar na prática um servidor DNS reverso com bind9;
- Implementar na prática um servidor Secundário com bind9;
- Melhorar a segurança no servidor DNS.

Anotações:

Servidor DNS

DNS – Domain Name System:

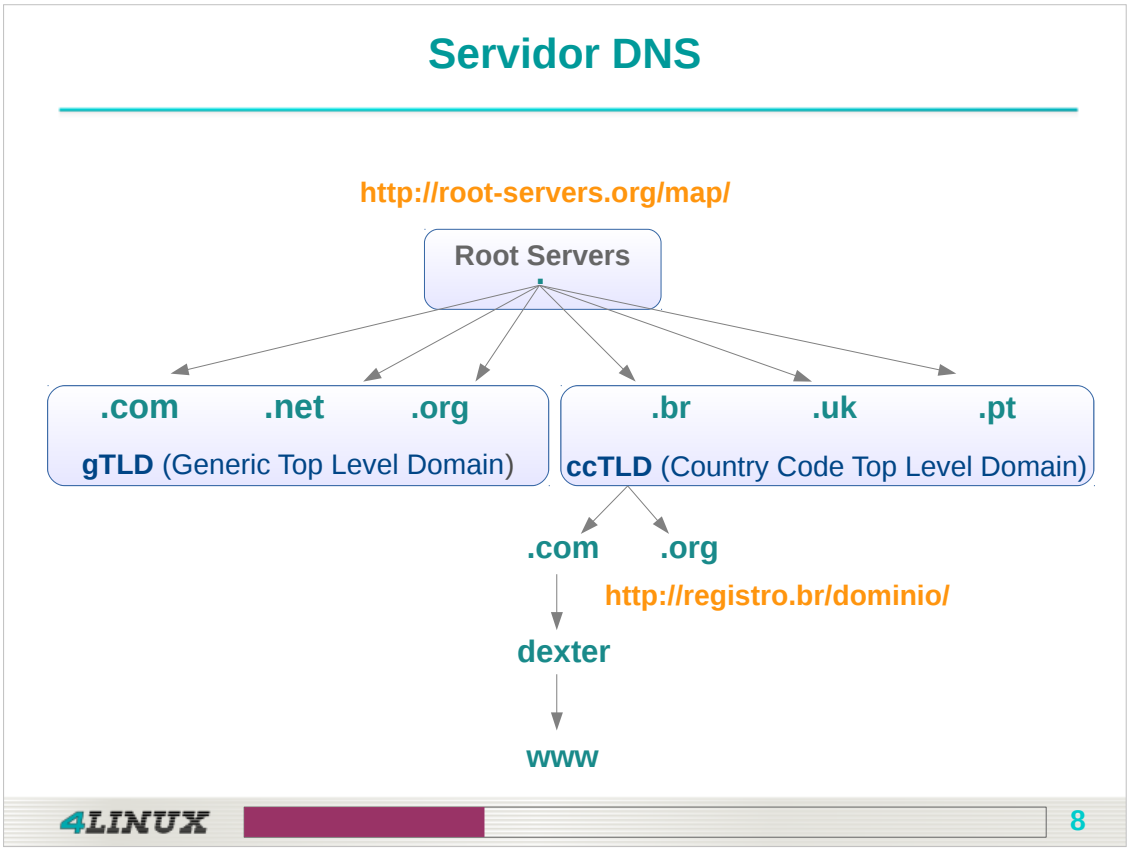
- Responsável pela resolução de Nome para IP e de IP para Nome;
- Criado e mantido pelo ISC (Internet System Consortium), mesmo grupo que mantém DHCP e NTP;
- Eles são divididos em "**gTLD**" (domínios genéricos "com", "edu", "gov", "mil", etc) e "**ccTLD**" (códigos de países ou "country-code", sempre com duas letras);
- A ICANN delega, de acordo com tratados internacionais, a responsabilidade pela administração de um "ccTLD";
- No caso do Brasil, essa responsabilidade pertence atualmente ao "CGI.br", mais especificamente ao "REGISTRO.br";

Anotações:

Servidor DNS

- Dois servidores, o primário e o secundário, devem ter um mecanismo configurado corretamente para que eles se mantenham sincronizados;
- O DNS reverso deve estar configurado;
- O servidor deve trabalhar de forma autoritativa, responsável apenas pelo domínio dexter.com.br;
- Configurar o servidor primário para notificar o secundário quando houver atualização na zona;
- Restringir acesso apenas para a rede interna realizar consulta recursiva;
- Restringir acesso apenas para o servidor secundário realizar transferência de Zona.

Anotações:



Resolução Recursiva

Tomando um navegador web como exemplo, a resolução para acesso a um "website" tem as seguintes etapas:

1.Usuário solicita acesso a "www.exemplo.com.br"

2.Navegador checa se já conhece o endereço IP do "hostname" solicitado (cache do"browser");

3.Se não conhece, o navegador passa a solicitação para a biblioteca de resolução - o "resolver";

4.O "resolver" procura o "hostname" solicitado no arquivo "/etc/hosts" local;

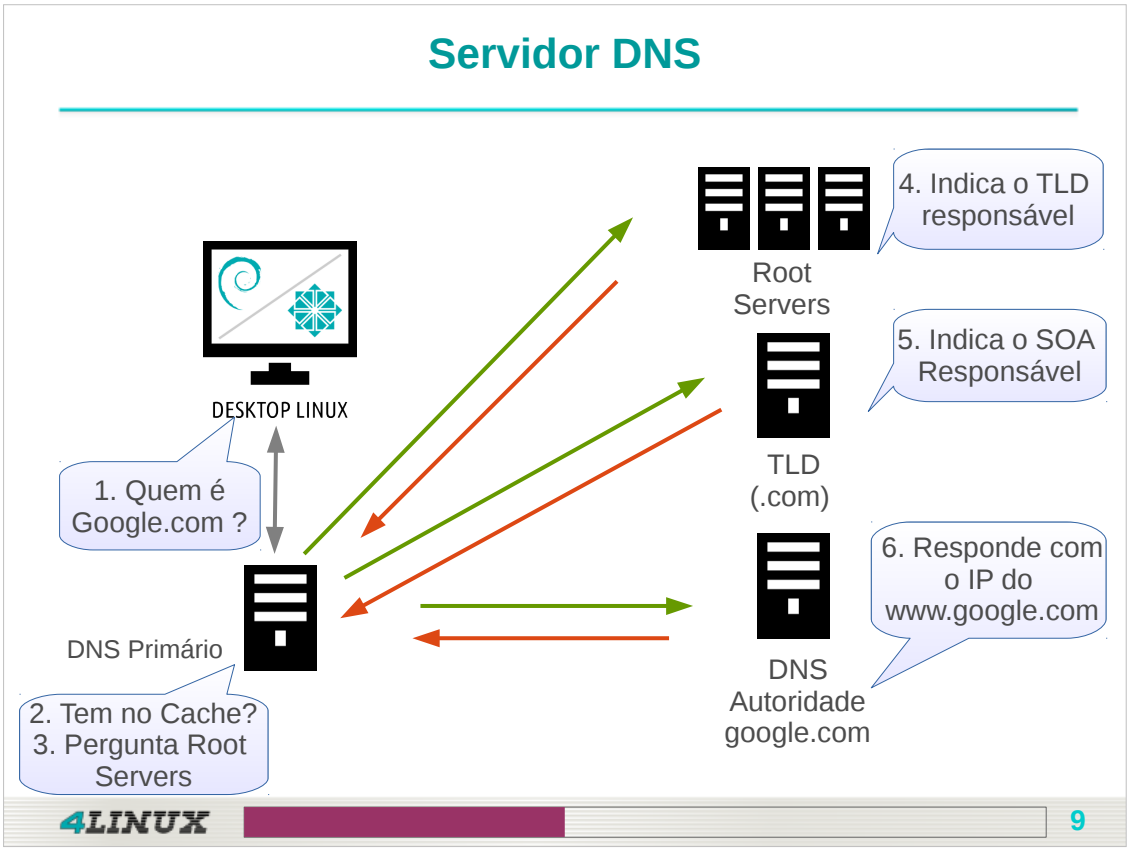
5.Se não encontrar, ele checa o arquivo "/etc/resolv.conf" para saber a quais "name-servers" deve solicitar a informação;

6.O "resolver" repassa a solicitação ao primeiro "nameserver" da lista, e logo após para o próximo até o fim da lista, aguardando por uma resposta de qualquer um deles;

7.O servidor de nomes acionado consulta seu "cache", se houver;

8.Se não encontrar em seu "cache", o servidor em questão vai diretamente ao servidor raiz e transfere a consulta - www.exemplo.com.br;

9.O servidor raiz não faz "cache", e também não é autoridade sobre zonas de baixo nível, então ele apenas responde uma parte da questão: "Não sei quem é, mas sei quem pode responder melhor: br.";



Resolução Recursiva

10.O servidor de nomes reenvia a consulta para o servidor ".br-www.exemplo.com.br;

11.".br" retorna o mesmo tipo de resposta, porém como uma dica mais próxima: "Não sei quem é, mas sei quem pode responder melhor: com.br.";

12. Passos 10 e 11 são efetuados mais uma vez, e agora a resposta é "Não sei quem é, mas sei quem pode responder melhor: exemplo.com.br.";

13. Após repetir o passo 10, finalmente a resposta será da autoridade sobre o domínio exemplo.com.br. Vai ser respondido o IP, juntamente ao TTL do registro, ou será respondido "inexistente";

14.O servidor de nomes fará "cache" da resposta, ao mesmo tempo que a repassa para o resolvedor original;

15.O resolvedor repassa a resposta para o navegador;

16.O navegador inicia uma conexão "HTTP" com o IP descoberto.

Servidor DNS

Tipos de DNS:

DNS AUTORITATIVO → O servidor autoritativo de um domínio possui os registros originais que associam aquele domínio a seu endereço de IP. Tem sua responsabilidade na humanidade;

DNS DE CACHE → Um cache DNS guarda localmente os resultados dessa pesquisa para utilização futura, evitando a repetição de pesquisas e aumentando drasticamente a velocidade de resposta.

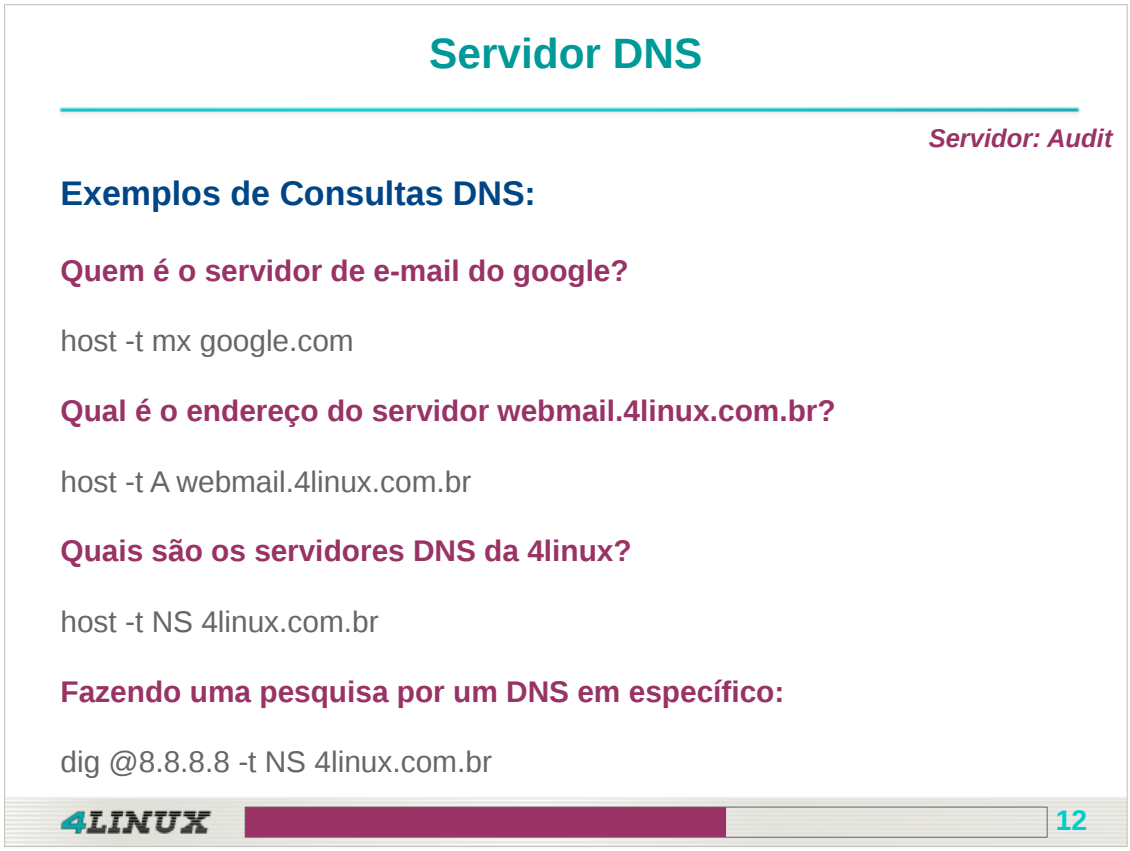
Anotações:

Servidor DNS

Tipos de Registros do DNS:

- **SOA** → Start Of Authotity - Indica onde começa a autoridade da zona;
- **NS** → Name Server - Indica um servidor de nomes para a zona;
- **A** → Address - Mapeamento de nome a endereço (IPv4);
- **AAAA** → Address - Mapeamento de nome a endereço (IPv6);
- **MX** → Mail eXchanger - Indica um servidor de email;
- **CNAME** → Canonical Name (Alias) - Mapeia um nome alternativo (Alias)
- **PTR** → Pointer Record (IP reverso);
- **TXT** → Text – Permite incluir uma entrada de texto curto. Mais usado para SPF.

Anotações:



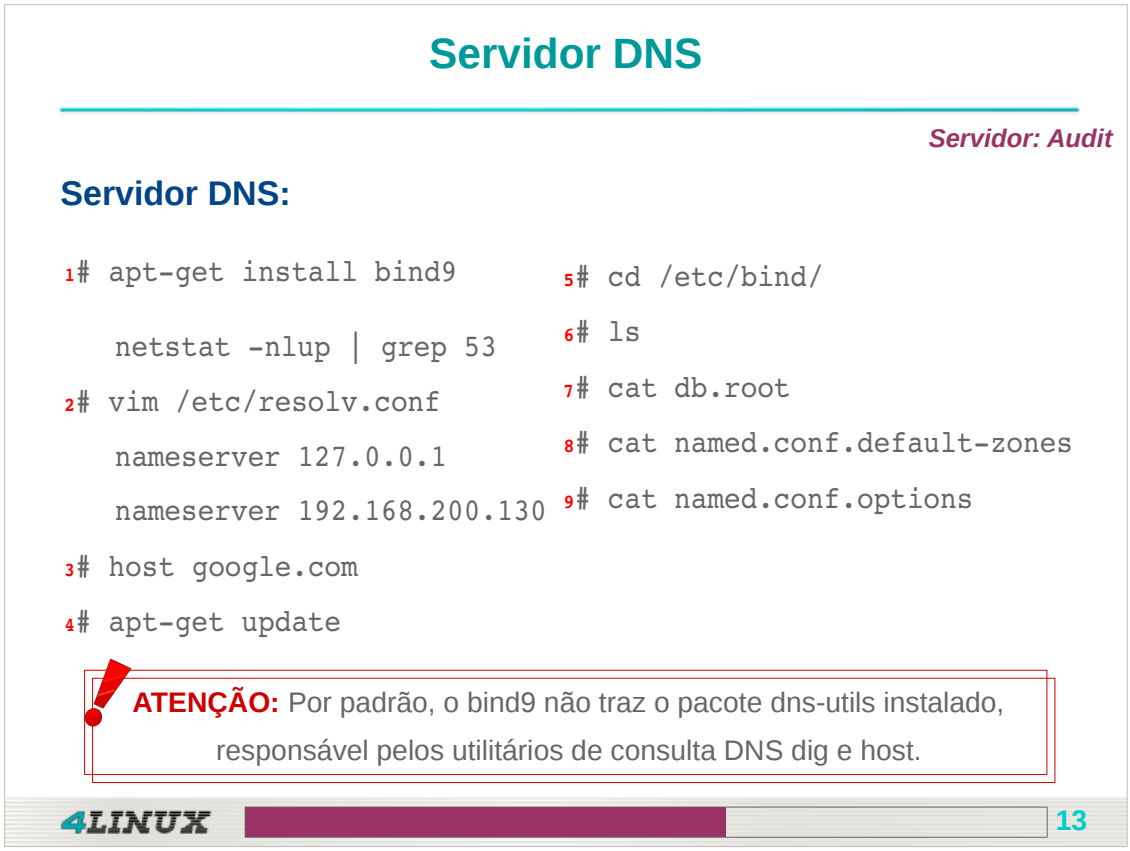
Comando host

O comando "host" é concebido para dar respostas objetivas, limitando-se na maioria dos casos a uma só linha. Repostas detalhadas podem ser obtidas com a utilização de parâmetros. Ao contrário do "dig", o "host" consulta a "search list" do arquivo "/etc/resolv.conf".

Comando dig

O comando "dig" é o acrônimo para "Domain Information Groper", que significa algo como "**aquele que busca por informações de domínio no escuro**", e ao mesmo tempo, a palavra "dig" em inglês significa literalmente "escavar".

O "dig" não utiliza a opção "search" do "/etc/resolv.conf", por isso é necessário utilizar "FQDN" em todas as buscas.

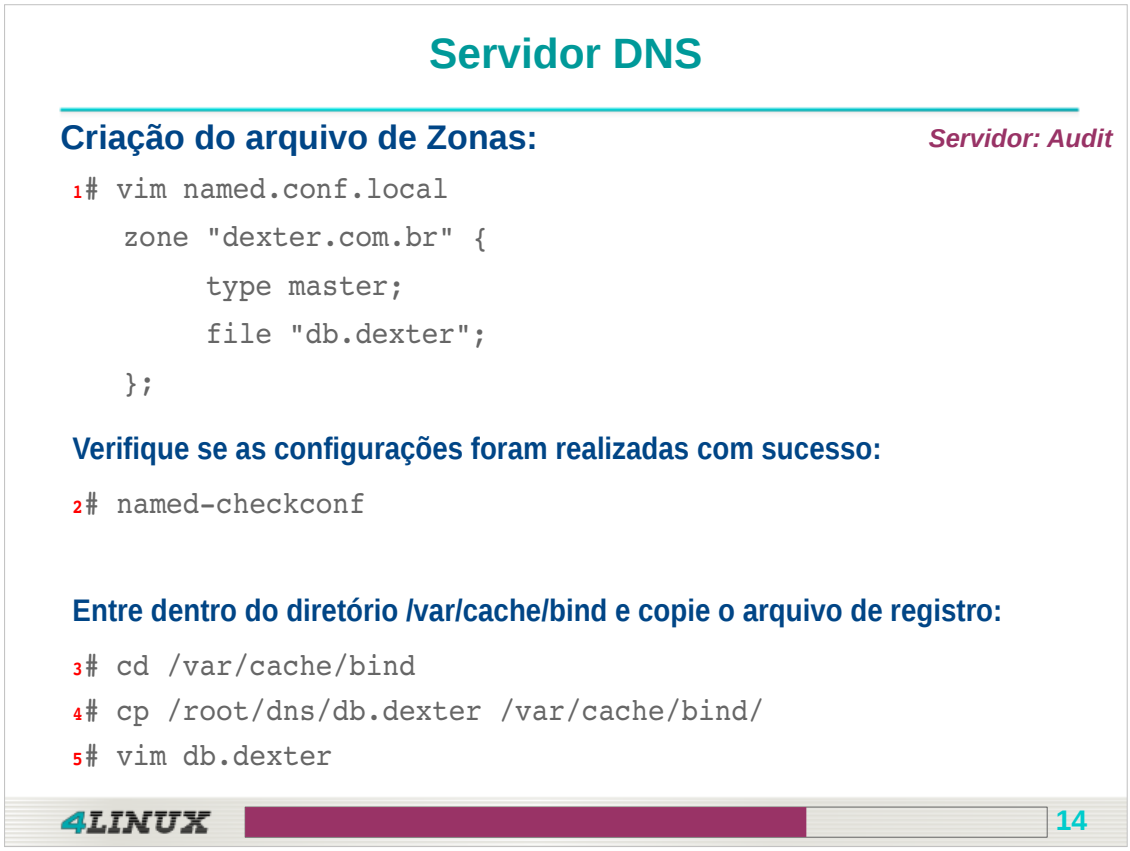


DNS com BIND (Berkeley Internet Name Domain)

O BIND é o servidor de nomes utilizado na grande maioria dos servidores da Internet, provendo uma estável e robusta arquitetura sobre a qual as organizações podem construir sua estrutura de nomes.

O principal arquivo do BIND é o arquivo **"/etc/bind/named.conf".** Esse arquivo utiliza a opção include para anexar os arquivos **"/etc/bind/named.conf.options"** e **"/etc/bind/named.conf.local"**. Sendo que o primeiro usado para personalizar as opções referentes ao funcionamento do próprio "BIND", enquanto o segundo serve para declarar as zonas pelas quais este servidor deve responder.

Completando o time temos o arquivo **"db.root"** (no RedHat localizado em **"/var/named/named.a"**) Este arquivo relaciona os endereços dos 13 servidores raiz e é lido como uma zona do tipo hint conceito a ser estudado em aula.



O "BIND" pode operar de acordo com 6 tipos de zonas:

MASTER → Zona de autoridade sobre o domínio. Os dados da "zona" serão criados, publicados e administrados a partir deste ponto.

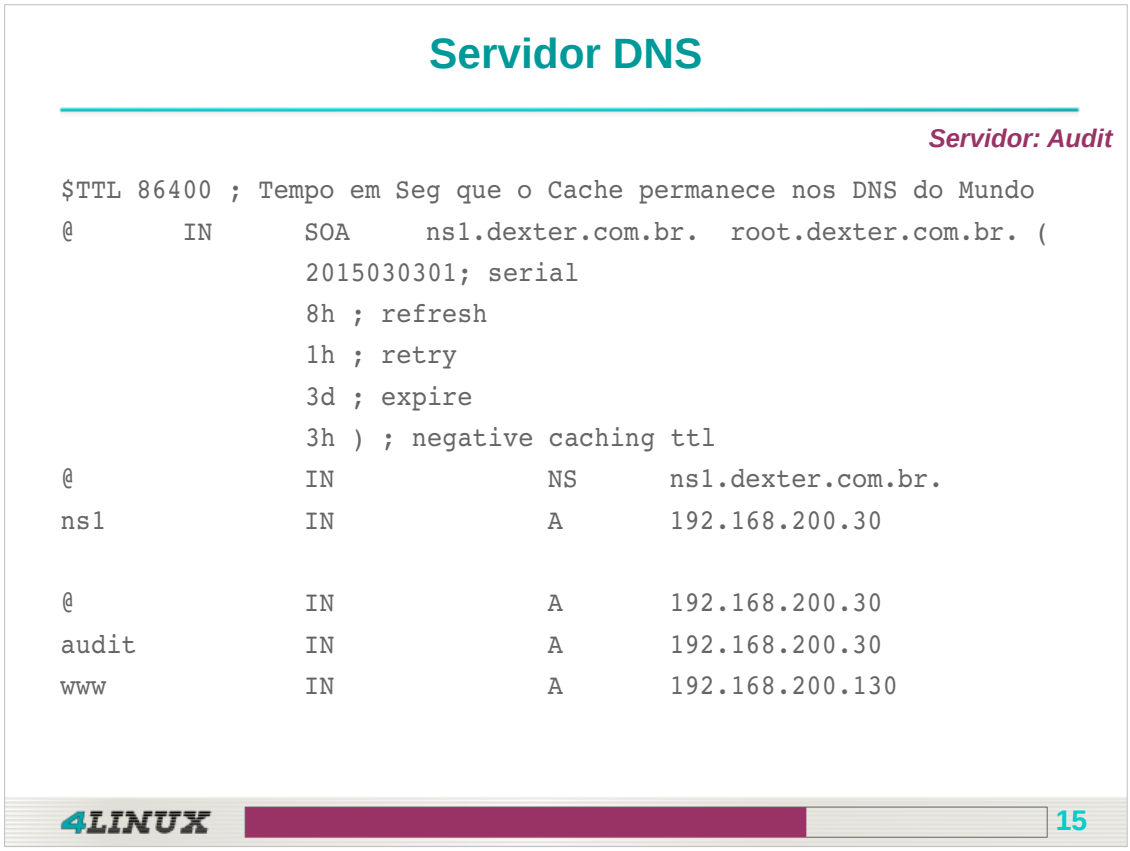
SLAVE → Basicamente uma “cópia” da zona original, nenhuma criação ou alteração respectiva a essa "zona" será feita diretamente neste DNS.

STUB → Tipo de "zona" similar a Slave não é previsto em nenhuma "RFC" foi implementado apenas no "BIND".

HINT → Específica para o "BIND" onde ele deve começar uma busca recursiva quando estiver operando como "cache".

FORWARD → Serve para orientar o "BIND"a encaminhar a consulta sobre uma determinada "zona"para outro servidor em especial.

DELEGATION-ONLY → Utilizada para evitar abusos de algumas autoridades sobre domínios de primeiro.



Informações encontradas em um Registro de Zona

Dono → É o nome do registro. Quando substituído pelo símbolo "@", o dono é o próprio domínio. Caso o dono fique em branco, o "BIND"assume o nome do registro imediatamente superior;

TTL → Um valor, em segundos, para a permanência dos dados deste registro no "cache"de um servidor. Raramente utilizado. classe - Podem ser "CH" (Chaos), "HS" (Hesiod) ou "IN" (Internet).

Tipo → No momento existem mais de 30 tipos de registro, dentre os quais veremos "SOA", "NS", "MX", "A", "CNAME", "TXT" e "PTR".

Serial → É a referência para os "slaves" saberem se a "zona" sofreu alterações;

Servidor DNS

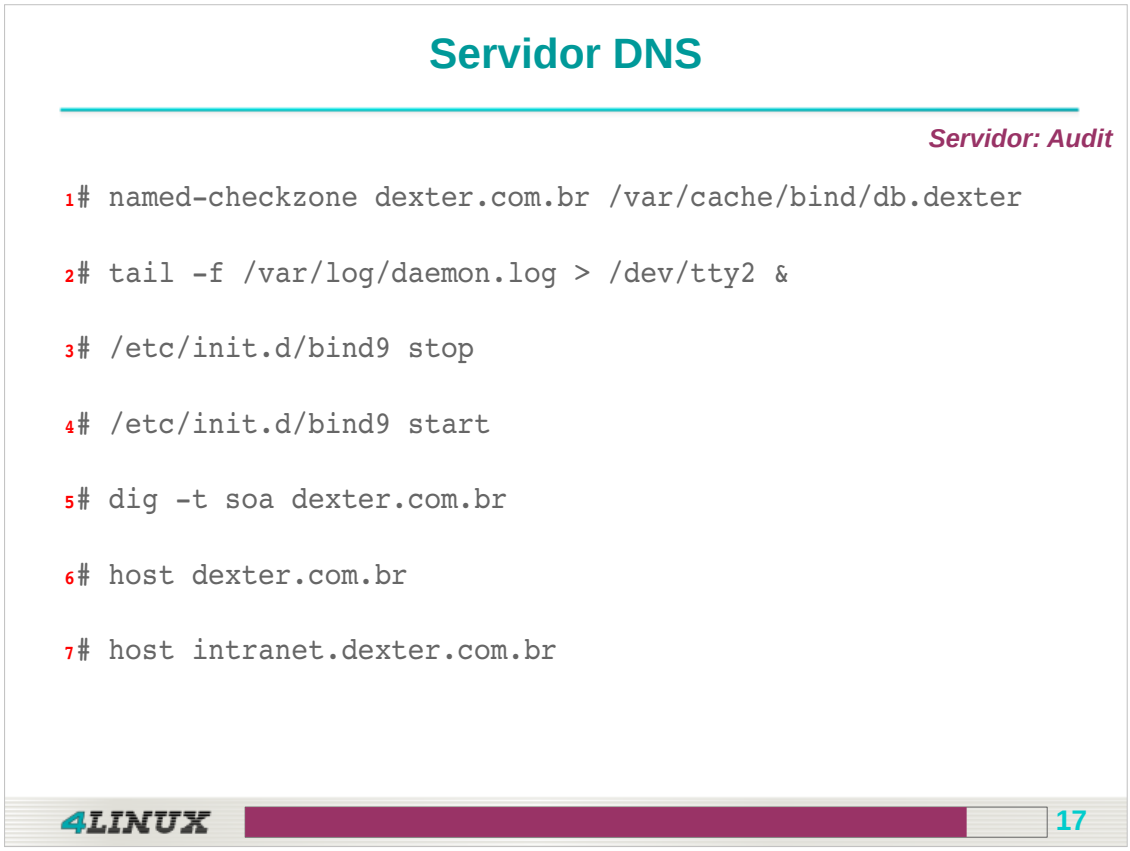
Servidor: Audit

```
intranet        IN              A       192.168.200.130
bkpreport       IN              CNAME   intranet
backup          IN              CNAME   intranet
webmail         IN              CNAME   intranet
sarg            IN              CNAME   intranet
ftp             IN              CNAME   intranet

@               IN              MX      10 mail.dexter.com.br.
mail            IN              A       192.168.200.131
smtp            IN              CNAME   mail
pop             IN              CNAME   mail
imap            IN              CNAME   mail
ldap            IN              CNAME   mail

; Configuração do DNS secundário
;@          IN          NS      ns2.dexter.com.br.
;ns2        IN          A       192.168.200.130
```


Anotações:



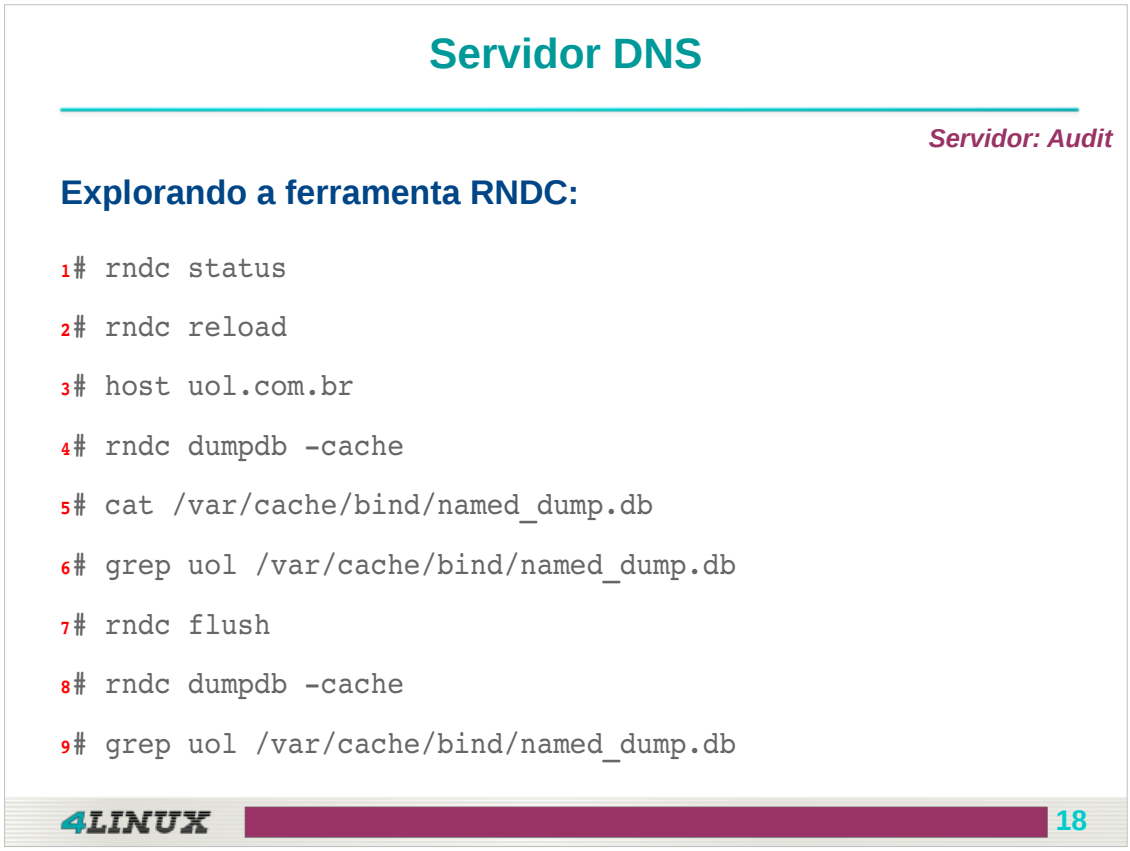
Informações encontradas em um Registro de Zona

Refresh → Tempo que o servidor secundário vai aguardar até checar se há atualizações no servidor primário;

Retry → Em caso de falha do "refresh", o tempo até a próxima verificação;

Expire → O tempo que o secundário aguardará o primário voltar, se esgotar, o secundário para de responder por essa zona;

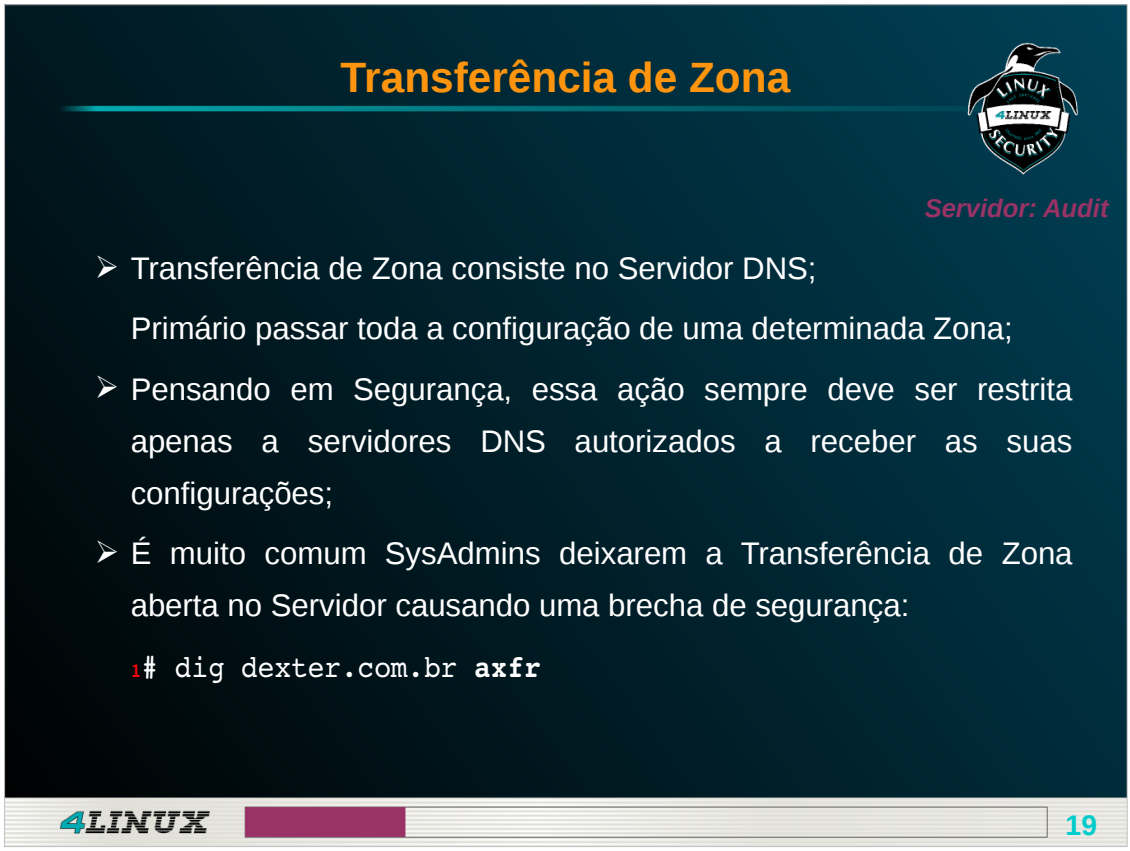
Negative caching TTL → Se a zona expirar, esse será o tempo pelo qual um servidor "cache" armazenará a informação "NXDOMAIN" antes de iniciar uma nova busca recursiva. O máximo são 3 horas.



Utilitário RNDC

O comando rndc (Remote Named Daemon Control) é uma ferramenta de gerenciamento do named.

A vantagem dessa ferramenta é que ela permite controlar o named muito facilmente sem ter que ficar enviando sinais ao processo do mesmo.



Canivete suíço da resolução de Nomes

No "dig" há dezenas de opções e incontáveis combinações entre elas, como o formato acima onde através do dig fizemos uma consulta de zona utilizando mecanismo AXFR (Protocolo para a replicação de dados entre servidores DNS).

Para entender bem o dig consultar o **"man"** e ter um forte domínio do funcionamento do sistema de nomes são itens necessários!

Transferência de Zona

Protegendo seu DNS

Servidor: Audit

```
1# vim /etc/bind/named.conf.local
   zone "dexter.com.br" {
          type master;
          file "db.dexter";
          allow-transfer { 192.168.200.130; };
          notify yes;
          also-notify { 192.168.200.130; };
   };
2# /etc/init.d/bind9 restart
3# dig dexter.com.br axfr
```

allow-transfer Restringir a transferência de zona apenas para Servidores Autorizados;

As opções **notify** e **also-notify** determinam se o servidor primário notifica servidores secundários quando a informação de zona for atualizada.

Anotações:

Servidor DNS

DNS Reverso:

Servidor: Audit

DNS reverso é um recurso que permite que outros servidores verifiquem a autenticidade do seu servidor. Para isso, ele checa se o endereço IP atual bate com o endereço IP informado pelo servidor DNS:

```
1# host mail.dexter.com.br
2# host 192.168.200.131
3# vim /etc/bind/named.conf.local

zone "200.168.192.in-addr.arpa" {
        type master;
        file "rev.dexter";
        allow-transfer { 192.168.200.130; };
        notify yes;
        also-notify { 192.168.200.130; };
};
```

Adicione abaixo da Zona Já exitente.

4LINUX 21

Configurando o DNS reverso

DNS reverso é um recurso que permite que outros servidores verifiquem a autenticidade do seu servidor. Para isso, ele checa se o endereço IP atual bate com o endereço IP informado pelo servidor DNS.

Os servidores de e-mail irão recusar seus e-mails ou classificá-los como spam caso o DNS reverso não esteja configurado.

Servidor DNS

DNS Reverso:

```
1# cp /root/dns/rev.dexter /var/cache/bind/
2# vim /var/cache/bind/rev.dexter
$TTL 86400
@         IN    SOA   ns1.dexter.com.br.
root.dexter.com.br.(
          2015010101; serial
          8h; refresh
          1h; retry
          3d; expire
          3d ); negative cache ttl

@         IN    NS        ns1.dexter.com.br.
ns1                 IN    A           192.168.200.30
131                 IN    PTR         mail.dexter.com.br.
```

Anotações:

Servidor DNS

Servidor: Audit

Checando o DNS Reverso:

```
1# /etc/init.d/bind9 restart
2# host mail.dexter.com.br
   mail.dexter.com.br has address 192.168.200.131
3# host 192.168.200.131
  131.200.168.192.in-addr.arpa domain name pointer
mail.dexter.com.br.200.168.192.in-addr.arpa.
```

Anotações:

Servidor DNS

DNS Secundário:

Servidor: WebServerInterno

Os servidores DNS Secundários ajudam a fornecer equilíbrio de carga e tolerância a falhas. Os servidores DNS secundários mantêm uma cópia somente leitura dos dados da zona transferidos periodicamente do servidor DNS Primário:

```
1# yum install bind bind-utils

2# vim /etc/named.conf
      include "/etc/named.conf.local";
```

Adicionar no final do Arquivo

```
3# vim /etc/resolv.conf
      nameserver 127.0.0.1
      nameserver 192.168.200.30

4# systemctl enable named.service
```

Anotações:

Servidor DNS

DNS Secundário:

Servidor: WebServerInterno

```
1# vim /etc/named.conf.local

zone "dexter.com.br" {
      type slave;
      masters { 192.168.200.30; };
      file "/var/named/slaves/db.slave.dexter";
};
zone "200.168.192.in-addr.arpa" {
      type slave;
      masters { 192.168.200.30; };
      file "/var/named/slaves/rev.slave.dexter";
};

2# systemctl restart named.service
3# ls /var/named/slaves/
```

Hmm ... algum problema

Anotações:

Servidor DNS

Servidor: Security Cloud

Mascaramento no Firewall:

Os servidores DNS não estão conseguindo se comunicar, pois os pacotes estão sendo mascarados pelo firewall ou seja, quando o pacote está indo com destino a Lan interna, o mesmo é mascarado e se perde, não chegando ao destino correto.

Devemos trabalhar com exceções, onde o pacote somente será mascarado se o destino for a **internet** e não as **Lans** internas.

Anotações:

Servidor DNS

Servidor: Security Cloud

Mascaramento no Firewall:

Abra o arquivo de configuração do firewall e edite as regras de mascaramento de ip:

```
1# vim +55 /root/firewall/rules
55 iptables -t nat -A POSTROUTING -s $LAN1 ! -d $LAN2 -j
MASQUERADE
```

Tudo que sair da Lan 192.168.200.0/25 será mascarado **EXCETO** se for com destino a Subnet2

```
56 iptables -t nat -A POSTROUTING -s $LAN2 ! -d $LAN1 -j
MASQUERADE
```

Tudo que sair da Lan 192.168.200.128/25 será mascarado **EXCETO** se for com destino a Subnet1

```
2# service firewall restart
```

Anotações:

Laboratório Dexter

Servidor: Webserver Interno

Validando a transferência de Zona

No servidor Webserver Interno, restarte o bind e verifique se a transferência de zona consegue ser realizada com sucesso:

```
1# systemctl restart named.service
2# ls /var/named/slaves/
```

Transferência de zona realizada com sucesso!

Anotações:

Laboratório Dexter

Servidor: Audit

Validando os Servidores DNS:

Validando o DNS MASTER:

```
1# dig @192.168.200.30 google.com.br
```

Validando o DNS SLAVE:

```
2# dig @192.168.200.130 google.com.br
```

Alguma coisa de errado no arquivo de conf. do servidor DNS Slave.

Encontre qual é o problema e resolva.

Anotações:

Servidor DNS

Servidor: Webserver Interno

Resolvendo o problema no DNS Slave:

```
1# vim /etc/named.conf
   options {
      listen-on port 53 {127.0.0.1; 192.168.200.0/25;
192.168.200.128/25; };
      listen-on-v6 port 53 { ::1;};
      directory "/var/named";
      dump-file “/var/named/data/cache_dump.db”;
      memstatistics-file “/var/named/data/named_stats.txt”;
      allow-query { localhost; 192.168.200.0/25;
192.168.200.128/25; };
};
2# systemctl restart named.service
```

Anotações:

DNS Recursivo

- DNS Recursivo é a funcionalidade que o DNS possui por padrão de realizar consultas para todos os domínios mesmo que ele não seja o servidor autoritativo daquele domínio;
- Para evitar abuso em servidores DNS que ficam disponíveis na internet, é importante limitar a recursividade apenas para redes autorizadas;

```
1# host 8.8.8.8
2# dig @8.8.8.8 -t a uol.com.br
3# host ns1.google.com
4# dig @216.239.32.10 -t a uol.com.br
```


Anotações:

Servidor DNS

DNS Recursivo no DNS Primário:

Servidor: Audit

```
1# vim /etc/bind/named.conf.options
   options {
      directory "/var/cache/bind";
      allow-recursion { 127.0.0.1; 192.168.200.0/25;
192.168.200.128/25; };
      allow-query { 127.0.0.1; 192.168.200.0/25;
192.168.200.128/25; };
      auth-nxdomain no;
      listen-on-v6 { any; };
};

2# /etc/init.d/bind9 restart
```

Anotações:

DICA

Criação de ACL no BIND

- O bind tem uma funcionalidade que é a criação de acls, uma forma de deixar seus arquivos de configuração mais limpos e organizados.

Exemplo de Criação de ACL

```
acl rede_dexter {
      127.0.0.1; 192.168.200.0/25; 192.168.200.128/25;
};

allow-recursion { rede_dexter; };
allow-query { rede_dexter; };
```

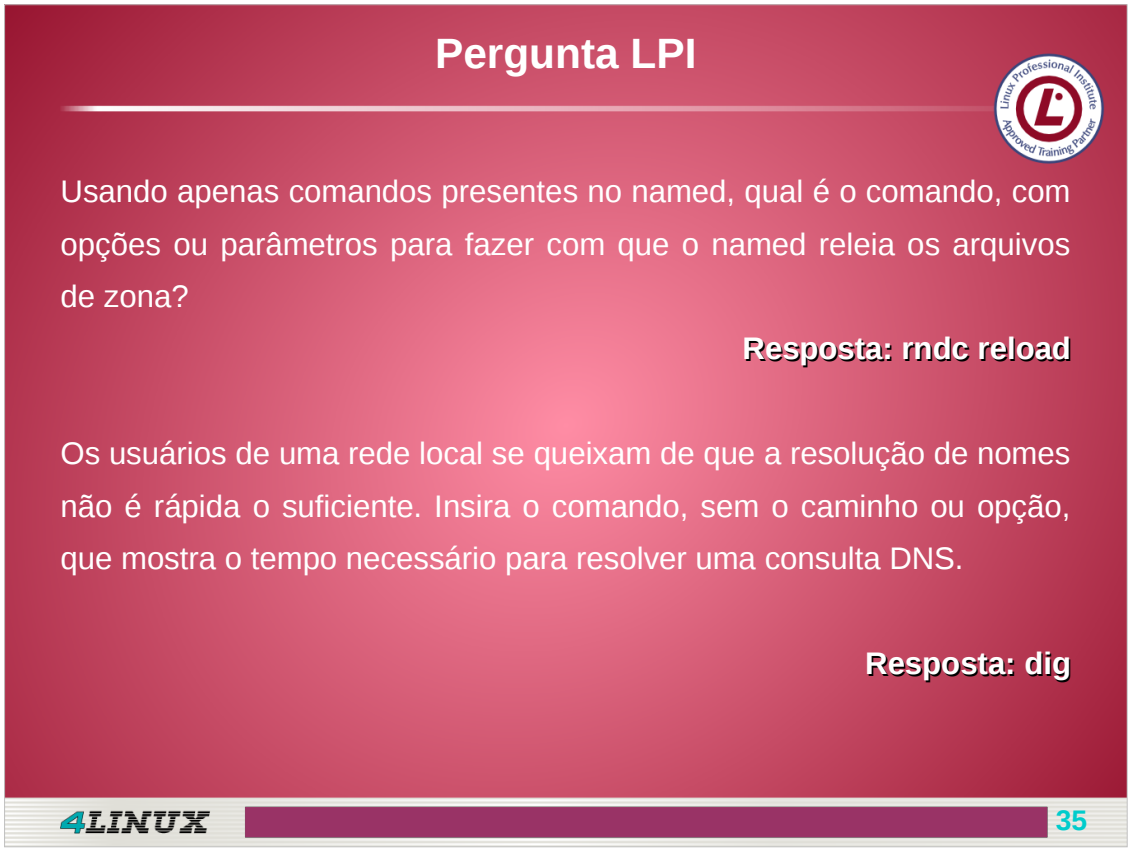
Anotações:

Pergunta LPI

Usando apenas comandos presentes no named, qual é o comando, com opções ou parâmetros para fazer com que o named releia os arquivos de zona?

Os usuários de uma rede local se queixam de que a resolução de nomes não é rápida o suficiente. Insira o comando, sem o caminho ou opção, que mostra o tempo necessário para resolver uma consulta DNS.

Anotações:



REPOSTA CORRETA: rndc reload

Ao efetuar alterações em arquivos de zona utilizamos o comando rndc para forçar a releitura do arquivo de zona acelerando o processo de difusão da informação alterada no daemon do DNS.

REPOSTA CORRETA: dig

O comando **dig** traz entre outras informações uma linha chamada **"Query time"**, aqui encontramos a informação do tempo que foi necessário para a resolução de nomes proposta.

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participes das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!