
Revisão do Tópico 207 – DNS (Domain Name Server)

207.1 – Configuração Básica de um Servidor DNS

Conceitos e Termos Importantes:

- NS (Name Server) : Armazena informações sobre uma parte do Domain Name Space, também chamado de zona.
- Root Domain : Referente ao domínio/zona raiz do DNS, representando pelo . (ponto). Os NSs responsáveis pelo Root Domain são chamados de Root Servers.
- TLD – Top Level Domains : Domínios imediatamente abaixo da raiz (.), por exemplo .com, .br, .net , .org e etc.
- DNS Resolver
  - Software ou biblioteca responsável por fazer a consulta de DNS
  - Utilizado no sistema local (DNS Client) e também é parte do DNS Server
  - Pode armazenar os resultados em cache
- BIND (Berkeley Internet Domain Server)
  - Open Source DNS Server
  - Implementa o protocolo DNS
  - Implementação de DNS Server mais utilizada
- Alternativas ao BIND
  - djbdns - Implementação DNS criada por Daniel J. Bernstein
  - dnsmasq – Combinação leve de um DNS Caching com DHCP
  - PowerDNS – Implementação DNS de grande porte. “Concorrente” do BIND

Tipos de NS:

- Primary (Master) : Servidor que possui autoridade sobre o domínio, definindo todas as informações sobre esta zona de DNS. No registro de um domínio, sempre deve haver ao menos um dos NS como master.
- Secondary (Slave) : O NS Slave transfere para si as informações definidas para um domínio a partir de um NS Master. Dessa forma as informações também ficam armazenadas no servidor e assim também possui autoridade sobre o domínio.

- Caching : O Servidor do tipo caching é capaz de fazer pesquisas recursivas para fazer a resolução DNS e armazena esse resultado em cache.
- Forwarding: Nesse caso o NS encaminha (delega) as pesquisas para outo servidor. Após receber a resposta o resultado também é armazenado em cache.

Arquivos e Diretórios de Configuração

Distribuições baseadas em RedHat seguem o padrão do BIND:

- **/etc/named.conf** : Arquivo de configuração principal
- **/var/named/** : Diretório que armazena os arquivos de zona e outros registros

Distribuições baseadas em Debian armazenam os arquivos de configuração no diretório /etc/bind.

Principais Configurações (seção options):

- listen-on : define a porta e os IPs que vão receber conexões no servidor DNS
  - O DNS utiliza a porta 53 e em geral o protocolo UDP, o protocolo TCP é usado apenas para transferências de zona.
- directory: indica o diretório base do servidor, normalmente o /var/named/
- recursion: indica se o servidor faz ou não pesquisas recursivas (resolução de nomes de outros domínios)

Configurações de um Servidor do tipo Caching-Only

```
zone "." IN {
	type hint;
	file "named.ca";
};
```

Configurações de Logging

Nas configurações de logs do servidor DNS, duas definições são importantes:

- **channel** – Define o local em que o log será registrado e qual nível/severidade será adotado
- **category** – Define o que será logado, indicando-se também o canal (channel) que será utilizado.

Lista de tipos de severidade e categorias: http://www.zytrax.com/books/dns/ch7/logging.html

Exemplo:

```
logging {
	channel ricardo {
		file "data/ricardo.log";
		severity dynamic;
	};
```

```
        category queries {
                ricardo;
        };
};
```

Principais Comandos

- **rndc** – Utilizado para realizar operações no servidor DNS. Principais opções:
  - reload : Recarrega todas as configurações, tanto do named.conf quanto de todas as zonas configuradas
    - reload <dominio> : Recarrega apenas as configurações de um domínio específico
  - reconfig : Recarrega as configurações do named.conf e de novas zonas de DNS criadas
  - flush : Limpa o cache do servidor DNS
  - retransfer <dominio> : Força a transferência de zona de um domínio em um servidor atuando como slave.
- **host** – Faz consultas DNS. Formas de uso:
  - # host www.lpi.org : Utiliza o servidor DNS configurado no ambiente
  - # host www.lpi.org 192.168.1.220 : Utiliza o servidor de DNS 192.168.1.220
  - # host -t MX lpi.org : Obtém o registro do tipo MX do dominiolpi.org
- **dig** – Faz consultas DNS mais elaboradas. Formas de uso:
  - # dig www.lpi.org
  - # dig www.lpi.org @192.168.1.220
  - # dig -t MX lpi.org
- **kill** – Com o sinal 1 (SIGHUP) pode ser utilizado para que o processo do BIND releia todas suas configurações:
  - # kill -1 PID
- **named-checkconf** – Valida a sintaxe das configurações do /etc/named.conf

207.2 – Criar e Manter Zonas de DNS

Domínio do Tipo Master:

No /etc/named.conf:

```
zone "dominioexemplo.com.br" IN {
        type master;
        file "dominioexemplo.zone";
};
```

No arquivo de zona (/var/named/dominioexemplo.zone):

```
$TTL 3h
@       IN      SOA     servidor.dominioexemplo.com.br. admin.dominioexemplo.com.br. (
        2018032801      ; serial. Número utilizado para indicar mudanças na zona
        28800           ; refresh. Após quanto tempo o NS slave deve verificar novamente por atualizações
        7200            ; retry. Em caso de falha no refresh, após quanto tempo deve haver uma retentativa
        2419200         ; expire. Validade das informações. Após quanto tempo as informações não atualizadas do slave deixarão de ser válidas
        150             ; negative caching. Por quanto tempo uma resposta negativa fica em cache
        )
                NS      servidor                ; name server
                MX      5       mailserver      ; mail exchange
servidor        A       192.168.1.5             ; glue record
mailserver      A       192.168.1.10
www             CNAME   servidor
mail            CNAME   mailserver
```

- $TTL – Tempo de vida dos dados no cache de quem obter as informações
- @ indica o nome do domínio indicado no named.conf
- No registro SOA (Start of Authority), o primeiro endereço refere-se ao NS e o segundo ao e-mail do administrador
- O . sempre deve ser utilizado no final da referência ao FQDN (Fully Qualified Domain Name, ou endereço completo). Na falta do . , o BIND inclui o domínio automaticamente
- Os números indicam tempos em segundos, mas também podem ser utilizados **h** (horas), **d** (dias) ou **w** (semanas).
- Glue Record é um registro do tipo A que relaciona o nome do NS do domínio ao seu endereço IP

Principais Tipos de Registros:

- A : Endereço IPv4
- AAAA : Endereço IPv6
- CNAME : Canonical Name (apelido)
- TXT : Texto
- SOA : Start of Authority
- NS : Name Server

- MX : Mail Exchange (Servidor de E-mail). É acompanhado de um número em que quanto menor o valor, maior a prioridade entre os servidores de e-mail.
- PTR : DNS Reverso

Domínio do Tipo Slave

No /etc/named.conf:

```
zone "dominioexemplo.com.br" {
        type slave;
        file "dominioexemplo.com.br.zone";
        masters { 192.168.1.220; };
};
```

- O slave transfere uma nova versão das informações a cada tempo de “refresh” (definido no registro SOA) e sempre que o serial no master for maior que no slave

---

Forwarding

No /etc/named.conf:

Para redirecionar para outro servidor DNS todas as consultas recursivas, deve ser incluída a seguinte configuração na seção “options”:

- forwarders { IP1; IP2; };

Para que o servidor encaminhe tanto as pesquisas recursivas quanto as pesquisas internas a outro servidor, deve ser incluída a configuração:

- forward only;

Para que apenas as consultas referentes a um domínio específico sejam encaminhadas, a zona deve ser criada com o tipo “forward”:

```
zone “dominioexemplo.com.br” IN {
        type forward;
        forwarders { IP1; IP2; };
};
```

DNS Reverso

Possibilita a descoberta de um nome de DNS a partir de um endereço IP.

Configuração no /etc/named.conf:

```
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "1.168.192.in-addr.arpa.zone";
};
```

Arquivo de zona (/var/named/1.168.192.in-addr.arpa.zone)

```
[root@linux-centos named]# cat 1.168.192.in-addr.arpa.zone
$TTL 3h
@       IN      SOA     servidor.dominioexemplo.com.br. admin.dominioexemplo.com.br. (
                        2018032801      ; serial
                        28800           ; refresh
                        7200            ; retry
                        2419200         ; expire
                        150             ; minium
                        )
                NS      servidor.dominioexemplo.com.br.
5       PTR     servidor.dominioexemplo.com.br.
10      IN      PTR     mailserver.dominioexemplo.com.br.
```

```
# host 192.168.1.5
5.1.168.192.in-addr.arpa domain name pointer servidor.prudenciato.com.br.
```

Comandos Relacionados

- **named-checkzone** <dominio> <arquivo-zona> : Verifica a sintaxe do arquivo de zona
  - # named-checkzone dominioexemplo.com.br /var/named/dominioexemplo.zone
- **named-compilezone** : Converte um arquivo de zona slave em formato texto legível
  - # named-compilezone -f raw -F text -o saida.txt exemplo.com.br examplo.zone
- **dig** : Pode ser utilizado para buscar informações referentes à transferência de zonas com o tipo axfr:
  - # dig @192.168.1.220 axfr dominioexemplo.com.br

207.3 – Segurança no Servidor DNS

Considerações Importantes para a Segurança do Serviço

- O serviço BIND deve estar sempre atualizado
- O processo do BIND (named) não pode ser executado pelo usuário root
- Em ambientes críticos o servidor DNS não deve compartilhar o servidor com outros serviços
- Considerar a separação (split) do serviço de DNS de acordo com o cenário. Ter servidores (ou views) diferentes para tipos de requests diferentes, por exemplo Internet e Intranet.

Configurações do named.conf para Segurança

- version “hidden” : Esconder a versão do software
- backhole : IPs/Redes que não serão respondidos pelo servidor
- allow-query : IPs/Redes que podem fazer consultas no servidor
- allow-recursion : IPs/Redes que podem fazer consultas recursivas no servidor
- allow-transfer : IPs/Redes que podem realizar operações de transferência de zonas
- acl : definir grupos de IPs/Redes
- view : Definir grupos de regras e declarações

TSIG – Transaction Signature

Utiliza uma **chave simétrica compartilhada** para aumentar a segurança na **comunicação entre servidores** DNS. Essa chave é utilizada para se **autorizar o acesso** às informações de um servidor. Muito utilizado para proteger a comunicação entre servidores master e slave.

O comando **dnssec-keygen** é utilizado para gerar as chaves. Exemplo:
dnssec-keygen -a HMAC-MD5 -b 256 -r /dev/urandom -n HOST chaves

Exemplo de Configuração no Master:

```
key exemplo {
        algorithm HMAC-MD5;
        secret “xxxxxxxxxxxxx”;
};

allow-transfer { key exemplo; };
```

Exemplo da Configuração no Slave:

```
key exemplo {
        algorithm HMAC-MD5;
        secret “xxxxxxxxxxxxx”;
};

server IP {
        keys { exemplo; };
};
```

DNSSEC (BIND DNS Security Extensions)

Utiliza chaves assimétricas (públicas e privadas) para assegurar a autenticidade e integridade das respostas enviadas pelos servidores DNS.

Através da chave privada uma zona de DNS é assinada e a chave pública possibilita garantir a autenticidade da resposta.

As chaves são geradas pelo comando **dnssec-keygen.** Por exemplo:
dnssec-keygen -a DSA -b 1024 -r /dev/urandom -n ZONE exemplo

O arquivo Kexemplo.+999.+99999.key conterá a chave pública, que deve ser inserida como um registro na zona de DNS.

O arquivo da zona de DNS deve ser assinado com o comando **dnssec-signzone**, utilizando o arquivo de chave privada Kexemplo.+999.+99999.private. Exemplo:
dnssec-signzone -P -r /dev/urandom -o exemplo.com.br exemplo.zone Kexemplo.
+999.+99999.private.

O comando dnssec-signzone gerará um arquivo de zona assinado (exemplo.zone.signed), que deve ser configurado no /etc/named.conf.

DANE (DNS -Based Authentication of Named Entities)

Solução criada para resolver o problema dos CAs (Certification Authorities), criando uma forma de associar um domínio a um CA específico através de um registro do tipo TLSA inserido dentro do arquivo de zona.

Enjaulamento de DNS (chroot jail)

Forma de executar o serviço de DNS em um ambiente isolado do resto do servidor, impedindo que brechas no serviço impactem a segurança do servidor como um todo.

Na prática, é criado um novo / exclusivo para o BIND, por isso chroot. Nessa nova raiz são instalados, criados e copiados todos os arquivos e diretórios utilizados pelo BIND, incluindo arquivos do /etc/, /lib, /sbin, /var/run e etc, em uma nova estrutura completa.

Na execução do processo bind, deve ser utilizada a opção -t para definir o diretório chroot, por exemplo:
named -u bind -t /chroot/