****

**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 – Configurações de Segurança no BIND do Linux**

Aqui veremos algumas configurações para deixar nosso Servidor **DNS BIND** mais seguro.

**2 – Removendo o Banner de Versão**

Para ocultar a versão nas consultas ao **Servidor DNS** basta incluirmos no arquivo de configuração do **BIND** (***named.conf***), em **options** a seguinte opção:

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

--==[ Resumido ]==--

acl net\_how2security {

192.168.5.0/24;

};

options {

directory "/var/named/namedb/master";

listen-on { 127.0.0.1; 192.168.5.128; };

listen-on-v6 { none; };

empty-zones-enable no;

**version "Not Available";**

allow-transfer { srv\_slaves; };

allow-recursion { net\_how2security; };

allow-query { any; };

};

"/etc/named/named.conf" 82L, 1311C written

dns-fusion:/#

Basta reiniciar o BIND para não ser visualizada nas consultas a versão do BIND.

**3 – Configurar o TSIG para Transferências de Base Entre Master e o Slave**

Para garantir quais **Servidores Slaves** irão sincronizar suas bases com nosso **Servidor Master** podemos implementar o **TSIG**, que utilizar chaves simétricas para garantir a autorização de transferências de base de dados do DNS.

**3.1 – Gerando a Chave do TSIG no Servidor Master**

Para utilizarmos o **TSIG** necessitamos criar a chave simétrica para garantirmos que apenas os **Servidores Slaves** que tenha essa chave que iremos criar, possa sincronizar as bases.

Para a criação da chave utilizaremos o utilitário **dnssec-keygen**. Esse utilitário vem junto com o **BIND** para gerar chaves para o **DNSSEC** e o **TSIG**. Vamos executar o seguinte comando em nosso **Servidor Master**.

dns-fusion:/etc/named# dnssec-keygen -a HMAC-SHA512 -b 512 -n HOST -r /dev/urandom how2security.com.br

Khow2security.com.br.+165+46427

Com isso, geramos a chave com as seguintes opções:

* **-a** 🡪 Especifica o algoritmo a ser utilizado Os algoritmo suportados pelo **TSIG** são: **HMAC-MD5**, **HMAC-SHA1**, **HMAC-SHA224**, **HMAC-SHA256**, **HMAC-SHA384** ou **HMAC-SHA512**. No nosso caso utilizamos o **HMAC-SHA512**.
* **-b** 🡪Especifica o tamanho da chave que pode variar entre **512** e **2048**. No nosso caso utilizamos **512**.
* **-n** 🡪 Especifica o tipo do dono da chave que pode ser **HOST**, **ZONE**, **ENTITY**, **USER**.
* **-r** 🡪Especifica uma origem randômica. No nosso caso utilizamos ***/dev/urandom***.

Foram gerados dois arquivos com o nome ***Khow2security.com.br.+165+46427.key*** e ***Khow2security.com.br.+165+46427.private*** Agora devemos pegar a chave gerada para criar o arquivo com o valor da chave. Para isso iremos fazer o seguinte:

dns-fusion:/etc/named# grep "Key" Khow2security.com.br.+165+46427.private

**Key**: vVpfdb5VmizK5gj0zB+yvJHoq52N16ULTrlH9DtsAkH2jDwrNhTqBIpqJ8mjfyu1TnjxJ9k5jqr0qa5qdOoPKw==

Agora vamos criar o arquivo com a assinatura do **TSIG**, o nome do arquivo será ***tsig.key*** e devemos fazer um include no arquivo de configuração ***/etc/named/named.conf***. Vejamos:

dns-fusion:/etc/named# vi tsig.key

key "how2sec" {

algorithm HMAC-SHA512;

secret "vVpfdb5VmizK5gj0zB+yvJHoq52N16ULTrlH9DtsAkH2jDwrNhTqBIpqJ8mjfyu1TnjxJ9k5jqr0qa5qdOoPKw==";

};

"tsig.key" [New] 4L, 155C written

dns-fusion:/etc/named# echo "include \"/etc/named/tsig.key\";" >> named.conf

Aqui criamos a chave com o nome “**how2sec**”, onde informamos o algoritmo usado e a chave secreta.

Agora vamos alterar nosso arquivo de configuração para garantir que nenhum servidor irá atualizar sua base com nosso **Servidor Master**. As alterações foram a remoção da **ACL** dos **Servidores Slaves** e o acréscimo das linhas em vermelho:

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

acl net\_how2security {

192.168.5.0/24;

};

options {

directory "/var/named/namedb/master";

listen-on { 127.0.0.1; 192.168.5.128; };

listen-on-v6 { none; };

empty-zones-enable no;

version "Not Available";

auth-nxdomain no; # conform to RFC1035

**allow-transfer { none; };**

allow-recursion { net\_how2security; };

allow-query { any; };

};

key "rndc.key" {

algorithm hmac-sha512;

secret "AqRRT8jO28q7WIUNrgCgu/THmZy4+2nHOZhPJF9coqyA5wQDBp1vSVKZJUT6N47j0B+j85s50ulLn8MsOrROuQ==";

};

controls {

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

};

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";

};

};

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";

**allow-transfer {**

**key "how2sec";**

**};**

};

zone "how2security.com" {

type master;

file "how2security.com";

};

**include "/etc/named/tsig.key";**

"named.conf" 86L, 1393C written

dns-fusion:

Em **options** negamos a transferência de zonas a todos os servidores, e na **Zona** **how2security.com.br** autorizamos a transferência para os **Servidores Slaves** que tenham a chave **how2sec**.

Para finalizar devemos reiniciar o serviço do BIND e transferir a chave para os **Servidores Slaves**.

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

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

dns-fusion:/etc/named# exit

exit

root@fusion:~# scp /opt/dns/etc/named/tsig.key root@192.168.5.129:/opt/dns/etc/bind/

The authenticity of host '192.168.5.129 (192.168.5.129)' can't be established.

ECDSA key fingerprint is 8c:92:f2:26:10:2e:8e:33:4e:72:da:fb:ad:6e:6c:f1.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '192.168.5.129' (ECDSA) to the list of known hosts.

root@192.168.5.129's password:

tsig.key 100% 155 0.2KB/s 00:00

root@fusion:~# chroot /opt/dns /bin/bash

dns-fusion:/#

**3.2 – Configurando o TSIG no Servidor Slave**

Primeiramente vamos incluir o arquivo ***tsig.key*** no arquivo de configuração do **Servidor Slave**, e depois vamos alterar o arquivo de chaves do **TSIG** que transferimos do **Servidor Master**, essa alteração é justamente para criar a função do Servidor Master que utiliza a chave simétrica “**how2sec**.

dns-corola:~# cd /etc/bind/

dns-corola:/etc/bind# echo "include \"/etc/bind/tsig.key\";" >> /etc/bind/named.conf

dns-corola:/etc/bind# vi tsig.key

key "how2sec" {

algorithm HMAC-SHA512;

secret "vVpfdb5VmizK5gj0zB+yvJHoq52N16ULTrlH9DtsAkH2jDwrNhTqBIpqJ8mjfyu1TnjxJ9k5jqr0qa5qdOoPKw==";

};

server 192.168.5.128 {

keys { how2sec; };

};

"tsig.key" 8L, 214C written

dns-corola:/etc/bind#

Após isso, basta reiniciar o serviço do BIND que está pronto.

dns-corola:/etc/bind# /etc/init.d/bind9 restart

Stopping domain name service...: bind9waiting for pid 5209 to die

.

Starting domain name service...: bind9.

dns-corola:/#

**3.3 – Testando o TSIG**

No **Servidor Master** vamos testar a transferência com o utilitário **DIG** para testarmos se ele só responde a solicitação de transferência de Servidores que tenha a chave. Primeiramente vamos solicitar a transferência sem as chaves

dns-fusion:/etc/named# dig @127.0.0.1 how2security.com.br axfr

; <<>> DiG 9.10.0rc2 <<>> @127.0.0.1 how2security.com.br axfr

; (1 server found)

;; global options: +cmd

**; Transfer failed.**

dns-fusion:

Como podemos observar a transferência falhou, pois não utilizamos a chave do **TSIG**. Agora vamos apontar a chave para ver a resposta do servidor:

dns-fusion:/etc/named# dig @127.0.0.1 how2security.com.br axfr -k /etc/named/tsig.key

; <<>> DiG 9.10.0rc2 <<>> @127.0.0.1 how2security.com.br axfr -k /etc/named/tsig.key

; (1 server found)

;; global options: +cmd

how2security.com.br. 43200 IN SOA fusion.how2security.com.br. suporte.how2security.com.br. 2014082000 28800 7200 604800 86400

how2security.com.br. 43200 IN TXT "v=spf1 +mx a ip4:192.168.5.0/24 -all"

how2security.com.br. 43200 IN SPF "v=spf1 +mx a ip4:192.168.5.0/24 -all"

how2security.com.br. 43200 IN MX 1 fusion.how2security.com.br.

how2security.com.br. 43200 IN NS fusion.how2security.com.br.

129.how2security.com.br. 43200 IN MX 5 corola.how2security.com.br.

129.how2security.com.br. 43200 IN NS corola.how2security.com.br.

corola.how2security.com.br. 43200 IN A 192.168.5.129

fusion.how2security.com.br. 43200 IN A 192.168.5.128

mail.how2security.com.br. 43200 IN CNAME fusion.how2security.com.br.

mail2.how2security.com.br. 43200 IN CNAME corola.how2security.com.br.

www.how2security.com.br. 43200 IN CNAME fusion.how2security.com.br.

how2security.com.br. 43200 IN SOA fusion.how2security.com.br. suporte.how2security.com.br. 2014082000 28800 7200 604800 86400

**how2sec. 0 ANY TSIG hmac-sha512. 1410289038 300 64 hld92ovVDeHhiPSJG7URrXGMVHFcPxMmSoKvkPKn3zMsIpTMV0TVSm7w UQphHDYlkUg33zg+Buwt7TJ+/tIAvA== 2660 NOERROR 0**

;; Query time: 93 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Tue Sep 09 18:57:18 UTC 2014

;; XFR size: 13 records (messages 1, bytes 505)

dns-fusion:/etc/named#

Agora sim obtivemos a resposta a solicitação de transferência, pois indicamos a chave do **TSIG**.

Ainda no **Servidor Master** vamos observar os logos antes de testarmos a transferência no **Servidor Slave**.

dns-fusion:/etc/named# tail -f /opt/dns/var/log/named/named.log

Vamos forçar a transferência da base do DNS apagando as bases contidas no **Servidor Slave** e reiniciando o serviço do BIND:

dns-corola:/# tail -f /var/log/named/named.log

Agora sim iremos forçar a replicação e analisar os logs.

dns-corola:/etc/bind# rm /var/cache/bind/how2security.com\*

dns-corola:/etc/bind# rm /var/cache/bind/192.168.5.x

dns-corola:/etc/bind# /etc/init.d/bind9 restart

Stopping domain name service...: bind9waiting for pid 5209 to die

.

Starting domain name service...: bind9.

dns-corola:/#

Olhe os logs do Servidor Master.

dns-fusion:/etc/named# tail -f /opt/dns/var/log/named/named.log

09-Sep-2014 20:06:25.929 security: client 192.168.5.129#34836/key how2sec (5.168.192.in-addr.arpa): zone transfer '5.168.192.in-addr.arpa/AXFR/IN' **denied**

09-Sep-2014 20:06:26.434 xfer-out: client 192.168.5.129#39571/key how2sec **(how2security.com.br): transfer of 'how2security.com.br/IN': AXFR started: TSIG how2sec (serial 2014082000)**

**09-Sep-2014 20:06:26.435 xfer-out: client 192.168.5.129#39571/key how2sec (how2security.com.br): transfer of 'how2security.com.br/IN': AXFR ended**

09-Sep-2014 20:06:26.436 security: client 192.168.5.129#59428/key how2sec (how2security.com): zone transfer 'how2security.com/AXFR/IN' **denied**

Como podemos observar a única **Zona** que tem permissão para transferência é a Zona **how2security.com.br**, as outras não tem permissão, fiz isso propositalmente para vermos que apenas os servidores que contém a chave e a política de transferência de base irá transferir a base.

Para que todas as bases possam transferir basta configuramos as Zonas no arquivo ***named.conf*** do **Servidor Master** da seguinte forma.

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

--==[ Resumido ]==--

zone "5.168.192.in-addr.arpa" {

type master;

file "192.168.5.x";

**allow-transfer {**

**key "how2sec";**

**};**

};

zone "how2security.com.br" {

type master;

file "how2security.com.br";

**allow-transfer {**

**key "how2sec";**

**};**

};

zone "how2security.com" {

type master;

file "how2security.com";

**allow-transfer {**

**key "how2sec";**

**};**

};

include "/etc/named/tsig.key";

"/etc/named/named.conf" 83L, 1309C written

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

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

dns-fusion:/#

Agora vamos abrir outro terminal no **Servidor Slave** e deixar o log sendo analisado, que iremos analisa-lo após reiniciar o serviço do BIND

dns-corola:/# tail -f /var/log/named/named.log

Agora vamos apagar o arquivo da base ***how2security.com.br*** e reiniciar o serviço do BIND para analisarmos os logs dos servidores.

dns-corola:/etc/bind# rm /var/cache/bind/how2security.com.br

dns-corola:/etc/bind# /etc/init.d/bind9 restart

Stopping domain name service...: bind9waiting for pid 5435 to die

.

Starting domain name service...: bind9.

dns-corola:/etc/bind#

Agora vamos analisar o log do Servidor Master:

dns-fusion:/etc/named# tail -f /opt/dns/var/log/named/named.log

09-Sep-2014 20:11:23.640 general: received control channel command 'stop'

09-Sep-2014 20:11:23.642 general: shutting down: flushing changes

09-Sep-2014 20:11:23.642 general: stopping command channel on 127.0.0.1#953

09-Sep-2014 20:11:23.655 general: exiting

09-Sep-2014 20:11:25.685 general: managed-keys-zone: loaded serial 0

09-Sep-2014 20:11:25.687 general: zone 0.0.127.in-addr.arpa/IN: loaded serial 2014082000

09-Sep-2014 20:11:25.687 general: zone 5.168.192.in-addr.arpa/IN: loaded serial 2014082000

09-Sep-2014 20:11:25.688 general: zone how2security.com.br/IN: loaded serial 2014082000

09-Sep-2014 20:11:25.688 general: zone how2security.com/IN: 'how2security.com' found SPF/TXT record but no SPF/SPF record found, add matching type SPF record

09-Sep-2014 20:11:25.688 general: zone how2security.com/IN: loaded serial 2014082000

09-Sep-2014 20:11:25.689 general: all zones loaded

09-Sep-2014 20:11:25.689 general: running

**09-Sep-2014 20:11:59.550 xfer-out: client 192.168.5.129#37406/key how2sec (5.168.192.in-addr.arpa): transfer of '5.168.192.in-addr.arpa/IN': AXFR started: TSIG how2sec (serial 2014082000)**

**09-Sep-2014 20:11:59.551 xfer-out: client 192.168.5.129#37406/key how2sec (5.168.192.in-addr.arpa): transfer of '5.168.192.in-addr.arpa/IN': AXFR ended**

**09-Sep-2014 20:12:00.051 xfer-out: client 192.168.5.129#52603/key how2sec (how2security.com): transfer of 'how2security.com/IN': AXFR started: TSIG how2sec (serial 2014082000)**

**09-Sep-2014 20:12:00.052 xfer-out: client 192.168.5.129#52603/key how2sec (how2security.com): transfer of 'how2security.com/IN': AXFR ended**

E por fim vamos analisar o log do Servidor Slave:

dns-corola:/# tail -f /var/log/named/named.log

09-Sep-2014 20:11:58.451 general: received control channel command 'stop -p'

09-Sep-2014 20:11:58.452 general: shutting down: flushing changes

09-Sep-2014 20:11:58.452 general: stopping command channel on 127.0.0.1#953

09-Sep-2014 20:11:58.452 general: stopping command channel on ::1#953

09-Sep-2014 20:11:58.463 general: exiting

09-Sep-2014 20:11:59.528 general: zone 0.in-addr.arpa/IN: loaded serial 1

09-Sep-2014 20:11:59.528 general: zone 127.in-addr.arpa/IN: loaded serial 1

09-Sep-2014 20:11:59.529 general: zone 0.0.127.in-addr.arpa/IN: loaded serial 2014082000

09-Sep-2014 20:11:59.533 general: zone 255.in-addr.arpa/IN: loaded serial 1

09-Sep-2014 20:11:59.536 general: zone how2security.com.br/IN: loaded serial 2014082000

09-Sep-2014 20:11:59.536 general: zone localhost/IN: loaded serial 2

09-Sep-2014 20:11:59.537 general: managed-keys-zone ./IN: loaded serial 7

09-Sep-2014 20:11:59.543 general: running

09-Sep-2014 20:11:59.547 general: zone 5.168.192.in-addr.arpa/IN: Transfer started.

09-Sep-2014 20:11:59.549 xfer-in: transfer of '5.168.192.in-addr.arpa/IN' from 192.168.5.128#53: connected using 192.168.5.129#37406

**09-Sep-2014 20:11:59.560 general: zone 5.168.192.in-addr.arpa/IN: transferred serial 2014082000: TSIG 'how2sec'**

**09-Sep-2014 20:11:59.560 xfer-in: transfer of '5.168.192.in-addr.arpa/IN' from 192.168.5.128#53: Transfer completed: 1 messages, 6 records, 329 bytes, 0.010 secs (32900 bytes/sec)**

**09-Sep-2014 20:12:00.049 general: zone how2security.com/IN: Transfer started.**

**09-Sep-2014 20:12:00.050 xfer-in: transfer of 'how2security.com/IN' from 192.168.5.128#53: connected using 192.168.5.129#52603**

**09-Sep-2014 20:12:00.065 general: zone how2security.com/IN: transferred serial 2014082000: TSIG 'how2sec'**

**09-Sep-2014 20:12:00.066 xfer-in: transfer of 'how2security.com/IN' from 192.168.5.128#53: Transfer completed: 1 messages, 12 records, 438 bytes, 0.015 secs (29200 bytes/sec)**

**4 – Configurar do DNSSEC Para Consultas Seguras**

O **DNSSEC (Domain Name System SECurity extensions)** é uma extensão do DNS, possibilitando uma maior segurança para os usuários.

Com isso, você garante a autenticidade e a integridade das consultas.

**4.1 – Criando as Chaves do DNSSEC**

Vamos criar o par de chaves (pública e privada) com o utilitário **dnssec-keygen**.

dns-fusion:/etc/named#

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

dns-fusion:/var/named/namedb/master# dnssec-keygen -r /dev/urandom -f KSK -a RSASHA512 -b 2048 -n ZONE how2security.com.br

Generating key pair..............+++ ............................................................+++

Khow2security.com.br.+010+03426

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

Onde temos as seguintes opções:

* **-a** 🡪 Especifica o algoritmo a ser utilizado Os algoritmo suportados pelo **DNSSEC** são: **RSAMD5**, **RSASHA1**, **DSA**, **NSEC3RSASHA1**, **NSEC3DSA**, **RSASHA256**, **RSASHA512**, **ECCGOST**, **ECDSAP256SHA256** ou **ECDSAP384SHA384**. No nosso caso utilizamos o **RSASHA512**.
* **-b** 🡪 Especifica o tamanho da chave que pode variar entre **512** e **2048**. No nosso caso utilizamos **2048**.
* **-f** 🡪 Define o tipo da chave.
* **-n** 🡪 Especifica o tipo do dono da chave que pode ser **HOST**, **ZONE**, **ENTITY**, **USER**.
* **-r** 🡪 Especifica uma origem randômica. No nosso caso utilizamos ***/dev/urandom***.

Em seguida especificamos o nome do domínio que estamos gerando as chaves.

Foram gerados dois arquivos com o nome ***Khow2security.com.br.+010+03426.key*** e ***Khow2security.com.br.+010+03426.private***.

**4.2 – Assinar o Domínio (Zona) com o DNSSEC**

Vamos assinar o arquivo de zona, mas antes disso, devemos incrementar o serial do registro **SOA**, para o **Servidor Slave** atualizar as alterações em seu banco de dados. E também temos que fazer o include do arquivo de chave pública no arquivo de zona.

dns-fusion:/var/named/namedb/master# echo "\$include Khow2security.com.br.+010+03426.key" >> how2security.com.br

Em fim vamos assinar a zona ***how2security.com.br*** com o utilitário **dnssec-signzone**.

dns-fusion:/var/named/namedb/master# dnssec-signzone -P -S -z -e 20160102120000 -o how2security.com.br /var/named/namedb/master/how2security.com.br

/var/named/namedb/master/how2security.com.br.signed

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

1 dsset-how2security.com.br. how2security.com.br.signed named.root

127.0.0.x how2security.com Khow2security.com.br.+010+03426.key

192.168.5.x how2security.com.br Khow2security.com.br.+010+03426.private

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

Onde:

* **-e** 🡪 Especifica um tempo de validade da assinatura, este **time** é informado por ano, mês, dia, hora, minutos e segundos (**YYYYMMDDhhmmss**). Por padrão será valido por 30 dias. No nosso caso irá expirar em 02/01/2014 as 12:00:00.
* **-o** 🡪 A zona origem, no nosso caso o nome da zona que estamos assinado.
* **-P** 🡪Desabilita a verificação por teste.
* **-S** 🡪 Instrui o **dnssec-signzone** a procurar no repositório uma chaves apropriada para a zona.
* **-z** 🡪 Ignora a flag **KSK** quando determinada na assinatura.

Por fim, informamos o nome do arquivo de banco de dados da zona. Que no nosso caso é o mesmo nome da zona.

Após assinar a zona será criado um arquivo com o mesmo nome do arquivo de banco de dados da zona com a extensão **.signed**, este arquivo será nosso novo banco de dados de zona.

**Observação:** Todas as vezes que alteramos o arquivo de bando de dados da zona (o arquivo sem assinatura), devemos executar este procedimento novamente, gerando outro arquivo de zona assinado. E não esquecer de incrementar o serial do registro **SOA** para a atualização das bases entre os **Servidores Master** e **Slaves**.

Para finalizar a configuração do **DNSSEC** devemos substituir o arquivo de zona pelo arquivo assinado em ***/etc/named/named.conf*** assim:

dns-fusion:/var/named/namedb/master# vi /etc/named/named.conf

--==[ Resumido ]==--

zone "how2security.com.br" {

type master;

**file "how2security.com.br.signed";**

allow-transfer {

key "how2sec";

};

};

zone "how2security.com" {

"/etc/named/named.conf" 83L, 1316C written

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

Agora vamos abrir outro terminal e executar o utilitário **tail** para analisarmos o log na reinicialização do serviço do BIND, para isso:

dns-fusion:/# tail -f /var/log/named/named.log

Agora vamos reiniciar o serviço do BIND e analisar o resultado no outro terminal.

dns-fusion:/var/named/namedb/master# /etc/init.d/dns restart

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

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

Log:

dns-fusion:/# tail -f /var/log/named/named.log

12-Sep-2014 15:08:15.761 general: received control channel command 'stop'

12-Sep-2014 15:08:15.762 general: shutting down: flushing changes

12-Sep-2014 15:08:15.763 general: stopping command channel on 127.0.0.1#953

12-Sep-2014 15:08:15.817 general: exiting

12-Sep-2014 15:08:17.821 general: managed-keys-zone: loaded serial 0

12-Sep-2014 15:08:17.832 general: zone 0.0.127.in-addr.arpa/IN: loaded serial 2014082000

12-Sep-2014 15:08:17.833 general: zone 5.168.192.in-addr.arpa/IN: loaded serial 2014082000

**12-Sep-2014 15:08:17.835 general: zone how2security.com.br/IN: loaded serial 2014082000 (DNSSEC signed)**

12-Sep-2014 15:08:17.836 general: zone how2security.com/IN: 'how2security.com' found SPF/TXT record but no SPF/SPF record found, add matching type SPF record

12-Sep-2014 15:08:17.836 general: zone how2security.com/IN: loaded serial 2014082000

12-Sep-2014 15:08:17.837 general: all zones loaded

12-Sep-2014 15:08:17.838 general: running

**4.3 – Forçar a Atualização do Slave**

Agora vamos forçar a atualização do **Servidor Slave** para vermos o resultado.

Antes de tudo abra um terminal e execute o utilitário **tail** para analisarmos

dns-corola:/# tail -f /var/log/named/named.log

Agora vamos forçar a atualização.

dns-corola:/# rm /var/cache/bind/how2security.com.br

dns-corola:/# /etc/init.d/bind9 restart

Stopping domain name service...: bind9

waiting for pid 3324 to die

.

Starting domain name service...: bind9.

dns-corola:/#

No outro terminal vamos analisar se houve a atualização

dns-corola:/# tail -f /var/log/named/named.log

12-Sep-2014 15:10:53.385 general: received control channel command 'stop -p'

12-Sep-2014 15:10:53.387 general: shutting down: flushing changes

12-Sep-2014 15:10:53.387 general: stopping command channel on 127.0.0.1#953

12-Sep-2014 15:10:53.388 general: stopping command channel on ::1#953

12-Sep-2014 15:10:53.410 general: exiting

12-Sep-2014 15:10:54.543 general: zone 0.in-addr.arpa/IN: loaded serial 1

12-Sep-2014 15:10:54.543 general: zone 127.in-addr.arpa/IN: loaded serial 1

12-Sep-2014 15:10:54.544 general: zone 0.0.127.in-addr.arpa/IN: loaded serial 2014082000

12-Sep-2014 15:10:54.544 general: zone 5.168.192.in-addr.arpa/IN: loaded serial 2014082000

12-Sep-2014 15:10:54.545 general: zone 255.in-addr.arpa/IN: loaded serial 1

12-Sep-2014 15:10:54.546 general: zone how2security.com/IN: loaded serial 2014082000

12-Sep-2014 15:10:54.546 general: zone localhost/IN: loaded serial 2

12-Sep-2014 15:10:54.547 general: managed-keys-zone ./IN: loaded serial 10

12-Sep-2014 15:10:54.551 general: running

12-Sep-2014 15:10:54.557 general: zone how2security.com.br/IN: Transfer started.

12-Sep-2014 15:10:54.562 xfer-in: transfer of 'how2security.com.br/IN' from 192.168.5.128#53: connected using 192.168.5.129#46946

**12-Sep-2014 15:10:54.570 general: zone how2security.com.br/IN: transferred serial 2014082000: TSIG 'how2sec'**

**12-Sep-2014 15:10:54.570 xfer-in: transfer of 'how2security.com.br/IN' from 192.168.5.128#53: Transfer completed: 1 messages, 39 records, 6604 bytes, 0.008 secs (825500 bytes/sec)**

Atualizada com sucesso, agora vamos ver como ficou nosso arquivo de banco de dados da zona ***how2security.com.br***.

dns-corola:/# cat /var/cache/bind/how2security.com.br

$ORIGIN .

$TTL 43200 ; 12 hours

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

2014082000 ; serial

28800 ; refresh (8 hours)

7200 ; retry (2 hours)

604800 ; expire (1 week)

86400 ; minimum (1 day)

)

RRSIG SOA 10 3 43200 20160102120000 (

20140912140607 3426 how2security.com.br.

WGYX37XFyUiCaobOiHru3BTrNI88OFszCaX5n5oTkxOd

1DPgkvVSrgn6xOmQthzWHmxvj1WJWSVy8xlREMNQzXzR

pX1Z4j5Xqq4usvr6sqemWcmWtyW8pxT+RPrO4MD29K4D

Lz9d4I1sGcUcPoHYsOO707Uro3tbCg10ilDqqA9S3r7+

+IKq4zkRzqxkLP13G8rUkNhV83qf/YtKAwp3GW2asa10

vJFW9+CA+Oe9dYczHxE2RlNYw0CfwShOlSN2SCqb7oEC

/zApPet20z2qf+aQ0ciIyg6zjjeJjFFh+AdD4F8yvvc2

Mk8H7fMsdCy7yIhYl4xsbkUvD4jyYL5Wnw== )

--==[ Resumido ]==--

$TTL 43200 ; 12 hours

www CNAME fusion

RRSIG CNAME 10 4 43200 20160102120000 (

20140912140607 3426 how2security.com.br.

XyJw1VxOLwAzd8QPbHXphwtakxZxZvU6tagH7fYy7+fz

UO9UEf/z+3R6pMqexJ/IxIWy2T999s+qNDxeGnbJLrwd

XS54vDgUNSoivkil8Dgrd8hicRYK0gLRiHKSsrCMoETG

ffKHBjWFETeB4UXxMSuIW4IuwsgWAdwqBV0V2YAqfSqm

jkffSl1vQuthfLA6RlpmP7IGb6+l19CD5UyZKxoj6ojs

oGWXMRWwIjNY6kxch4CGI5WDJwcigSMYsTRwExEpNgJE

8XuIzgF7jwR+weoBeVsRl/KwJnioS1u1koG+yyKBX1jJ

Anexg6eCfQMZJrSn+ExoghCiIq6ZCW3Sfw== )

$TTL 86400 ; 1 day

NSEC how2security.com.br. CNAME RRSIG NSEC

RRSIG NSEC 10 4 86400 20160102120000 (

20140912140607 3426 how2security.com.br.

SpTpT6O6LDM22L19nBImL+5tYYey8thrcR/4MtcehrbX

CvKJQkHrS94NdX5ghK5KWHCgaJY2tJcsb/Y+QsI/zide

7eeY8KM+cjsevUpEX4U4au5z5agpEHuqno66ap8XD8KW

5OHkkOkOe1PE1kHUDfljbUXPYMC4m3xpuVmT4oMnOe0F

N4wUEosO6gKWvuDUhcCBxLZsnmZpb+FJjpZmbxDOmJNY

3adDjrNV5qJ1BRGXzEhGP98vw16T5MEsYKiV7dl/qSJ8

qHlt5h7ADU4tLSo8R/jHlxbQDU66PDE3jQHruA3Hr9XA

PDmya7cRNw3R5h/4sDE1A88SZ13Ch4NiDA== )

dns-corola:/#

Como podemos observar o arquivo está assinado.

**4.4 – Registrando o DS no Registro.br**

Necessitamos copiar os dados de **KeyTag** e **Digest** do arquivo ***dsset-how2security.com.br*** para a interface no site do Registro.br.

dns-fusion:/var/named/namedb/master# cat dsset-how2security.com.br. | head -1

how2security.com.br. IN DS **3426** 10 1 **D21CD8A15868D9D448E059646B371D6D12117906**

**\\_/ \\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**

**| |**

**| +--> Digest**

**+---> KeyTag**

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

Em posse dessas informações, devemos entrar na área administrativa do **Registro.br** e cadastrar seu **KeyTag** e **Digest**.



Figura 01 – Formulário de Registro dos Servidores DNS do Domínio

**Observação:** Todas as vezes que for alterada alguma informação no banco de dados do **Servidor Autoritativo** devemos incrementar o serial do registro **SOA** e reassinar a zona utilizando o utilitário **dnssec-segnzone**. Também não se esquecer de reassinar a zona antes das assinaturas expirarem.

**4.5 – Configurar DNSSEC em Servidores Recursivos**

Para utilizarmos nosso **Servidor DNS** com **BIND** como um **Servidor Recursivo** devemos utilizar a assinatura da raiz do sistema DNS como **Trust Anchor** em suas configurações (tanto **Servidores Master** como **Servidores Slaves** que sejam recursivos).

A chave encontra-se originalmente no site da **IANA ()**. Caso deseje fazer download e validação manualmente utilizando um script feito pelo **Registro.br** da seguinte forma:

dns-fusion:/# cd /etc/named/

dns-fusion:/etc/named# aptitude install xsltproc

dns-fusion:/etc/named# wget ftp://ftp.registro.br/pub/doc/fetch\_root\_anchor.sh

--2014-09-17 17:21:48-- ftp://ftp.registro.br/pub/doc/fetch\_root\_anchor.sh

=> `fetch\_root\_anchor.sh'

Resolving ftp.registro.br (ftp.registro.br)... 200.160.2.8, 2001:12ff:0:2::8

Connecting to ftp.registro.br (ftp.registro.br)|200.160.2.8|:21... connected.

Logging in as anonymous ... Logged in!

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

==> TYPE I ... done. ==> CWD (1) /pub/doc ... done.

==> SIZE fetch\_root\_anchor.sh ... 1902

==> PASV ... done. ==> RETR fetch\_root\_anchor.sh ... done.

Length: 1902 (1,9K) (unauthoritative)

100%[========================================================>] 1.902 --.-K/s in 0,03s

2014-09-17 17:21:49 (58,2 KB/s) - `fetch\_root\_anchor.sh' saved [1902]

dns-fusion:/etc/named#

Agora em posse do script vamos torna-lo executável, e em seguida executá-lo.

dns-fusion:/etc/named# chmod 700 fetch\_root\_anchor.sh

dns-fusion:/etc/named# ./fetch\_root\_anchor.sh

. initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=";

dns-fusion:/etc/named#

**Observação:** Devido um erro de certificado no site do **IANA** o **wget** não confiava no site e consequentemente ele não baixava o arquivo **XSL** dando o seguinte erro:

dns-fusion:/etc/named# ./fetch\_root\_anchor.sh

**warning: failed to load external entity "root-anchors.xml"**

**unable to parse root-anchors.xml**

**diff: root-anchors.txt: No such file or directory**

Isso porque o **wget** não estava baixando o arquivo ***root-anchor.xml***, para resolver eu editei o script e em **wget** eu coloquei o seguinte parâmetro para não checar o certificado do **IANA**:

wget **--no-check-certificate** -q https://data.iana.org/root-anchors/root-anchors.xml

Por fim devemos editar o arquivo ***/etc/named/named.conf*** para incluir a chave dos **Root Servers** no **Trust Anchor** e reiniciar o serviço BIND.

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

options {

directory "/var/named/namedb/master";

listen-on { 127.0.0.1; 192.168.5.128; };

listen-on-v6 { none; };

empty-zones-enable no;

version "Not Available";

**dnssec-enable yes;**

**dnssec-validation yes;**

allow-transfer { none; };

allow-recursion { net\_how2security; };

allow-query { any; };

};

--==[ Resumido ]==--

**managed-keys {**

**/\* Root Keys \*/**

**. initial-key 257 3 8 "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjFFVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoXbfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaDX6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpzW5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relSQageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulqQxA+Uk1ihz0=";**

**};**

"named.conf" 91L, 1772C written

dns-fusion:/etc/named#

dns-fusion:/etc/named# named-checkconf

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

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

dns-fusion:/etc/named#

**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](file:///C:\Users\Aline\Documents\How2Sec%20-%20Feito\02%20-%20Sistemas%20Operacionais\001%20-%20Linux\BIND\%3c%20http:\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](ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf%20) >. Acessado em: 16/09/2014.

**[13]** Registro.BR. Disponível em: <[https://registro.br/tecnologia/root-anchor.html](https://registro.br/tecnologia/root-anchor.html%20) >. Acessado em: 16/09/2014.

**[14]** Registro.BR. Disponível em: <[ftp://ftp.registro.br/pub/doc/dns-fw.pdf](ftp://ftp.registro.br/pub/doc/dns-fw.pdf%20) >. Acessado em: 16/09/2014.

**[15]** Registro.BR. Disponível em: <[https://registro.br/tecnologia/root-anchor.html](https://registro.br/tecnologia/root-anchor.html%20) >. Acessado em: 17/09/2014.