****

**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 – Instalação e Configuração do Nosso Cenário DNS no Linux**

**1.1 – Configurando o Servidor Master - Fusion**

Agora iremos para a pratica, iremos configurar o servidor Fusion como nosso Servidor DNS Master (ou Primário).

**1.1.1 – Configurando o RNDC - Fusion**

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:/#

Agora vamos criar os arquivos uma cópia dessa chave nos arquivos ***/etc/named/named.conf*** e ***/etc/named/rndc.key***.

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:/# cat /etc/named/rndc.key

key "rndc.key" {

algorithm hmac-sha512;

secret "HEHTs9psYldIA9UEOsfW9NxE8ZvV8WuQxEDnZ+eaRIXPWyW2uiNHxYU3P/AJeMAFS3CxFx3wEtcm20rEevs7wQ==";

};

dns-fusion:/#

**1.1.2 – Configurando o NAMED - Fusion**

Agora vamos configurar as diretivas do arquivo ***/etc/named/named.conf***.

**1.2.1 – Configurando o ACL - Fusion**

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

acl srv\_slaves {

127.0.0.1;

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:/#

**1.2.2 – Configurando o OPTIONS - Fusion**

options {

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

listen-on { 127.0.0.1; 192.168.5.128; };

listen-on-v6 { none; };

version “Not Available”;

empty-zones-enable no;

allow-transfer { srv\_slaves; };

allow-recursion { net\_how2security; };

allow-query { any; };

dnssec-validation auto;

auth-nxdomain no; # RFC1035

};

**1.2.3 – Configurando RNDC e CONTROLS - Fusion**

key "rndc.key" {

algorithm hmac-sha512;

secret "HEHTs9psYldIA9UEOsfW9NxE8ZvV8WuQxEDnZ+eaRIXPWyW2uiNHxYU3P/AJeMAFS3CxFx3wEtcm20rEevs7wQ9,5

==";

};

controls {

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

};

**1.2.4 – Configurando SERVER - Fusion**

server 192.168.5.128 {

provide-ixfr yes;

transfer-format many-answers;

};

**1.2.5 – Configurando LOGGING - Fusion**

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";

};

};

**1.2.6 – Configurando ZONE - Fusion**

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:/#

**1.3 – Configurando o Arquivo de Root Servers - Fusion**

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/namedb/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#

**1.4 – Configurando as Zonas - Fusion**

Agora vamos configurar as zonas as quais nosso Servidor DNS será autoridade para essa zona. Os arquivos de zonas iremos armazenar em ***/var/named/namedb/master***.

**1.4.1 – Configurando a Zona Reversa e de Loopback - Fusion**

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

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

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

**1.4.2 – Configurando a Zona Direta - Fusion**

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

E para completar todas as zonas que criamos no arquivo ***/etc/named/named.conf*** iremos criar a versão internacional do nosso domínio. Lembrando que para isso, devemos registrar esse domínio em um **ISP** responsável pela domínio **.com**.

dns-fusion:/var/named/namedb/master# vi /var/named/namedb/master/how2security.com

$TTL 43200 ; 12 Horas

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

2014082000 ; Serial YYYYMMDDid

8H ; Refresh

2H ; Retry

1W ; Expire

1D) ; Minimum

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

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

@ IN MX 1 fusion.how2security.com.

129 IN MX 5 corola.how2security.com.

how2security.com. 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.

mail2 IN CNAME corola.how2security.com.

www IN CNAME www.how2security.com.

"how2security.com" 18L, 567C written

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

**1.5 – Script de Inicialização do BIND – Fusion**

Esse script inicializa o BIND dentro da jaula.

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

}

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

;;

\*)

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

exit 1

;;

esac

exit 0

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

dns-fusion:/#

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:~#

Também temos que criar um script para iniciar os serviços direto do host, para isso utilizaremos o script a seguir.

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:~#

**2 – Configurando o Servidor Slave - Corola**

Agora iremos configurar o servidor Corola como nosso Servidor DNS Slave (ou Secundário).

**2.1 – Configurando o RNDC - Corola**

Como nós instalamos via repositório o BIND no Corola não há necessidade de configurar o **RNDC**, pois o pacote pré-compilado já vem configurado. Mas o procedimento para configura-lo é igual ao do Fusion.

**2.2 – Configurando o named.Conf.Options - Corola**

dns-corola:/etc/bind# vi named.conf.options

acl net\_how2security {

192.168.5.0/24;

};

options {

directory "/var/cache/bind";

listen-on { 127.0.0.1; 192.168.5.129; };

listen-on-v6 { none; };

empty-zones-enable no;

allow-recursion { net\_how2security; };

allow-query { any; };

// forwarders {

// 0.0.0.0;

// };

dnssec-validation auto;

auth-nxdomain no; # conform to RFC1035

};

server 192.168.5.129 {

request-ixfr yes;

};

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-in" {

"named\_log";

};

category "xfer-out" {

"named\_log";

};

category "general" {

"named\_log";

};

};

"named.conf.options" 47L, 699C written

dns-corola:/etc/bind#

Aqui eu retirei a maioria das linhas que estavam comentadas para ficar um arquivo mais limpo.

**2.3 – Configurando o named.conf.local - Corola**

Agora vamos criar nossas zonas como **Slave**, para replicar do nosso **Servidor Master**.

dns-corola:/etc/bind# vi named.conf.local

zone "5.168.192.in-addr.arpa" {

type slave;

file "192.168.5.x";

masters {

192.168.5.128;

};

};

zone "how2security.com.br" {

type slave;

file "how2security.com.br";

masters {

192.168.5.128;

};

};

zone "how2security.com" {

type slave;

file "how2security.com";

masters {

192.168.5.128;

};

};

"named.conf.local" 31L, 407C written

dns-corola:/etc/bind#

dns-corola:/etc/bind# mkdir -p /var/log/named/

dns-corola:/etc/bind# chown bind.bind /var/log/named –R

dns-corola:/etc/bind# chown -R bind /var/named

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

Stopping domain name service...: bind9waiting for pid 4524 to die

.

Starting domain name service...: bind9.

dns-corola:/etc/bind#

**2.4 – Configurando o named.conf.default-zones – Corola**

Agora vamos remover as linhas existente neste arquivo e criar as zonas padrão para o Servidor Slave.

dns-corola:/etc/bind# vi named.conf.default-zones

zone "." {

type hint;

file "named.root";

};

zone "0.0.127.in-addr.arpa" {

type master;

file "127.0.0.x";

};

zone "localhost" {

type master;

file "localhost";

};

"named.conf.default-zones" 31L, 407C written

dns-corola:/etc/bind#

Agora vamos criar os arquivos de zona padrão do Servidor Slave.

dns-corola:/# vi /var/named/namedb/slave/127.0.0.x

$TTL 604800

@ IN SOA localhost. suporte.localhost. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS localhost.

1 IN PTR localhost.

"127.0.0.x" 31L, 207C written

dns-corola:/# cat /var/named/namedb/slave/localhost

$TTL 604800

@ IN SOA localhost. suporte.localhost. (

2 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

;

@ IN NS localhost.

@ IN A 127.0.0.1

@ IN AAAA ::1

"localhost" 31L, 207C written

dns-corola:/#

Agora vamos fazer o download do arquivo dos servidores raízes.

dns-corola:/# cd /var/named/namedb/slave/

dns-corola:/var/named/namedb/slave# wget

wget ftp://ftp.rs.internic.net/domain/named.root

--2015-05-19 17:37:28-- ftp://ftp.rs.internic.net/domain/named.root

=> `named.root.1'

Resolving ftp.rs.internic.net (ftp.rs.internic.net)... 199.7.50.73

Connecting to ftp.rs.internic.net (ftp.rs.internic.net)|199.7.50.73|:21... connected.

Logging in as anonymous ... Logged in!

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

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

==> SIZE named.root ... 3175

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

Length: 3175 (3.1K) (unauthoritative)

100%[======================================>] 3,175 --.-K/s in 0.007s

2015-05-19 17:37:34 (442 KB/s) - `named.root.1' saved [3175]

dns-corola:/var/named/namedb/slave#

**2.5 – Script de Inicialização do BIND – Corola**

Não temos a necessidade de criar um script para iniciar o serviço dentro da jaula porque a instalação via repositório já cuidou disso para nós, porém continuamos a ter que criar um script para iniciar os serviços direto do host, para isso utilizaremos o script a seguir.

root@corola:~# 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/bind9"

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" [New] 70L, 1333C written

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

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

update-rc.d: using dependency based boot sequencing

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

[-]Reiniciando Servicos Enjaulados...

Stopping domain name service...: bind9waiting for pid 4569 to die

.

Starting domain name service...: bind9.

root@corola:~#