

Instituto Federal do Sudeste de Minas Gerais – Campus Barbacena
Curso Superior de Tecnologia em Sistemas para Internet

2ª Avaliação de Gerência e Configuração de Serviços de Internet – ERE **198/99 pts**

Nome: Lucas Cristovam Henriques Fonseca **Data:** _____

AVISOS:

- 1 – avaliação individual com consulta permitida a livros impressos e materiais na Internet;
- 2 – não serão consideradas as respostas que por ventura sejam cópias (plágios), sejam de livros, artigos de Internet, colegas e outros meios;
- 3 – havendo cópia (plágio), mesmo que seja de uma questão apenas, toda a prova será anulada sem direito à segunda chance;
- 4 – as respostas escritas deverão ser preenchidas neste mesmo arquivo dentro das caixas de texto correspondentes, com fonte arial 12, espaçamento simples e mesmo tamanho de margem deste arquivo original;
- 5 – o arquivo final, em formato ODT, deverá ser postado no Sigaa em local a ser definido pelo professor até às 23:59 hs do dia 07/02/2022. Se o Sigaa estiver com problemas no momento de envio, o aluno poderá enviar o arquivo como anexo para o e-mail herlon.camargo@ifsudestemg.edu.br respeitando o prazo definido acima;
- 6 – o nome do arquivo texto final deverá ser: SERVIÇOS-221-ERE-SEUNOME.odt, onde “SEUNOME” deverá ser alterado para o primeiro nome do aluno em maiúsculas;
- 7 – a máquina virtual servidora VM-1, e somente ela, deverá ser enviada em formato .OVA (Appliance), com todas as configurações de rede, vídeo e armazenamento realizadas no VirtualBox, de forma que o professor possa executá-la sem a necessidade de realizar nenhuma configuração no VirtualBox (se houver a necessidade do professor realizar alguma configuração no VirtualBox para executar a máquina virtual haverá uma penalidade de 50% na nota final desta avaliação);
- 8 – o nome do arquivo .OVA deverá ser SERVIDOR-221-ERE-SEUNOME.oVA, onde “SEUNOME” deverá ser alterado para o primeiro nome do aluno em maiúsculas;
- 9 – após o fechamento da Appliance, calcular o hash MD5 do arquivo .OVA e informá-lo no campo apropriado abaixo;
- 10 – fazer upload do arquivo .OVA para o Google Drive, compartilhar de forma privada entre o aluno e o professor, e disponibilizar o link para download em campo apropriado abaixo;
- 11 – é de inteira responsabilidade do aluno deixar o arquivo .OVA íntegro no Google Drive (integridade será conferida através do hash MD5 após o professor fazer o download – hashes diferentes indicam adulteração na máquina virtual e, portanto, será atribuída nota zero nesta avaliação, sem direito à segunda chance);
- 12 – o envio de link errado que não corresponda ao arquivo .OVA desta avaliação implicará em nota zero sem direito à segunda chance;
- 12 – havendo indícios de compartilhamento do arquivo .OVA com alguma outra pessoa, além do professor e do próprio aluno, a prova será anulada sem direito à segunda chance;
- 13 – qualquer outra orientação que se julgar pertinente e necessária será informada através do grupo da disciplina no Telegram;
- 13 – Valor desta avaliação: $200 / 2 = 100$ pts.

Hash MD5: 9634f30b07a7c4e4f555a3207647a947

Link do arquivo .OVA:

https://drive.google.com/file/d/1m5QNUaaDgO6diXWrZ5vgmHqahYQprHy_/view?usp=sharing

Instruções para a realização das questões:

1 – instalar duas VMs Servidoras (VM-1 e VM-2) baseadas no sistema operacional **Rocky Linux 8.5** com armazenamento de 8GB, memória RAM de 768 MB a 1024 MB, uma interface de rede em modo bridge e senha do root igual a “prova”;

2 – valor de IP para a VM-1: ip fixo a sua escolha, com último octeto igual a 201 (configuração manual, não pode ser por DHCP), configurado no arquivo de configuração da placa de rede;

3 – valor de IP para a VM-2: ip fixo a sua escolha, com último octeto igual a 202 (configuração manual, não pode ser por DHCP), configurado no arquivo de configuração da placa de rede;

4 – qualquer configuração que tenha sido feita nas VMs deverá ficar ativa após a sua inicialização. O professor não irá executar comando algum para ativar qualquer configuração ou serviço;

5 – as questões deverão atender a “condições necessárias para correção” - CNC descritas em cada questão para que possam ser corrigidas;

NOTA: O provedor mexeu no roteador e deixou a configuracao de rede de uma forma muito esquisita. Mas como ia demorar pra consertarem acabei usando ela assim mesmo. Vai notar nas configuracoes de placa de rede que a mascara tá /23 e o endereco de gateway tá como 10.0.1.0 antes deles mexerem era /24 e o gateway 10.0.1.1.

1 – (60 pts) – Instalar e configurar o servidor de nomes Bind, versão 9, nas máquinas virtuais VM-1 e VM-2. O servidor de nomes deverá atender às seguintes características em cada máquina virtual:

- servidor DNS master na VM-1 respondendo pelos domínios: “seunome.com.br” (substituir “seunome” pelo seu primeiro nome em minúsculas); “animais.com.br”; e “meuprovedor.com”;
- **(01 pts)** – configurar o nome da VM-1 igual a “server1” em ambos os domínios;
- **(01 pts)** – configurar o nome da VM-2 igual a “server2” em ambos os domínios;
- **(04 pts)** – criar um alias nos domínios “seunome.com.br”, “animais.com.br” e “meuprovedor.com” apontando para a VM-1 igual a “www”;
- **(02 pts)** – criar um alias no domínio “meuprovedor.com” apontando para a VM-1 igual a “ftp”;
- **(02 pts)** – criar uma entrada regular no serviço DNS da VM-1 no domínio “seunome.com.br”, apontando para a VM-1, igual a “mail”, que definirá o servidor de e-mail desse domínio como sendo na VM-1;
- **(02 pts)** – criar uma entrada regular no serviço DNS da VM-1 no domínio “animais.com.br”, apontando para a VM-2, igual a “mail”, que definirá o servidor de e-mail desse domínio como sendo na VM-2;
- **(02 pts)** – em todos os domínios, criar a entrada “ns1” apontando para a VM-1 como registro do tipo servidor de nomes;

- **(02 pts)** – em todos os domínios, criar a entrada “ns2” apontando para a VM-2 como registro do tipo servidor de nomes;
- **(05 pts)** – configurar a VM-2 para responder como servidor DNS slave de todos os domínios, inclusive as zonas reversas;
- **(01 pts)** – definir como sendo 03 minutos o intervalo de atualização entre os servidores master e slave;
- **(01 pts)** – definir como sendo 01 minuto o tempo que o servidor slave espera para tentar sincronizar novamente com o servidor master caso este falhe;
- **(01 pts)** – definir como sendo 01 hora o tempo máximo que o servidor slave pode responder pelo domínio no caso de falha do servidor master;
- **(01 pts)** – definir como sendo 5 minutos o tempo mínimo que o servidor slave levará para devolver o domínio ao servidor master quando ele se recuperar;
- **(05 pts)** – configurar a zona reversa para os domínios “seunome.com.br” e “animais.com.br” com informação referente ao registro “mail”;
- **(30 pts)** – no quadro abaixo, fazer um mini-relatório (tutorial) **citando e explicando** todos os passos envolvidos para a resolução desta questão.

CNC: pelo menos um dos servidores DNS deverá responder a uma consulta a algum domínio, seja autoritativo ou externo.

Instalação

Para a instalação do serviço, foi usado o comando abaixo (o parametro -y indica que a instalacao sera realizada sem a necessidade de confirmação):

```
root@server1 ~]# yum install bind bind-utils -y
```

Após a instalação do serviço, foi acessado o arquivo `/etc/named.conf` e na seção options, foram alteradas as opcoes `listen-on` e `allow-query` ambos passaram a ter o valor `any`:

```
root@server1 ~]# vim /etc/named.conf
options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file   "/var/named/data/named.secroots";
    recursing-file  "/var/named/data/named.recursing";
    allow-query     { any; };
}
```

O arquivo foi salvo e então o serviço foi iniciado e habilitado para ser inicializado no boot da máquina:

```
root@server1 ~]# systemctl start named
root@server1 ~]# systemctl enable named
```

Foi realizado o teste usando a ferramenta `dig` para confirmação do funcionamento:

```

root@server1 ~]# dig www.google.com.br @127.0.0.1

<<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> www.google.com.br @127.0.0.1
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 38308
; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: bcaa278c4c4f69e56fa0850f61f96a8098debc390ebea76e (good)
; QUESTION SECTION:
www.google.com.br.          IN      A

; AUTHORITY SECTION:
google.com.br.              5       IN      SOA     ns1.google.com. dns-admin.google.com. 425320538 900 900
1800 60

; Query time: 0 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Tue Feb 01 14:14:40 -03 2022
; MSG SIZE rcvd: 135

```

Uma vez confirmado o funcionamento adequado do servidor de DNS, foi realizada a alteração nas configurações de rede para que use o DNS configurado como DNS padrão:

```

TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=28866342-3b36-4cd3-b616-047eb0fddd20
DEVICE=enp0s3
ONBOOT=yes
IPADDR=10.0.1.201
PREFIX=23
DNS1=127.0.0.1
GATEWAY=10.0.1.0

```

Após isso, a placa de rede foi desligada através do comando *ifdown* e inicializada *ifup*.

Configuração das zonas:

Para a criação das zonas, foi criado o arquivo */etc/named/named.local.conf* e o mesmo foi referenciado no arquivo */etc/named.conf* através da diretiva *include*:

```

root@server1 ~]# vim /etc/named.conf
include "/etc/named/named.local.conf";
root@server1 ~]# vim /etc/named/named.local.conf

```

Então, dentro do arquivo */etc/named/named.local.conf*, foram criadas as zonas conforme a seguir:

```

zone "lucas.com.br" IN {
    type master;
    file "/var/named/data/db.lucas.com.br";
    allow-update { none; };
    allow-transfer { 10.0.1.202; };
};

zone "animais.com.br" IN {
    type master;
    file "/var/named/data/db.animais.com.br";
    allow-update { none; };
    allow-transfer { 10.0.1.202; };
};

zone "meuprovedor.com" IN {
    type master;
    file "/var/named/data/db.meuprovedor.com";
    allow-update { none; };
    allow-transfer { 10.0.1.202; };
};

```

Após a criação das zonas, foi confirmado que o arquivo `*/etc/named/named.local.conf*` permite leitura ao grupo outros:

```

[root@server1 ~]# ls -l /etc/named/named.conf
-rw-r--r--. 1 root root 435 Feb  1 14:38 /etc/named/named.conf

```

Para a configuração do domínio *lucas.com.br*, foi realizada a cópia do arquivo `/var/named/named.localhost` para o diretório `/var/named/data` com o nome `db.lucas.com.br` para facilitar a configuração:

```

[root@server1 ~]# cd /var/named/
[root@server1 named]# cp named.localhost ./data/db.lucas.com.br

```

Após a cópia, o arquivo `db.lucas.com.br` foi alterado conforme abaixo:

```

$TTL 10
@      IN SOA      @ netadmin.lucas.com.br. (
                                2022020101      ; serial
                                3m                ; refresh
                                1m                ; retry
                                1H                ; expire
                                5m )              ; minimum

      NS       ns1
      NS       ns2
      MX  10    mail
      A        10.0.1.201
server1  A      10.0.1.201
server2  A      10.0.1.202
ns1      A      10.0.1.201
ns2      A      10.0.1.202
mail     A      10.0.1.201
www      CNAME   server1

```

Para a configuração do domínio *animais.com.br* foi realizada a cópia do arquivo usado para a configuração do domínio *lucas.com.br* a fim de facilitar a configuração:

```
[root@server1 named]# cp ./data/db.lucas.com.br ./data/db.animais.com.br
```

Após a cópia, o arquivo foi alterado conforme abaixo:

```
$TTL 1D
@      IN SOA      @ netadmin.animais.com.br. (
                                                2022020101      ; serial
                                                3m                ; refresh
                                                1m                ; retry
                                                1H                ; expire
                                                5m                ; minimum

        NS         ns1
        NS         ns2
        MX 10      mail
        A          10.0.1.201
server1  A        10.0.1.201
server2  A        10.0.1.202
ns1      A        10.0.1.201
ns2      A        10.0.1.202
mail     A        10.0.1.202
www      CNAME     server1
```

Para a configuração do domínio meuprovedor.com foi realizada a cópia do arquivo usado para a configuração do domínio lucas.com.br a fim de facilitar a configuração:

```
[root@server1 named]# cp ./data/db.lucas.com.br ./data/db.meuprovedor.com
```

Após a cópia, o arquivo foi alterado conforme abaixo:

```
$TTL 1D
@      IN SOA      @ netadmin.meuprovedor.com. (
                                                2022020101      ; serial
                                                3m                ; refresh
                                                1m                ; retry
                                                1H                ; expire
                                                5m                ; minimum

        NS         ns1
        NS         ns2
        A          10.0.1.201
server1  A        10.0.1.201
server2  A        10.0.1.202
ns1      A        10.0.1.201
ns2      A        10.0.1.202
www      CNAME     server1
ftp      CNAME     server1
```

Após essas configurações, o grupo dos arquivos foi alterado para o grupo *named*:

```
[root@server1 named]# chown :named ./data/db*
[root@server1 named]# ls -l ./data/
total 20
-rw-r----- 1 root  named  303 Feb  1 16:03 db.animais.com.br
-rw-r----- 1 root  named  301 Feb  1 15:58 db.lucas.com.br
-rw-r----- 1 root  named  290 Feb  1 16:09 db.meuprovedor.com
-rw-r--r--  1 named named 5790 Feb  1 15:11 named.run
```

Testando

Feito isso, foram realizados testes com a ferramenta dig:


```
[root@server1 named]# dig www.animais.com.br

;<<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> www.animais.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17820
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b82a033ba1bd8b087b88c0e561f98dd06704a1c8e80007f0 (good)
;; QUESTION SECTION:
;www.animais.com.br.          IN      A

;; ANSWER SECTION:
www.animais.com.br.          86400   IN      CNAME   server1.animais.com.br.
server1.animais.com.br.      86400   IN      A        10.0.1.201

;; AUTHORITY SECTION:
animais.com.br.              86400   IN      NS       ns2.animais.com.br.
animais.com.br.              86400   IN      NS       ns1.animais.com.br.

;; ADDITIONAL SECTION:
ns1.animais.com.br.          86400   IN      A        10.0.1.201
ns2.animais.com.br.          86400   IN      A        10.0.1.202

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 01 16:45:20 -03 2022
;; MSG SIZE rcvd: 181
```

```
<<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> www.lucas.com.br
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43595
; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 5bf35bf6d49f47f99d55d54b61f98f3ef3e5519a4e061606 (good)
; QUESTION SECTION:
;www.lucas.com.br.          IN      A

; ANSWER SECTION:
www.lucas.com.br.          86400   IN      CNAME   server1.lucas.com.br.
server1.lucas.com.br.      86400   IN      A        10.0.1.201

; AUTHORITY SECTION:
lucas.com.br.              86400   IN      NS       ns2.lucas.com.br.
lucas.com.br.              86400   IN      NS       ns1.lucas.com.br.

; ADDITIONAL SECTION:
ns1.lucas.com.br.          86400   IN      A        10.0.1.201
ns2.lucas.com.br.          86400   IN      A        10.0.1.202

; Query time: 0 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Tue Feb 01 16:51:26 -03 2022
; MSG SIZE rcvd: 179
```

DNS Reverso

Para a configuração de zona reversa para os domínios *lucas.com.br* e *animais.com.br*, foi adicionada uma nova zona no arquivo */etc/named/named.local.conf*:

```
zone "1.0.10.in-addr.arpa" IN {
    type master;
    file "/var/named/data/db.1.0.10.in-addr.arpa";
    allow-update { none; };
    allow-transfer { 10.0.1.202; };
};
```

Entao, foi realizada a cópia do arquivo `/var/named/name.loopback` para facilitar a configuracao:

```
root@server1 named]# cp /var/named/name.loopback /var/named/data/db.1.0.10.in-addr.arpa
```

E entao foram realizadas as alterações necessárias:

```
$TTL 1D
@      IN SOA      @ lucaschfonseca.gmail.com. (
                                                2022020101      ; serial
                                                3m      ; refresh
                                                1m      ; retry
                                                1H      ; expire
                                                5m )    ; minimum
      NS       ns1
      NS       ns2
      A        10.0.1.201
ns1    A        10.0.1.201
ns2    A        10.0.1.202
202    PTR     mail.animais.com.br.
201    PTR     mail.lucas.com.br.
```

Em seguida foi realizada a troca do grupo para o arquivo para *named*:

```
root@server1 ~]# chown :named /var/named/data/db.1.0.10.in-addr.arpa
```

E o serviço foi reiniciado:

```
root@server1 ~]# systemctl restart named
```

Foram realizados os testes em ambos os emails:


```

; <<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> -x 10.0.1.202
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9984
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d7e640187744a5c4d5a5300a61f9ae9e5d57eb43bbf33168 (good)
;; QUESTION SECTION:
;202.1.0.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
202.1.0.10.in-addr.arpa. 86400 IN      PTR      mail.animais.com.br.

;; AUTHORITY SECTION:
1.0.10.in-addr.arpa.      86400 IN      NS        ns2.1.0.10.in-addr.arpa.
1.0.10.in-addr.arpa.      86400 IN      NS        ns1.1.0.10.in-addr.arpa.

;; ADDITIONAL SECTION:
ns1.1.0.10.in-addr.arpa. 86400 IN      A         10.0.1.201
ns2.1.0.10.in-addr.arpa. 86400 IN      A         10.0.1.202

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Feb 01 19:05:18 -03 2022
;; MSG SIZE rcvd: 181

```

Sincronização DNS Master-Slave

No server2 (slave) foi instalado o serviço bind:

```
[root@server2 ~]# yum install bind bind-utils -y
```

foi configurada a placa de rede da seguinte forma:

```

TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=ab2b87d7-fdb0-40cb-9305-d3a676857def
DEVICE=enp0s3
ONBOOT=yes
IPADDR=10.0.1.202
PREFIX=23
DNS1=8.8.8.8
GATEWAY=10.0.1.0_

```

Foi acessado o arquivo de configuracao do *named* e na sessao options, foram alterados os parametros *allow-port* e *allow-query* conforme mostrado abaixo:

```
options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file   "/var/named/data/named.secroots";
    recursing-file  "/var/named/data/named.recursing";
    allow-query     { any; };
}
```

E ao final do arquivo foi incluida a referencia ao arquivo externo */etc/named/named.local.conf*:

```
include "/etc/named/named.local.conf";
```

E nele foram criadas as zonas a serem recebidas do master, conforme a seguir:

```
zone "lucas.com.br" IN {
    type slave;
    file "/var/named/slaves/db.lucas.com.br";
    masters { 10.0.1.201; };
};

zone "animais.com.br" IN {
    type slave;
    file "/var/named/slaves/db.animais.com.br";
    masters { 10.0.1.201; };
};

zone "meuprovedor.com" IN {
    type slave;
    file "/var/named/slaves/db.meuprovedor.com";
    masters { 10.0.1.201; };
};

zone "1.0.10.in-addr.arpa" IN {
    type slave;
    file "/var/named/slaves/db.1.0.10.in-addr.arpa";
    masters { 10.0.1.201; };
};
```

feito isso, foi reiniciado o servico e habilitado para iniciar ao ligar a maquina:

```
[root@server2 ~]# systemctl start named
[root@server2 ~]# systemctl enable named
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.
```

Verificando sincronizacao

para verificar se a sincronizacao foi realizada com sucesso, foi usado o comando abaixo:

```
[root@server2 ~]# ls -l /var/named/slaves/
total 16
-rw-r--r--. 1 named named 512 Feb  2 00:22 db.1.0.10.in-addr.arpa
-rw-r--r--. 1 named named 611 Feb  2 00:25 db.animais.com.br
-rw-r--r--. 1 named named 579 Feb  2 00:22 db.lucas.com.br
-rw-r--r--. 1 named named 584 Feb  2 00:26 db.meuprovedor.com
```

Em seguida, foram realizados testes com a ferramenta *dig*:

```
[root@server2 named]# dig www.lucas.com.br @10.0.1.202
;
; <<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> www.lucas.com.br @10.0.1.202
;
; global options: +cmd
; Got answer:
; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 34767
; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3
;
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: aabfc579810088f41682503061f9ebd943b1845cf264d6e7 (good)
; QUESTION SECTION:
;www.lucas.com.br.      IN      A
;
; ANSWER SECTION:
www.lucas.com.br.      86400   IN      CNAME   server1.lucas.com.br.
server1.lucas.com.br. 86400   IN      A        10.0.1.201
;
; AUTHORITY SECTION:
animais.com.br.        86400   IN      NS       ns1.animais.com.br.
animais.com.br.        86400   IN      NS       ns2.animais.com.br.
;
; ADDITIONAL SECTION:
ns1.animais.com.br.    86400   IN      A        10.0.1.201
ns2.animais.com.br.    86400   IN      A        10.0.1.202
```

Apos a confirmação do funcionamento, foi realizada a alteração do DNS na configuração da placa de rede, passando a usar o dns do serviço configurado:

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=ab2b87d7-fdb0-40cb-9305-d3a676857def
DEVICE=enp0s3
ONBOOT=yes
IPADDR=10.0.1.202
PREFIX=23
DNS1=127.0.0.1
GATEWAY=10.0.1.0
```

e a placa foi reiniciada através dos comandos `ifdown` e `ifup`.

58 pts 2 – (60 pts) – Instalar e configurar o servidor Web Apache, versão 2.4, na VM-1, de forma que ele atenda às seguintes características:

- Apache deverá responder pelos sites “www.seunome.com.br”, “www.animais.com.br” e “www.meuprovedor.com”;
- **(03 pts)** – o site “www.seunome.com.br” deverá ter seu diretório raiz em “/var/www/html/seunome.com.br”; o site “www.animais.com.br” deverá ter seu diretório raiz em “/var/www/html/animais.com.br”; e o site “www.meuprovedor.com” deverá ter seu diretório raiz em “/var/www/html/meuprovedor.com”;
- **(08 pts)** – o site “www.animais.com.br” deverá ter sua estrutura de páginas com seus respectivos links idêntica à apresentada nas videoaulas;
- **(02 pts)** – os sites “www.seunome.com.br” e “www.meuprovedor.com” poderão conter apenas uma página “index.html” identificando o respectivo site;
- **(10 pts)** – todas as páginas de todos os sites deverão suportar https em sua porta padrão e, caso sejam chamadas via http em sua porta padrão, deverão ser redirecionadas automaticamente para https tanto para as páginas existentes quanto para as possíveis futuras novas páginas. Os sites deverão apresentar seus respectivos certificados em seus próprios nomes;
- **(04 pts)** – exibir o conteúdo do site “www.meuprovedor.com” caso o servidor seja contatado por endereço IP ou por um domínio não existente mas que leve a esse servidor;
- **02 pts (03 pts)** – exibir uma página com o texto “Ops! A página que você procurou no site ‘www.DOMÍNIO’ não foi encontrada” caso uma página inexistente tenha sido solicitada a esse DOMÍNIO. Atentar que é uma página diferente para cada domínio (substituir DOMÍNIO por “seunome.com.br”, “animais.com.br” ou “meuprovedor.com” conforme o caso);
- **(30 pts)** – no quadro abaixo, fazer um mini-relatório (tutorial) **citando e explicando** todos os passos envolvidos para a resolução desta questão.

CNC: o servidor Web deverá apresentar, no mínimo, uma página qualquer.

para configurar os nomes com os quais a máquina deve ser reconhecida, foi acessado o arquivo hosts

```
[root@server1 ~]# vim /etc/hosts
```

e adicionada a seguinte linha:

```
10.0.1.201 www.animais.com.br www.lucas.com.br www.meuprovedor.com
```

Então, foi realizado o teste de ping:

```
[root@server1 ~]# ping www.lucas.com.br
PING www.animais.com.br (10.0.1.201) 56(84) bytes of data.
64 bytes from www.animais.com.br (10.0.1.201): icmp_seq=1 ttl=64 time=0.041 ms
64 bytes from www.animais.com.br (10.0.1.201): icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from www.animais.com.br (10.0.1.201): icmp_seq=3 ttl=64 time=0.057 ms
```

Uma vez confirmado o funcionamento, foi instalada a ferramenta httpd:

```
[root@server1 ~]# yum install httpd -y
```

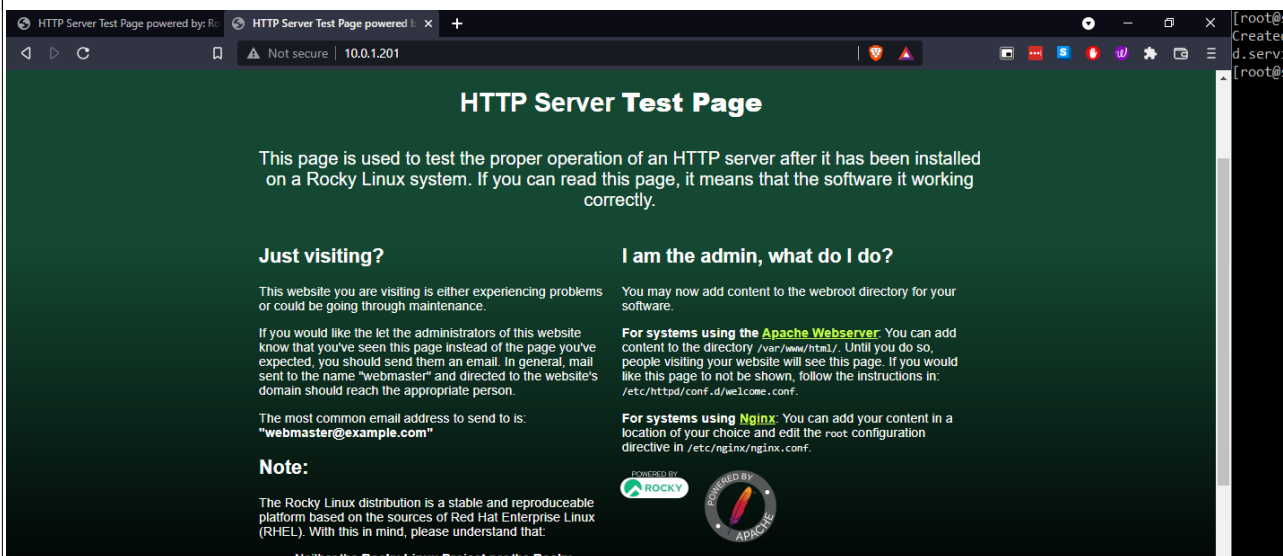
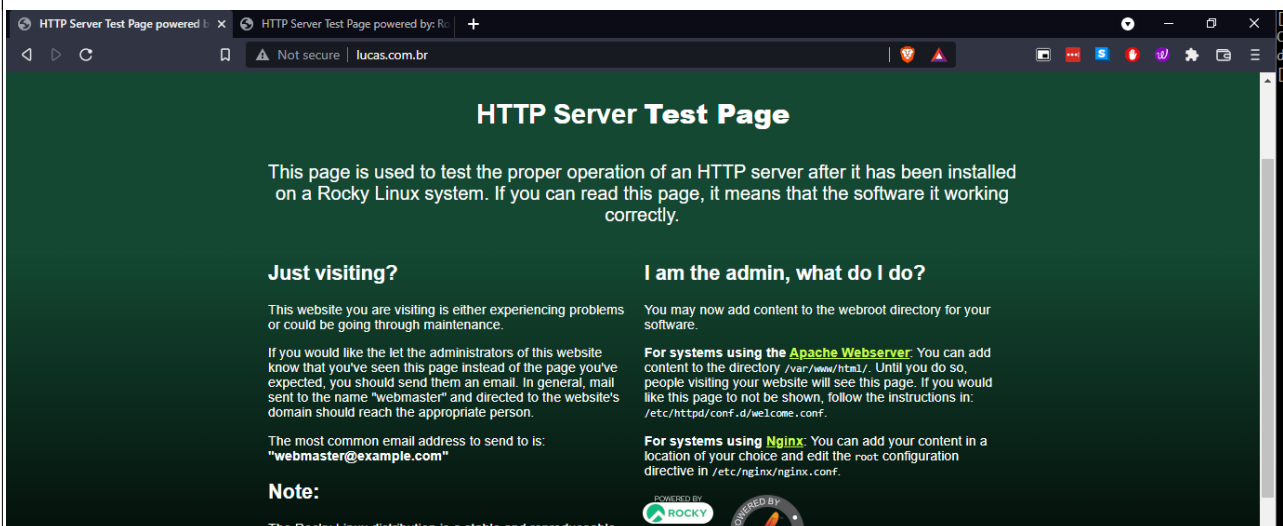
Feita a instalação, foi realizada a inicializacao do servico:

```
[root@server1 ~]# systemctl start httpd
[root@server1 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
```

No cliente (windows) foi adicionada a seguinte linha no arquivo *C:\Windows\System32\drivers\etc\hosts*:

```
10.0.1.201 www.animais.com.br www.lucas.com.br www.meuprovedor.com
```

Entao, foram realizados acessos de teste:



Uma vez confirmado o funcionamento do servico, foi realizada a configuracao dos sites.

Foi criado um arquivo conf no diretorio *etc/httpd/conf.d* para cada um dos sites :

```
[root@server1 ~]# cd /etc/httpd/conf.d/
```

Para o site *animais.com.br*

```
[root@server1 conf.d]# vim www.animais.com.br.conf
```

```
<VirtualHost *:80>
    ServerName www.animais.com.br
    DocumentRoot "/var/www/html/animais.com.br"
</VirtualHost>
```

para o site *lucas.com.br*

```
[root@server1 conf.d]# vim www.lucas.com.br.conf
```

```
<VirtualHost *:80>
    ServerName www.lucas.com.br
    DocumentRoot "/var/www/html/lucas.com.br/"
</VirtualHost>
```

Para o site *meuprovedor.com*:

```
[root@server1 conf.d]# vim www.meuprovedor.com.conf
```

```
<VirtualHost *:80>
    ServerName www.meuprovedor.com
    DocumentRoot "/var/www/html/meuprovedor.com/"
</VirtualHost>
```

Entao, foi reiniciado o servico.

O conteudo dos sites foi criado no windows e copiado via winSCP para o diretorio *var/www/html* da VM.

```
▼ animais.com.br
  ▼ caninos
    <> cao.html
    <> index.html
    <> raposa.html
  ▼ felinos
    ▼ gato
      <> index.html
    ► leao
      <> index.html
    ► figuras
      <> erro_404.html
      <> index.html
  ▼ lucas.com.br
    <> erro_404.html
    <> index.html
  ▼ meuprovedor.com
    <> erro_404.html
    <> index.html
```


O conteudo do site animais é o mesmo do apresentado em aula, por isso não vou detalhar.

No site *lucas.com.br*, há apenas uma pagina *index.html* com uma saudacao:

```
1  <html>
2      <center>
3          <h1>
4              Bem vindo à pagina do lucas!
5          </h1>
6      </center>
7  </html>
```

No site *meuprovedor.com*, tambem há apenas uma pagina *index.html* :

```
<html>
  <center>
    <h1>
      Bem vindo à pagina do meu provedor!
    </h1>
  </center>
</html>
```

Entao, foi realizado o acesso em todos eles:



www.animais.com.br

www.lucas.com.br

www.meuprovedor.com

+

Not secure | meuprovedor.com

Bem vindo à pagina do meu provedor!

(não vou colocar as imagens de todos os testes porque ficaria muito grande)

Confirmado o funcionamento de ambos os sites, foi removida a pagina padrao de teste. Para isso foi acessado o arquivo *welcome.conf* localizado em */etc/httpd/conf.d* e, todo o seu conteudo foi comentado:

```
[root@server1 html]# vim /etc/httpd/conf.d/welcome.conf
```

```
#
# This configuration file enables the default "Welcome" page if there
# is no default index page present for the root URL.  To disable the
# Welcome page, comment out all the lines below.
#
# NOTE: if this file is removed, it will be restored on upgrades.
#
#<LocationMatch "^/+>$">
#   Options -Indexes
#   ErrorDocument 403 /.noindex.html
#</LocationMatch>
#
#<Directory /usr/share/httpd/noindex>
#   AllowOverride None
#   Require all granted
#</Directory>
#
#Alias /.noindex.html /usr/share/httpd/noindex/index.html
#Alias /poweredby.png /usr/share/httpd/icons/apache_pb3.png
```

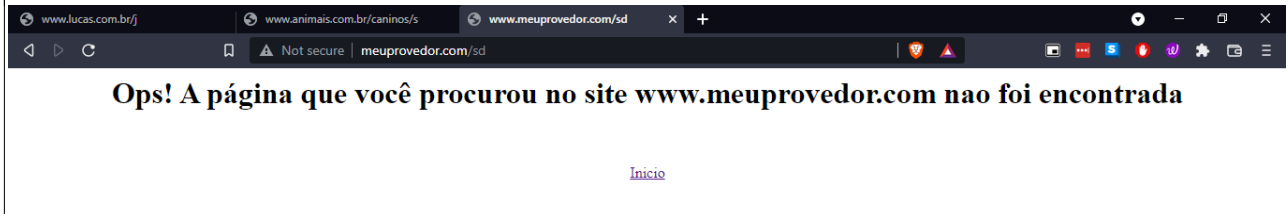
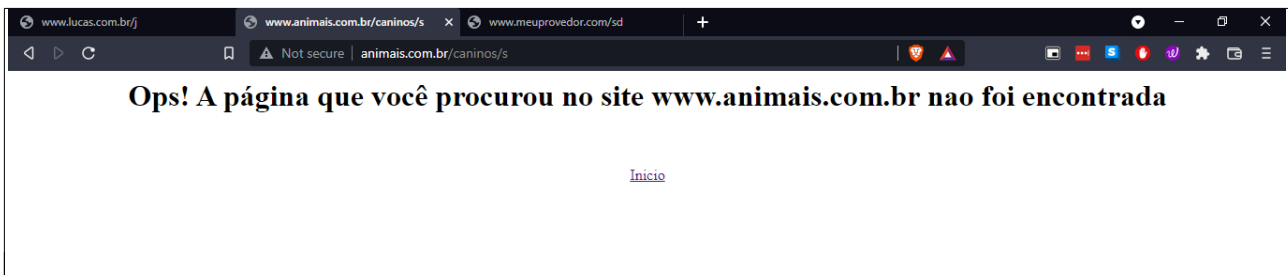
Para definir o site www.meuprovedor.com como site padrao, foi criado o arquivo *000-default.conf* no diretorio *conf.d*:

```
[root@server1 html]# cd /etc/httpd/conf.d/
[root@server1 conf.d]# vim 000-default.conf
```

e nele foi definido o seguinte conteudo:

```
<VirtualHost *:80>
    DocumentRoot "/var/www/html/meuprovedor.com"
</VirtualHost>
```

Entao, foi reiniciado o servico e executado o teste de acesso:



Para habilitar o https, no arquivo *openssl.cnf*:

```
[root@server1 ~]# vim /etc/pki/tls/openssl.cnf
```

foi alterada a diretiva *home*

```
HOME = $ENV::HOME
```

e a diretiva *dir* na sessão *CA_default*:

```
[ CA_default ]
dir = $HOME/CA
```

então, foi criada a estrutura de diretórios e arquivos:

```
[root@server1 ~]# mkdir -p ~/CA/private
[root@server1 ~]# mkdir ~/CA/newcerts
[root@server1 ~]# touch ~/CA/index.txt
[root@server1 ~]# echo 01 > ~/CA/serial
```

Feito isso foi criada a chave privada e o certificado CA:

```
[root@server1 ~]# cd ~/CA
[root@server1 CA]# openssl req -nodes -new -x509 -keyout ./private/cakey.pem -out cacert.pem -days 365
Generating a RSA private key
.....+++++
.....+++++
writing new private key to './private/cakey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:BR
State or Province Name (full name) []:MG
Locality Name (eg, city) [Default City]:Barbacena
Organization Name (eg, company) [Default Company Ltd]:ICP Prova servicoes
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
[root@server1 CA]#
```

Entao, foi gerada a chave publica:

```
[root@server1 CA]# openssl rsa -in ./private/cakey.pem -pubout -
writing RSA key
[root@server1 CA]#
```

Foram criadas chaves para as seguintes maquinas:

www.lucas.com.br

www.animais.com.br

www.meuprovedor.com

mail.lucas.com.br

mail.animais.com.br

[ftp.meuprovedor.com](ftp://meuprovedor.com)

NOTA: Nao vou colocar o screenshot de todas pois o arquivo já esta muito grande

```
[root@server1 CA]# openssl req -nodes -new -addext "subjectAltName = DNS:localhost" -keyout priv-www.lu
as.com.br.pem -out req-www.lucas.com.br.csr -days 365
Ignoring -days; not generating a certificate
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'priv-www.lucas.com.br.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:BR
State or Province Name (full name) []:Minas Gerais
Locality Name (eg, city) [Default City]:Barbacena
Organization Name (eg, company) [Default Company Ltd]:Lucas LTDA
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:www.lucas.com.br
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@server1 CA]#
```

```
[root@server1 CA]# ls -l
total 60
-rw-r--r--. 1 root root 1265 Feb  2 16:58 cacert.pem
-rw-r--r--. 1 root root  451 Feb  2 17:00 cackeypub.pem
-rw-r--r--. 1 root root   0 Feb  2 16:31 index.txt
drwxr-xr-x. 2 root root  6 Feb  2 16:31 newcerts
drwxr-xr-x. 2 root root 23 Feb  2 16:56 private
-rw-----. 1 root root 1704 Feb  2 17:33 priv-ftp.meuprovedor.com.pem
-rw-----. 1 root root 1704 Feb  2 17:22 priv-mail.animais.com.br.pem
-rw-----. 1 root root 1708 Feb  2 17:21 priv-mail.lucas.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:19 priv-www.animais.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:13 priv-www.lucas.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:31 priv-www.meuprovedor.com.pem
-rw-r--r--. 1 root root 1070 Feb  2 17:33 req-ftp.meuprovedor.com.csr
-rw-r--r--. 1 root root 1062 Feb  2 17:22 req-mail.animais.com.br.csr
-rw-r--r--. 1 root root 1058 Feb  2 17:22 req-mail.lucas.com.br.csr
-rw-r--r--. 1 root root 1062 Feb  2 17:19 req-www.animais.com.br.csr
-rw-r--r--. 1 root root 1058 Feb  2 17:15 req-www.lucas.com.br.csr
-rw-r--r--. 1 root root 1070 Feb  2 17:31 req-www.meuprovedor.com.csr
-rw-r--r--. 1 root root   3 Feb  2 16:31 serial
```

Criadas as chaves, foi realizada a assinatura das chaves:


```

[root@server1 CA]# openssl x509 -req -in req-www.lucas.com.br.csr -CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial -out cert-www.lucas.com.br.pem -days 365
Signature ok
subject=C = BR, ST = Minas Gerais, L = Barbacena, O = Lucas LTDA, CN = www.lucas.com.br
Getting CA Private Key
[root@server1 CA]# openssl x509 -req -in req-www.animais.com.br.csr -CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial -out cert-www.animais.com.br.pem -days 365
Signature ok
subject=C = BR, ST = Minas Gerais, L = Barbacena, O = Animais SA, CN = www.animais.com.br
Getting CA Private Key
[root@server1 CA]# openssl x509 -req -in req-www.meuprovedor.com.csr -CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial -out cert-www.meuprovedor.com.pem -days 365
Signature ok
subject=C = BR, ST = Minas Gerais, L = Barbacena, O = Meu provedor LTDA, CN = www.meuprovedor.com
Getting CA Private Key
[root@server1 CA]# openssl x509 -req -in req-mail.animais.com.br.csr -CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial -out cert-mail.animais.com.br.pem -days 365
Signature ok
subject=C = BR, ST = Minas Gerais, L = Barbacena, O = Animais SA, CN = mail.animais.com.br
Getting CA Private Key
[root@server1 CA]# openssl x509 -req -in req-mail.lucas.com.br.csr -CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial -out cert-mail.lucas.com.br.pem -days 365
Signature ok
subject=C = BR, ST = Minas Gerais, L = Barbacena, O = Lucas LTDA, CN = mail.lucas.com.br
Getting CA Private Key
[root@server1 CA]# openssl x509 -req -in req-ftp.meuprovedor.com.csr -CA ./cacert.pem -CAkey ./private/cakey.pem -CAserial ./serial -out cert-ftp.meuprovedor.com.pem -days 365
Signature ok
subject=C = BR, ST = Minas Gerais, L = Barbacena, O = Meu provedor LTDA, CN = ftp.meuprovedor.com
Getting CA Private Key
[root@server1 CA]#

```

```

root@server1 CA]# ls -l
total 84
-rw-r--r--. 1 root root 1265 Feb  2 16:58 cacert.pem
-rw-r--r--. 1 root root  451 Feb  2 17:00 cackeypub.pem
-rw-r--r--. 1 root root 1168 Feb  2 17:37 cert-ftp.meuprovedor.com.pem
-rw-r--r--. 1 root root 1159 Feb  2 17:37 cert-mail.animais.com.br.pem
-rw-r--r--. 1 root root 1155 Feb  2 17:37 cert-mail.lucas.com.br.pem
-rw-r--r--. 1 root root 1159 Feb  2 17:36 cert-www.animais.com.br.pem
-rw-r--r--. 1 root root 1155 Feb  2 17:36 cert-www.lucas.com.br.pem
-rw-r--r--. 1 root root 1168 Feb  2 17:37 cert-www.meuprovedor.com.pem
-rw-r--r--. 1 root root   0 Feb  2 16:31 index.txt
-rwxr-xr-x. 2 root root   6 Feb  2 16:31 newcerts
-rwxr-xr-x. 2 root root  23 Feb  2 16:56 private
-rw-----. 1 root root 1704 Feb  2 17:33 priv-ftp.meuprovedor.com.pem
-rw-----. 1 root root 1704 Feb  2 17:22 priv-mail.animais.com.br.pem
-rw-----. 1 root root 1708 Feb  2 17:21 priv-mail.lucas.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:19 priv-www.animais.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:13 priv-www.lucas.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:31 priv-www.meuprovedor.com.pem
-rw-r--r--. 1 root root 1070 Feb  2 17:33 req-ftp.meuprovedor.com.csr
-rw-r--r--. 1 root root 1062 Feb  2 17:22 req-mail.animais.com.br.csr
-rw-r--r--. 1 root root 1058 Feb  2 17:22 req-mail.lucas.com.br.csr
-rw-r--r--. 1 root root 1062 Feb  2 17:19 req-www.animais.com.br.csr
-rw-r--r--. 1 root root 1058 Feb  2 17:15 req-www.lucas.com.br.csr
-rw-r--r--. 1 root root 1070 Feb  2 17:31 req-www.meuprovedor.com.csr
-rw-r--r--. 1 root root   3 Feb  2 17:37 serial

```

Apos a geracao dos certificados e das chaves, foram copiadas as chaves privadas e os certificados para o diretorio `/etc/ssl/mycerts`

```

root@server1 CA]# cp cert-* /etc/ssl/mycerts/
root@server1 CA]# cp priv-* /etc/ssl/mycerts/
root@server1 CA]# ls -l /etc/ssl/mycerts/
total 48
-rw-r--r--. 1 root root 1168 Feb  2 17:44 cert-ftp.meuprovedor.com.pem
-rw-r--r--. 1 root root 1159 Feb  2 17:44 cert-mail.animais.com.br.pem
-rw-r--r--. 1 root root 1155 Feb  2 17:44 cert-mail.lucas.com.br.pem
-rw-r--r--. 1 root root 1159 Feb  2 17:44 cert-www.animais.com.br.pem
-rw-r--r--. 1 root root 1155 Feb  2 17:44 cert-www.lucas.com.br.pem
-rw-r--r--. 1 root root 1168 Feb  2 17:44 cert-www.meuprovedor.com.pem
-rw-----. 1 root root 1704 Feb  2 17:44 priv-ftp.meuprovedor.com.pem
-rw-----. 1 root root 1704 Feb  2 17:44 priv-mail.animais.com.br.pem
-rw-----. 1 root root 1708 Feb  2 17:44 priv-mail.lucas.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:44 priv-www.animais.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:44 priv-www.lucas.com.br.pem
-rw-----. 1 root root 1704 Feb  2 17:44 priv-www.meuprovedor.com.pem

```

foi então alterado o grupo das chaves privadas para o grupo apache e foi dada a permissão de leitura ao grupo:

```

[root@server1 mycerts]# chown :apache priv-*
[root@server1 mycerts]# chmod g+r priv-*
[root@server1 mycerts]# ls -l
total 48
-rw-r--r--. 1 root root 1168 Feb  2 17:44 cert-ftp.meuprovedor.com.pem
-rw-r--r--. 1 root root 1159 Feb  2 17:44 cert-mail.animais.com.br.pem
-rw-r--r--. 1 root root 1155 Feb  2 17:44 cert-mail.lucas.com.br.pem
-rw-r--r--. 1 root root 1159 Feb  2 17:44 cert-www.animais.com.br.pem
-rw-r--r--. 1 root root 1155 Feb  2 17:44 cert-www.lucas.com.br.pem
-rw-r--r--. 1 root root 1168 Feb  2 17:44 cert-www.meuprovedor.com.pem
-rw-r-----. 1 root apache 1704 Feb  2 17:44 priv-ftp.meuprovedor.com.pem
-rw-r-----. 1 root apache 1704 Feb  2 17:44 priv-mail.animais.com.br.pem
-rw-r-----. 1 root apache 1708 Feb  2 17:44 priv-mail.lucas.com.br.pem
-rw-r-----. 1 root apache 1704 Feb  2 17:44 priv-www.animais.com.br.pem
-rw-r-----. 1 root apache 1704 Feb  2 17:44 priv-www.lucas.com.br.pem
-rw-r-----. 1 root apache 1704 Feb  2 17:44 priv-www.meuprovedor.com.pem

```

Feito isso, foi instalado a ferramenta *mod_ssl*:

```
[root@server1 mycerts]# yum install mod_ssl -y
```

Feito isso, foi realizada uma copia de todos os arquivos de configuracoes dos sites transformando-os em ssl:

```
[root@server1 mycerts]# cd /etc/httpd/conf.d/
[root@server1 conf.d]# cp
000-default.conf          ssl.conf                  www.animais.com.br.conf
autoindex.conf            userdir.conf             www.lucas.com.br.conf
README                    welcome.conf             www.meuprovedor.com.conf
[root@server1 conf.d]# cp www.animais.com.br.conf ssl-www.animais.com.br.conf
[root@server1 conf.d]# cp www.lucas.com.br.conf ssl-www.lucas.com.br.conf
[root@server1 conf.d]# cp www.meuprovedor.com.conf ssl-www.meuprovedor.com.conf
[root@server1 conf.d]# ls -l
total 56
-rw-r--r--. 1 root root  75 Feb  2 12:01 000-default.conf
-rw-r--r--. 1 root root 2926 Jan 25 13:27 autoindex.conf
-rw-r--r--. 1 root root  400 Jan 25 13:27 README
-rw-r--r--. 1 root root 8720 Jan 25 13:25 ssl.conf
-rw-r--r--. 1 root root  138 Feb  2 17:58 ssl-www.animais.com.br.conf
-rw-r--r--. 1 root root  134 Feb  2 17:58 ssl-www.lucas.com.br.conf
-rw-r--r--. 1 root root  143 Feb  2 17:59 ssl-www.meuprovedor.com.conf
-rw-r--r--. 1 root root 1252 Jan 25 13:25 userdir.conf
-rw-r--r--. 1 root root  584 Feb  2 11:53 welcome.conf
-rw-r--r--. 1 root root  138 Feb  2 12:17 www.animais.com.br.conf
-rw-r--r--. 1 root root  134 Feb  2 12:24 www.lucas.com.br.conf
-rw-r--r--. 1 root root  143 Feb  2 12:27 www.meuprovedor.com.conf
```

E em todos os arquivos ssl foram inseridas as informacoes SSL:

```
<VirtualHost *:443>
    ServerName www.animais.com.br
    DocumentRoot "/var/www/html/animais.com.br/"
    ErrorDocument 404 /erro_404.html

    SSLEngine on
    SSLCertificateFile "/etc/ssl/mycerts/cert-www.animais.com.br.pem"
    SSLCertificateKeyFile "/etc/ssl/mycerts/priv-www.animais.com.br.pem"
</VirtualHost>
```

```
<VirtualHost *:443>
    ServerName www.lucas.com.br
    DocumentRoot "/var/www/html/lucas.com.br/"
    ErrorDocument 404 /erro_404.html

    SSLEngine on
    SSLCertificateFile "/etc/ssl/mycerts/cert-www.lucas.com.br.pem"
    SSLCertificateKeyFile "/etc/ssl/mycerts/priv-www.lucas.com.br.pem"
</VirtualHost>
```

```
<VirtualHost *:443>
    ServerName www.meuprovedor.com
    DocumentRoot "/var/www/html/meuprovedor.com/"
    ErrorDocument 404 /erro_404.html

    SSLEngine on
    SSLCertificateFile "/etc/ssl/mycerts/cert-www.meuprovedor.com.pem"
    SSLCertificateKeyFile "/etc/ssl/mycerts/priv-www.meuprovedor.com.pem"
</VirtualHost>
```

Para a ativação do uso obrigatório do https, foram alterados os arquivos de configuração :
para o animais.com.br:

```
<VirtualHost *:80>
    ServerName www.animais.com.br
    DocumentRoot "/var/www/html/animais.com.br/"
    ErrorDocument 404 /erro_404.html

    <Directory "/var/www/html/animais.com.br/">
        SSLRequireSSL
    </Directory>

    Redirect / https://www.animais.com.br/
</VirtualHost>
```

para lucas.com.br:

```
<VirtualHost *:80>
    ServerName www.lucas.com.br
    DocumentRoot "/var/www/html/lucas.com.br/"
    ErrorDocument 404 /erro_404.html

    <Directory "/var/www/html/lucas.com.br/">
        SSLRequireSSL
    </Directory>

    Redirect / https://www.lucas.com.br/
</VirtualHost>
```

e para meuprovedor.com:

```
<VirtualHost *:80>
    ServerName www.meuprovedor.com
    DocumentRoot "/var/www/html/meuprovedor.com/"
    ErrorDocument 404 /erro_404.html

    <Directory "/var/www/html/meuprovedor.com/">
        SSLRequireSSL
    </Directory>

    Redirect / https://www.meuprovedor.com/
</VirtualHost>
```

Feito isso foi reiniciado o serviço e acessadas as páginas:



3 – (20 pts) – Instalar e configurar o servidor FTP vsftpd, na VM-1, atendendo às seguintes características:

- **(01 pts)** – não permitir nenhum tipo de acesso anônimo;
- **(02 pts)** – permitir que o usuário “seunome”, com senha “123456”, acesse remotamente, via FTP, somente o seu respectivo diretório “home” (/var/www/html/seunome.com.br) e seus subdiretórios, e possa ler e gravar arquivos com o mínimo de permissão necessária;
- **(02 pts)** – permitir que o usuário “animais”, com senha “123456”, acesse remotamente, via FTP, somente o seu respectivo diretório “home” (/var/www/html/animais.com.br) e seus subdiretórios, e possa ler e gravar arquivos com o mínimo de permissão necessária;
- **(03 pts)** – permitir que se possa fazer acesso via “FTP sobre TLS (STARTTLS)” de forma obrigatória, utilizando certificado em nome de “ftp.meuprovedor.com”;
- **(02 pts)** – permitir que o servidor Web Apache exiba as páginas dos respectivos diretórios citados acima, com o mínimo de permissão necessária;
- **(10 pts)** – no quadro abaixo, fazer um mini-relatório (tutorial) **citando** e **explicando** todos os passos envolvidos para a resolução desta questão.

CNC: o servidor FTP deverá permitir um acesso remoto satisfatório com pelo menos um dos usuários, seja com criptografia ou não.

Instalação

Para a instalação do serviço, foi usado o comando abaixo (o parametro -y indica que a instalacao sera realizada sem a necessidade de confirmação):

```
[root@server1 ~]# yum install vsftpd -y
```

Feita a instalação, foi acessado o arquivo de configuracao do *vsftpd*:

```
[root@server1 ~]# vim /etc/vsftpd/vsftpd.conf
```

e alterada a *umask local* para 027 para restringir as permissões

```
# Default umask for local users is 077. You may wish to change this to 022,  
# if your users expect that (022 is used by most other ftpd's)  
local_umask=027
```

A fim de restringir o acesso do usuario à somente seu diretório home, foram definidas as diretivas:

```
allow_writeable_chroot=YES  
chroot_local_user=YES
```

Foi então iniciado e habilitado o serviço:

```
[root@server1 ~]# systemctl start vsftpd
[root@server1 ~]# systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@server1 ~]#
```

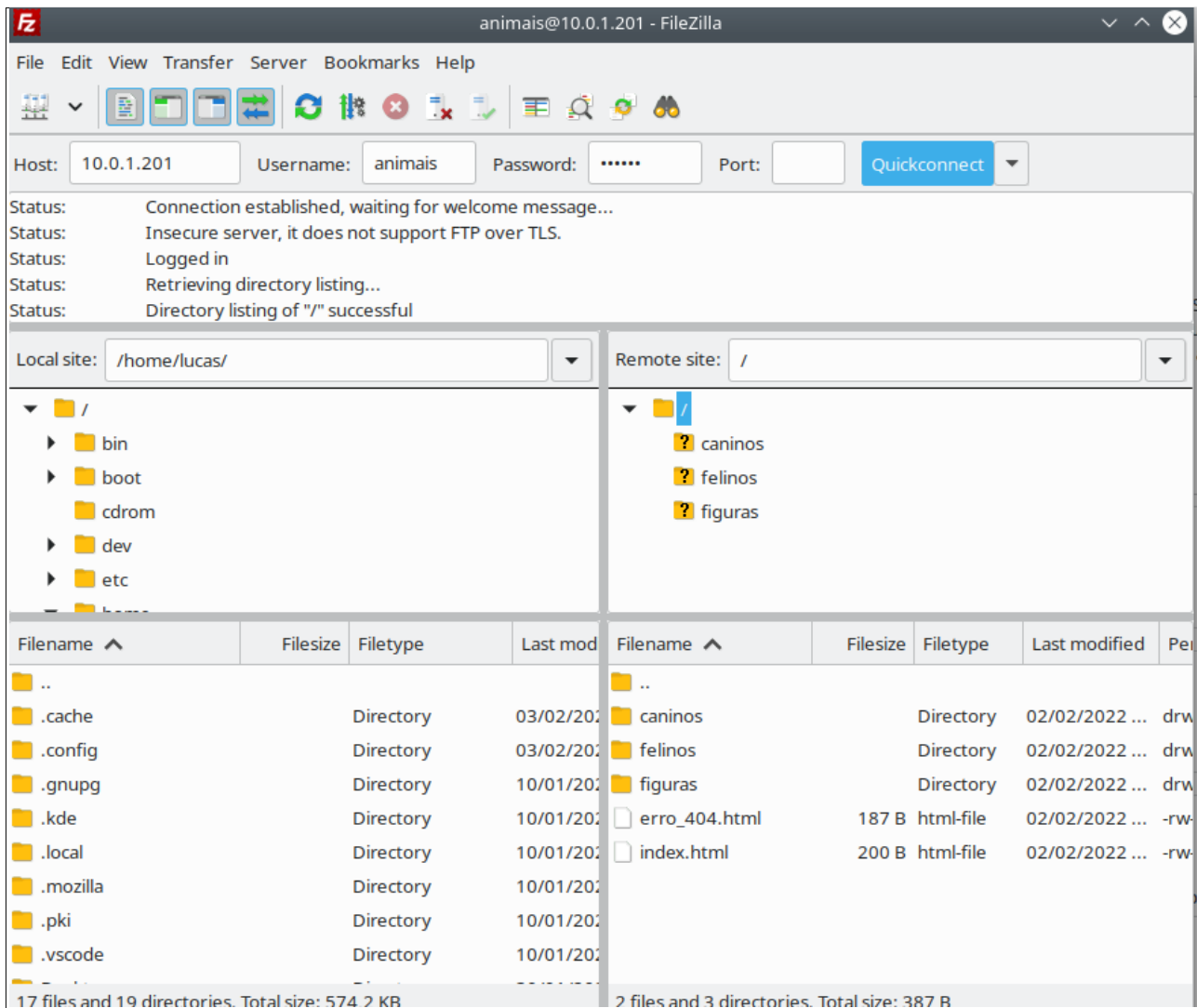
Foram criados os usuarios *lucas* e *animais* ambos com as senhas 123456

```
[root@server1 ~]# useradd -d /var/www/html/animais.com.br animais
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
[root@server1 ~]# passwd animais
Changing password for user animais.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server1 ~]# useradd -d /var/www/html/lucas.com.br lucas
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
[root@server1 ~]# passwd lucas
Changing password for user lucas.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server1 ~]#
```

e então, foram configuradas as permissões e informações de grupos dos diretórios:

```
[root@server1 ~]# chown -R lucas:apache /var/www/html/lucas.com.br
[root@server1 ~]# chown -R animais:apache /var/www/html/animais.com.br
[root@server1 ~]# chmod g+s /var/www/html/lucas.com.br
[root@server1 ~]# chmod g+s /var/www/html/animais.com.br
[root@server1 ~]# ls -l /var/www/html/
total 0
drwxr-sr-x. 5 animais apache 90 Feb  2 12:19 animais.com.br
drwxr-sr-x. 2 lucas   apache 45 Feb  2 12:19 lucas.com.br
drwxr-xr-x. 2 root   root   45 Feb  2 12:19 meuprovedor.com
```

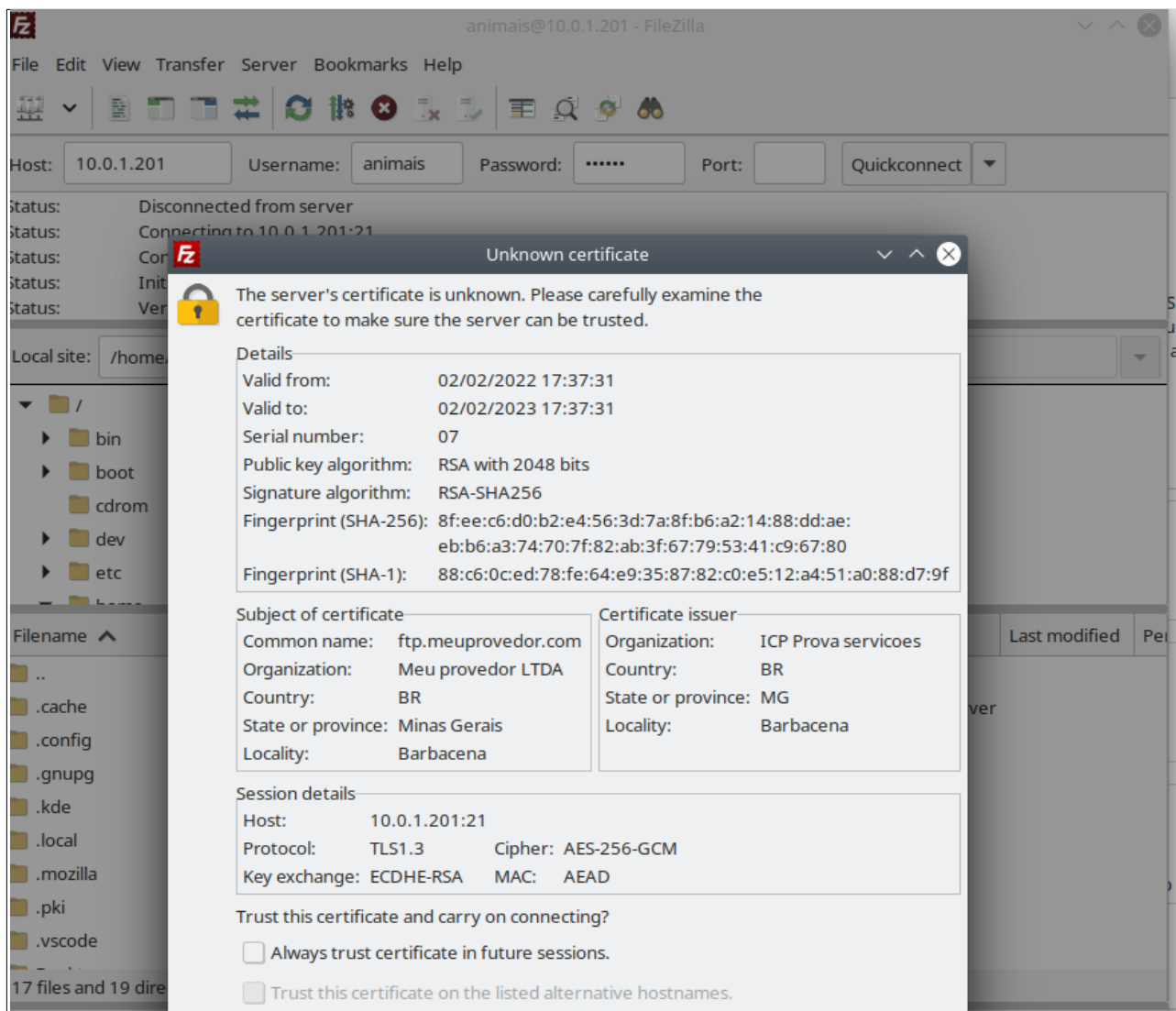
E foi realizado um acesso para confirmação através do filezila



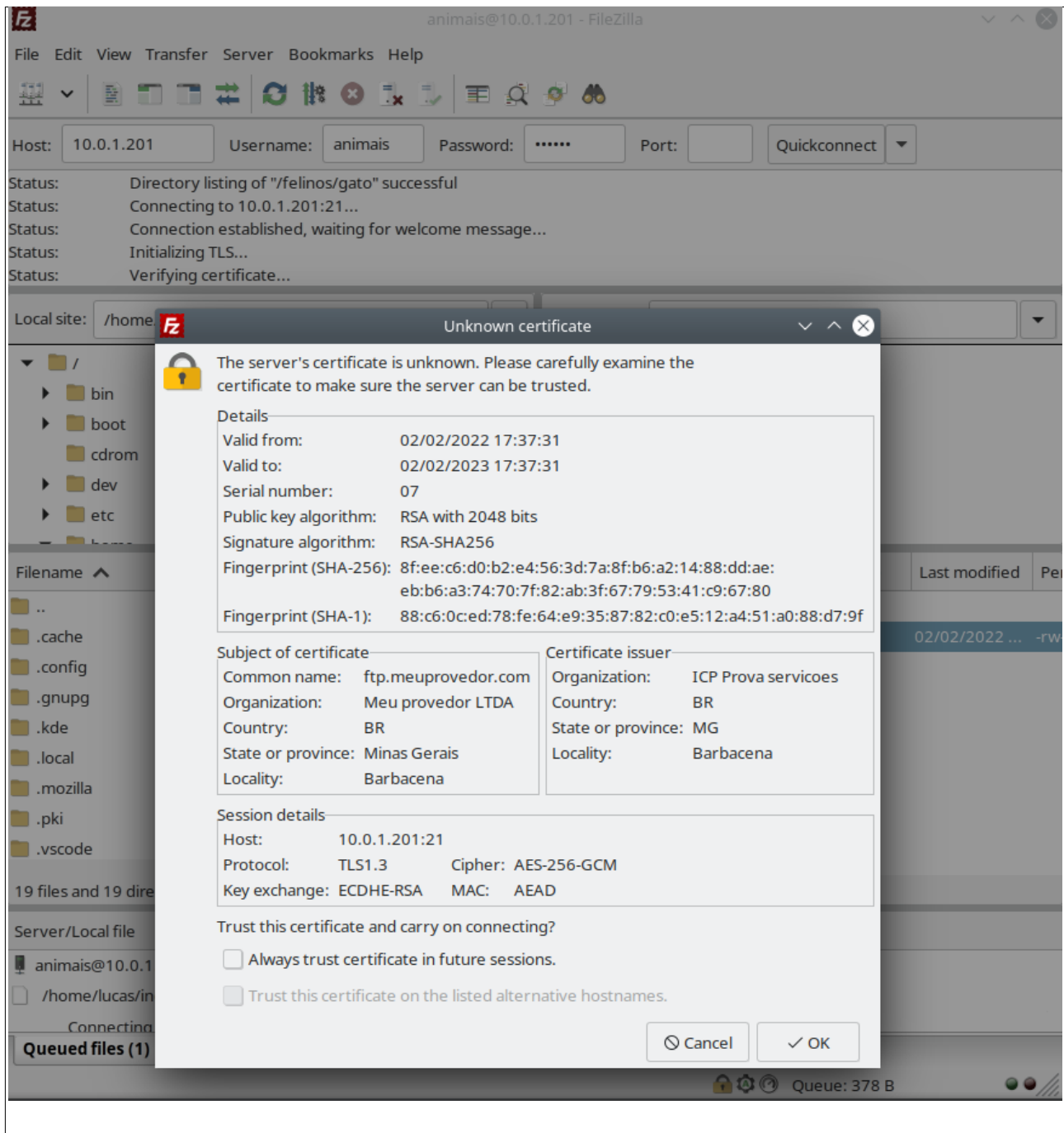
Para permitir que se possa fazer acesso via “FTP sobre TLS (STARTTLS)” de forma obrigatória, utilizando certificado em nome de ftp.meuprovedor.com e o controle de acesso criptografado, foram adicionadas as seguintes diretivas no arquivo `/etc/vsftpd/vsftpd.conf`:

```
#Criptografia
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
rsa_cert_file=/etc/ssl/mycerts/cert-ftp.meuprovedor.com.pem
rsa_private_key_file=/etc/ssl/mycerts/priv-ftp.meuprovedor.com.pem
```

Agora ao tentar conectar, e carregado o certificado cadastrado:



E ao tentar baixar ou enviar um arquivo, tambem é exibido o certificado



4 – (60 pts) – Instalar e configurar dois servidores smtp Postfix e imap Dovecot, um para cada domínio, atendendo às seguintes características:

- **(02 pts)** – VM-1 respondendo pelo domínio “seunome.com.br”;
- **(02 pts)** – VM-2 respondendo pelo domínio “animais.com.br”;
- ipc
- **(01 pts)** – em ambos os domínios, permitir que os usuários possam usar o endereço de e-mail no formato “login@dominio”;
- **(02 pts)** – em ambos os domínios, permitir que o Postfix receba e-mails de MUA pela porta 587;

- **(10 pts)** – em ambos os domínios, permitir que os usuários possam enviar e-mails, através de clientes de e-mail, de qualquer rede para qualquer rede, necessitando de autenticação (não poderá ser permitido o envio de e-mails sem autenticação);
- **(04 pts)** – em ambos os domínios, permitir que os usuários possam receber e-mails, através de MUA, em qualquer rede, utilizando o protocolo imap com autenticação;
- **(01 pts)** – criar os usuários “marcelo” e “bonfa” no servidor de e-mail do domínio “seunome.com.br” com senha “123456” para serem usados nos testes;
- **(01 pts)** – criar os usuários “renato” e “russo” no servidor de e-mail do domínio “animais.com.br” com senha “123456” para serem usados nos testes;
- **(06 pts)** – permitir que os usuários possam utilizar conexão criptografada STARTTLS, de forma obrigatória, para smtp nos dois domínios;
- **(30 pts)** – no quadro abaixo, fazer um mini-relatório (tutorial) **citando** e **explicando** todos os passos envolvidos para a resolução desta questão.

CNC: pelo menos um dos servidores de e-mail deverá ser capaz de enviar e receber e-mail.

Antes da configuracao, foi realizado uma verificacao para ver se os dominios estao ok:

```

root@server1 ~]# dig -t mx animais.com.br

;<<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> -t mx animais.com.br
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50494
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ece8c5e18f3e4948150dfb7861fc1f930667d6ac97779b6b (good)
; QUESTION SECTION:
; animais.com.br.                IN      MX

; ANSWER SECTION:
animais.com.br.                  86400   IN      MX      10 mail.animais.com.br.

; AUTHORITY SECTION:
animais.com.br.                  86400   IN      NS      ns2.animais.com.br.
animais.com.br.                  86400   IN      NS      ns1.animais.com.br.

; ADDITIONAL SECTION:
mail.animais.com.br.             86400   IN      A       10.0.1.202
ns1.animais.com.br.              86400   IN      A       10.0.1.201
ns2.animais.com.br.              86400   IN      A       10.0.1.202

; Query time: 0 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: Thu Feb 03 15:31:47 -03 2022
; MSG SIZE rcvd: 176

```

```
[root@server1 ~]# dig -t mx lucas.com.br

; <<>> DiG 9.11.26-RedHat-9.11.26-6.el8 <<>> -t mx lucas.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8953
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 782527537eaca3103b78e22b61fc1f958e42d691479971c5 (good)
;; QUESTION SECTION:
;lucas.com.br.                IN      MX

;; ANSWER SECTION:
lucas.com.br.                86400   IN      MX      10 mail.lucas.com.br.

;; AUTHORITY SECTION:
lucas.com.br.                86400   IN      NS      ns1.lucas.com.br.
lucas.com.br.                86400   IN      NS      ns2.lucas.com.br.

;; ADDITIONAL SECTION:
mail.lucas.com.br.           86400   IN      A       10.0.1.201
ns1.lucas.com.br.            86400   IN      A       10.0.1.201
ns2.lucas.com.br.            86400   IN      A       10.0.1.202

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Feb 03 15:31:49 -03 2022
;; MSG SIZE rcvd: 174
```

Foi então instalada a ferramenta postfix:

```
[root@server1 ~]# yum install postfix -y
```

Após instalada a ferramenta, foi alterado as informacoes do nome de servidor e o dominio responsavel por esse e-mail através do arquivo de configuracao `/etc/postfix/main.cf`:

VM 1- lucas.com.br

```
myhostname = mail.lucas.com.br
#myhostname = virtual.domain.tld

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
mydomain = lucas.com.br
```

VM 2- animais.com.br

```

myhostname = mail.animais.com.br
#myhostname = virtual.domain.tld

# The mydomain parameter specifies the local internet domain name.
# The default is to use $myhostname minus the first component.
# $mydomain is used as a default value for many other configuration
# parameters.
#
mydomain = animais.com.br

```

Foi também definido o modo de endereçamento dos e-mails em myorigin. E também foi definida a escuta em todas as interfaces, e o uso de todos os protocolos IP:

```

myorigin = $mydomain

# RECEIVING MAIL

# The inet_interfaces parameter specifies the network interface
# addresses that this mail system receives mail on. By default,
# the software claims all active interfaces on the machine. The
# parameter also controls delivery of mail to user@[ip.address].
#
# See also the proxy_interfaces parameter, for network addresses that
# are forwarded to us via a proxy or network address translator.
#
# Note: you need to stop/start Postfix when this parameter changes.
#
inet_interfaces = all
#inet_interfaces = $myhostname
#inet_interfaces = $myhostname, localhost
#inet_interfaces = localhost

# Enable IPv4, and IPv6 if supported
inet_protocols = all

```

Foi alterada a diretiva mydestination:

```

# See also below, section "REJECTING MAIL FOR UNKNOWN LOCAL USERS".
#
mydestination = $myhostname, $mydomain, localhost.$mydomain, localhost

```

E também a diretiva mynetworks:

```

#
mynetworks = 127.0.0.0/8

```

Foi definido um relay host vazio para que o serviço não seja terceirizado:

```

#relayhost = [an.ip.add.ress]
relayhost =

```


Foi definido o modo de armazenamento como sendo Maildir:

```
#home_mailbox = Mailbox
home_mailbox = Maildir/
```

Para forçar o uso da autenticação, foi inserido no final do arquivo:

```
# autenticação
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
smtpd_relay_restrictions= permit_sasl_authenticated, reject_unauth_destination
```

No arquivo `/etc/postfix/master.cf` foi habilitado o uso da porta 587 e ativadas algumas :

```
#submission inet n      -      n      -      smtpd
-   -o syslog_name=postfix/submission
-   -o smtpd_tls_security_level=encrypt
-   -o smtpd_sasl_auth_enable=yes
-   -o smtpd_tls_auth_only=yes
#   -o smtpd_reject_unlisted_recipient=no
#   -o smtpd_client_restrictions=$mua_client_restrictions
#   -o smtpd_helo_restrictions=$mua_helo_restrictions
#   -o smtpd_sender_restrictions=$mua_sender_restrictions
#   -o smtpd_recipient_restrictions=
-   -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
#   -o milter_macro_daemon_name=ORIGINATING
#smtps      inet  n      -      n      -      smtpd
```

E então foi instalada a ferramenta dovecot:

```
[root@server1 ~]# yum install dovecot -y
```

E então, no arquivo `/etc/dovecot/dovecot.conf` foram definidos quais os protocolos e versão do IP vão ser usados:

```
# Protocols we want to be serving.
protocols = imap pop3 lmtp

# A comma separated list of IPs or hosts where to listen in for connections.
# "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
# If you want to specify non-default ports or anything more complex,
# edit conf.d/master.conf.
listen = *
```

Feito isso, no arquivo `/etc/dovecot/conf.d/10-auth.conf` foram alteradas as seguintes

```
# See also ssl=required setting.   diretivas:
disable_plaintext_auth = no
```

```
# NOTE: See also disable_plaintext_auth setting.
auth_mechanisms = plain login
```

Feito isso, no arquivo `/etc/dovecot/conf.d/10-mail.conf`, foi alterada a seguinte diretiva:

```
# See doc/wiki/Variables.txt for full list. Some examples:
#
mail_location = maildir:~/Maildir
```

Feito isso, no arquivo `/etc/dovecot/conf.d/10-ssl.conf` foi desabilitada a criptografia

```
# plain imap and pop3 are still allowed for local connections
ssl = no
```

Feito isso, no arquivo `/etc/dovecot/conf.d/10-master.conf`, foi alterada a diretiva conforme abaixo:

```
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
}
```

e então foram inicializados os serviços dovecot e postfix:

```
[root@server1 ~]# systemctl stop dovecot
[root@server1 ~]# systemctl start dovecot
[root@server1 ~]# systemctl enable dovecot
Created symlink /etc/systemd/system/multi-user.target.wants/dovecot.service → /usr/lib/systemd/system/dovecot.service.
[root@server1 ~]# systemctl stop postfix
[root@server1 ~]# systemctl start postfix
[root@server1 ~]# systemctl enable postfix
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /usr/lib/systemd/system/postfix.service.
```

e verificado o status dos mesmos:

```
[root@server1 ~]# ps aux | grep dovecot
root      3919  0.0  0.5  67360  5812 ?        Ss   16:12   0:00 /usr/sbin/dovecot -F
dovecot   3920  0.0  0.2  22240  2268 ?        S    16:12   0:00 dovecot/anvil
root      3921  0.0  0.4  22376  4228 ?        S    16:12   0:00 dovecot/log
root      3922  0.0  0.5  35120  5716 ?        S    16:12   0:00 dovecot/config
root      4058  0.0  0.1  12136  1104 pts/0    S+   16:13   0:00 grep --color=auto dovecot
[root@server1 ~]# ps aux | grep postfix
root      4029  0.0  0.6 123136  6124 ?        Ss   16:13   0:00 /usr/libexec/postfix/master -w
postfix   4030  0.0  1.0 150440 10268 ?        S    16:13   0:00 pickup -l -t unix -u
postfix   4031  0.0  1.0 150492 10304 ?        S    16:13   0:00 qmgr -l -t unix -u
root      4060  0.0  0.1  12136  1036 pts/0    S+   16:14   0:00 grep --color=auto postfix
```

foram então adicionados os usuários ambos com a senha 123456:

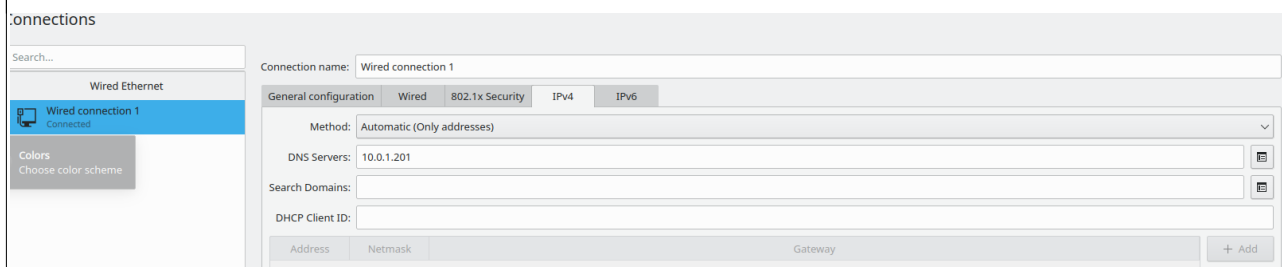
VM 1- lucas.com.br

```
[root@server1 ~]# useradd marcelo
[root@server1 ~]# passwd marcelo
Changing password for user marcelo.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server1 ~]# useradd bonfa
[root@server1 ~]# passwd bonfa
Changing password for user bonfa.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server1 ~]#
```

VM 2- animais.com.br

```
[root@server2 ~]# useradd renato
[root@server2 ~]# passwd renato
Changing password for user renato.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server2 ~]# useradd russo
[root@server2 ~]# passwd russo
Changing password for user russo.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@server2 ~]#
```

Entao foi configurado o DNS da VM para o servidor DNS configurado anteriormente



Entao, foram registrados os usuarios no thunderbird:

Set Up Your Existing Email Address

To use your current email address fill in your credentials.

Thunderbird will automatically search for a working and recommended server configuration.

Your full name

marcelo



Email address

marcelo@lucas.com.br



Password



☐ Remember password

✓ Configuration found by trying common server names.

Available configurations

☒ **IMAP**

Keep your folders and emails synced on your server

Incoming

IMAP mail.lucas.com.br **No Encryption**

Outgoing

SMTP mail.lucas.com.br STARTTLS

Username

marcelo

☐ **POP3**

Keep your folders and emails on your computer

[Configure manually](#)

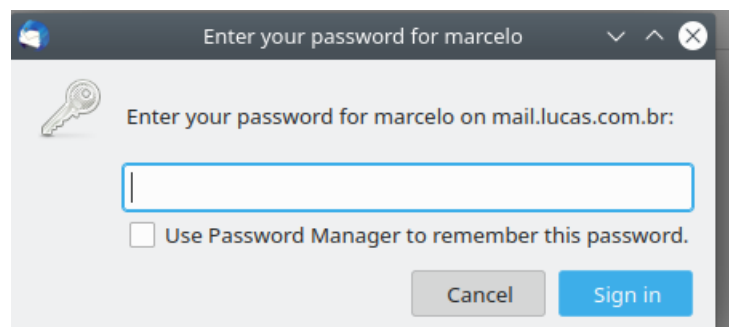
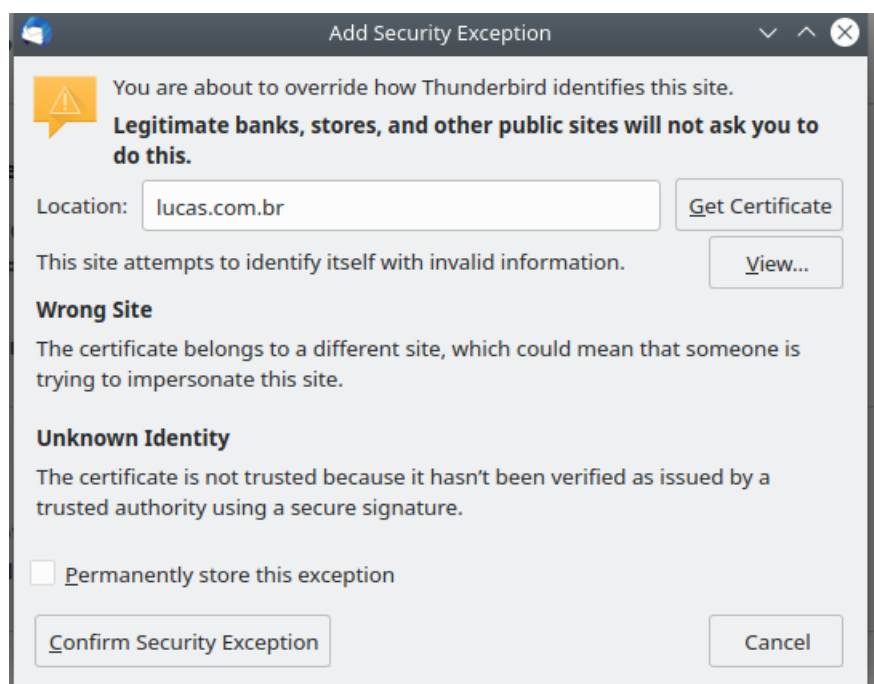
Cancel

Done



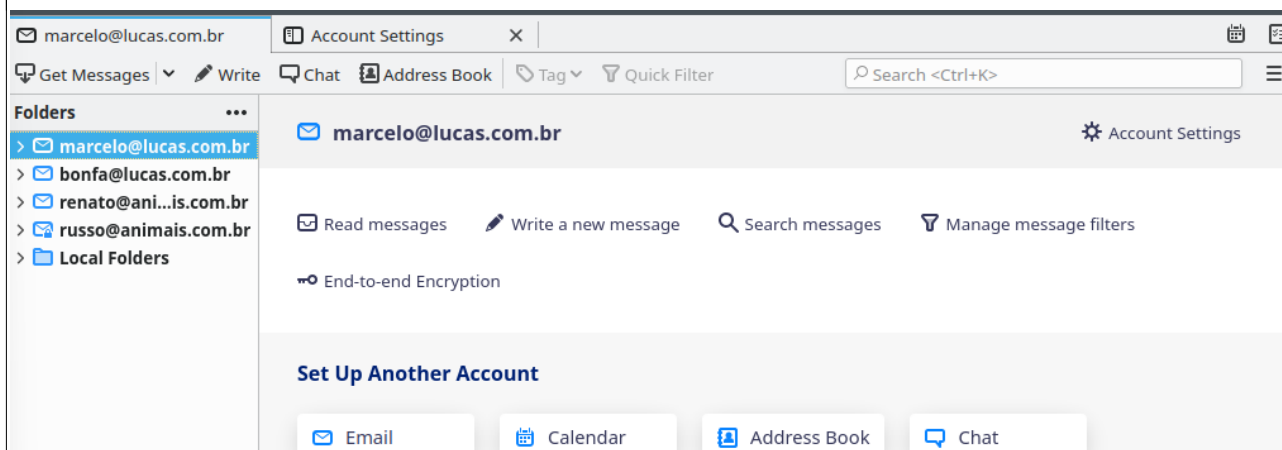
Not sure what to select?

[Setup documentation](#) - [Support forum](#) - [Privacy policy](#)

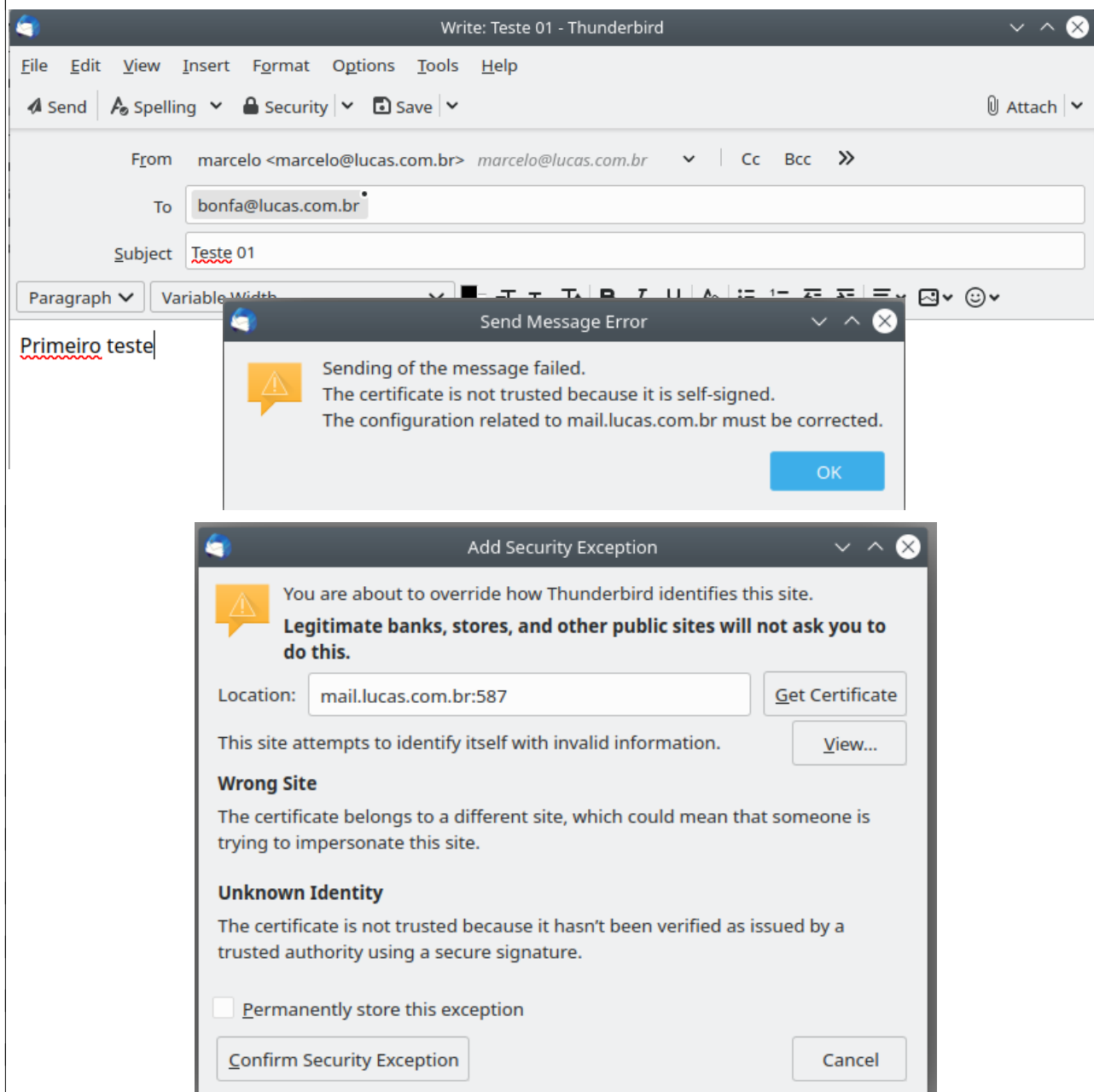


Foram realizadas as mesmas etapas para a inclusao dos usuario *bonfa*, *renato* e russo

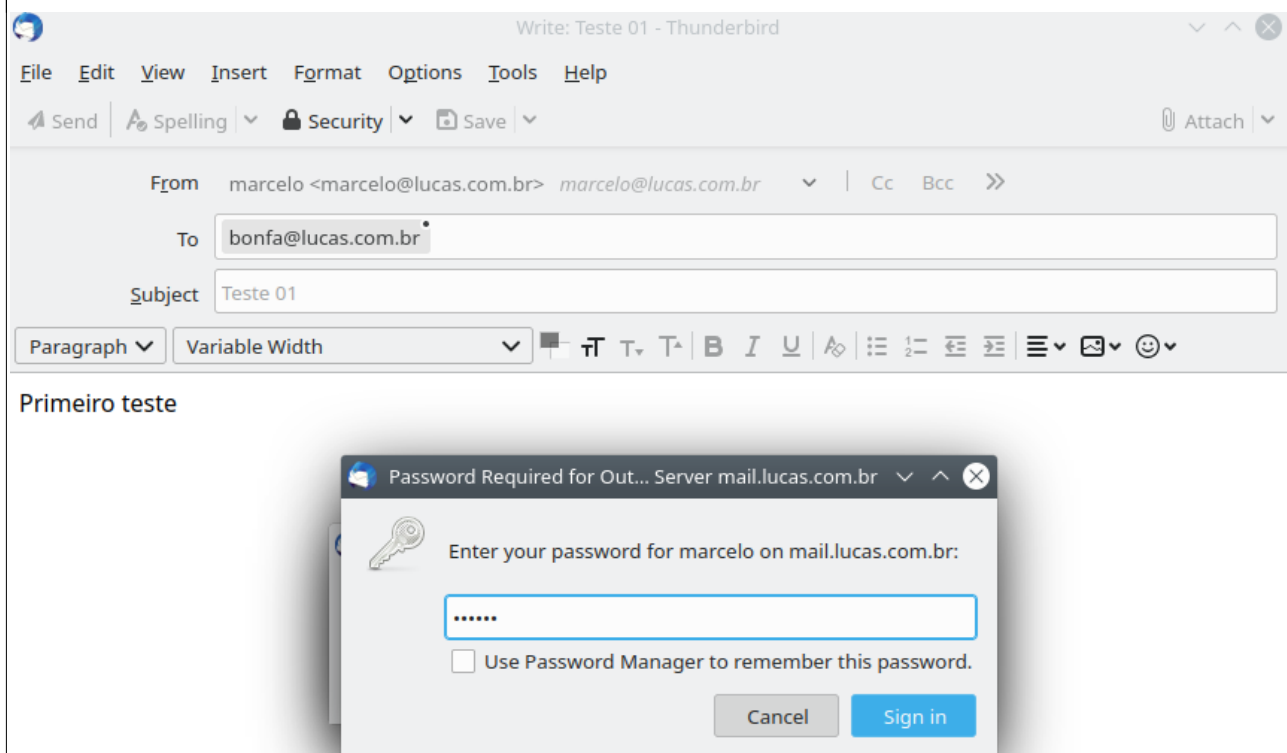
Feito isso, as contas já aparecem:



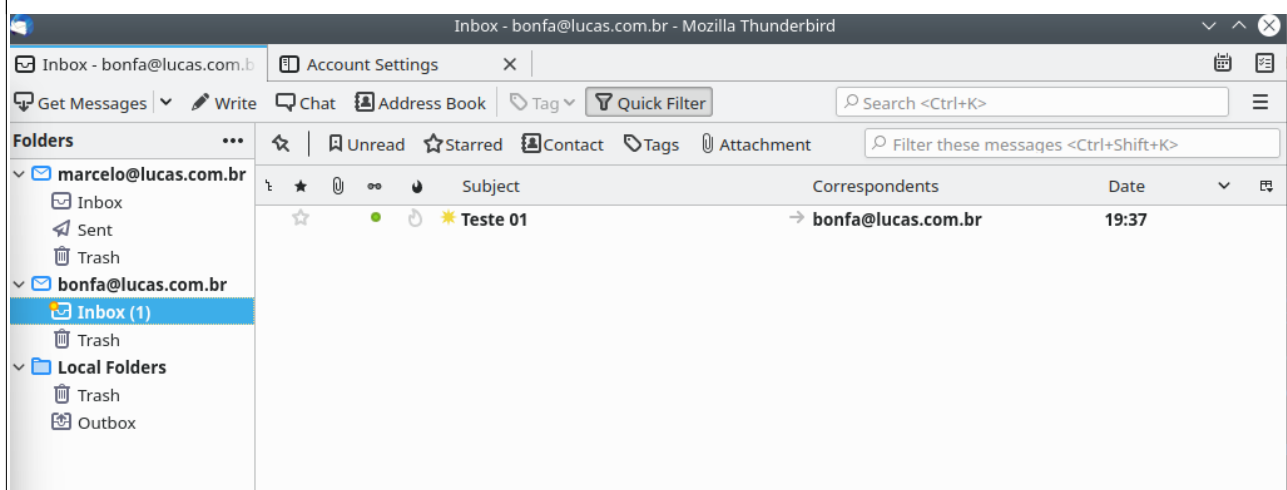
Foi realizado então um teste de envio:



Ao confirmar a exceção de segurança, o envio é cancelado e, ao clicar em *enviar* novamente, é solicitada a senha de usuário:



E a mensagem é enviada:



Criptografia SMTP:

para configurar a criptografia SMTP, no arquivo `/etc/postfix/main.cf`, foram comentadas as linhas a seguir:


```
#smtpd_tls_cert_file = /etc/pki/tls/certs/postfix.pem

# The full pathname of a file with the Postfix SMTP server RSA private key
# in PEM format. The private key must be accessible without a pass-phrase,
# i.e. it must not be encrypted.
#
#smtpd_tls_key_file = /etc/pki/tls/private/postfix.key

# Announce STARTTLS support to remote SMTP clients, but do not require that
# clients use TLS encryption (opportunistic TLS inbound).
#
#smtpd_tls_security_level = may

# Directory with PEM format Certification Authority certificates that the
# Postfix SMTP client uses to verify a remote SMTP server certificate.
#
#smtp_tls_CApath = /etc/pki/tls/certs

# The full pathname of a file containing CA certificates of root CAs
# trusted to sign either remote SMTP server certificates or intermediate CA
# certificates.
#
#smtp_tls_CAfile = /etc/pki/tls/certs/ca-bundle.crt

# Use TLS if this is supported by the remote SMTP server, otherwise use
# plaintext (opportunistic TLS outbound).
#
#smtp_tls_security_level = may
#meta_directory = /etc/postfix
#shlib_directory = /usr/lib64/postfix
```

Em seguida, foram adicionadas as seguintes linhas no final do arquivo:

VM1-lucas.com.br

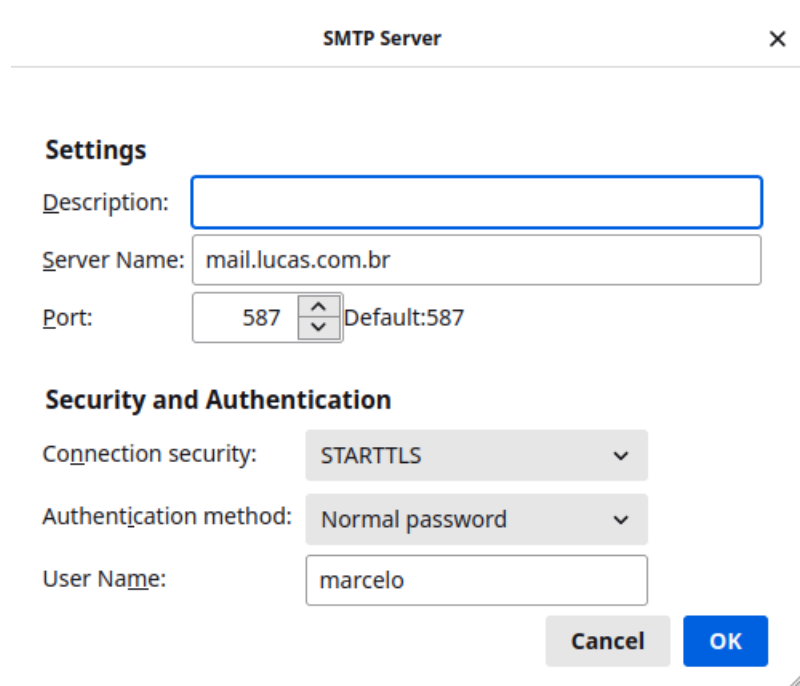
```
# criptografia
smtpd_tls_security_level = may
smtpd_tls_key_file = /etc/ssl/mycerts/priv-mail.lucas.com.br.pem
smtpd_tls_cert_file = /etc/ssl/mycerts/cert-mail.lucas.com.br.pem
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_cache
tls_random_source = dev:/dev/urandom
tls_random_exchange_name = /var/lib/postfix/prng_exch
smtpd_tls_auth_only = yes
smtpd_sasl_tls_security_options = noanonymous
```

VM2-animais.com.br

```
smtpd_tls_security_level = may
smtpd_tls_key_file = /etc/ssl/mycerts/priv-mail.animais.com.br.pem
smtpd_tls_cert_file = /etc/ssl/mycerts/cert-mail.animais.com.br.pem
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_cache
tls_random_source = dev:/dev/urandom
tls_random_exchange_name = /var/lib/postfix/prng_exch
smtpd_tls_auth_only = yes
smtpd_sasl_tls_security_options = noanonymous
```

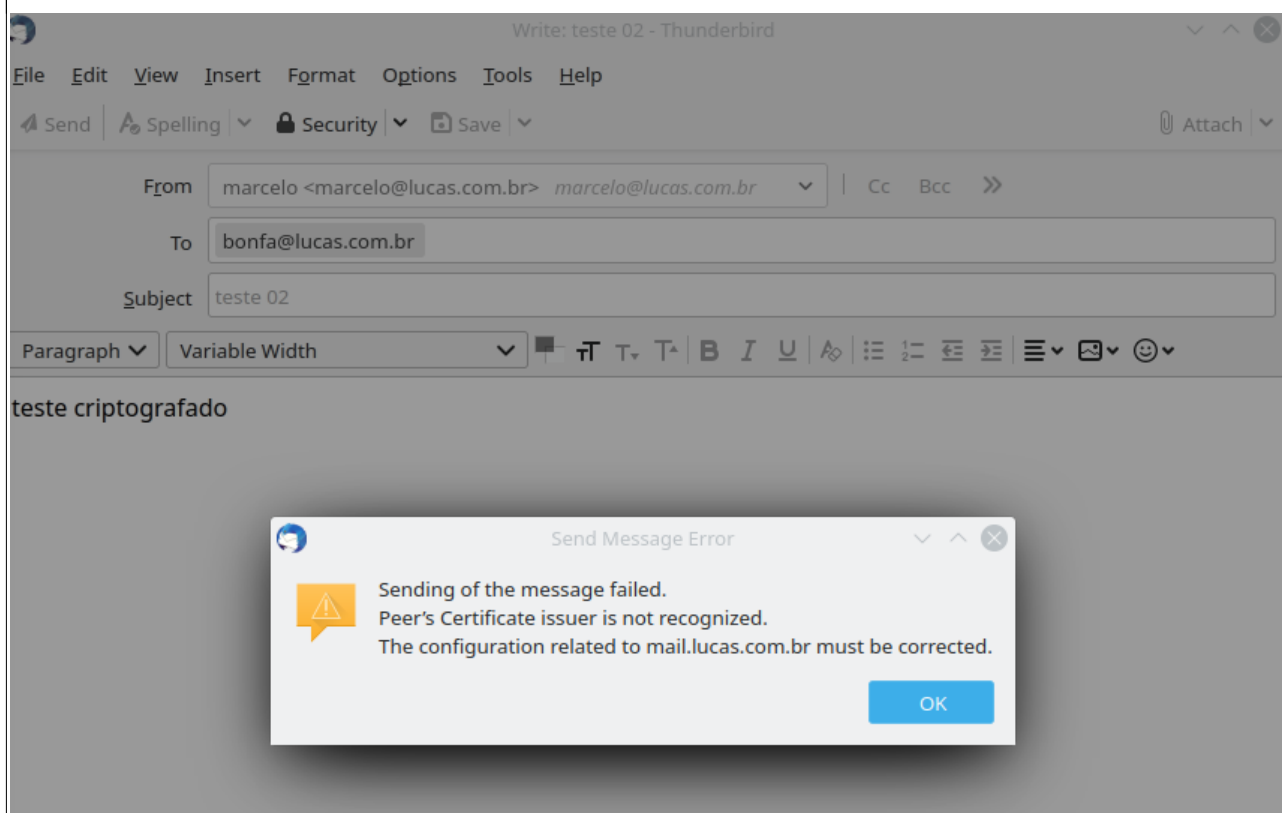
E então o serviço *postfix* foi reiniciado


No *Thunderbird* foi então ativada a criptografia



The screenshot shows the 'SMTP Server' configuration window. Under the 'Settings' section, the 'Description' field is empty, 'Server Name' is 'mail.lucas.com.br', and 'Port' is '587' with a 'Default:587' label. The 'Security and Authentication' section shows 'Connection security' set to 'STARTTLS', 'Authentication method' set to 'Normal password', and 'User Name' set to 'marcelo'. 'Cancel' and 'OK' buttons are at the bottom right.

E foi realizada uma nova tentativa de envio:





You are about to override how Thunderbird identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: Get Certificate

This site attempts to identify itself with invalid information. View...

Unknown Identity

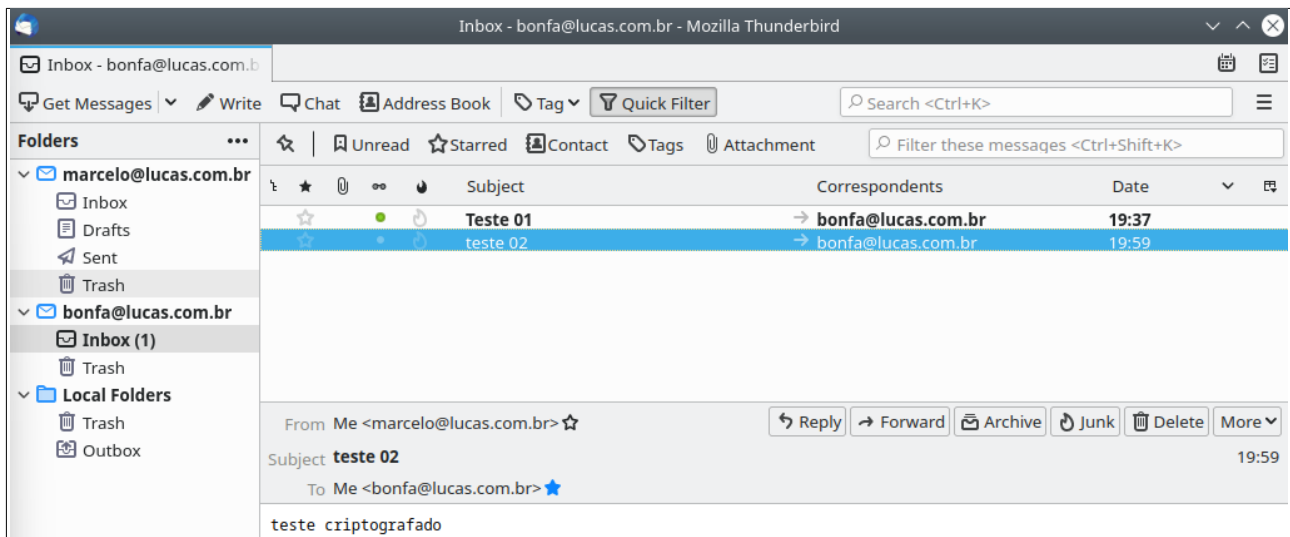
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☒ **Permanently store this exception**

Confirm Security Exception Cancel

Certificate

mail.lucas.com.br	
Subject Name	
Country	BR
State/Province	Minas Gerais
Locality	Barbacena
Organization	Lucas LTDA
Common Name	mail.lucas.com.br
Issuer Name	
Country	BR
State/Province	MG
Locality	Barbacena
Organization	ICP Prova servicoes
Validity	
Not Before	Wed, 02 Feb 2022 20:37:26 GMT
Not After	Thu, 02 Feb 2023 20:37:26 GMT
Public Key Info	
Algorithm	RSA



Foi realizado um teste sem criptografia:

SMTP Server

Settings

Description:

Server Name:

Port: Default: 587

Security and Authentication

Connection security:

Authentication method:

User Name:

Settings

Description:

Server Name:

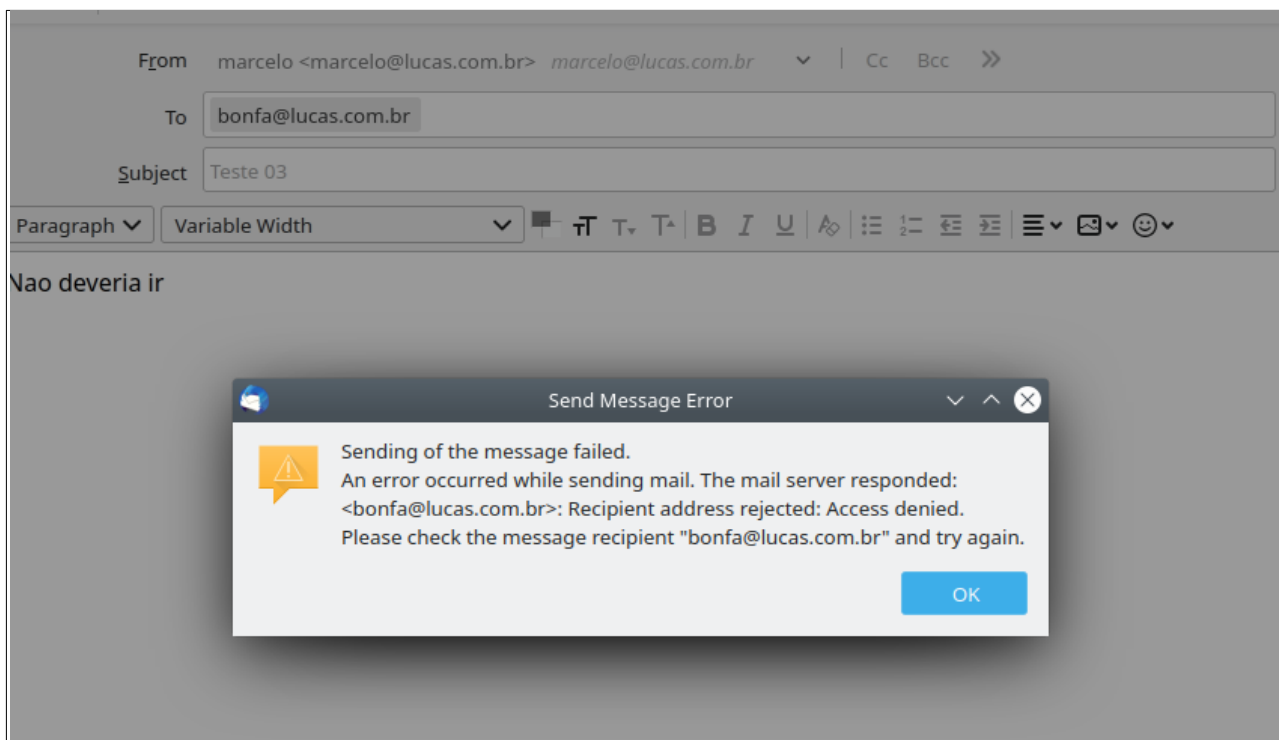
Port: Default: 587

Security and Authentication

Connection security:

Authentication method:

User Name:



Criptografia dovecot

Para a criptografia *dovecot*, no arquivo */etc/dovecot/conf.d/10-ssl.conf*, foram alteradas as seguintes diretivas:

VM1- lucas.com.br

```
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
###ssl_cert = </etc/pki/dovecot/certs/dovecot.pem
###ssl_key = </etc/pki/dovecot/private/dovecot.pem

ssl_cert = </etc/ssl/mycerts/cert-mail.lucas.com.br.pem
ssl_key = </etc/ssl/mycerts/priv-mail.lucas.com.br.pem
```

VM2 – animais.com.br

```
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
#ssl_cert = </etc/pki/dovecot/certs/dovecot.pem
#ssl_key = </etc/pki/dovecot/private/dovecot.pem

ssl_cert = </etc/ssl/mycerts/cert-mail.animais.com.br.pem
ssl_key = </etc/ssl/mycerts/priv-mail.animais.com.br.pem

# Minimum SSL protocol version to use. Potentially recognized values are SSLv3,
# TLSv1, TLSv1.1, and TLSv1.2, depending on the OpenSSL version used.
ssl_min_protocol = TLSv1
```

Entao foi reiniciado o servico *dovecot* e realizada uma checagem no status:

```
[root@server1 ~]# systemctl stop dovecot
[root@server1 ~]# systemctl start dovecot
[root@server1 ~]# ps aux | grep dovecot
root      5368  0.2  0.6 67360 5988 ?        Ss   20:13   0:00 /usr/sbin/dovecot -F
dovecot    5370  0.0  0.2 22240 2272 ?        S    20:13   0:00 dovecot/anvil
root      5371  0.0  0.4 22376 4148 ?        S    20:13   0:00 dovecot/log
root      5372  0.2  0.5 35120 5812 ?        S    20:13   0:00 dovecot/config
root      5374  0.0  0.1 12136 1072 pts/0    S+   20:13   0:00 grep --color=auto dovecot
```

No thunderbird, foram atualizadas as configuracoes de seguranca do servidor para todos os e-mails:

The screenshot shows the 'Server Settings' window for the account 'marcelo@lucas.com.br'. The left sidebar lists various settings categories, with 'Server Settings' selected. The main pane is divided into 'Server Settings' and 'Security Settings'. Under 'Server Settings', the 'Server Type' is 'IMAP Mail Server', 'Server Name' is 'mail.lucas.com.br', 'Port' is '143' (with a dropdown arrow), and 'User Name' is 'marcelo'. Under 'Security Settings', 'Connection security' is set to 'STARTTLS' and 'Authentication method' is set to 'Normal password'. At the bottom, there is a section labeled 'Server Settings'.

Como pode ser visto abaixo, ha um problema que impede a inicializacao do tls com o *dovecot*, por isso, a exigencia de criptografia foi retirada do thunderbird(para todas contas):

```
user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<mh66ZiXX0MYKAAFT>  
Feb 3 20:22:00 server1 dovecot[5371]: imap-login: Disconnected: TLS initialization failed. (no auth attempts in 0 secs): user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<1R66ZiXX0sYKAAFT>  
Feb 3 20:22:00 server1 dovecot[5371]: imap-login: Disconnected: TLS initialization failed. (no auth attempts in 0 secs): user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<mh66ZiXX0MYKAAFT>  
Feb 3 20:22:08 server1 dovecot[5371]: imap-login: Error: Failed to initialize SSL server context: Can't load SSL certificate: error:0E065068:configuration file routines:str_copy:variable has  
user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<zclUvZyXX0sYKAAFT>  
Feb 3 20:22:08 server1 dovecot[5371]: imap-login: Error: Failed to initialize SSL server context: Can't load SSL certificate: error:0E065068:configuration file routines:str_copy:variable has  
user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<8MUvZyXX0LMYKAAFT>  
Feb 3 20:22:08 server1 dovecot[5371]: imap-login: Disconnected: TLS initialization failed. (no auth attempts in 0 secs): user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<zclUvZyXX0sYKAAFT>  
Feb 3 20:22:08 server1 dovecot[5371]: imap-login: Disconnected: TLS initialization failed. (no auth attempts in 0 secs): user=<>, rip=10.0.1.109, lip=10.0.1.201, session=<8MUvZyXX0LMYKAAFT>
```

▼ **marcelo@lucas.com.br**

Server Settings

Copies & Folders

Composition & Addressing

Junk Settings

Synchronization & Storage

End-To-End Encryption

Return Receipts

▼ **bonfa@lucas.com.br**

Server Settings

Copies & Folders

Server Settings

Server Type: IMAP Mail Server

Server Name: mail.lucas.com.br

Port:

143

Default: 143

User Name: marcelo

Security Settings

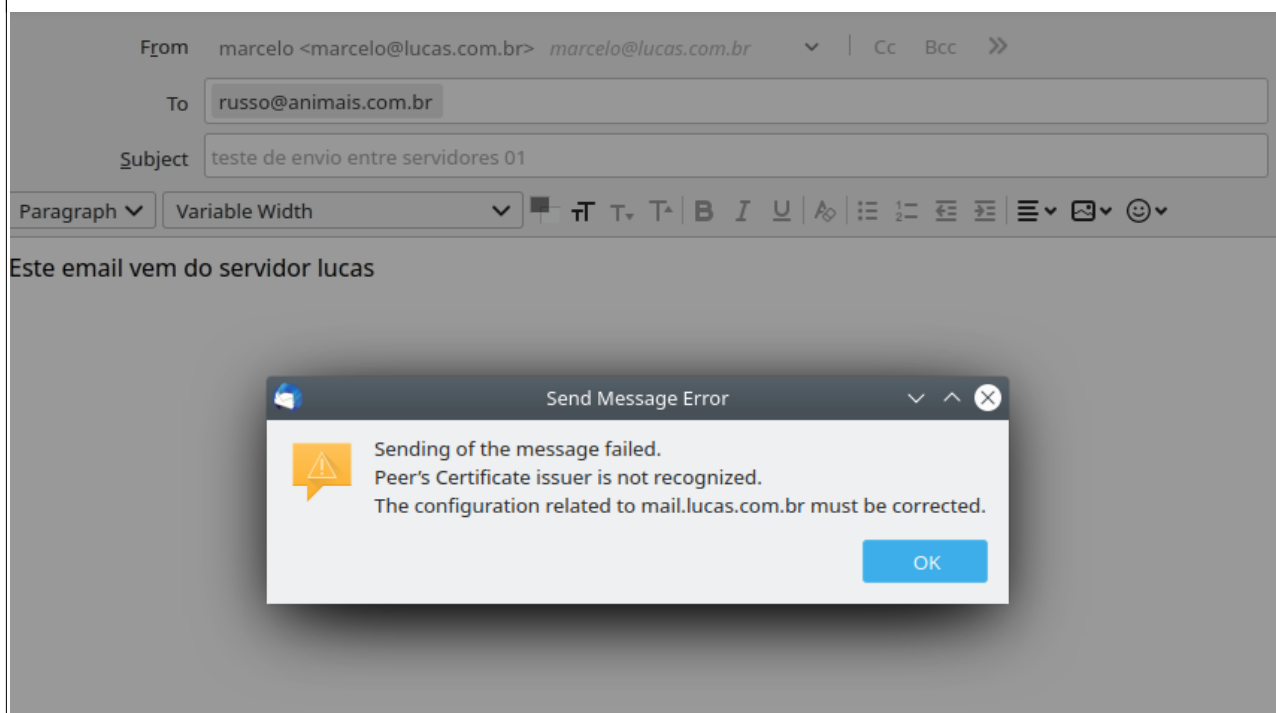
Connection security:

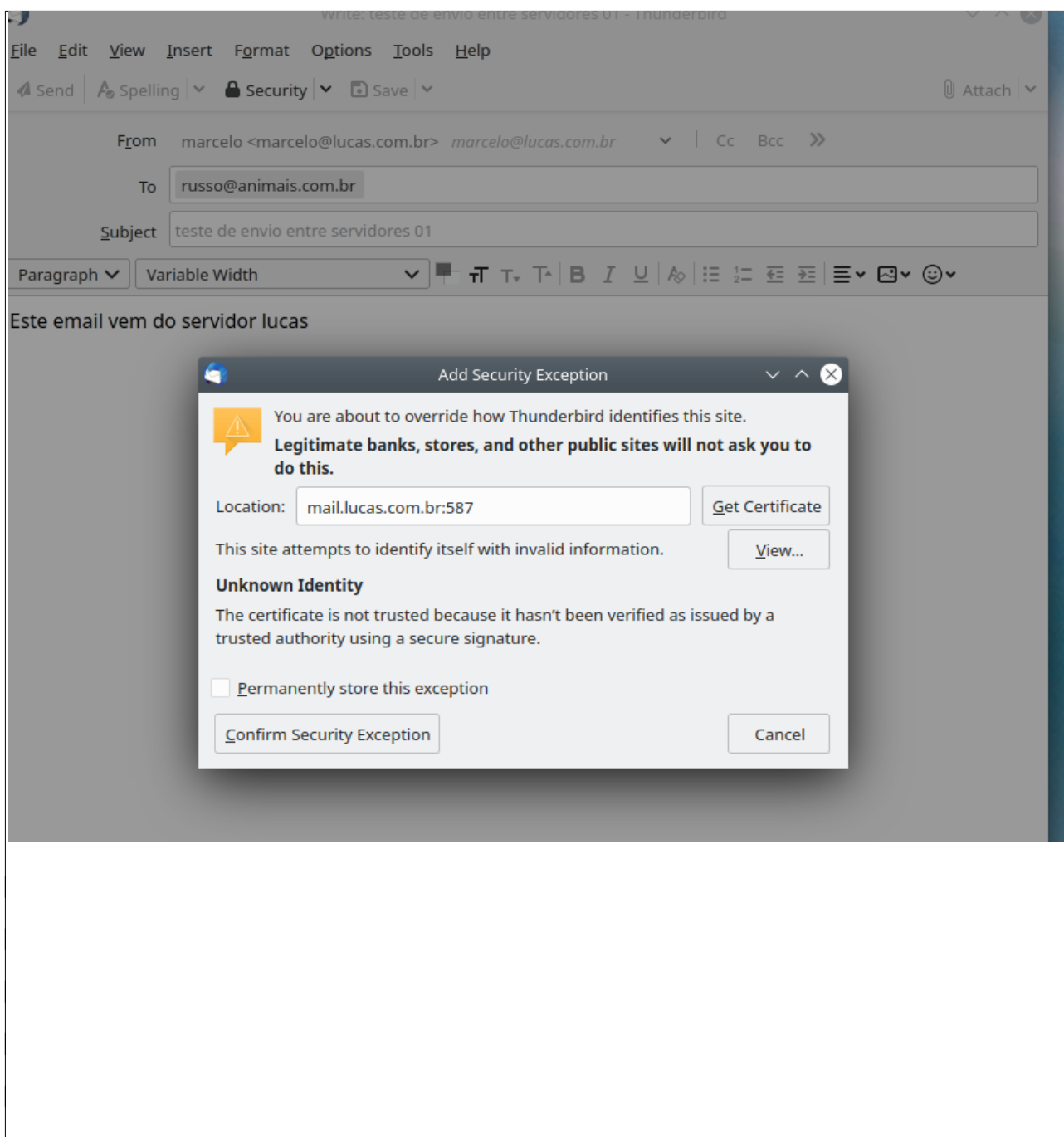
None

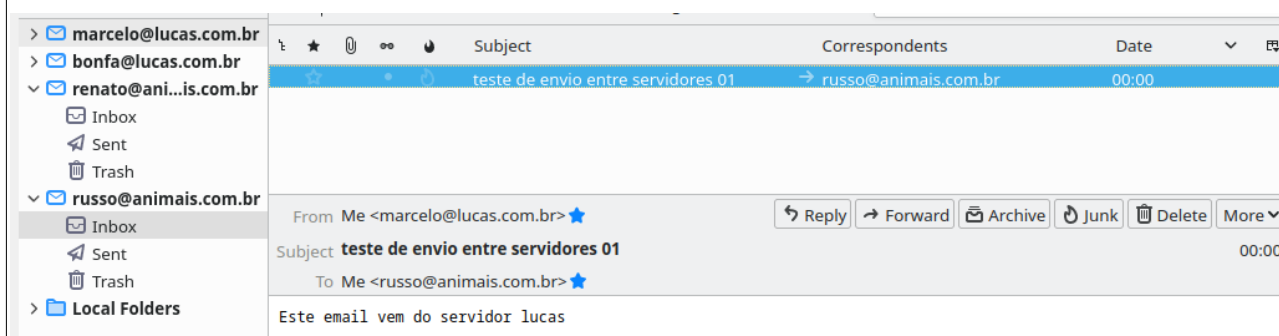
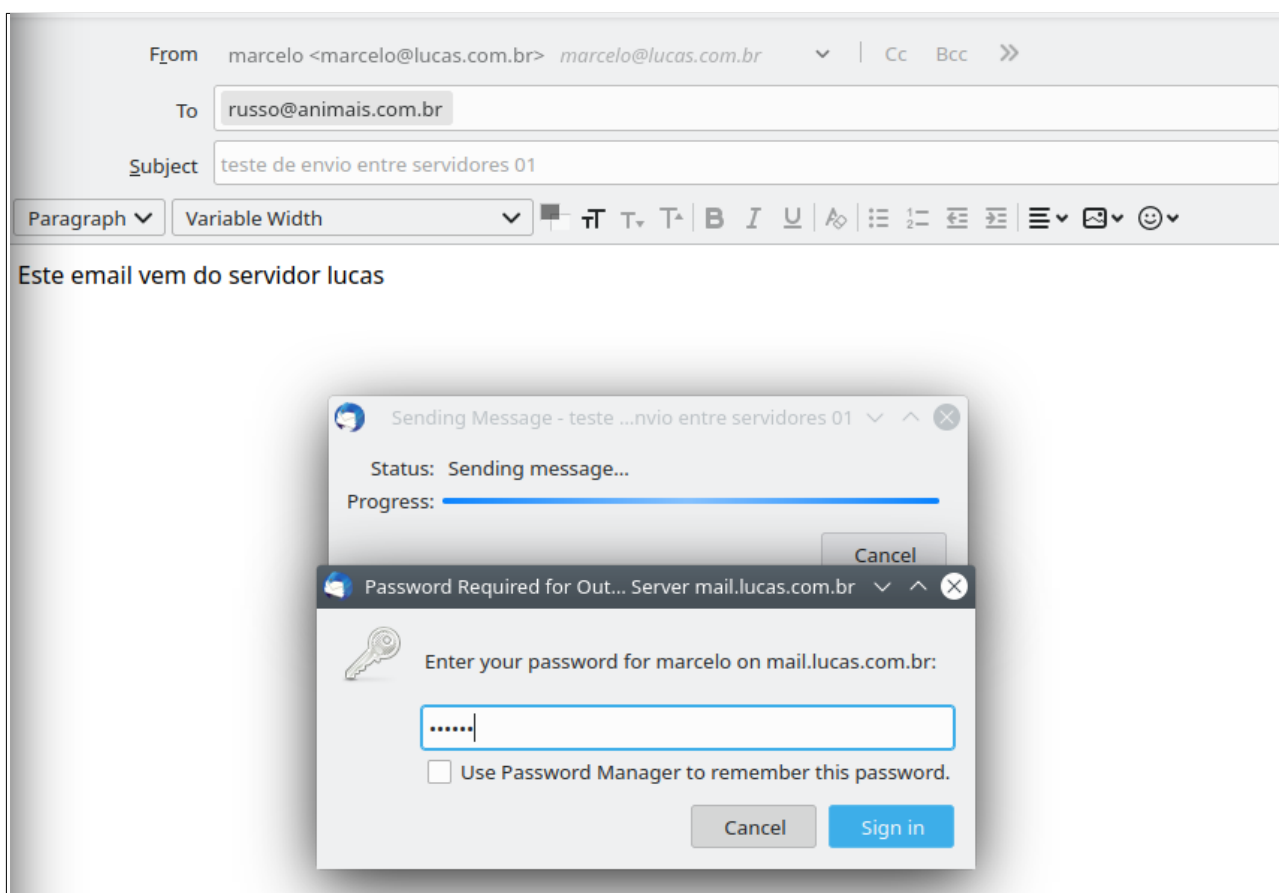
Authentication method:

Password, transmitted insecurely

Foram realizados testes de envio entre os dois servidores de e-mail:







Foi testado com outros e-mails mas não vou colocar aqui já que o arquivo esta muito grande.

Em seguida foi removida a configuracao de authenticacao e tentado o envio de email (Nao pode ser realizado o envio sem a configuracao de autenticao):

Details of selected server:

Description: <not specified>
Server Name: mail.lucas.com.br
Port: 587
User Name: marcelo
Authentication method: No authentication
Connection Security: STARTTLS

Details of selected server:

Description: <not specified>
Server Name: mail.lucas.com.br
Port: 587
User Name: bonfa
Authentication method: No authentication
Connection Security: STARTTLS

Details of selected server:

Description: <not specified>
Server Name: mail.animais.com.br
Port: 587
User Name: renato
Authentication method: No authentication
Connection Security: STARTTLS

Details of selected server:

Description: <not specified>
Server Name: mail.animais.com.br
Port: 587
User Name: russo
Authentication method: No authentication
Connection Security: STARTTLS

