****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.

**Licença**



Esta licença permite que outros remixem, adapte, e criem obras derivadas sobre a obra original, desde que com fins não comerciais e contanto que atribuam crédito ao autor e licenciem as novas criações sob os mesmos parâmetros. Outros podem fazer download ou redistribuir a obra da mesma forma que na licença anterior, mas eles também podem traduzir, fazer remixes e elaborar novas histórias com base na obra original. Toda nova obra feita a partir desta deverá ser licenciada com a mesma licença, de modo que qualquer obra derivada, por natureza, não poderá ser usada para fins comerciais.

This license lets other remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.

Para maiores informações sobre o método de licenciamento acesse os seguintes sites:

Brasil:

<http://creativecommons.org.br/as-licencas/>

<http://creativecommons.org/licenses/by-nc-sa/3.0/br/>

Internacional:

<http://creativecommons.org/licenses/by-nc-sa/3.0/>

<http://creativecommons.org/licenses/by-nc-sa/3.0/legalcode>

**1 – Configurando o BIND DNS no Linux**

Agora iremos configurar o **BIND DNS** em partes para que possamos de forma organizada estruturar este documento.

**2 – Configuração do RNDC (Remote Named Daemon Control) no Linux**

O **RNDC** é um utilitário que controla as operações do **Servidor BIND**. O **RNDC** comunica com o **Servidor BIND** através de uma conexão **TCP**, opcional enviando os comandos autenticados com assinatura digital.

**Observação:** Devemos parar o serviço do **BIND**, caso ele esteja em execução para configurarmos o utilitário **RNDC**.

**2.1 – Gerando o Arquivo /etc/named/rndc.conf com o rndc-confgen**

Precisamos criar o arquivo ***/etc/named/rndc.conf***, onde serão armazenadas as assinaturas digitais geradas aleatoriamente, para isso execute:

dns-fusion:/# rndc-confgen -a -A hmac-sha512 -c /etc/named/rndc.conf -k rndc.key -b 512

wrote key file "/etc/named/rndc.conf"

dns-fusion:/#

Onde as opções do utilitário **rndc-confgen** são:

* **-a** 🡪 Configuração do **RNDC** automaticamente.
* **-A <Algoritimo>🡪** Aqui especificamos o algoritmo de criptografia que iremos utilizar para o **TSIG**. As possibilidades são: **hmac-md5**, **hmac-sha1**, **hmac-sha224**, **hmac-sha256**, **hmac-sha384** e **hmac-sha512**. Se não especificado o padrão será o **hmac-md5**.
* **-b <tamanho>** 🡪 Especifica o tamanho da chave de autenticação em bits. O tamanho da chave deve ter um tamanho de **1** a **512 bits**. Por padrão é o tamanho do **hash (128 bits)**. É recomendado que seja utilizado um tamanho superior a **256 bits** se o seu **Servidor BIND** for usado fora da rede local.
* **-c <arquivo>** 🡪 É utilizado com a opção **–a** para especificar um lugar alternativo para a localização do arquivo ***rndc.conf***.
* **-k <nome>** 🡪 Especifica o nome da assinatura digital que será gerado. O padrão é ***rndc.key.*** É altamente recomendado alterar o nome da assinatura digital quando você quiser utilizar o **RNDC** para acessar um **Servidor BIND** em outra máquina.
* **-p <porta>** 🡪 Especifica uma porta **TCP** para comunicação com o **named**, está porta ficará na escuta aguardando os comandos **RNDC**. Por padrão é a **953/TCP**.
* **-s <endereço>** 🡪 Especifica um endereço IP onde o **named** ficará na escuta para conexão com o **RNDC**. Por padrão o IP é o de **Loopback 127.0.0.1**.
* **-t <dir chroot>** 🡪 Usado com a opção **–a** para especificar um diretório onde o **named** será executado como um daemon dentro de uma **Jail**.
* **-u <user>** 🡪 Usado com a opção **–a** para indicar um proprietário do arquivo ***rndc.key*** gerado.

**2.2 – Configurando o Arquivo /etc/named/rndc.conf**

Este é o arquivo de configuração do **RNDC**, que é a ferramenta de controle do **BIND9** e substitui o **NDC**, que era a ferramenta de controle das versões anteriores do **BIND**. Sua principal função é fornecer uma chave secreta para o funcionamento do **RNDC**. Uma cópia dessa chave deve estar nos arquivos ***/etc/named/named.conf*** e ***/etc/named/rndc.key*** (dependendo da configuração) para que o **BIND** inicialize.

dns-fusion:/# cat /etc/named/rndc.conf > /etc/named/rndc.key

dns-fusion:/# cat /etc/named/rndc.conf > /etc/named/named.conf

dns-fusion:/#

Agora iremos configurar o **RNDC** acrescentando os blocos ***options*** e ***Server***:

dns-fusion:/# vi /etc/named/rndc.conf

options {

default-key "rndc.key";

default-server 127.0.0.1;

};

server localhost {

key "rndc.key";

};

key "rndc.key" {

algorithm hmac-sha512;

secret "HEHTs9psYldIA9UEOsfW9NxE8ZvV8WuQxEDnZ+eaRIXPWyW2uiNHxYU3P/AJeMAFS3CxFx3wEtcm20rEevs7wQ==";

};

"/etc/named/rndc.conf" 13L, 250C written

dns-fusion:/#

**2.3 – Configurando o Arquivo /etc/named/rndc.key**

Este é um arquivo onde temos a cópia da chave secreta que o **RNDC** usa para controlar o **BIND**. Esse arquivo é utilizado, se o arquivo ***/etc/named/named.conf*** não possui a chave. Neste caso é necessário colocar a diretiva ***include “/etc/named/rndc.key”*** no arquivo ***/etc/named/named.conf***.

Um exemplo do arquivo ***/etc/named/rndc.key***:

dns-fusion:/# cat /etc/named/rndc.key

key "rndc.key" {

algorithm hmac-sha512;

secret "HEHTs9psYldIA9UEOsfW9NxE8ZvV8WuQxEDnZ+eaRIXPWyW2uiNHxYU3P/AJeMAFS3CxFx3wEtcm20rEevs7wQ==";

};

dns-fusion:/#

Observação: Caso você esteja utilizando os pacotes pré-compilados do BIND, ele gera a chave e a configuração automaticamente. Então para não dar erro de acesso ao arquivo de chave você deve alterar o dono e as permissões para o usuário do BIND, como podemo ver no exemplo abaixo:

dns-fusion:/# chown root:bind /etc/bind/rndc.key

dns-fusion:/# chmod 640 /etc/bind/rndc.key

dns-fusion:/#

Com os arquivos instalados vem o momento da configuração de várias diretivas do software. O

**3 – Configuração do BIND no Linux**

**3.1 – Configurando o Arquivo /etc/named/named.conf**

Com os arquivos instalados vem o momento da configuração de várias diretivas do software. O arquivo de configuração é o ***named.conf*** e deve ser criado no diretório especificado no momento da compilação (***--sysconfdir=DIR***), no nosso caso ***/etc/named***.

Neste exemplo que segue iremos mostrar as configurações vitais de um **Servidor DNS**, **logging**, **zonas**, **servidores slaves** (secundários), **diretivas de segurança** entre **outros**.

**Observação:** Algumas diretivas são, nesta versão, obrigatórias e precisam ser configuradas para que o servidor possa ser iniciado, são elas:

* **$TTL** 🡪 Cada arquivo de zona deve conter essa diretiva. Usado como padrão para todos os registros que não possuem **TTL** especificado. Deve constar na primeira linha do arquivo de zona.
* **SOA (com o Serial Number)**🡪O Número serial deve ser um valor inteiro (**Integer**). Versões anteriores a **BIND9** permite usar o número serial como este: “**3.002**”.

**3.1.1 – Configurando ACL em /etc/named/named.conf**

Com as **ACL (Access Control Lists)** podemos criar lista de endereços IP e designarmos nomes a essas listas, com o único objetivo de quando formos nos referir a endereços IP usarmos nomes em vez de números. Algumas **ACL** já existem e podem ser usadas:

* **any** 🡪 Todos os hosts.
* **none** 🡪 Nenhum host.
* **localhosts** 🡪 Todos os endereços IP das interfaces do **Servidor DNS**.
* **localnets** 🡪 A rede inteira a qual o **Servidor DNS** faz parte.



**Observação:** O arquivo de configuração no **Debian** fica em ***/etc/bind/named.conf***, e nas distribuições **Red Hat** e **Suse** ficam em ***/etc***. No **Debian** o arquivo de configuração é dividido em quatro, sendo o ***named.conf*** o principal e três includes para ***named.conf.options*** onde são configurado todas as opções referente ao funcionamento do **BIND**, ***named.conf.local*** que serve para declarar todas as zonas pelas quais este servidor deve responder, e ***named.conf.default-zones*** onde estão as zonas padrões como **Loopback** e **Root Servers**.

Por exemplo:

dns-fusion:/# vi /etc/named/named.conf

acl srv\_slaves {

192.168.5.129/32;

192.168.130/32;

};

acl net\_how2security {

192.168.5.0/24;

};

"/etc/named/named.conf" 13L, 245C written

dns-fusion:/#

**3.1.2 – Configurando OPTIONS em /etc/named/named.conf**

A diretiva **options** define as opções globais que influenciam a operação do **BIND** e do **Protocolo** **DNS**.

Por exemplo:

options {

directory "/var/named/db/master";

listen-on { 127.0.0.1; 192.168.5.128; };

listen-on-v6 { none; };

empty-zones-enable no;

allow-transfer { srv\_slaves; };

allow-recursion { net\_how2security; };

allow-query { any; };

};

Onde:

* **directory <”caminho”>;** 🡪 A opção **directory** indica o diretório onde são armazenados os arquivos de zonas do **DNS**, que no nosso exemplo é: ***directory “/var/named/db/master”***.
* **listen-on { IP\_1; IP\_2; };** 🡪 Endereços IP que o **Servidor DNS** irá escutar as conexões de consultas. Podemos utilizar uma **ACL** criada pelo administrador do DNS.
* **listen-on-v6 { IPv6\_1; IPv6\_2; };** 🡪 Endereços IP que o **Servidor DNS** irá escutar as conexões de consultas que utilizam a versão 6 do IP. Aqui utilizamos uma **ACL** existente de nome “**none**”. Podemos utilizar uma **ACL** criada pelo administrador do DNS.
* **empty-zones-enable <”no”>** 🡪 A nova versão do **BIND9** por padrão gera zonas vazias ou fantasma. Em seu log você poderá observar mensagens como esta: “***Aug 18 16:25:03 server named[5610]: automatic empty zone 127.IN-ADDR.ARPA”***. Com isso, ele gera zonas automáticas. Eu desabilitei esse recurso.
* **allow-transfer { IP|ACL; };** 🡪 Endereços IP dos **Servidores DNS** com permissão de replicar a base DNS (**Slaves** ou **Secundários**). No nosso caso usamos uma **ACL srv\_slaves**.
* **allow-recursion { IP|ACL; };** 🡪 Endereços IP ou **ACL** com permissão de fazer consultas recursivas. Que no nosso caso usamos uma **ACL net\_how2security**.
* **allow-query {IP|ACL; };** 🡪 Endereços IP ou **ACL** com permissão de fazer consultas. No nosso caso usamos uma **ACL any**, para que todos possam fazer consultas em nosso servidor.
* **forwarders {IP\_1; IP\_2; };** 🡪 Esta é a opção de transformar nosso Servidor DNS em um Servidor DNS Cache, onde ele repassa as consultas para um Servidor DNS, que resolve os nomes ou os endereços IP, após isso, um registro é armazenado no Cache DNS para futuras consultas (até que o TTL expire). Entre as chaves devemos colocar os endereços IP dos Servidores DNS que gostaríamos de encaminhar as consultas.

**Observação:** Se alteramos o diretório padrão do BIND9, não esqueça torna o usuário dono do diretório, o usuário do **BIND9** com o comando:

**dns-server**:/# chown bind /var/named -R

**3.1.3 – Configurando RNDC e CONTROLS em /etc/named/named.conf**

A diretiva **RNDC** e **controns** são utilizadas para autorizar o controle do **BIND** através do **RNDC**.

key "rndc.key" {

algorithm hmac-sha512;

secret "HEHTs9psYldIA9UEOsfW9NxE8ZvV8WuQxEDnZ+eaRIXPWyW2uiNHxYU3P/AJeMAFS3CxFx3wEtcm20rEevs7wQ==";

};

controls {

inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndc.key"; };

};

**3.1.4 – Configurando SERVER em /etc/named/named.conf**

A diretiva **server** deve ser configurada nos servidores dependendo do seu papel na rede no caso do **Master** fica assim:

server 192.168.5.128 {

provide-ixfr yes;

transfer-format many-answers;

};

E no caso do **Slave**:

server 192.168.5.129 {

request-ixfr yes;

};

A transferência de zona incremental (**IXFR**) tem como finalidade diminuir a quantidade de informações trocadas, transferindo somente as mudanças feitas nas zonas do **Servidor Master** para o **Servidor Slave**.

Com essa configuração estamos dizendo que o **Servidor Master** fornecerá esse recurso de transferência e o **Servidor Slave** sempre que possível utilizará. Quando por algum motivo o **Servidor Master** recusar um **IXFR**, uma **AXFR** (que é a transferência de zona convencional) será realizada para manter as bases integras.

**3.1.5 – Configurando LOGGING em /etc/named/named.conf**

A diretiva **logging** são os registros das mensagens do **BIND**. É importante saber que somente entrará em vigor as opções de logging depois que todo o arquivo ***named.conf*** for lido e o servidor for inicializado, antes disso as mensagens de erro serão enviadas para o sistema de **syslog**.

Por exemplo:

logging {

channel "named\_log" {

file "/var/log/named/named.log" versions 2 size 50m;

print-time yes;

print-category yes;

};

category "security" {

"named\_log";

};

category "xfer-out" {

"named\_log";

};

category "xfer-in" {

"named\_log";

};

category "general" {

"named\_log";

};

};

O registro de logs no **BIND9** é dividido da seguinte forma:

* **channel** 🡪 Usado para especificar onde e que tipo de informação deve ser registrado. Como Níveis (**error, info, dynamic, etc**). Nele você pode configurar o **BIND** tanto para usar o **syslog**, como um arquivo qualquer. No nosso caso utilizamos um arquivo local em ***/var/log/named/named\_log***.
* **category** 🡪 Categoria de log do **BIND**. Existem várias categorias que podem ser usadas, tais como: **security, xfer-out, xfer-in, notify, network, etc**. Como os próprios nomes dizem, em **security** – informações de segurança, em **notify** – notificações de mudanças nas zonas primárias, etc.
  + **default** 🡪 A categoria default define as opções de registro para essa categoria.
  + **database** 🡪 Mensagens referente as bases usadas, como nome dos servidores, zonas e dados de cache.
  + **security** 🡪 Mensagens de consultas aprovadas e negadas.
  + **config** 🡪 Mensagens de configurações e processos.
  + **resolver** 🡪 Mensagens de resolução de nomes, consultas recursivas, etc.
  + **xfer-in** 🡪 Recebimento de Zonas.
  + **xfer-out** 🡪 Envio de Zonas.
  + **notify** 🡪 O protocolo **NOTIFY**.
  + **client** 🡪 Requisições de clientes.
  + **network** 🡪 Operações de rede.
  + **update** 🡪 Atualizações dinâmicas.
  + **update-security** 🡪 Atualizações aprovadas ou negadas.
  + **queries** 🡪 Mensagens de consultas.
  + **queries-errors** 🡪 Mensagens de erro de consultas.



**Observação:** Por padrão no **Debian** os logs do **BIND** irão para ***/var/log/daemon.log*** e nas distribuições **Red Hat** e **Suse** irão para ***/var/log/messages.***

**Observação:** Se alteramos o diretório padrão do BIND9 de gravar logs, não esqueça torna o usuário dono do diretório, o usuário do BIND9 com o comando:

**dns-server**:/# chown bind /var/log/named -R

**3.1.6 – Configurando VIEW em /etc/named/named.conf**

A diretiva **view** nos permite fazer o **Split DNS**, ou seja, separar em dois ou mais diretiva de visualização de registros no **Servidor DNS**. Os registros que podem ser acessados por toda Internet e os que podem ser acessado apenas na rede interna. Essa configuração é usada principalmente em redes desmilitarizadas, onde os **Servidor DNS** se encontra na **DMZ**, de acesso público e contém registros de rede interna também. Por questão de segurança é bom separar o que as pessoas de fora podem ver dentro da nossa rede, como os nomes dos dispositivos como câmeras IP, impressoras, workstations, etc.

Com o exemplo abaixo, o nosso entendimento deste recurso ficará mais claro.

view "public" IN {

match-clients { any; };

zone-statistics yes;

recursion no;

zone "how2security.com.br" {

type master;

file "how2security-externo.com.br";

};

};

view "private" IN {

match-clients { 192.168.5.0/24; };

zone-statistics yes;

recursion yes;

zone "how2security.com.br" {

type master;

file "how2security-interno.com.br";

};

};

Neste exemplo, a zona “**how2security-externo.com.br**” contém o mapeamento dos hosts públicos e pode ser acessada por todos. Já a zona “**how2security-interno.com.br**” somente é acessado pelos hosts interno, ou seja, todos da rede **192.168.5.0/24**.

Se nenhuma **view** for especificada, o **BIND** tratará, por padrão, as zonas como sendo da classe **IN (Internet)**. Dentro das **views** são especificada a configuração das zonas primárias e secundárias.

**3.1.7 – Configurando ZONA em /etc/named/named.conf**

A diretiva de **zonas** as quais o servidor responderá como autoridade. Nela se configura as zonas primárias, secundárias, reversas e outros tipos. Também deve constar nessa configuração a zona **raiz** “.” Do tipo **hint** (raiz da internet).

Por exemplo:

zone "." {

type hint;

file "named.root";

};

zone "0.0.127.in-addr.arpa" {

type master;

file "127.0.0.x";

};

zone "5.168.192.in-addr.arpa" {

type master;

file "192.168.5.x";

};

zone "how2security.com.br" {

type master;

file "how2security.com.br";

};

zone "how2security.com" {

type master;

file "how2security.com";

};

"/etc/named/named.conf" 81L, 1284C written

dns-fusion:/#

**4 – Configuração das Zonas DNS no Linux**

Os arquivos de **Zonas** são banco de dados contendo os registros sobre sua autoridade.

O **BIND** opera com 6 tipos de zonas, sendo elas:

* **master** 🡪 O **BIND** responde como autoridade sobre o domínio e o arquivo é leitura e escrita.
* **slave** 🡪 O **BIND** também responde como autoridade sobre o domínio, porém o arquivo é somente leitura. As alterações são replicadas do **Master**.
* **stub** 🡪 É uma implementação do **BIND**, não sendo padrão **DNS**, Ele é parecido com as **Zonas Slave**, mas replica apenas os registros **NS** do **Master**. Está em desuso.
* **hits** 🡪 São os registros dos **Servidores Root Servers**, eles são necessários quando utilizamos o **Servidor DNS** como **Servidor Cache**.
* **forward** 🡪 Encaminha as consultas sobre determinadas **Zonas** para outro S**ervidor DNS**. Podemos encaminhar as consultas de forma global.
* **delegation-only** 🡪 Para evitar abusos de algumas autoridades sobre os domínios de primeiro nível podemos apenas delegara Zona. Qualquer resposta que não tenha uma delegação explícita ou implícita na seção autoridade será transformada em uma resposta **NXDOMAIN**.

Estes arquivos contêm diversos tipos diferentes de registros **DNS** disponíveis.

Alguns deles são:

* **SOA (Start Of Authority)** 🡪 Indica o responsável por respostas autoritativas por um domínio.
  + **@ (At)** 🡪 Define a localização deste domínio.
  + **Serial** 🡪 Serve para avisar aos **Servidores Slaves** sobre as atualizações do banco de dados. O **Servidor Slave** pergunta periodicamente ao **Servidor Master** sobre o registro **SOA**. Se o número serial no registro **SOA** do **Servidor Master** for maior que do **Servidor Slave**, este transfere toda zona do **Servidor Master**. De outra forma, o **Servidor Slave** assume ter uma cópia igual e sai da transferência de zona. O número serial deve ser incrementado todas as vezes que o domínio for atualizado para manter o **Servidor Slave** sincronizado com o **Servidor Master**. O valor recomendado pela **RFC 1912**, são 10 dígitos que correspondem a ano, mês, dia e versão que é iniciado em 0 (zero).
  + **Refresh** 🡪 Intervalo de tempo, em segundos, que o **Servidor Slave** compara seu número serial com o **Servidor Master** (em segundos).
  + **Retry** 🡪 Caso o **Servidor Master** pare o seu funcionamento, o **Servidor Slave** tentará reatar comunicação com o **Servidor Master** repetidamente considerando o tempo estipulado, em segundos, em **Retry**.
  + **Expire** 🡪 Tempo de vida útil do banco de dados do domínio em um **Servidor Slave**. Caso este tempo seja ultrapassado sem ser realizado uma conexão com o **Servidor Master**, os dados ali armazenados são considerados desatualizados. Em certos casos, o Servidor poderá parar de resolver nomes DNS.
  + **Minimum (TTL- Time To Live)** 🡪 Indica o tempo de resposta de um Servidor em caso de pedido de resolução de um nome contido em seu banco de dados. Máximo de 3 horas.
* **NS (Name Server)** 🡪 Especifica **Servidores DNS** para o domínio ou subdomínio.
* **A (Address)** 🡪 Mapeamento de nomes para Endereços IP. Especificando um Endereço IP para nome direto.
* **AAAA (Address IPv6)** 🡪 Mapeamento de nomes para endereços IPv6.
* **CNAME (Canonical Name)** 🡪 Um apelido para outros hostnames (**Aliases**).
* **MX (Mail Exchange)** 🡪 O Servidor de e-mails. O registro **MX** é seguido de um número que determina a prioridade do Servidor. Quando menor o número, maior será a prioridade do Servidor. O faixa de valores numéricos permitido é de **0** até **65535**.
* **PTR (Pointer)** 🡪 Mapeamento de Endereços IP para nomes. Apontando o hostname/domínio reverso a partir de um endereço IP.
* **TXT (Text)** 🡪 Permite incluir um texto curto em um hostname. Eles também são utilizados de acordo com o formato definido pelo projeto S**ender Policy Framework (SPF)** e que virou uma **(RFC 4408)** para servidor de e-mails com controle de **SPAM**. Este registro diz quem pode enviar e-mails em nome do domínio. Outra forma de controle é o endereço reverso, pois garante que a fonte do e-mail é um provedor e não uma máquina zumbi.
* **WKS (Well Know Services)** 🡪 Serviços bem conhecidos.
* **HINFO (Hosat Information)** 🡪 Informações sobre um computador.
* **SRV (Services)** 🡪 Permite definir serviços disponíveis em um domínio.

Dentro do arquivo temos uma sintaxe para incluir os registros sendo:

***Dono TTL Classe Tipo Dados***

Onde:

* **Dono** 🡪 É o nome do registro.
* **TTL** 🡪 Tempo de vida desse registro.
* **Classe** 🡪 O padrão é **Internet (IN)**, mas temos outros como **CH** e **HS**.
* **Tipo** 🡪 Como vimos acima **A**, **AAAA**, **CNAME**, etc.
* **Dados** 🡪 Depende do tipo de registro, pode ser o **Endereço IP** , um **FQDN**, **Aliases**, etc.

Temos outros e que podem ser consultados no documento **Mensagens DNS**.

**4.1 – Configurando o Arquivo de Root Servers**

O arquivo de **Root Servers** contém os principais **Servidores DNS** do mundo, e devem ser atualizados regularmente. O **InterNIC**, disponibiliza via **FTP** anônimo no site deles no endereço:

dns-fusion:/var/named/db/master# wget ftp://ftp.rs.internic.net/domain/named.root

--2014-08-20 15:24:26-- ftp://ftp.rs.internic.net/domain/named.root

=> `named.root'

Resolving ftp.rs.internic.net (ftp.rs.internic.net)... 199.7.52.73

Connecting to ftp.rs.internic.net (ftp.rs.internic.net)|199.7.52.73|:21... connected.

Logging in as anonymous ... Logged in!

==> SYST ... done. ==> PWD ... done.

==> TYPE I ... done. ==> CWD (1) /domain ... done.

==> SIZE named.root ... 3170

==> PASV ... done. ==> RETR named.root ... done.

Length: 3170 (3,1K) (unauthoritative)

100%[==============================================>] 3.170 --.-K/s in 0s

2014-08-20 15:24:51 (56,2 MB/s) - `named.root' saved [3170]

dns-fusion:/var/named/namedb/master# cd

dns-fusion:~#

Aqui baixamos o arquivo no diretório ***/var/named/db/master***, pois é nosso diretório de banco de dados do **Servidor DNS** (no caso do **Servidor Master**).



**Observação:** Este arquivo no **Debian** chama-se /**etc/bind/db.root** e no **Red Hat** é ***/var/named/named.ca***.

**4.2 – Configurando o Arquivo de Zone Reverse (Zona Reversa)**

Este arquivo é a base de dados de consulta reversa que mapeia Endereços IP para nomes.

Quando alguém faz uma pesquisa do tipo **Reverse Lookup** é feito um pedido para mapear em Endereço IP para um nome. Isso é muito utilizado quando se conhece o Endereço IP, mas há a intenção de saber o nome de domínio associado a esse endereço. Por exemplo, se você monitora conexões IP feitas a um servidor, pode-se utilizar um **reverse lookup** para localizar o nome de domínio associado ao Endereço IP do computador de conexão. Esse tipo de solicitação é feito para resolução de Endereços para nomes.

dns-fusion:~# vi /var/named/db/master/192.168.5.x

$TTL 43200 ; 12 Horas

@ IN SOA fusion.how2security.com.br. suporte.how2security.com.br. (

2014082000 ; Serial YYYYMMDDid

8H ; Refresh

2H ; Retry

1W ; Expire

1D) ; Minimum

how2security.com.br. IN NS fusion.how2security.com.br.

how2security.com.br. IN NS corolla.how2security.com.br.

129 IN NS corola.how2security.com.br.

128 IN PTR fusion.how2security.com.br.

129 IN PTR corola.how2security.com.br.

"192.168.5.x" [New] 12L, 343C written

dns-fusion:~#

**Observação:** Teremos que ter uma zona reversa para cada range de Endereços IP que tivemos.

Podemos aproveitar para criarmos o **Reverso do Loopback**, ficando assim:

dns-fusion:~# vi /var/named/db/master/127.0.0.x

$TTL 3600

@ IN SOA localhost. suporte.localhost. (

2014082000 ; Serial YYYYMMDDid

1H ; Refresh

2H ; Retry

1W ; Expire

1D) ; Minimum

how2security.com.br. IN NS localhost.

1 IN PTR localhost.

"127.0.0.x" [New] 10L, 191C written

dns-fusion:~#

**4.3 – Configurando o Arquivo de Zone Forward (Zona Direta)**

Este arquivo é a base de dados de consulta direta que mapeia nomes para Endereços IP.

Este é o tipo mais comum de pesquisa, sendo utilizado para localizar um Endereço IP de modo que possa ser feita uma conexão a esse servidor. Esse tipo de solicitação é feito para resolução de nomes para Endereço IP.

dns-fusion:~# vi /var/named/db/master/how2security.com.br

$TTL 43200 ; 12 Horas

@ IN SOA fusion.how2security.com.br. suporte.how2security.com.br. (

2014082000 ; Serial YYYYMMDDid

8H ; Refresh

2H ; Retry

1W ; Expire

1D) ; Minimum

how2security.com.br. IN NS fusion.how2security.com.br.

how2security.com.br. IN NS corola.how2security.com.br.

@ IN MX 1 fusion.how2security.com.br.

129 IN MX 5 corola.how2security.com.br.

how2security.com.br. IN TXT "v=spf1 +mx a ip4:192.168.5.0/24 -all"

@ IN SPF "v=spf1 +mx a ip4:192.168.5.0/24 -all"

fusion IN A 192.168.5.128

corola IN A 192.168.5.129

mail IN CNAME fusion.how2security.com.br.

mail2 IN CNAME corola.how2security.com.br.

www IN CNAME www.how2security.com.br.

"how2security.com.br" [New] 18L, 594C written

dns-fusion:~#

**4.4 – Configurando o Arquivo HOSTS**

Os arquivos hosts era a forma de resolução de nomes no passado. Ele continua tendo uma importância no processo de resolução de nomes, pois ele é a segunda fonte a ser consultada pelo **Resolver**.

**Observação:** Este comportamento pode ser alterado através do arquivo ***/etc/nsswitch***.

dns-fusion:~# vi /etc/hosts

192.168.5.128 fusion.how2security.com.br fusion

127.0.0.1 localhost

::1 localhost ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

"/etc/hosts" 9L, 206C written

dns-fusion:~#

Aqui é configurado um endereço por linha, onde temos, **Endereço IP**, **Hostname Canônico** e um **Aliases**. É desejável que o **Hostname Canônico** seja o **FQDN** e o **Aliases** pode ser outro nome (apelido) ou o sufixo do nome.

**4.5 – Configurando o Arquivo de Inicialização do Serviço**

Dentro da **Jail** temos que criar o arquivo que irá inicializar o serviço do **BIND**, para isso vamos criar o arquivo em ***/etc/init.d/dns***:

dns-fusion:/# vi /etc/init.d/dns

#!/bin/bash

#

### BEGIN INIT INFO

# Provides: dns

# Required-Start: $remote\_fs

# Required-Stop: $remote\_fs

# Should-Start: $network $syslog

# Should-Stop: $network $syslog

# Default-Start: 2 3 4 5

# Default-Stop: 0 1 6

# Short-Description: Iniciar e Parar o Servico DNS/BIND9

# Description: O BIND eh um Servidor DNS para traduzir enderecos IP para Nome e Vive-Versa

#

### END INIT INFO

### CORES

amarelo="\e[33;1m"

azul="\e[34;1m"

verde="\e[32;1m"

vermelho="\e[31;1m"

fim="\e[m"

PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin

DNS=`which named`

RNDC=`which rndc`

dns\_start()

{

$DNS -u named & 2>1&

}

dns\_stop()

{

$RNDC stop 2>1&

}

dns\_restart()

{

dns\_stop

sleep 2

dns\_start

}

dns\_reload()

{

$RNDC reload > /dev/null

}

dns\_status()

{

$RNDC status

}

dns\_reconfig()

{

$RNDC reconfig

}

case $1 in

start)

echo -e "$verde[-]Iniciando o Servico de Nonme de Dominio...$fim"

dns\_start

;;

stop)

echo -e "$vermelho[-]Parando o Sertvico de Nome de Dominio...$fim"

dns\_stop

;;

restart)

echo -e "$azul[-]Reiniciando o Servico de Nome de Dominio...$fim"

dns\_restart

;;

reload|force-reload)

echo -e "$azul[-]Recarregando o Servico de Nome de Dominio...$fim"

dns\_reload

;;

status)

echo -e "$amarelo[-]Verificando o Status do Servico de Nome de Dominio...$fim"

dns\_status

;;

reconfig)

echo -e "$azul[-]Reconfigurando o Servico de Nome de Dominio...$fim"

dns\_reconfig

;;

\*)

echo -e "$vermelho[-]ERRO: Use $0 {start|stop|reload|force-reload|restart|reconfig|status}$fim"

exit 1

;;

esac

exit 0

"/etc/init.d/dns" 56L, 851C written

dns-fusion:/#

Agora iremos transformar nosso script em executáveis e criar os links simbólicos nos **rcX.d** assim:

dns-fusion:~# chmod 700 /etc/init.d/dns

dns-fusion:~# update-rc.d -f dns defaults

update-rc.d: using dependency based boot sequencing

dns-fusion:~#

Testando nosso script.

dns-fusion:/# /etc/init.d/dns start

**[-]Iniciando o Servico de Nonme de Dominio...**

dns-fusion:/# /etc/init.d/dns status

**[-]Verificando o Status do Servico de Nome de Dominio...**

WARNING: key file (/etc/named/rndc.key) exists, but using default configuration file (/etc/named/rndc.conf)

version: 9.10.0rc2 <id:a326778a>

boot time: Wed, 27 Aug 2014 14:37:30 GMT

last configured: Wed, 27 Aug 2014 14:37:30 GMT

CPUs found: 1

worker threads: 1

UDP listeners per interface: 1

number of zones: 5

debug level: 0

xfers running: 0

xfers deferred: 0

soa queries in progress: 0

query logging is OFF

recursive clients: 0/0/1000

tcp clients: 0/100

server is up and running

dns-fusion:/# /etc/init.d/dns restart

**[-]Reiniciando o Servico de Nome de Dominio...**

dns-fusion:/# /etc/init.d/dns reload

**[-]Recarregando o Servico de Nome de Dominio...**

WARNING: key file (/etc/named/rndc.key) exists, but using default configuration file (/etc/named/rndc.conf)

dns-fusion:/# /etc/init.d/dns stop

**[-]Parando o Sertvico de Nome de Dominio...**

dns-fusion:/#

Agora temos que garantir que se o host reiniciar, os serviços da **Jail** irá subir, para isso, devemos criar o script de inicialização fora da **Jail**. Vejamos:

root@fusion:~# vi /etc/init.d/jail

#!/bin/bash

#

### BEGIN INIT INFO

# Provides: jail

# Required-Start: $remote\_fs

# Required-Stop: $remote\_fs

# Should-Start: $network $syslog

# Should-Stop: $network $syslog

# Default-Start: 2 3 4 5

# Default-Stop: 0 1 6

# Short-Description: Iniciar e Parar o Servico Enjauldados

# Description: Os serviços enjaulados necessitam ser iniciados|parados diretamente do Host

#

### END INIT INFO

### CORES

amarelo="\e[33;1m"

azul="\e[34;1m"

verde="\e[32;1m"

vermelho="\e[31;1m"

fim="\e[m"

### VARIAVEIS

JAIL="/opt/dns"

MNT=`which mount`

UMNT=`which umount`

CHRT=`which chroot`

DNS="/etc/init.d/dns"

LOG="/etc/init.d/rsyslog"

jail\_start()

{

echo -e "$verde[-]Iniciando Servicos Enjaulados...$fim"

$MNT -o bind /proc $JAIL/proc

$MNT -o bind /dev $JAIL/dev

$CHRT $JAIL $LOG start

$CHRT $JAIL $DNS start

}

jail\_stop()

{

echo -e "$vermelho[-]Parando Servicos Enjaulados...$fim"

$CHRT $JAIL $DNS stop

$UMNT $JAIL/dev

$UMNT $JAIL/proc

}

jail\_restart()

{

echo -e "$azul[-]Reiniciando Servicos Enjaulados...$fim"

$CHRT $JAIL $DNS restart

}

case $1 in

start)

jail\_start

;;

stop)

jail\_stop

;;

restart)

jail\_restart

;;

\*)

echo -e "$vermelho[-]ERRO: Use $0 {start|stop|restart}$fim"

exit 1

;;

esac

exit 0

"/etc/init.d/jail" 70L, 1325C written

root@fusion:~# chmod 700 /etc/init.d/jail

root@fusion:~# update-rc.d -f jail defaults

update-rc.d: using dependency based boot sequencing

root@fusion:~# /etc/init.d/jail restart

**[-]Reiniciando Servicos Enjaulados...**

**[-]Reiniciando o Servico de Nome de Dominio...**

root@fusion:~#

**Observação:** Se após configurar e tentar iniciar o **BIND** nada acontecer, execute o **Daemon Named** com a opção de **Debug** assim:

dns-fusion:/# named -u named –g

27-Aug-2014 15:12:20.164 starting BIND 9.10.0rc2 -u named -g

27-Aug-2014 15:12:20.164 built with '--with-openssl=/usr/local/ssl' '--sysconfdir=/etc/named'

27-Aug-2014 15:12:20.164 ----------------------------------------------------

27-Aug-2014 15:12:20.165 BIND 9 is maintained by Internet Systems Consortium,

27-Aug-2014 15:12:20.165 Inc. (ISC), a non-profit 501(c)(3) public-benefit

27-Aug-2014 15:12:20.165 corporation. Support and training for BIND 9 are

27-Aug-2014 15:12:20.165 available at https://www.isc.org/support

27-Aug-2014 15:12:20.165 ----------------------------------------------------

27-Aug-2014 15:12:20.165 adjusted limit on open files from 4096 to 1048576

27-Aug-2014 15:12:20.165 found 1 CPU, using 1 worker thread

27-Aug-2014 15:12:20.166 using 1 UDP listener per interface

27-Aug-2014 15:12:20.166 using up to 4096 sockets

27-Aug-2014 15:12:20.171 loading configuration from '/etc/named/named.conf'

27-Aug-2014 15:12:20.171 reading built-in trusted keys from file '/etc/named/bind.keys'

--==[ Resumido ]==--

27-Aug-2014 15:12:20.190 all zones loaded

27-Aug-2014 15:12:20.191 running

Desta forma os erros serão mostrados na console.

**5 – BIND DNS em Linux – Referencias**

**Referencias Bibliográficas**

**[1]** Freitas, Andrey Rodrigues de – Perícia forense aplicada à informática: em ambientes Microsoft, 1º Ed, Rio de Janeiro, 2006, Brasport.

**[2]** Forouzan, Behrouz A. – Protocolo TCP/IP, 3º Ed, São Paulo, 2008, McGraw-Hill.

**[3]** Freitas, Andrey Rodrigues de – Perícia forense aplicada à informática: em ambientes Microsoft, 1º Ed, Rio de Janeiro, 2006, Brasport.

**[4]** Registro BR. Disponível em: < http://registro.br/dominio/categoria.html >. Acessado em: 15/04/2014.

**[5]** Gregoriano. Disponível em: <http://www.gregoriano.org.br/portinha/005.htm>. Acessado em: 15/04/2014.

**[6]** Wikipedia. Disponível em: <http://pt.wikipedia.org/wiki/Anexo:Lista\_de\_TLDs>. Acessado em: 16/04/2014.

**[7]** Hugo Azevedo. Disponível em: <http://www.hugoazevedo.eti.br/html/nscd.html>. Acessado em: 05/08/2014.

**[8]** Alex. Disponível em: <http://alex.laner.net.br/?p=10 >. Acessado em: 12/08/2014.

**[9]** RNP. Disponível em: <http://www.pop-ba.rnp.br/Site/ConfDNSSecundario >. Acessado em: 05/08/2014.

**[10]** ISC (Internet System Conbsortium). Disponível em: <http://lamejournal.com/2013/06/10/bind-enabling-tsig-for-zone-transfers/>. Acessado em: 09/09/2014.

**[11]** ISC (Internet System Conbsortium). Disponível em: <http://www.isc.org/downloads/bind/doc/bind-9-10/ >. Acessado em: 11/09/2014.

**[12]** Registro.BR. Disponível em: <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf >. Acessado em: 16/09/2014.

**[13]** Registro.BR. Disponível em: <https://registro.br/tecnologia/root-anchor.html >. Acessado em: 16/09/2014.

**[14]** Registro.BR. Disponível em: <ftp://ftp.registro.br/pub/doc/dns-fw.pdf >. Acessado em: 16/09/2014.

**[15]** Registro.BR. Disponível em: <https://registro.br/tecnologia/root-anchor.html >. Acessado em: 17/09/2014.