Curso de Pós-Graduação em Redes de Computadores

Módulo Laboratório de Linux – Apostila 2

Serviço DNS

Introdução

DNS é o Servidor de Nomes do Domínio. Ele converte os nomes das máquinas para números IP, que são os endereços das máquinas, mapeando de nome para endereço e de endereço para nome.

O serviço de nomes no Linux é feito por um programa servidor denominado `named`. Ele é integrante do pacote Bind, cuja versão utilizada nesse documento é a 9. Esse servidor de nomes está incluído na maioria das distribuições Linux e é usualmente instalado como `/usr/sbin/named`.

O principal arquivo de configuração do Bind é o arquivo "named.conf". Esse arquivo geralmente está localizado em /etc/named.conf. É nele onde estão definidas as zonas (dominios) e o local onde estão os mapeamentos de cada zona.

Em algumas distribuições de Linux podem existir também os arquivos "named.conf.options" e "named.conf.local". Esses são na verdade apenas uma outra forma de organização das configurações do Bind. O conteúdo desses arquivos, por exemplo, poderia ser todo escrito sem problemas no arquivo "named.conf". A vantagem desse tipo de estrutura é que há uma melhor organização dos dados e, consequentemente isso facilita a manutenção e administração do sistema: o administrador pode, por exemplo, colocar o campo "options" separado no arquivo "named.conf.options" e as definições de zonas locais no arquivo "named.conf.local".

Este documento utiliza a distribuição Fedora 3, a qual utiliza somente o arquivo named.conf para as configurações do Bind. A seguir, uma descrição do arquivo "named.conf" e dos arquivos de mapeamento.

Configuração do Bind

Uma vez instalado o pacote Bind, será gerado o arquivo "named.conf" com o seguinte conteúdo:

```
// Default named.conf generated by install of bind-9.2.4-2
options {
        directory "/var/named";
```

```
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
};
include "/etc/rndc.key";
```

Esse arquivo contêm apenas o campo “options”. Não há definições de zonas ainda. Elas serão criadas no decorrer dessa seção.

A primeira linha é um comentário. Para criar um comentário, basta colocar // no começo da linha.

A linha 'directory' indica onde os arquivos de mapeamento das zonas e outras configurações devem estar localizados. Todos os arquivos subseqüentes serão relativos a este.

A linha 'dump-file' define onde estará o arquivo de cache.

A linha 'statistics-file' define onde estará o arquivo de estátisticas.

A linha 'include' inclui o arquivo '/etc/rndc.key' Observe que essa linha não faz parte do campo de options.

No campo ' optins' serão acrescentadas as linhas:

```
forwarders {
  <ip_dns_externo>;
};
```

Essas linhas indicam que o servidor dns repassará requisições para o servidor de ip <ip_dns_externo> caso essas não possam ser resolvidas. Desse modo, <ip_dns_externo> deve ser substituido pelo endereço ip do servidor de dns externo. O arquivo “named.conf” ficará então:

```
// Default named.conf generated by install of bind-9.2.4-2
options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        forwarders {
                <ip_dns_externo>;
        };
};
include "/etc/rndc.key";
```

O próximo passo é criar a zona “.” :

```
zone "." {
        type hint;
```

```
        file "data/db.root";
};
```

Essa zona define a raiz do dns. O arquivo 'db.root' descreve o nome dos servidores raiz no mundo. O conteúdo desse arquivo pode mudar com o passar do tempo e *tem que* ser atualizado permanentemente.

Entretanto, o arquivo 'db.root' ainda tem que ser criado. A maneira mais fácil de se fazer isso é usar o utilitário dig, o qual deve ser executado inicialmente sem argumentos, gerando um db.root adequado ao servidor. A seguir deve ser perguntado a um dos servidores relacionados o seguinte:

$ dig @rootserver.

A saida gerada por esse comando é exatamente o que o arquivo 'db.root' deve conter. Desse modo é possível atualizar esse arquivo através de uma simples consulta dns. Para gerar o arquivo 'db.root' execute dentro do diretório /var/named/data o comando:

$dig @e.root-servers.net . ns >db.root"

Esse comando redireciona a saida do comando dig para o arquivo db.root, criando desse modo o arquivo de que necessitamos.

A próxima zona a ser criada é "localhost":

```
zone "localhost" {
        type master;
        file "data/db.local";
};
```

Isto nos diz que podemos definir uma zona "localhost" na qual nos somos os servidores principais (type master) e que as informações estão guardadas em um arquivo chamado "data/db.local". O arquivo 'db.local' deve estar no diretório "/var/named/data/". Seu conteudo é:

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                1               ; Serial
                604800          ; Refresh
                        86400           ; Retry
                2419200         ; Expire
                        604800 )        ; Negative Cache TTL
;
@       IN      NS      localhost.
```

```
        @       IN      A       127.0.0.1
```

Nesse arquivo, as linhas que começam com ' ' são comentários. Este 'arquivo de zona ' contém 3 'registros de recursos' (RRs): SOA, NS, A. SOA é a contração para Início de Autoridade. O ` @' é uma observação especial que significa origem e desde que a coluna do campo para este arquivo diz localhost, a primeira linha realmente quer dizer

```
localhost.    IN      SOA ...
```

NS é o nome do servidor RR. Assim na linha NS se lê

```
localhost.    IN      NS      localhost.
```

Indicando ao DNS que a máquina é o servidor de nomes do domínio `localhost` é chamada `localhost`.

A linha

```
@   IN      A       127.0.0.1
```

indica que localhost. tem um ip mapeado em 127.0.0.1.

A linha com o comentário '; Serial' é um numero usado pelo servidor de dns secundários para saber se o servidor primário sofreu alterações. O servidor aqui configurado é primário e admite-se que não há servidores secundários.

' Refresh': intervalo de tempo dado em segundos que o servidor secundário leva para verificar, através do serial, se houve atualização das informações no primário.

' Retry': tempo dado em segundos que o servidor secundário leva para fazer nova consulta por atualização ao primário caso a primeira tentativa falhe.

' Expire' tempo dado em segundos que o servidor secundário leva para parar de responder a consultas feitas a zona em questão. Caso esse tempo seja atingido, a zona expira.

' Negative Cache TTL' :TTL significa ' Time To Live' (tempo de vida). É o tempo que deve ser esperado por um cliente para uma nova consulta caso receba uma resposta negativa do servidor de nomes.

O próximo passo é criar uma zona reversa para o dominio "localhost" já criado anteriormante. Para isso, basta acresentar as linhas no arquivo 'named.conf' :

```
zone "127.in-addr.arpa" {
        type master;
        file "data/db.127";
};
```

Uma zona reversa mapeia ips para nomes. O modo como se define uma zona reversa será melhor explicado na criação da zona da rede local. O arquivo db.127 segue abaixo:

```
;
; BIND reverse data file for local loopback interface
;
```

```
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                  1             ; Serial
             604800         ; Refresh
                    86400           ; Retry
             2419200        ; Expire
                    604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
```

Nesse arquivo há um novo tipo de RR: PTR. Do mesmo jeito que o registro A, PTR significa que o ip 1.0.0 possui um nome e esse nome é localhost.

Pode-se agora criar um domínio próprio. Como exemplo, nós iremos criar a zona "genevix.inf.ufes.br":

```
zone "genevix.inf.ufes.br" {
        type master;
        file "data/genevix.inf.ufes.br";
};
```

O arquivo "genevix.inf.ufes.br" segue abaixo:

```
$TTL 86400

@       IN      SOA     ns1.genevix.inf.ufes.br.      root.ns1.genevix.inf.ufes.br. (
             2005013001      ; serial number YYMMDDNN
             28800          ; Refresh
             7200           ; Retry
             864000         ; Expire
             86400          ; Min TTL

                                    )

genevix.inf.ufes.br.    IN      NS      ns1.genevix.inf.ufes.br.
tetris                  IN          A       192.168.0.1
```

```
ns1             IN      A       192.168.0.1
arkanoid        IN      A       192.168.0.2
doom            IN      A       192.168.0.3
pitfall         IN      A       192.168.0.4
pimball         IN      A       192.168.0.5
lemmings        IN      A       192.168.0.6
```

Uma coisa que não foi comentada até agora: no registro SOA, "root.ns1.genevix.inf.ufes.br." pode ser entendido como "root@ns1.genevix.inf.ufes.br.". Esse é o endereço de e-mail do administrador do serviço. Atenção para o uso de '.' no lugar de '@'.

Como se pode ver no arquivo acima, existem 5 máquinas no subdomínio genevix.inf.ufes.br mais o próprio servidor de dns e essas máquinas estão na rede 192.168.0.0/24.

Como passo final, falta apenas configurar o reverso para o domínio genevix.inf.ufes.br. Isso é feito acrescentando-se as linhas abaixo em "named.conf":

```
zone "0.168.192.in-addr.arpa" {
        type master;
        file "192.168.0.genevix.inf.ufes.br";
};
```

Observe como a zona é nomeada. Primeiramente, tem-se o ip que caracteriza o subdomínio genevix.inf.ufes.br (0.168.192) seguido então de ".in-addr.arpa". Isso também foi seguido na nomeação da zona reversa de localhost. O 'arpa' na verdade é um domínio e 'in-addr' é seu subdomínio. Do mesmo modo '192' está abaixo de 'in-addr'. Desse modo, o servidor de dns realiza consultas reversas do mesmo modo que faria numa consulta à zona genevix.inf.ufes.br. Para finalizar, o arquivo "192.168.0.genevix.inf.ufes.br":

```
$TTL 86400

@       IN      SOA     ns1.genevix.inf.ufes.br.      root.ns1.genevix.inf.ufes.br. (
          2005013001; serial number YYMMDDNN
          28800; Refresh
          7200; Retry
          864000; Expire
          86400; Min TTL
          )
```

```
@     IN    NS     ns1.genevix.inf.ufes.br.
1     IN          PTR    tetris.genevix.inf.ufes.br.
2     IN          PTR    arkanoid.genevix.inf.ufes.br.
3     IN          PTR    doom.genevix.inf.ufes.br.
4     IN          PTR    pitfall.genevix.inf.ufes.br.
5     IN          PTR    pimball.genevix.inf.ufes.br.
6     IN          PTR    lemmings.genevix.inf.ufes.br.
```

Isso encerra a configuração do Bind. Existem muitos outros recursos que podem ser utilizados, mas que fogem ao escopo desse curso. Para maiores informações, favor visitar:

http://www.isc.org

Ou então consultar o livro “DNS and BIND, 4Th Edition – O'Reilly”

Configuração dos Clientes

A configuração dos clientes é feita no arquivo “/etc/resolv.conf”. Basta acrescentar nesse arquivo a linha:

nameserver <ip_dns_server_1> <ip_dns_server_2>