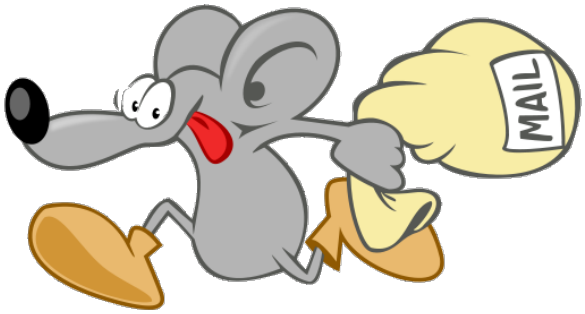
Curso 452

Linux Security Servers in Cloud

Versão 2015_3.0

Servidor Postfix – Parte I



Postfix Mail Agent Transport

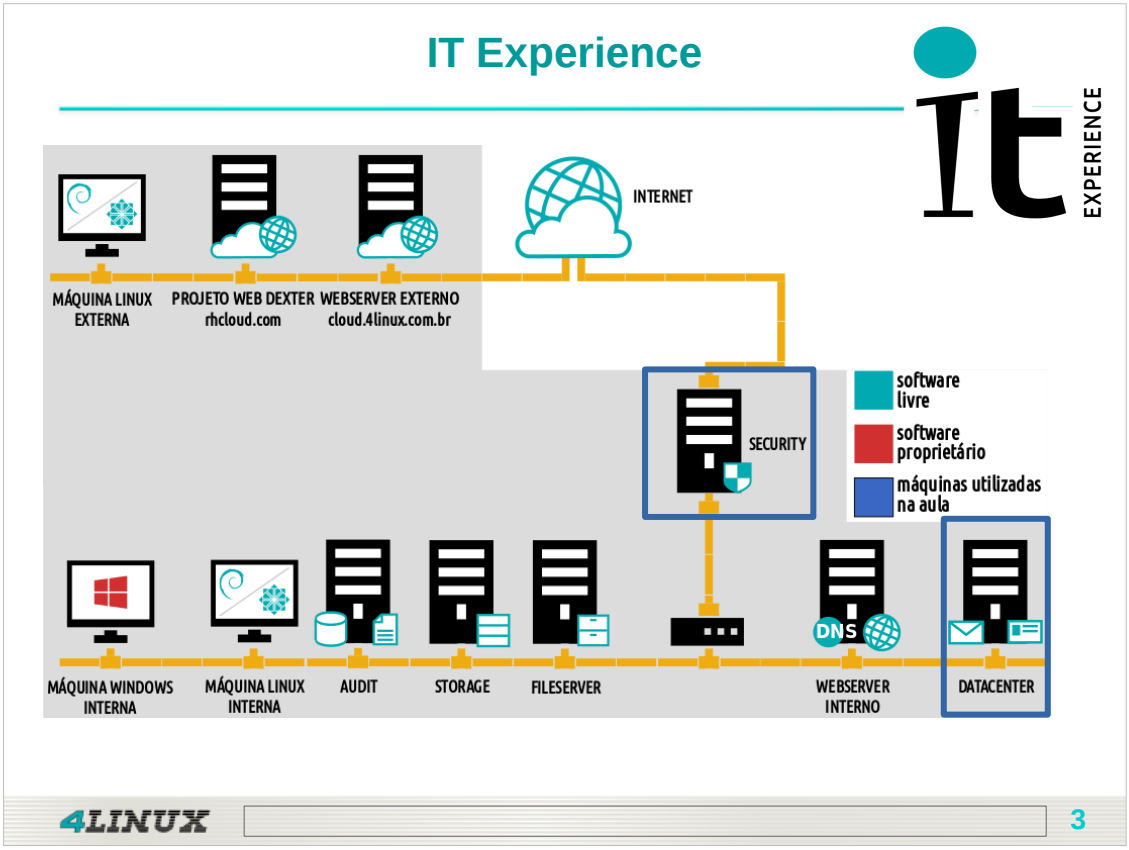
Características do Postfix

• Sistema multitarefa - O "Postfix" possui um conjunto de módulos que desempenham um papel específico para cada etapa do tráfego de e-mails, este comportamento permite melhor desempenho em equipamentos multiprocessados.

• Separação de privilégios - O "Postfix" pode ser executado em "chroot" que restringe o acesso a arquivos internos à uma "jaula", tornando sua execução muito mais segura..

• Modular - É possível criar módulos para trabalhar em conjunto com o "Postfix",tornando-o facilmente extensível.

• Compatibilidade - O "Postfix" foi desenvolvido para suportar os formatos de armazenamentos de mensagens existentes.


IT Experience
IT EXPERIENCE
INTERNET
MÁQUINA LINUX EXTERNA
PROJETO WEB DEXTER rhcloud.com
WEBSERVER EXTERNO cloud.4linux.com.br
SECURITY
software livre
software proprietário
máquinas utilizadas na aula
MÁQUINA WINDOWS INTERNA
MÁQUINA LINUX INTERNA
AUDIT
STORAGE
FILESERVER
DNS
WEBSERVER INTERNO
DATACENTER
4LINUX
3

Anotações:

Objetivos da Aula

Aula 05

- Introdução ao Postfix;
- Entender os conceitos de MTA, MUA e MDA;
- Instalar e configurar o Postfix no Servidor Datacenter;
- Ativar os protocolos POP e IMAP;
- Criar alias de e-mail.

Anotações:

Agentes de E-mail

Glossário:

- **MTA** → Mail Transfer Agent → **SMTP**
- **MDA** → Mail Delivery Agent → **POP/IMAP**
- **MUA** → Mail User Agent → **Cliente de Email**
- **SMTP** → Simple Mail Transfer Protocol → **Porta 25 / SSL: 465 / TLS:**
- **IMAP** → Internet Message Access Protocol → **Porta 143 / SSL: 993**
- **POP** → Post Office Protocol → **Porta 110 / SSL: 995**

Anotações:

Agentes de E-mail

Mail User Agent (MUA):

- É a aplicação designada como cliente de e-mail do usuário;
- Sua função é fornecer uma interface para compor, enviar e receber mensagens de e-mail, através de um MTA;
- Existem muitos suítes de e-mail onde o MUA utilizado é uma interface web criando um webmail, como por exemplo o Zimbra.
- São exemplos de MUA: **Thunderbird**, Evolution, Microsoft Outlook.

Anotações:

Agentes de E-mail

Mail Transport Agent (MTA):

- É o servidor de e-mails propriamente dito. Certamente a parte mais importante de um sistema de correio;
- O MTA é responsável pelo recebimento e envio de mensagens assegurando que elas cheguem ao seus destinos;
- Ele se comunica diretamente com o MDA para entrega de correspondências;
- São exemplos de MTA: **Postfix**, Sendmail, Qmail, Exim, Microsoft Exchange, etc.

Anotações:

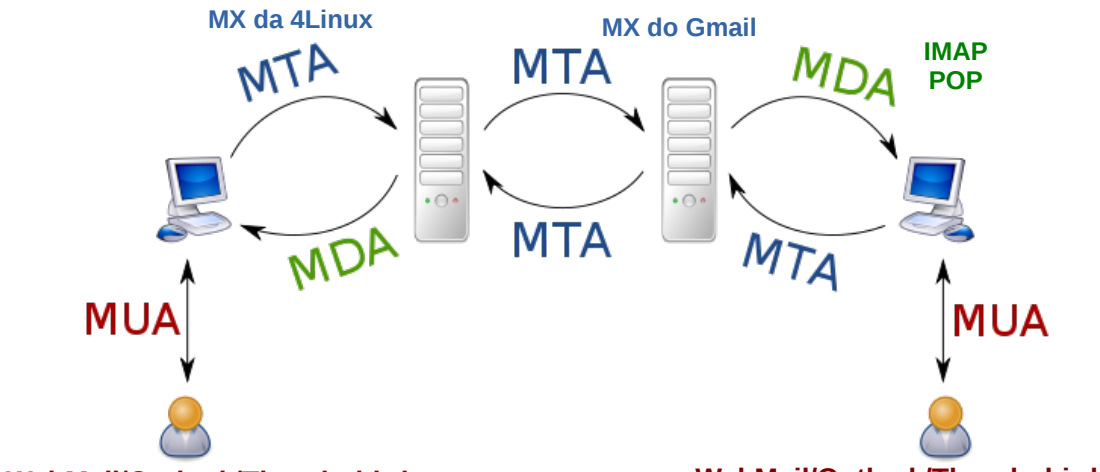
Agentes de E-mail

Mail Delivery Agent (MDA):

- É o responsável por controlar a entrega final das mensagens para destinatários de um sistema;
- Um MDA é usado para aplicar filtros anti-spam, remover vírus em anexos, categorizar mensagens e fazer encaminhamento de e-mails para outros endereços;
- São exemplos de MDA: Procmail, Fetchmail, **Courier**, Dovecot, Maildrop, Postdrop e etc.

Anotações:

Servidor Postfix



Anotações:

Servidor Postfix

Introdução:

- Escrito em linguagem C, a primeira versão oficial do "Postfix" como Software Livre foi lançada em Dezembro de 1998;
- Seu criador é o holandês **Wietse Venema**, programador e físico conhecido por diversos trabalhos relacionados à segurança da informação.

Wietse Venema, 2005.

Anotações:

Servidor Postfix

Características do Postfix:

Sistema modular/multitarefa → O Postfix possui um conjunto de módulos que desempenha um papel específico para cada etapa do tráfego de e-mails, com a possibilidade de adicionar módulos, o que o torna facilmente extensível;

Separação de privilégios → Permite execução em "chroot", o que restringe o acesso a arquivos internos da máquina aumentando a segurança;

Compatibilidade → Desenvolvido para suportar os formatos de armazenamento de mensagens existentes.

Anotações:

Servidor Postfix

Servidor: Datacenter

Instalação e Configuração:

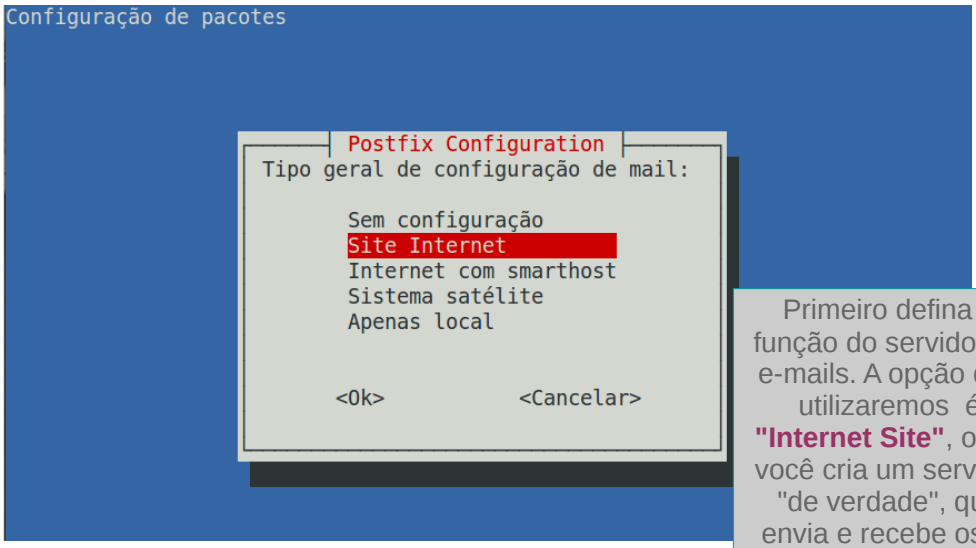
1 – Para instalar o Postfix execute:

```
1# apt-get install postfix procmail bsd-mailx courier-imap
courier-pop
2# netstat -nlt | egrep "25|143|110"
3# telnet localhost 25
   Banner: 220 datacenter.dexter.com.br ESMTP Postfix
(Debian/GNU)
4# cd /etc/postfix
5# ls
```


Anotações:

Servidor Postfix

Servidor: Datacenter

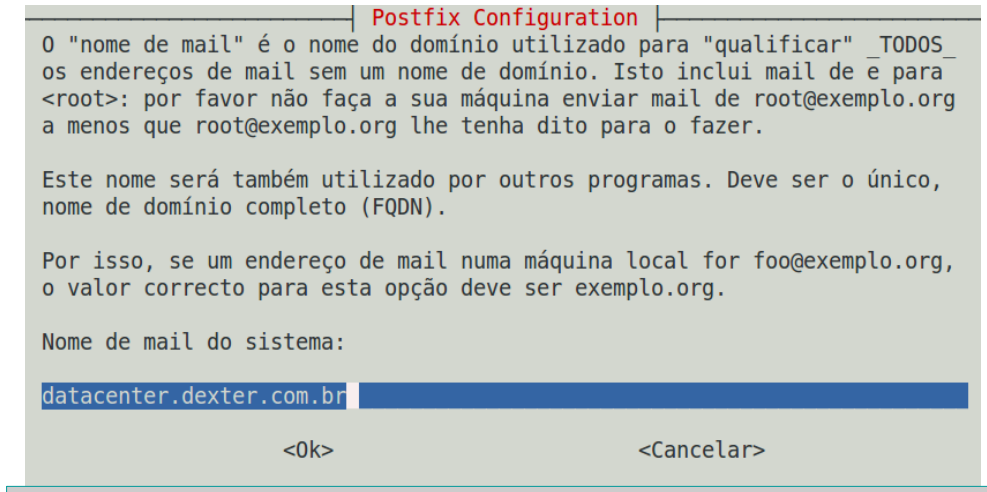


Primeiro defina a função do servidor de e-mails. A opção que utilizaremos é **"Internet Site"**, onde você cria um servidor "de verdade", que envia e recebe os e-mails diretamente.

Anotações:

Servidor Postfix

Servidor: Datacenter

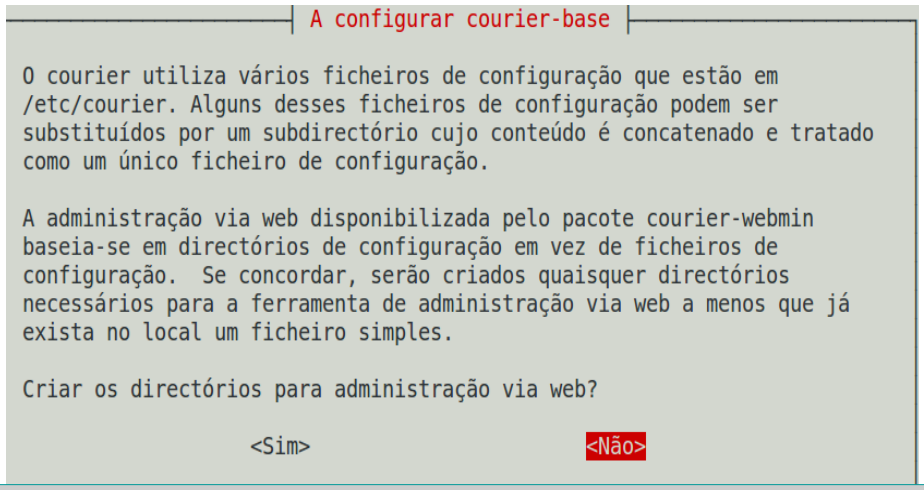


Em seguida, defina o domínio do servidor a ser incluído no envio de mensagens. Utilize o padrão **dexter.com.br**.

Anotações:

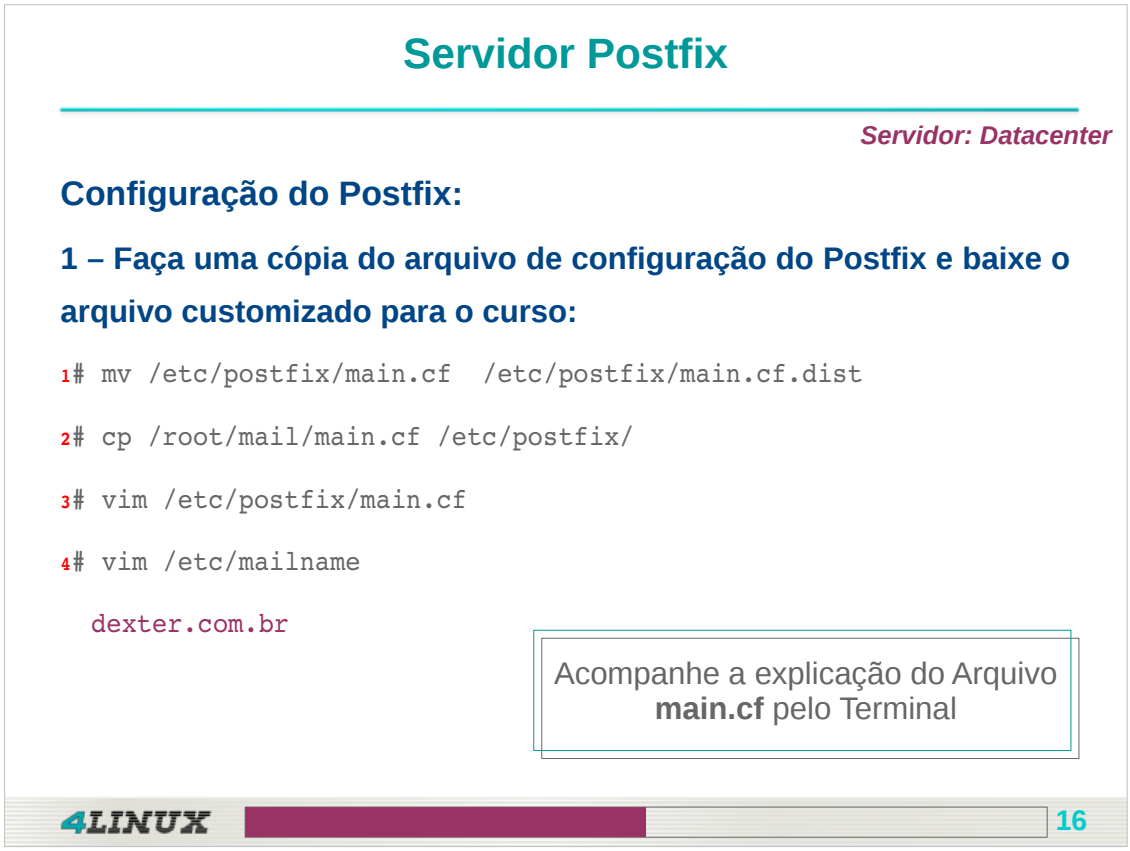
Servidor Postfix

Servidor: Datacenter



Otimizar o Postfix para administração web através do courier-webmin. Não utilizaremos essa ferramenta, portanto marque **<Não>**.

Anotações:



Arquivos de configuração

Os arquivos de configuração do "Postfix", podem ser encontrados no diretório "/etc/postfix", onde os seus principais arquivos são:

main.cf - Arquivo principal do "Postfix" onde ficam todas as configurações principais relacionadas ao funcionamento do "Postfix".

master.cf - É o arquivo que controla a ação de cada "daemon" do "Postfix". Nele podemos dizer quantos processos "smtpd" estarão em execução, por exemplo. Caso tenhamos uma estrutura grande de máquina, uma ajuste nesses "daemons" serão bem compensadores em termos de performance.

Servidor Postfix

Servidor: Datacenter

Testando o Postfix:

1 - Reinicie o postfix e em outro terminal abra o log de e-mail:

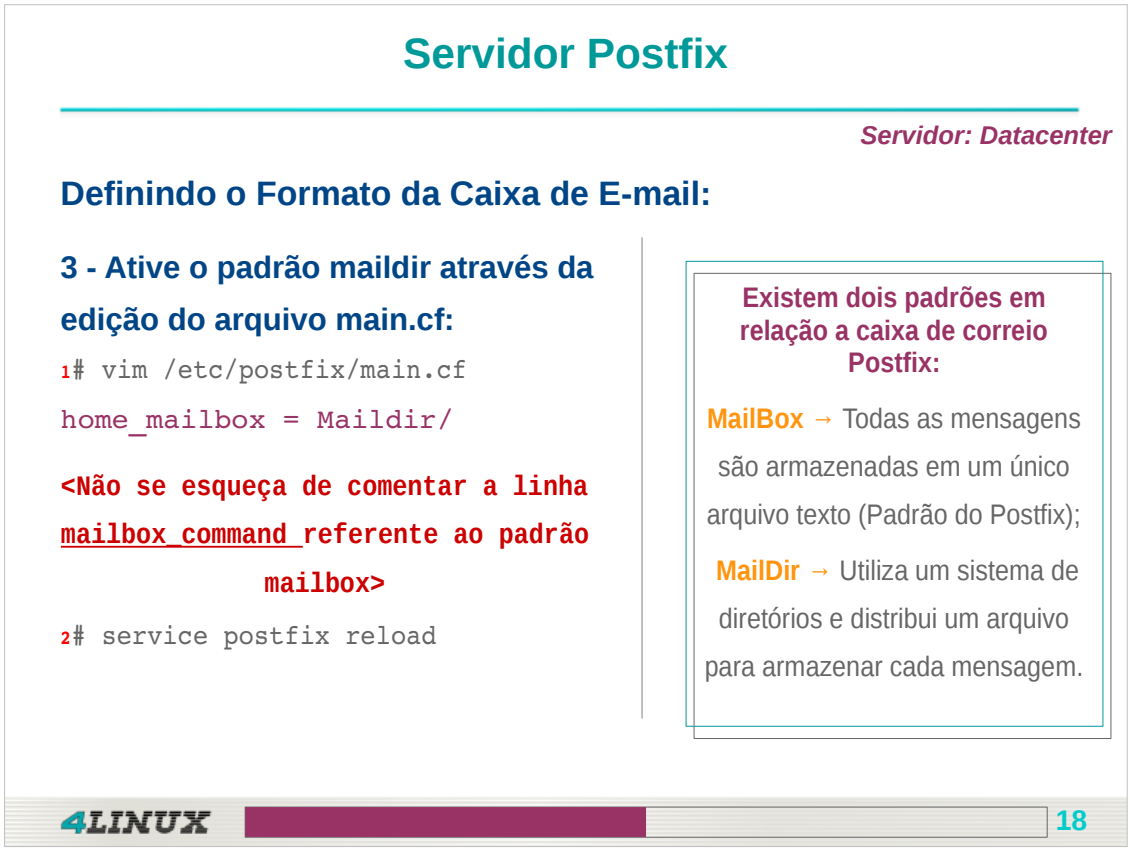
```
1# service postfix restart
2# tail -f /var/log/mail.log
```

2 - Envie um e-mail de teste e verifique o spool:

```
3# echo "Teste de Envio" | mail -s "Primeiro Email" suporte@dexter.com.br
4# cat /var/spool/mail/suporte
```

<Envie uma nova mensagem e verifique que o destino dela será sempre o mesmo arquivo>

Anotações:



MailBox ou Mbox - é o formato padrão para caixa de correio do Postfix. Este formato armazena todas as mensagens em um único arquivo de texto. Esses arquivos são nomeados de acordo com o nome do usuário e armazenados em geral em /var/mail ou /var/spool/mail.

Desvantagens:

• Encarece a exclusão de mensagens (requer regravação no arquivo inteiro, exceto se a mensagem a ser excluída for a última);

MailDir - usa diretórios e um arquivo por mensagem. A exclusão de mensagens sempre é muito rápida.

Desvantagem:

• O tempo para varrer a caixa de correio e produzir uma lista de mensagens é maior, pois todos os arquivos devem ser abertos e lidos.

Servidor Postfix

IMAP (Internet Message Access Protocol):

- Assim como o Pop, também é um protocolo utilizado para coletar mensagens em uma caixa de correio eletrônico;
- Diferente do padrão utilizado pelo POP, o Imap foi projetado para permitir que o usuário armazene as mensagens permanentemente no servidor;
- Com o Imap o usuário pode acessar todas as mensagens a a partir de qualquer lugar do mundo.

Anotações:

Servidor Postfix

Servidor: Datacenter

Configurando as Pastas para o IMAP:

1 - Crie os diretórios de e-mail através do comando maildirmake:

```
1# maildirmake /home/suporte/Maildir
2# maildirmake /home/suporte/Maildir/.Enviados
3# maildirmake /home/suporte/Maildir/.Rascunhos
4# maildirmake /home/suporte/Maildir/.Lixeira
5# maildirmake /home/suporte/Maildir/.Spam
6# chown -R suporte:suporte /home/suporte
7# echo "Teste de Envio" | mail -s "Segundo Email"
suporte@dexter.com.br
```


Anotações:

Servidor Postfix

Servidor: Datacenter

POP (Post Office Protocol):

- Protocolo utilizado para coletar mensagens em uma caixa de correio eletrônico;
- Uma característica do POP que hoje pode ser considerada pouco vantajosa é o seu formato, onde as mensagens são baixadas para o computador local e excluídas do servidor. Assim, o POP não pode ser utilizado para armazenamento permanente de mensagens;
- A porta 110 é padrão para este protocolo. Quando implementada uma camada de segurança ao POP ele deverá trabalhar na porta 995.

Anotações:

Servidor Postfix

Servidor: Datacenter

Acessando Caixa Postal – POP:

1 – Utilize o telnet para acessar a caixa postal utilizando o POP:

```
1# telnet mail.dexter.com.br 110
      user suporte
+OK Password required
      pass 4linux
+OK logged in.
      list
      retr 1
      quit
```


Anotações:

Desativando o VRFY

Servidor: Datacenter

- Por padrão o Postfix irá responder solicitações SMTP VRFY;
- Este recurso é usado por spammers e crackers para coletar informações sobre e-mail válidos sistema:

```
# telnet localhost 25
helo dexter.com.br
vrfy linus  … Uhhh... Não existe.
Vrfy suporte … Há encontrei!
quit
```


Anotações:

Desativando o VRFY

Servidor: Datacenter

- É possível bloquear esta configuração através da edição do arquivo main.cf conforme abaixo:

```
1# vim /etc/postfix/main.cf
     disable_vrfy_command = yes
2# service postfix reload
3#  telnet localhost 25
     helo dexter.com.br
     vrfy suporte
     502 5.5.1 VRFY command is disabled
   quit
```

<Adicione a linha abaixo ao final do arquivo>

Anotações:

Servidor Postfix

Servidor: Datacenter

Testando o Envio de E-mail Utilizando o Telnet:

4 - Envie um e-mail via telnet para validar o funcionamento do Postfix:

```
1# telnet localhost 25
   Trying ::1...
   Connected to localhost.
   Escape character is '^]'.
   220 datacenter.dexter.com.br ESMTP Postfix (Debian/GNU)
   helo dexter.com.br
   250 datacenter.dexter.com.br
   mail from: root@dexter.com.br
   250 2.1.0 Ok
   rcpt to: suporte@dexter.com.br
   250 2.1.5 Ok
```


Anotações:

Servidor Postfix

Servidor: Datacenter

Testando o Envio de E-mail Utilizando o Telnet:

```
data
354 End data with <CR><LF>.<CR><LF>
subject: Teste de e-mail na 4linux
Obrigado Wietse!
.
250 2.0.0 Ok: queued as 7FFF6195
quit
```

5 – Verifique a caixa de mensagens do usuário suporte:

```
1# ls -la /home/suporte
2# ls /home/suporte/Maildir/new
```


Anotações:

Servidor Postfix

Servidor: Datacenter

Configurando as Pastas para o IMAP:

2 - Crie mais um usuário e seus respectivos diretórios de e-mail:

```
1# adduser seu_nome
2# maildirmake /home/seu_nome/Maildir/
3# maildirmake /home/seu_nome/Maildir/.Rascunhos
4# maildirmake /home/seu_nome/Maildir/.Lixeira
5# maildirmake /home/seu_nome/Maildir/.Spam
6# chown -R seu_nome:seu_nome /home/seu_nome
```


Anotações:

Servidor Postfix

Servidor: Datacenter

Criando Alias de Email:

1 - Crie uma lista de distribuição através do arquivo aliases:

```
1# vim /etc/aliases
helpdesk: suporte,seu_nome
```

2- Para validar essas modificações e gerar o arquivo de "hash", use o comando "postalias" ou o comando "newaliases":

```
1# postalias /etc/aliases ou
newaliases
```

<Envie um e-mail para helpdesk@dexter.com.br e verifique a caixa de e-mail do usuário suporte>

Anotações:

Pergunta LPI

São arquivos de configuração do Postfix: (Selecione duas opções corretas):

A. /etc/postfix/main.cf

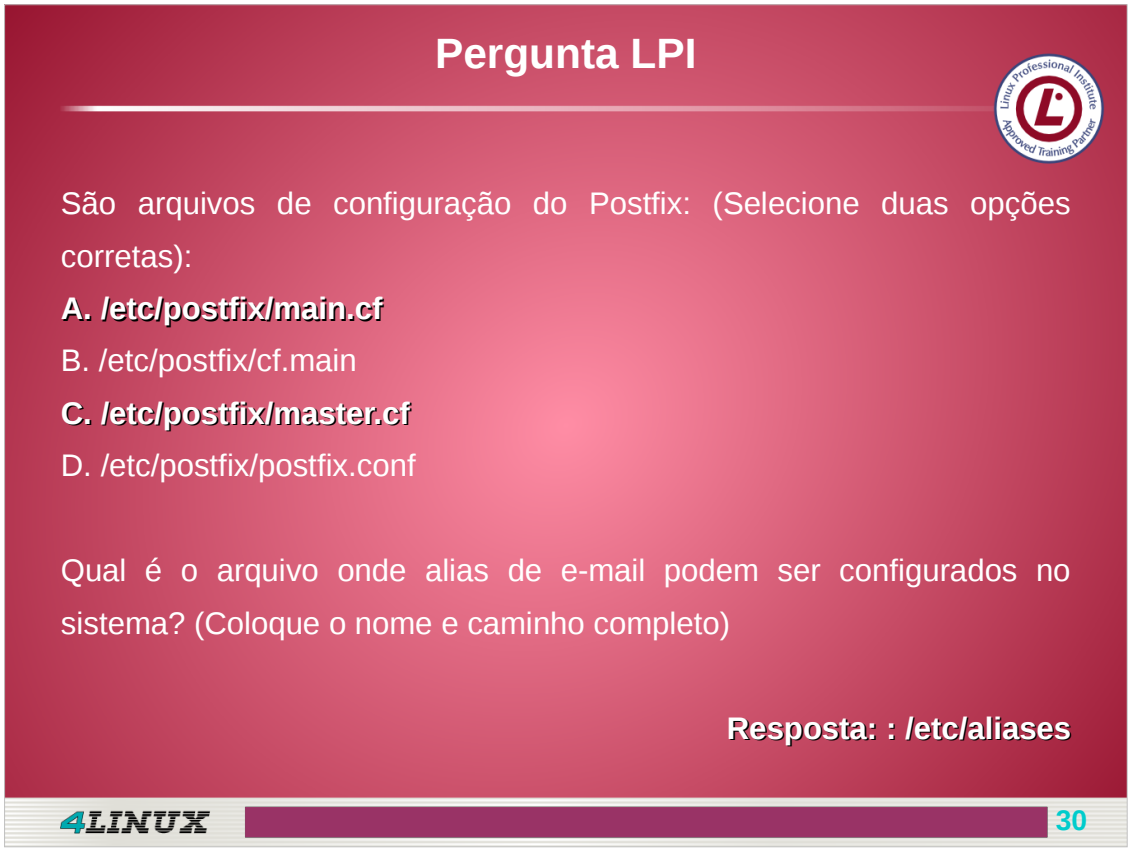
B. /etc/postfix/cf.main

C. /etc/postfix/master.cf

D. /etc/postfix/postfix.conf

Qual é o arquivo onde alias de e-mail podem ser configurados no sistema? (Coloque o nome e caminho completo)

Anotações:



Alternativas Corretas: A & C

main.cf → Cuida das configurações do E-mail;
master.cf → Cuida do comportamento do Daemon;

Estes são os principais arquivos de configuração do Postfix podendo aparecer em provas LPI.

REPOSTA CORRETA: /etc/aliases

Alias de e-mails podem sempre serão configurados através do arquivo /etc/aliases este arquivo constante aparece em provas LPI.

Próximos Passos

Para que você tenha um melhor aproveitamento do curso, participes das seguintes atividades disponíveis no Netclass:

- Executar as tarefas do **Practice Lab**;
- Resolver o **Desafio Appliance Lab** e postar o resultado no Fórum Temático;
- Responder as questões do **Teste de Conhecimento** sobre o conteúdo visto em aula.

Mãos à obra!