

Sessão 8: DNS e NFS

Nestas atividades, você deve trabalhar com duas máquinas virtuais (*Server_Linux* e *Client_Linux*). Ambas devem estar na mesma rede. Como estabelecido na topologia de rede de curso, o endereço 192.168.0.10 será o da máquina *Server_Linux*, e o endereço 192.168.0.20 será o da máquina *Client_Linux*. Teste o funcionamento da rede através do comando **ping** antes de prosseguir com os exercícios.

1) Servidor de DNS Primário



Esta configuração será realizada na máquina virtual *Server_Linux*.

Instale o serviço **ntp** na máquina *Server_Linux*, e configure corretamente sua *timezone*. Em seguida, pare o *daemon ntp*, atualize o relógio do sistema para a hora correta usando **ntpd -gq** e reinicie o **ntp**.

Feito isso, configure o servidor DNS. Considerando a rede 192.168.0.0/24, cujo domínio é **empresa.com.br**, configure o servidor de DNS Primário de modo que ele tenha as seguintes máquinas registradas, com tipos de registro associados:

Tabela 1. Configuração DNS

Nome	Endereço IP	Tipo de registro
servidor.empresa.com.br	192.168.0.10	NS
email.empresa.com.br	192.168.0.15	MX
cliente.empresa.com.br	192.168.0.20	A
windows.empresa.com.br	192.168.0.25	A
www.empresa.com.br	192.168.0.10	CNAME
meusite.empresa.com.br	192.168.0.10	CNAME
pop.empresa.com.br	192.168.0.15	CNAME
smtp.empresa.com.br	192.168.0.15	CNAME

Não se esqueça de configurar a resolução de nomes reversa.

1. Instale os seguintes aplicativos:

```
# apt-get install ntp bind9 bind9utils
```

2. Configure a *timezone* do sistema, via **dpkg-reconfigure tzdata**. Escolha **America**, e em seguida **Sao_Paulo**.

```
# dpkg-reconfigure tzdata

Current default time zone: 'America/Sao_Paulo'
Local time is now:      Sat Sep 22 10:47:12 -03 2018.
Universal Time is now:  Sat Sep 22 13:47:12 UTC 2018.
```

Pare o **ntp**, atualize o relógio do sistema e reinicie o **ntp**.

```
# systemctl stop ntp ; ntpd -gq ; systemctl start ntp
ntpd: time set +2.651545s
```

Verifique a hora do sistema.

```
# date
Sat Sep 22 10:49:46 -03 2018
```

3. Vamos agora configurar o **bind**. Ajuste os arquivos de configuração da seguinte forma:

- **/etc/bind/named.conf.options** — opções do servidor **bind**:

```
options {
    directory "/var/cache/bind";

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

    dnssec-validation auto;
    auth-nxdomain no;

    allow-transfer { none; };
    allow-query { internals; };
    allow-recursion { internals; };

    listen-on { 127.0.0.1; 192.168.0.10; };
    listen-on-v6 { none; };

    version none;
};
```

- **/etc/bind/named.conf.local** — configurações locais do servidor **bind**:

```

acl internals { 127.0.0.0/8; 192.168.0.0/24; };

zone "empresa.com.br" {
    type master;
    file "/etc/bind/db.empresa.com.br";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0.168.192";
};

include "/etc/bind/zones.rfc1918";

```

- `/etc/bind/db.empresa.com.br` — arquivo de zona do domínio `empresa.com.br`:

```

$TTL 86400 ; (1 day)
$ORIGIN empresa.com.br.
@      IN      SOA      servidor.empresa.com.br. admin.empresa.com.br. (
                                2018080900 ;Serial (YYYYMMDDnn)
                                14400      ;Refresh (4 hours)
                                1800       ;Retry (30 minutes)
                                1209600    ;Expire (2 weeks)
                                3600       ;Negative Cache TTL (1 hour)
)

@      IN      NS       servidor.empresa.com.br.

@      IN      MX       10  email.empresa.com.br.

servidor IN  A       192.168.0.10
email    IN  A       192.168.0.15
cliente  IN  A       192.168.0.20
windows  IN  A       192.168.0.25

www      IN  CNAME    servidor
meusite  IN  CNAME    servidor
pop      IN  CNAME    email
smtp     IN  CNAME    email

```

- `/etc/bind/db.0.168.192` — arquivo de resolução reversa do domínio `empresa.com.br`:

```
$TTL 86400 ; (1 day)
$ORIGIN 0.168.192.in-addr.arpa.
@      IN      SOA      servidor.empresa.com.br. admin.empresa.com.br. (
                                2018080900 ;Serial (YYYYMMDDnn)
                                14400      ;Refresh (4 hours)
                                1800       ;Retry (30 minutes)
                                1209600    ;Expire (2 weeks)
                                3600       ;Negative Cache TTL (1 hour)
)
@      IN      NS       servidor.empresa.com.br.
@      IN      MX       10  email.empresa.com.br.
10     IN      PTR      servidor.empresa.com.br.
15     IN      PTR      email.empresa.com.br.
20     IN      PTR      cliente.empresa.com.br.
25     IN      PTR      windows.empresa.com.br.
```

- `/etc/resolv.conf` — configuração de resolução de nomes para o *Server_Linux*:

```
domain empresa.com.br
search empresa.com.br
nameserver 127.0.0.1
```

4. Como a interface de rede `eth0` da máquina *Server_Linux* está configurada para obter endereço via DHCP, o *daemon* `dhclient` irá sobrescrever as alterações que fizemos ao arquivo `/etc/resolv.conf` no próximo *reboot*. Para prevenir isso, podemos ativar o atributo `immutable` do arquivo, impedindo sua alteração:

```
# chattr +i /etc/resolv.conf
```

5. Reinicie o `bind` e verifique por possíveis erros:

```
# systemctl restart bind9.service

# systemctl status bind9.service
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since Qui 2018-08-09 21:23:48 -03; 5s ago
     Docs: man:named(8)
  Process: 14402 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 14406 (named)
    CGroup: /system.slice/bind9.service
            └─14406 /usr/sbin/named -f -u bind

Ago 09 21:23:48 servidor named[14406]: zone 22.172.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: zone 16.172.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: zone 27.172.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: zone 127.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: zone 26.172.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: zone 25.172.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: zone localhost/IN: loaded serial 2
Ago 09 21:23:48 servidor named[14406]: zone 28.172.in-addr.arpa/IN: loaded serial 1
Ago 09 21:23:48 servidor named[14406]: all zones loaded
Ago 09 21:23:48 servidor named[14406]: running
```

6. Teste os registros com o uso das ferramentas **nslookup** e **dig**:

```
# nslookup servidor.empresa.com.br
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   servidor.empresa.com.br
Address: 192.168.0.10

# dig -x 192.168.0.25 +noquestion

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> -x 192.168.0.25 +noquestion
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5625
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; ANSWER SECTION:
25.0.168.192.in-addr.arpa. 86400 IN      PTR      windows.empresa.com.br.

;; AUTHORITY SECTION:
0.168.192.in-addr.arpa. 86400  IN      NS       servidor.empresa.com.br.

;; ADDITIONAL SECTION:
servidor.empresa.com.br. 86400  IN      A        192.168.0.10

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Aug 09 21:26:41 -03 2018
;; MSG SIZE rcvd: 129
```

2) Servidor de DNS Secundário



Esta configuração será realizada na máquina virtual *Client_Linux*.

Instale o serviço **ntp** na máquina *Client_Linux*, e configure corretamente sua *timezone*. Em seguida, pare o *daemon* **ntp**, atualize o relógio do sistema para a hora correta usando **ntpd -gq** e reinicie o **ntp**.

Feito isso, configure o servidor de DNS Secundário para o domínio **empresa.com.br**. Importante:

- Não se esqueça de informar o endereço IP do servidor secundário no parâmetro **allow-transfer** do servidor primário.
- Habilite a notificação de servidores secundários via diretiva **notify yes;** no arquivo **named.conf.options** do servidor primário.
- Inclua o servidor secundário nas entradas **NS** das zonas direta e reversa.
- Os arquivos de zona que forem transferidos devem ser gravados no diretório **/etc/bind/sec** do

servidor secundário já que o *daemon* executa como usuário **bind**, que não tem permissão de escrita direta no diretório **/etc/bind**.

1. Antes de mais nada, configure o *Server_Linux* para permitir transferência de zona a partir do servidor secundário *Client_Linux*, e notifiçá-lo sempre que zonas forem atualizadas:

```
# hostname  
servidor
```

```
# egrep -A1 '^ *allow-transfer' /etc/bind/named.conf.options  
allow-transfer { 192.168.0.20; };  
notify yes;
```

2. Adicione entradas para o servidor DNS secundário nos arquivos de zona direta e reversa do domínio **empresa.com.br**, e reinicie o **bind**:

```
# egrep -A1 '^@ *IN *NS' /etc/bind/db.empresa.com.br  
@      IN      NS          servidor.empresa.com.br.  
@      IN      NS          cliente.empresa.com.br.
```

```
# egrep -A1 '^@ *IN *NS' /etc/bind/db.0.168.192  
@      IN      NS          servidor.empresa.com.br.  
@      IN      NS          cliente.empresa.com.br.
```

```
# systemctl restart bind9.service
```

3. A seguir, instale o servidor DNS **bind** e o serviço **ntp** na máquina *Client_Linux*:

```
# hostname  
cliente
```

```
# apt-get install ntp bind9 bind9utils
```

4. Configure a *timezone* do sistema, via **dpkg-reconfigure tzdata**. Escolha **America**, e em seguida **Sao_Paulo**.

```
# dpkg-reconfigure tzdata  
  
Current default time zone: 'America/Sao_Paulo'  
Local time is now:      Sat Sep 22 10:52:48 -03 2018.  
Universal Time is now:  Sat Sep 22 13:52:48 UTC 2018.
```

Pare o **ntp**, atualize o relógio do sistema e reinicie o **ntp**.

```
# systemctl stop ntp ; ntpd -gq ; systemctl start ntp
ntpd: time slew +0.001848s
```

Verifique a hora do sistema.

```
# date
Sat Sep 22 10:53:15 -03 2018
```

5. Agora, configure o **bind**. Ajuste os arquivos de configuração da seguinte forma:

- **/etc/bind/named.conf.options** — opções do servidor **bind**:

```
options {
    directory "/var/cache/bind";

    forwarders {
        192.168.0.10;
    };

    dnssec-validation auto;
    auth-nxdomain no;

    allow-transfer { none; };
    allow-query { internals; };
    allow-recursion { internals; };

    listen-on { 127.0.0.1; 192.168.0.20; };
    listen-on-v6 { none; };

    version none;
};
```

- **/etc/bind/named.conf.local** — configurações locais do servidor **bind**:


```
acl internals { 127.0.0.0/8; 192.168.0.0/24; };

zone "empresa.com.br" {
    type slave;
    file "/etc/bind/sec/db.empresa.com.br";
    masters { 192.168.0.10; };
};

zone "0.168.192.in-addr.arpa" {
    type slave;
    file "/etc/bind/sec/db.0.168.192";
    masters { 192.168.0.10; };
};

include "/etc/bind/zones.rfc1918";
```

- `/etc/resolv.conf` — configuração de resolução de nomes para o *Client_Linux*:

```
domain empresa.com.br
search empresa.com.br
nameserver 127.0.0.1
```

6. Observe que iremos escrever os arquivos transferidos no diretório `/etc/bind/sec`, que ainda não existe. Vamos criá-lo e atribuir permissionamento:

```
# mkdir /etc/bind/sec
# chown bind.root /etc/bind/sec
```

7. Reinicie o `bind` e verifique se os arquivos de zona foram transferidos corretamente:

```
# systemctl restart bind9.service

# systemctl status bind9.service -l
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled)
   Drop-In: /run/systemd/generator/bind9.service.d
            └─50-insserv.conf-$named.conf
   Active: active (running) since Qui 2018-08-09 21:41:27 -03; 2s ago
     Docs: man:named(8)
  Process: 5549 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
 Main PID: 5553 (named)
    CGroup: /system.slice/bind9.service
            └─5553 /usr/sbin/named -f -u bind

Ago 09 21:41:27 cliente named[5553]: all zones loaded
Ago 09 21:41:27 cliente named[5553]: running
Ago 09 21:41:27 cliente named[5553]: zone empresa.com.br/IN: Transfer started.
Ago 09 21:41:27 cliente named[5553]: transfer of 'empresa.com.br/IN' from
192.168.0.10#53: connected using 192.168.0.20#48366
Ago 09 21:41:27 cliente named[5553]: zone empresa.com.br/IN: transferred serial
2018080900
Ago 09 21:41:27 cliente named[5553]: transfer of 'empresa.com.br/IN' from
192.168.0.10#53: Transfer completed: 1 messages, 12 records, 312 bytes, 0.001 secs
(312000 bytes/sec)
Ago 09 21:41:28 cliente named[5553]: zone 0.168.192.in-addr.arpa/IN: Transfer
started.
Ago 09 21:41:28 cliente named[5553]: transfer of '0.168.192.in-addr.arpa/IN' from
192.168.0.10#53: connected using 192.168.0.20#35160
Ago 09 21:41:28 cliente named[5553]: zone 0.168.192.in-addr.arpa/IN: transferred
serial 2018080900
Ago 09 21:41:28 cliente named[5553]: transfer of '0.168.192.in-addr.arpa/IN' from
192.168.0.10#53: Transfer completed: 1 messages, 8 records, 261 bytes, 0.001 secs
(261000 bytes/sec)

# ls -lh /etc/bind/sec/
total 8,0K
-rw-r--r-- 1 bind bind 569 Ago  9 21:41 db.0.168.192
-rw-r--r-- 1 bind bind 720 Ago  9 21:41 db.empresa.com.br
```

8. Finalmente, teste a resolução de nomes no servidor secundário:

```
# nslookup pop.empresa.com.br 192.168.0.20
Server:      192.168.0.20
Address:     192.168.0.20#53

pop.empresa.com.br      canonical name = email.empresa.com.br.
Name:   email.empresa.com.br
Address: 192.168.0.15

# dig -x 192.168.0.10 +noquestion @192.168.0.20

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> -x 192.168.0.10 +noquestion @192.168.0.20
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30045
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; ANSWER SECTION:
10.0.168.192.in-addr.arpa. 86400 IN      PTR      servidor.empresa.com.br.

;; AUTHORITY SECTION:
0.168.192.in-addr.arpa. 86400  IN      NS       servidor.empresa.com.br.

;; ADDITIONAL SECTION:
servidor.empresa.com.br. 86400  IN      A        192.168.0.10

;; Query time: 2 msec
;; SERVER: 192.168.0.20#53(192.168.0.20)
;; WHEN: Thu Aug 09 21:52:36 -03 2018
;; MSG SIZE  rcvd: 121
```

3) Configuração de servidor NFS



Esta configuração será realizada na máquina virtual *Server_Linux*.

Crie e exporte o diretório */dados* via NFS na máquina *Server_Linux* (192.168.0.10), para a máquina *Client_Linux* (192.168.0.20).

1. Instale os pacotes abaixo no servidor:

```
# apt-get install nfs-kernel-server
```

2. Crie o diretório a ser exportado:

```
# mkdir /dados
```

3. Edite o arquivo */etc/exports* para configurar o compartilhamento da pasta:

```
/dados 192.168.0.20(rw,no_root_squash,async,no_subtree_check)
```

4. Finalmente, exporte o diretório e reinicie o serviço NFS. Teste se o *mapping* de pasta está correto.

```
# exportfs -a

# systemctl restart nfs-kernel-server.service
# systemctl restart nfs-common.service

# showmount -e
Export list for servidor:
/dados 192.168.0.20
```

4) Configuração de cliente NFS



Esta configuração será realizada na máquina virtual *Client_Linux*.

Instale e configure o cliente NFS na máquina *Client_Linux* (192.168.0.20), monte o diretório remoto */dados* do servidor no diretório */mnt/remoto*. Finalmente, realize as configurações necessárias para que sempre que a máquina for reiniciada o diretório */dados* seja montado automaticamente.

1. Crie o diretório de montagem:

```
# mkdir /mnt/remoto
```

2. Execute a montagem temporária do diretório NFS e verifique seu funcionamento:

```
# mount -t nfs 192.168.0.10:/dados /mnt/remoto/

# mount | grep '^192.168.0.10:/dados '
192.168.0.10:/dados on /mnt/remoto type nfs4
(rw,relatime,vers=4.0,rsize=65536,wsiz=65536,namlen=255,hard,proto=tcp,timeo=600,r
etrans=2,sec=sys,clientaddr=192.168.0.20,local_lock=none,addr=192.168.0.10)
```

3. Adicione a linha a seguir ao arquivo `/etc/fstab` para que a montagem se torne automática após o *boot*. Reinicie a máquina e verifique seu funcionamento.

```
# tail -n1 /etc/fstab
192.168.0.10:/dados /mnt/remoto nfs defaults 0 0
```

5) Testando o funcionamento do serviço NFS

Na máquina *Server_Linux*, crie um arquivo de nome `teste` no diretório `/dados` e verifique se este aparece no cliente. Depois, edite o arquivo `teste` a partir da máquina *Client_Linux* adicionando a data atual ao conteúdo do arquivo. Volte ao servidor e verifique se o arquivo foi alterado.

1. No servidor, execute:

```
# hostname
servidor

# touch /dados/teste
# ls /dados/
teste
```

2. No cliente, verifique e edite o arquivo:

```
# hostname
cliente

# ls /mnt/remoto/
teste
# echo "$( date )" >> /mnt/remoto/teste
```

3. De volta ao servidor, cheque se o arquivo foi editado com sucesso:

```
# hostname  
servidor  
  
# cat /dados/teste  
Sex Ago 10 14:35:52 -03 2018
```