

THIAGO TASSAR DE ALMEIDA

Orientador: Daniel Fernandes Macedo

**ESTUDO DE CASO: IMPLEMENTAÇÃO DE UM SERVIÇO
DE E-MAIL PARA O DEPARTAMENTO DE COMPUTAÇÃO**

Ouro Preto
Novembro de 2010

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

ESTUDO DE CASO: IMPLEMENTAÇÃO DE UM SERVIÇO DE E-MAIL PARA O DEPARTAMENTO DE COMPUTAÇÃO

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação da Universidade Federal de Ouro Preto como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação.

THIAGO TASSAR DE ALMEIDA

Ouro Preto
Novembro de 2010



UNIVERSIDADE FEDERAL DE OURO PRETO

FOLHA DE APROVAÇÃO

ESTUDO DE CASO: IMPLEMENTAÇÃO DE UM SERVIÇO DE
E-MAIL PARA O DEPARTAMENTO DE COMPUTAÇÃO

THIAGO TASSAR DE ALMEIDA

Monografia defendida e aprovada pela banca examinadora constituída por:

Prof. DANIEL FERNANDES MACEDO – Orientador
Universidade Federal de Ouro Preto

Prof. RICARDO AUGUSTO RABELO DE OLIVEIRA
Universidade Federal de Ouro Preto

Prof. FABRÍCIO BENEVENUTO DE SOUZA
Universidade Federal de Ouro Preto

Ouro Preto, Novembro de 2010

Resumo

Este trabalho consiste em implementar um servidor de e-mail para o Departamento de Computação da UFOP utilizando conexão segura e com autenticação centralizada através de uma base de dados LDAP já existente. Para esta implementação foi feito um levantamento de todos os softwares que serão utilizados, definição das documentações necessárias, criação de ambientes de testes utilizando máquinas virtuais, instalação dos softwares nestes ambientes e realização de testes. O trabalho obteve dois resultados: primeiro, um guia de instalação para que outras universidades ou empresas possam replicar a configuração realizada nesta monografia. Segundo, um servidor seguro, com suporte a Webmail e lista de usuários foi instalado e será implantado no Departamento de Ciência da Computação.

Palavras-chave: Postfix, Servidor, E-mail, SMTP, POP3, IMAP, Linux.

Abstract

This work implemented an e-mail server for the Computer Science Department of UFOP using secure connection with authentication through an existing centralized LDAP database. For this implementation are surveyed all software to be used, defining the required documentation, creating test environments using virtual machines, installing the software in these environments and testing. The work had two results: first, an installation guide for other universities or companies to replicate the configuration performed in this monograph. Second, a secure server, has been installed, supporting Webmail and user lists. It will be deployed in the Computer Science Department.

Keywords: Postfix, Server, E-mail, SMTP, POP3, IMAP, Linux.

Dedico este trabalho à minha namorada Jordana e aos meus pais pelo apoio incondicional durante a minha caminhada

Agradecimentos

Primeiramente à Deus, por me dar força e saúde para conquistar os meus objetivos.

Aos meus pais, Weliton e Dária, que sempre me incentivaram e que lutaram para que eu chegasse até aqui.

À minha namorada Jordana pela compreensão, carinho e paciência pelo período de desenvolvimento deste projeto.

Aos meus avós, pela torcida e apoio.

Ao professor Daniel Macedo por sua orientação e oportunidade de trabalho.

Aos amigos que fiz durante toda graduação, que me ajudaram nesta caminhada.

A todos os professores do DECOM, por todo aprendizado e amizade.

Sumário

1	Introdução	1
1.1	Justificativa	1
1.2	Objetivos	2
1.2.1	Objetivo geral	2
1.2.2	Objetivos específicos	2
2	Referencial Teórico	4
2.1	Organização de um serviço de e-mail	4
2.1.1	Componentes de um e-mail	4
2.1.2	Principais Protocolos de E-mail	5
2.2	DNS	7
2.3	LDAP	8
2.3.1	Diretório	9
2.3.2	LDIF	10
3	Desenvolvimento	11
3.1	Identificação dos softwares a serem instalados	11
3.2	Instalação dos serviços em ambiente de teste	11
3.3	Segurança/disponibilidade dos serviços	14
3.4	Realização de testes	14
3.5	Integração com o LDAP	15
3.6	Implantação em produção	15
4	Conclusões	17
	Referências Bibliográficas	18
A	Documentação para instalação do servidor de e-mail	20
A.1	Instalação do Sistema Operacional	20
A.2	Instalação dos serviços de E-mail	27
A.2.1	iRedMail	27

A.2.2	Configuração das aplicações para uso de LDAP externo	32
A.2.3	Alteração do LDAP externo para uso do serviço de e-mail	33
A.3	Informações para acesso às aplicações	34
B	Arquivos importantes gerados no projeto e modos de uso	35
B.1	add_group.ldif	35
B.2	add_group_user.ldif	35
B.3	create_mail_user_OpenLDAP.sh	36
B.4	create_mail_users.sh	37
B.5	modify_mail_password_users_all.ldif	39
C	Administração e utilização do serviço de e-mail	47
C.1	Criação de contas de e-mail	47
C.1.1	Utilizando o create_mail_user_OpenLDAP.sh	47
C.1.2	Utilizando o painel iRedAdmin	48
C.2	Criação de listas de e-mail	49
C.3	Utilização do serviço de e-mail	50
C.3.1	Através de um cliente de e-mail	50
C.3.2	Através do webmail	51
C.4	Atualização do antivírus e antispam	52
C.4.1	ClamAV Antivírus	52
C.4.2	SpamAssassin Antispam	52
C.5	Desativar o <i>Greylisting</i> do Policyd	52
C.6	Firewall do sistema	52

Lista de Figuras

2.1	Fluxo do envio de uma mensagem	5
2.2	Exemplo de um diálogo entre o cliente e o servidor via SMTP	6
2.3	Exemplo da Estrutura de um LDAP	9
2.4	Exemplo de um arquivo LDIF	10
3.1	Tela de administração do VMware Server	12
3.2	Console de uma máquina virtual	12
3.3	Principais componentes e processo de trabalho do serviço de e-mail [13]	13
A.1	Tela inicial de instalação	20
A.2	Escolha do idioma do sistema	21
A.3	Escolha do idioma do sistema	21
A.4	Definição do Layout do teclado	22
A.5	Configuração do host da máquina	22
A.6	Configuração do domínio	22
A.7	Configuração do timezone do sistema	23
A.8	Exemplo da tabela de partições criada	23
A.9	Seleção de softwares a serem instalados	24
A.10	Instalação do GRUB na MBR	24
A.11	Final da instalação	25
A.12	Firewall implementado após a instalação do SO	26
A.13	Tela inicial da instalação	28
A.14	Configuração da pasta de mensagens	28
A.15	Definição da base de dados	28
A.16	Definição do sufixo da base LDAP	29
A.17	Senha de administração do LDAP	29
A.18	Senha de administração do MySQL	29
A.19	Definição do domínio decom.ufop.br	30
A.20	Senha para o administrador do domínio postmaster@decom.ufop.br	30
A.21	Senha para o usuário www@decom.ufop.br	30
A.22	Lista dos softwares	31

A.23	Definição do idioma do webmail Round Cube	31
B.1	Árvore LDAP do DECOM	37
B.2	Tela após seleção do ou=People	37
B.3	Tela de exportação de dados do phpLDAPadmin	37
C.1	Tela inicial do painel iRedAdmin	48
C.2	Opções do painel iRedAdmin	48
C.3	Tela de criação de e-mail do painel iRedAdmin	49
C.4	Tela de login do RoundCube	51
C.5	Tela principal do RoundCube	51

Lista de Tabelas

2.1	Agentes de e-mail	5
A.1	Aplicações do servidor de e-mail do DECOM.	34

Capítulo 1

Introdução

O e-mail é um dos meios de comunicação mais utilizados no mundo devido principalmente à facilidade de comunicação com qualquer parte do mundo e com um custo praticamente nulo. Para concluir o meu curso, escolhi como projeto de monografia montar um servidor de e-mail para o departamento de computação (DECOM). Para a realização desse trabalho foi utilizado o Postfix, software livre bastante popular no mundo Linux, e autenticação de usuários via base de dados LDAP. Hoje, a autenticação da rede sem fio do departamento utiliza esta base de dados, o que é bastante interessante e útil, pois centraliza a autenticação em apenas um local. Esse é um dos principais benefícios do LDAP, uma base suportada para serviços diversos. O servidor de e-mails apresentado nessa monografia tem autenticação, anti-spam e um sistema para leitura de e-mails como protocolo POP3. Hoje a grande maioria dos e-mails que circulam na internet são spam, o que gera muito lixo e perda de produtividade. Todos os acessos utilizam conexão segura para maior confiabilidade e segurança. Todo o processo foi documentado produzindo assim uma documentação detalhando a instalação e a configuração dos programas instalados.

1.1 Justificativa

O departamento de computação da UFOP há muito tempo tem planos de criar um servidor de e-mail próprio para uma maior independência do NTI. Desenvolver/projetar um servidor de e-mail para o DECOM foi um trabalho bastante interessante e de um aprendizado enorme. O trabalho pode servir de exemplo para qualquer profissional que planeje criar um servidor de e-mail com as características que serão propostas. Para desenvolvimento do trabalho foi necessário muita pesquisa em diversos sites, livros e documentação de produtos para definir os melhores softwares a serem utilizados e a melhor forma de configurá-los. A empresa onde trabalho, atualmente não possui um servidor de e-mail localmente e é um projeto futuro implantarmos tal serviço. Esse trabalho me dará conhecimento e experiência suficiente para realizar o mesmo procedimento profissionalmente. Já tive a oportunidade de configurar um

servidor de e-mail para uso de uma aplicação específica mas isso não demandou muito estudo e aprofundamento, procedimentos bastante importantes neste projeto.

1.2 Objetivos

1.2.1 Objetivo geral

O objetivo deste trabalho é a construção de um servidor de e-mail em produção no departamento de computação (DECOM) implementado utilizando softwares livres em ambiente Linux. Este servidor tem conexão segura e acesso autenticado tanto para envio quanto para recebimento de mensagens. A autenticação é realizada através de uma base LDAP já existente e também possui suporte a redirecionamento de mensagens, webmail e anti-spam.

1.2.2 Objetivos específicos

Para cumprir o objetivo geral proposto desse projeto, foi necessária a realização de determinadas atividades que estão descritas abaixo.

- **Aprendizado de LDAP e protocolos e serviços de e-mail (POP, SMTP, IMAP)**

Foi realizado um estudo sobre os principais protocolos envolvidos no projeto e os softwares que os utilizam. No caso, o Postfix para SMTP, Dovecot para POP/IMAP e OpenLDAP para LDAP.

- **Instalação de um servidor de e-mail, a ser homologado posteriormente, para uso no DECOM**

Todos os softwares foram instalados em um ambiente de testes (servidores virtualizados) e todo o procedimento documentado para implantação em produção. Tal procedimento foi utilizado no servidor de produção do DECOM e este será homologado para uso definitivo pelo departamento.

- **Independência do departamento dos serviços providos pelo departamento de informática da UFOP (NTI), provendo mais autonomia e flexibilidade para o DECOM**

Com o projeto, o DECOM dispõe de mais um serviço disponível. A criação de e-mails para os usuários do departamento ou qualquer alteração necessária era direcionada para o NTI e agora não será mais necessário. O próprio departamento cuidará do serviço, o deixando da forma mais adequada às suas necessidades.

- **Gerência interna das listas de e-mails do departamento, que hoje se encontram sob a responsabilidade de terceiros (por exemplo Google)**

Com este novo serviço existe a possibilidade de criação de grupos de e-mails internos para utilização do departamento.

Capítulo 2

Referencial Teórico

2.1 Organização de um serviço de e-mail

Ao contrário da maioria das soluções proprietárias de e-mail, onde um único pacote de software faz tudo, o serviço de e-mail é constituído de vários padrões e protocolos que definem como as mensagens são compostas e transferidas de um remetente para um destinatário. Há diversos softwares envolvidos, cada um para lidar com uma etapa diferente na entrega da mensagem. O Postfix trata apenas de uma parte do processo. A grande maioria dos usuários de e-mail só são familiarizados com o software que eles usam para ler e escrever mensagens, conhecido como MUA (*Mail User Agent*) ou cliente de e-mail como é mais popularmente conhecido. Exemplo de alguns mais comuns incluem Mozilla Thunderbird e Microsoft Outlook.

2.1.1 Componentes de um e-mail

Quando solicitamos ao programa cliente para enviar uma mensagem, ele simplesmente envia a mensagem para um servidor de e-mail rodando um MTA (*Mail Transfer Agent*) ou agente de transferência de e-mails. A figura 2.1 mostra os componentes envolvidos em um simples envio de e-mail de um remetente a um destinatário. MTAs como o Postfix encaminham uma mensagem de um sistema para outro. Quando ele recebe uma solicitação para aceitar uma mensagem de e-mail, o MTA determina se deve aceitar a mensagem ou não. Um MTA geralmente aceita mensagens para seus próprios usuários locais. Diversos servidores na Internet estão configurados como *Open Relay*, ou seja, aceitam o envio de mensagens onde o remetente e o destinatário não são usuários do servidor. Servidores configurados desta forma são uma ameaça à rede pois são utilizados por *spammers* para enviar seus e-mails sem limite. Este foi um dos pontos abordados nos testes iniciais deste projeto.

Se o MTA estiver configurado sem *Open Relay* (o mais usual), a mensagem é encaminhada para o MTA responsável pelo tal domínio do e-mail. Um exemplo é o envio de uma mensagem para josedasilva@gmail.com. O MTA de origem conectará no MTA da Google e este enviará a

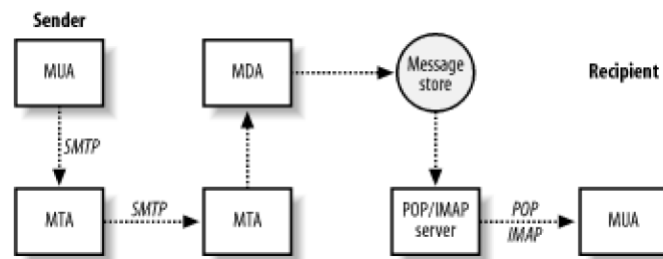


Figura 2.1: Fluxo do envio de uma mensagem

mensagem para o usuário final. Quando uma mensagem é destinada a um usuário do próprio sistema, ela é encaminhada para um MDA (*Mail Delivery Agent*) para encaminhamento final. O MDA pode armazenar a mensagem como um arquivo simples ou passá-la para um banco de dados especializado. O armazenamento da mensagem é realizado independentemente de como e onde ela será mantida pois o MDA já possui em suas configurações uma definição do local de armazenamento. Esse local é chamado de *Message store* e neste projeto, ele está localizado na pasta */var/vmail*. A tabela 2.1 mostra a definição dos tipos de agentes citados.

Agente	Nome	Descrição
MUA	Mail User Agent	Cliente de e-mail utilizado para compor, enviar, e receber mensagens. Envia mensagens através de um MTA. Recebe mensagens de uma caixa de mensagens diretamente ou através de um servidor POP/IMAP.
MTA	Mail Transfer Agent	Servidor que recebe e envia e-mail. Determina a rota da mensagem e as redireciona para outros servidores. As mensagens entregues localmente são enviadas para um MDA para a entrega final.
MDA	Mail Delivery Agent	Programa que controla a entrega final das mensagens para os destinatários locais de um sistema. MDAs muitas vezes podem filtrar ou classificar as mensagens no momento da entrega. O MDA também pode determinar que uma mensagem deva ser enviada para outro endereço de e-mail.

Tabela 2.1: Agentes de e-mail

2.1.2 Principais Protocolos de E-mail

As comunicações que ocorrem entre cada um desses componentes do sistema de e-mail são definidos por normas e protocolos. Os documentos padrões são mantidos pelo *Internet Engineering Task Force* (IETF) [8] e são publicados como documentos *Request For Comments* (RFC), que são documentos numerados que explicam uma determinada tecnologia ou protocolo.

O SMTP (*Simple Mail Transport Protocol*) é usado para envio de mensagens, e o POP (*Post Office Protocol*) ou IMAP (*Internet Mail Application Protocol*) são usados para recuperar mensagens do servidor. O SMTP, definido na RFC 2821 [10], descreve como acontece a comunicação realizada entre dois hosts em uma rede para troca de mensagens. Os protocolos IMAP (RFC 3501) [12] e o POP (RFC 1939) [11] descrevem como recuperar as mensagens de um local de armazenamento. O protocolo IMAP foi desenvolvido após o POP e oferece recursos adicionais. Uma diferença básica entre os dois protocolos é que com o IMAP, o usuário conecta na sua caixa de mensagem e visualiza em tempo real o conteúdo desta. Já no POP, o cliente recebe as mensagens de tempo em tempo (parâmetro configurado no MUA) e as armazena localmente. É possível configurar o MUA para que não apague as mensagens após o recebimento mas este não é o procedimento padrão. A figura 2.2 mostra um exemplo de comunicação via SMTP de um cliente com um servidor.

```
C: inicia a conexão com o servidor!!!
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

Figura 2.2: Exemplo de um diálogo entre o cliente e o servidor via SMTP

2.1.2.1 SMTP

SMTP é usado para o envio de e-mail e para a transmissão de mensagens entre MTAs. Quando um MUA comunica com um MTA para ter uma mensagem encaminhada, ele usa SMTP. SMTP também é usado quando um MTA realiza comunicação com outro MTA para retransmitir ou entregar uma mensagem. Originalmente, o SMTP não tinha meios para autenticar usuários, mas hoje já é possível caso seja necessário. No SMTP deste projeto, só é possível o envio de uma mensagem por um usuário através de uma conexão autenticada.

2.1.2.2 POP/IMAP

Quando os usuários querem recuperar suas mensagens, eles usam seu MUA para se conectar a um servidor POP ou IMAP. Usuários POP geralmente fazem o *download* de suas mensagens do servidor e gerenciam seus e-mails localmente. Já o IMAP oferece recursos que tornam mais fácil para gerenciar e-mails utilizando o próprio servidor. Muitos servidores já oferecem ambos os protocolos, inclusive o deste projeto.

2.2 DNS

Domain Name System, ou sistema de nomes de domínio, é um protocolo utilizado basicamente para transformar nomes de domínios em IPs. Esse protocolo foi criado para que não seja necessário realizar acessos diversos na Internet utilizando IPs, pois são difíceis de memorizar e podem ser alterados a qualquer momento pelo administrador do sistema.

O DNS em um serviço de e-mail é bastante importante pois ao invés de realizar um envio utilizando *usuario@200.233.221.50* (IP qualquer utilizado como exemplo), o envio é realizado utilizando *usuario@dominio.do.usuario*. A primeira forma citada é de difícil memorização como foi dito anteriormente.

O servidor DNS é composto por diversos tipos de registros e um deles se chama MX (*Mail Exchanger*). Este registro é o responsável por indicar quem é o servidor de e-mail de um determinado domínio. Segue abaixo um exemplo de consulta:

```
; <<>> DiG 9.6-ESV-R1 <<>> mx decom.ufop.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47681
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;decom.ufop.br.                IN      MX

;; ANSWER SECTION:
decom.ufop.br.                8616    IN      MX      10 mail.decom.ufop.br.
```

O resultado acima é referente a uma consulta realizada utilizando o comando *dig* pesquisando pelo MX do domínio *decom.ufop.br*. É indicado que o responsável pelo serviço de e-mail do domínio é o servidor que possui o endereço *mail.decom.ufop.br*. Existe um número 10 em frente do domínio e isto indica a prioridade. Podem existir mais de um MX definido para um mesmo domínio. Ao realizar a mesma consulta para o domínio *gmail.com*, obtemos o seguinte resultado:

```

; <<>> DiG 9.6-ESV-R1 <<>> mx gmail.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58622
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;gmail.com.                IN      MX

;; ANSWER SECTION:
gmail.com.                 306     IN      MX      20 alt2.gmail-smtp-in.l.google.com.
gmail.com.                 306     IN      MX      5  gmail-smtp-in.l.google.com.
gmail.com.                 306     IN      MX      10 alt1.gmail-smtp-in.l.google.com.
gmail.com.                 306     IN      MX      30 alt3.gmail-smtp-in.l.google.com.
gmail.com.                 306     IN      MX      40 alt4.gmail-smtp-in.l.google.com.

```

Percebe-se que existem cinco servidores de e-mail responsáveis pelo envio/recebimento de mensagens e cada um deles com um nível de prioridade. Os servidores que possuem um número menor definido são os que possuem maior prioridade de acesso.

Outro tipo de registro existente no DNS se chama A (*Address*). Este registro é o responsável por armazenar a informação do IP de um determinado nome. Segue um exemplo de consulta:

```

mail:~# nslookup mail.decom.ufop.br
Server:          200.131.208.82
Address:         200.131.208.82#53

```

```

Non-authoritative answer:
Name:   mail.decom.ufop.br
Address: 200.131.25.185

```

O exemplo mostra que o IP referente ao nome *mail.decom.ufop.br* é *200.131.25.185*. Observe que a consulta MX realizada anteriormente referente ao domínio do DECOM mostra que o servidor responsável pelo serviço de e-mail é o *mail.decom.ufop.br* e através do registro do tipo A, é localizado o IP do servidor.

2.3 LDAP

Lightweight Directory Access Protocol, ou Protocolo Leve de Acesso a Diretórios, ou apenas LDAP, é um protocolo utilizado para atualizar e pesquisar diretórios, rodando sobre o pro-

protocolo de rede TCP/IP. Ele define não apenas a linguagem de consulta às informações, mas também o protocolo de rede que transporta as requisições e respostas do cliente para o servidor [6]. Ao contrário de um banco de dados relacional, o LDAP utiliza bibliotecas livres para implementar o seu protocolo de rede. Sendo assim, qualquer cliente pode obter informações em qualquer servidor de diretório LDAP, já que o protocolo foi padronizado pelo IETF (*Internet Engineering Task Force*) [8].

O LDAP é baseado no modelo cliente-servidor. Um ou mais servidores LDAP contêm os dados criando a árvore de Diretório LDAP. Um cliente LDAP conecta-se a um servidor, geralmente pela porta padrão 389, e faz uma requisição. O servidor responde ou exibe um ponteiro para onde o cliente pode conseguir a informação (tipicamente, outro servidor LDAP).

2.3.1 Diretório

Um Diretório é uma base de dados especializada definida de forma hierárquica, otimizada para leitura com suporte a sofisticados métodos de pesquisa, proporcionando respostas rápidas a um enorme volume de consultas [15]. Em relação à estrutura, podemos fazer uma analogia às pastas que encontramos em nossos computadores. Em relação à funcionalidade, cabe uma analogia com o serviço de ajuda de uma companhia telefônica, que nos informa o número do telefone de uma pessoa se soubermos o nome, o endereço, ou mesmo alguns dados dessa pessoa. Dado um conjunto de atributos de uma pessoa, máquina ou outro recurso, o serviço de diretório retorna o endereço desse recurso na rede, e outras informações sobre ele.

Cada entrada no Diretório descreve um objeto (uma pessoa, um equipamento, uma rede, etc.), que tem um identificador único chamado *Distinguished Name* (DN). Uma entrada consiste de uma coleção de atributos, sendo que, para uma pessoa, estes atributos podem ser nome, endereço, e-mail, etc. A figura 2.3 mostra a estrutura de um diretório.

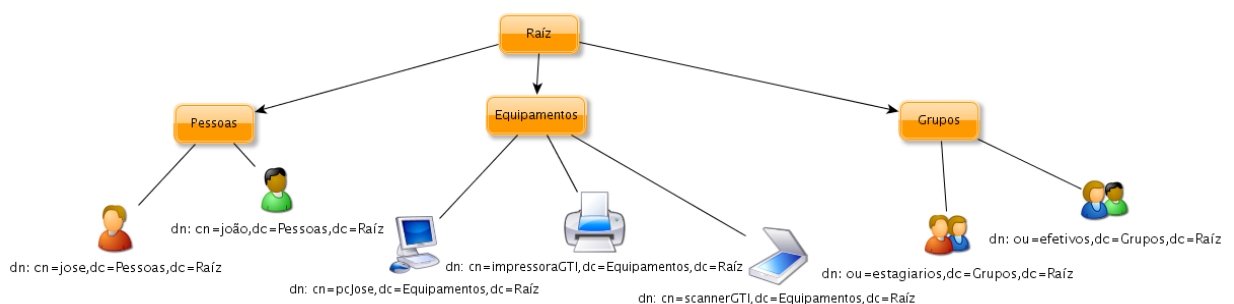


Figura 2.3: Exemplo da Estrutura de um LDAP

2.3.2 LDIF

LDAP Data Interchange Format, ou apenas LDIF, é um arquivo de texto usado para importar dados para o diretório, alterar objetos existentes, criar *backup* do diretório, e por fim, realizar replicação da base. Todos os dados devem obedecer ao esquema do diretório. A figura 2.4 mostra um exemplo de um arquivo no formato LDIF.

```
dn: mail=grupo@decom.ufop.br,ou=Groups,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
objectclass: mailList
accesspolicy: domain
accountstatus: active
cn: Lista de Teste
enabledservice: mail
enabledservice: deliver
mail: grupo@decom.ufop.br
```

Figura 2.4: Exemplo de um arquivo LDIF

Nesse arquivo usado como exemplo, está sendo criada uma nova lista de e-mail. O arquivo gerado é formatado basicamente da seguinte maneira:

- DN (*Distinguished Name*) ou nome distinto – Primeira linha
- Tipo do componente inserido (no caso mailList) – Segunda linha
- Atributos – Terceira linha até a última

Todo arquivo gerado no formato LDIF deve estar como texto puro.

Capítulo 3

Desenvolvimento

3.1 Identificação dos softwares a serem instalados

Primeiramente, foi realizado um levantamento dos componentes necessários para a implementação de um serviço de e-mail, lista de softwares para implementação destes serviços e maneiras de realizar a instalação/configuração de todos eles de forma que trabalhem integrados. Todos os passos realizados, desde pesquisa de softwares, instalação e testes, foram documentados pois assim qualquer um que precisar realizar algum tipo de alteração neste servidor não terá dificuldades (vide apêndice A). Houve uma grande preocupação em relação aos SPAMs, que hoje é o que gera o maior volume de e-mails da Internet.

O capítulo 2 mostra os diversos componentes que compõem um serviço de e-mail, o que gera diversas soluções diferentes para implementação deste serviço.

3.2 Instalação dos serviços em ambiente de teste

Após o levantamento dos softwares e possíveis modos de implementação, foi iniciada a etapa de instalação em ambientes virtuais. Esta etapa foi bastante importante pois qualquer falha durante o processo poderia impactar no projeto como um todo. Um exemplo seria um arquivo de configuração com algum parâmetro incorreto ou até mesmo não presente. O software utilizado para criação deste ambiente foi o VMware Server na sua versão 2.0.2 instalado em uma máquina com processador Phenom X4 e 8GB de RAM.

Para realização das instalações foram utilizadas várias máquinas virtuais, cada uma com uma solução diferente. O sistema operacional utilizado foi o Debian Linux na versão Lenny (5.X) 64 bits. As figuras 3.1 e 3.2 mostram como é a interface de administração e a de acesso à máquina virtual.

A solução final para este projeto foi a utilização de um software auxiliar que se chama iRedMail. Esta aplicação faz toda a integração necessária de todos os softwares que serão

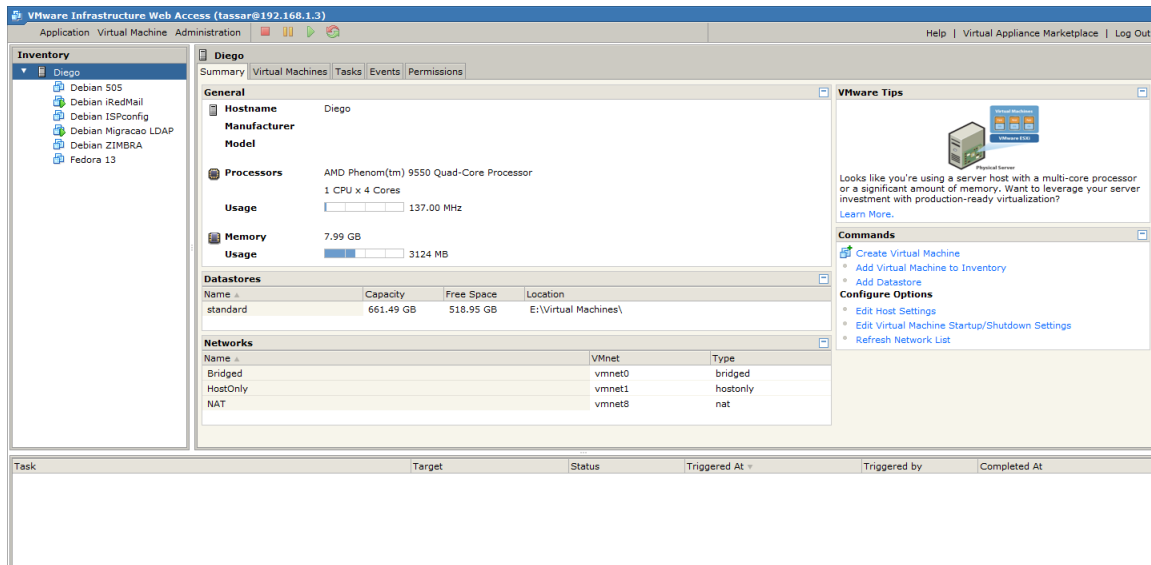


Figura 3.1: Tela de administração do VMware Server

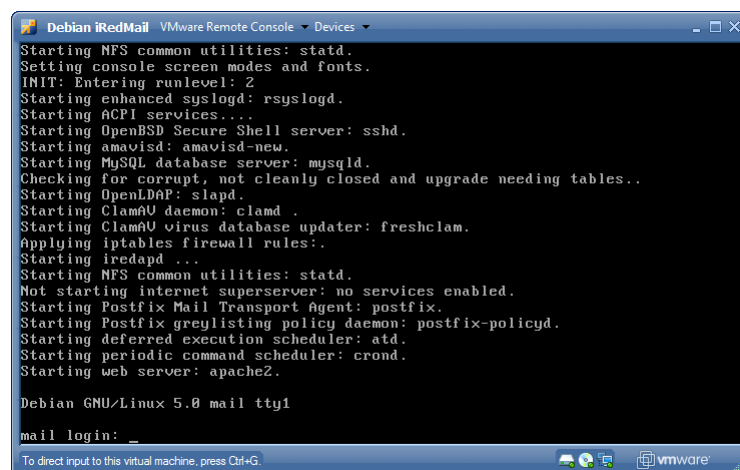


Figura 3.2: Console de uma máquina virtual

utilizados para o bom funcionamento do serviço de e-mail. A figura 3.3 mostra como é feita essa integração. Seguem abaixo os principais softwares utilizados:

- Postfix – Envio de mensagens (SMTP)
- Dovecot – Recebimento de mensagens (POP3 e IMAP)
- OpenLDAP – Implementa o protocolo LDAP no Linux
- AMaViS – A Mail Virus Scanner - Faz a integração do MTA com o antivírus e o antispam
- ClamAV – Antivírus

- SpamAssassin – Antispam
- RoundCube – Webmail para acesso a caixa de mensagem sem utilização de um MTU
- phpLDAPadmin – Ferramenta para administração da base de dados LDAP
- phpMyAdmin – Ferramenta para administração de dados do MySQL
- iRedAdmin – Painel de administração de domínios e contas de e-mail

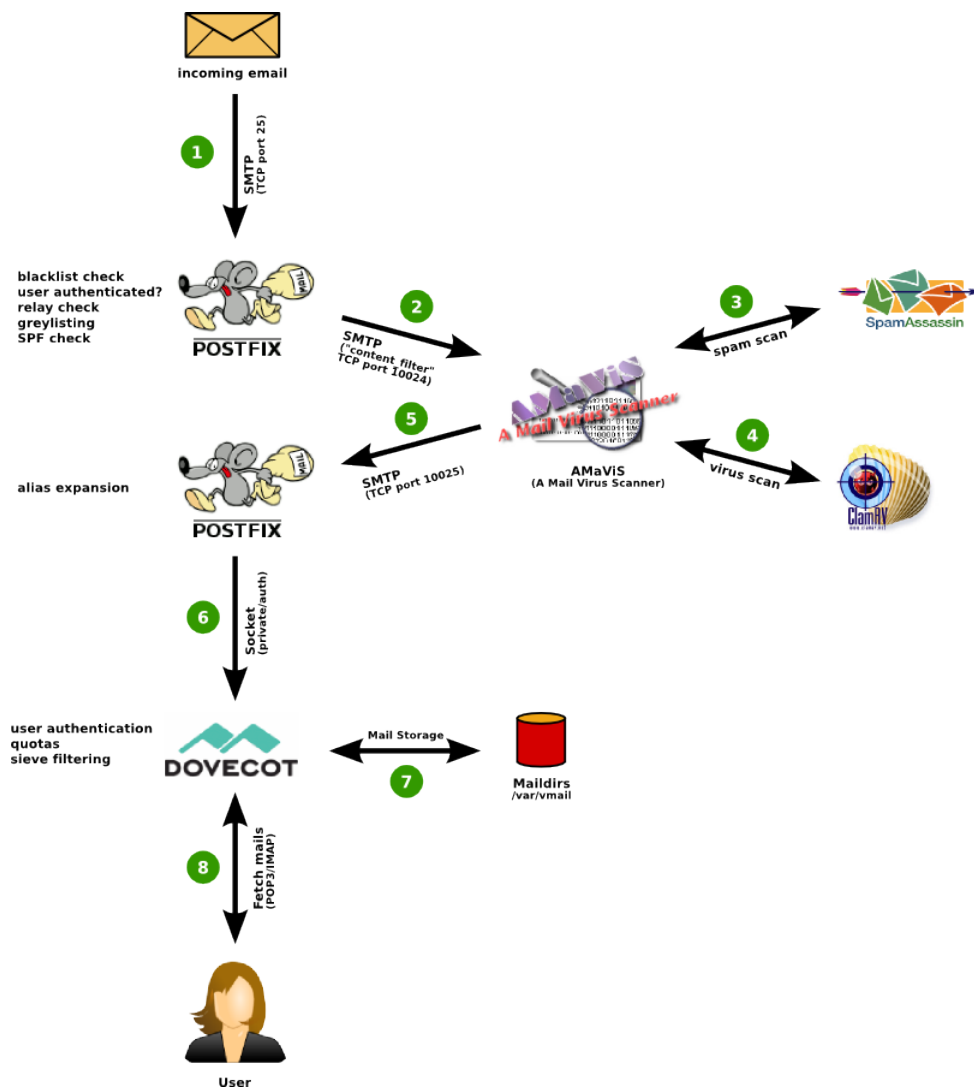


Figura 3.3: Principais componentes e processo de trabalho do serviço de e-mail [13]

3.3 Segurança/disponibilidade dos serviços

Foram definidas medidas de segurança e diretivas que mantêm o servidor com o máximo de disponibilidade possível. Um serviço de e-mail nunca pode parar e foram criadas regras de firewall para evitar ataques de pessoas mal intencionadas.

O firewall implementado foi utilizando o *iptables* [5], software que já está instalado no sistema por padrão, com regras de INPUT e FORWARD (entrada e redirecionamentos) bloqueadas por padrão e foram liberadas apenas as portas que devem possuir acesso externo. A porta 3306 por exemplo, porta do MySQL, apesar de estar aberta no servidor, não deve ser acessada externamente. A regra de OUTPUT (saída) está por padrão liberada. Segue abaixo o trecho do firewall inserido pelo *iRedMail* que estabelece tais regras:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

# Keep state.
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# http/https, smtp/smtps, pop3/pop3s, imap/imap, ssh
-A INPUT -p tcp -m multiport --dport 80,443,25,465,110,995,143,993,587,465,22222 -j ACCEPT
```

Outra medida de segurança realizada foi a alteração da porta SSH do servidor de 22 para 22222 para evitar possíveis ataques. A alteração de porta não evita tentativas de invasão no servidor mas as diminui consideravelmente. No futuro, caso o DECOM julgue ser necessário, podem ser criadas regras individuais para a porta 22222 liberando apenas algumas redes ou IPs.

3.4 Realização de testes

Após todo o processo de configuração, foram realizados diversos testes no sistema validando cada funcionalidade necessária para o bom funcionamento do serviço de e-mail. Os principais testes realizados foram os seguintes:

- Criação de uma nova conta de e-mail na base LDAP
Resultado: E-mail criado com sucesso.
- Envio de mensagem através de um MUA (Microsoft Outlook) sem autenticação
Resultado: Ao tentar realizar este envio, o servidor negou.
- Envio de mensagem através de um MUA (Microsoft Outlook) com autenticação
Resultado: O e-mail foi enviado com sucesso.

- Recebimento de mensagens utilizando o protocolo POP3
Resultado: As mensagens foram recebidas corretamente.
- Recebimento de mensagens utilizando o protocolo IMAP4
Resultado: A conexão e visualização das mensagens que estavam na caixa de mensagem do servidor ocorreu corretamente.
- Acesso à caixa de mensagens através do Webmail (realização de teste de envio e recebimento de mensagens)
Resultado: Webmail funcionou corretamente. As mensagens foram enviadas sem nenhum problema e a caixa de mensagens foi exibida corretamente.

3.5 Integração com o LDAP

Após a verificação do funcionamento do serviço de e-mail, foram iniciados os testes de integração com uma base LDAP já existente. Um *dump* da base do LDAP de produção do DECOM foi feito e esta importada em uma das máquinas virtuais criadas. Vários erros ocorreram na tentativa de importação desta base e após a verificação do arquivo de configuração do LDAP do DECOM, foi identificado que existiam alguns *schemas* a mais (samba e pykora) e estes precisaram ser copiados para a máquina de teste para conclusão da importação.

Com a base importada, foi necessário realizar algumas alterações na máquina onde estão instalados os serviços de e-mail. Nem todas as aplicações, utilizam a base LDAP para seu funcionamento. As que utilizam precisaram ter alguns de seus arquivos de configuração alterados. Todo o procedimento da alteração destes arquivos de configuração está documentado no apêndice A na seção A.2.

3.6 Implantação em produção

Nesta etapa, todo o procedimento realizado e aprovado durante as etapas anteriores foi aplicado no servidor de produção com exceção da migração da base de dados para o LDAP já existente.

Foi solicitado ao departamento de informática da UFOP (NTI) a criação de um registro DNS com o nome de *mail.decom.ufop.br* resolvendo para o IP *200.131.25.185* (IP do servidor criado) e a criação de um registro do tipo MX (*Mail Exchanger*) para o domínio *decom.ufop.br* para que as mensagens enviadas a este domínio tenham um destino.

Uma conta para teste *tassar@decom.ufop.br* foi criada e os mesmos testes da seção 3.4 foram realizados em produção. Houve um diferencial pois somente em produção foi possível testar o recebimento de uma mensagem de origem externa e funcionou corretamente.

Após os testes, utilizando os dados do *dump* do LDAP do DECOM, foi realizado um levantamento dos usuários que deveriam ter o e-mail criado no servidor. Grande parte dos

usuários existentes era do tipo *com000000*, sendo os zeros o número de matrícula do aluno e estes foram desconsiderados.

Foram identificados 56 usuários e foi desenvolvido um script para a criação de todos eles no sistema. Após a criação, foi gerado um arquivo LDIF para alteração da senha de todos eles para que fiquem com a mesma senha já utilizada na base existente do departamento (vide Apêndice B).

A última fase da implantação, ainda não realizada, é migrar toda essa base de dados para a base já existente realizando os procedimentos do Apêndice A na seção referente a uso de LDAP externo.

Capítulo 4

Conclusões

Conforme apresentado, um servidor de e-mail possui diversos componentes e estes precisam trabalhar de forma correta e em conjunto para um bom funcionamento do sistema. Foi necessário muito estudo, muita pesquisa e muitos testes em ambientes virtuais para homologar todo o procedimento realizado e depois realizar a implantação em uma máquina de produção.

O departamento está cada vez mais independente e agora conta com mais um serviço sob a sua própria administração. Isto facilita bastante qualquer tipo de alteração de configuração do serviço ou até mesmo uma simples criação de conta de e-mail, o que também é muito bom para o departamento de informática da universidade (NTI).

O serviço já foi implementado no servidor de produção do departamento de computação e está disponível para uso, porém ainda falta migrar os dados para a base já existente do departamento. A fase de testes em ambiente de homologação teve resultados satisfatórios. Foram realizados também testes no ambiente de produção obtendo bons resultados, entretanto serão realizados novos após a migração da base de dados para que possa ser usado em definitivo como o servidor de e-mail oficial do DECOM.

Todo o procedimento de instalação encontra-se documentado nos apêndices para que outros profissionais ou interessados possam implementar o serviço proposto neste trabalho.

Referências Bibliográficas

- [1] A enciclopédia livre, Wikipédia. Postfix. Disponível em: <http://pt.wikipedia.org/wiki/Postfix>
- [2] Site oficial do projeto Postfix. Disponível em: <http://www.postfix.org/>
- [3] Site oficial do projeto SpamAssassin. Disponível em: <http://spamassassin.apache.org/>
- [4] Site oficial do projeto Dovecot. Disponível em: <http://www.dovecot.org/>
- [5] Debian Wiki - iptables. Disponível em: <http://wiki.debian.org/iptables>
- [6] Campos, Augusto. Integração de Rede com Diretórios LDAP. Revista do Linux. Disponível em: <http://augustocampos.net/revista-do-linux/025/rede.html> - Acesso em: 11 Nov. 2010.
- [7] Trigo, Clodonil Honório. OpenLDAP: Uma abordagem integrada. São Paulo, SP. Novatec Editora, 2007.
- [8] The Internet Engineering Task Force. Disponível em: <http://www.ietf.org/> - Acesso em 11 Nov. 2010.
- [9] O'Reilly. Postfix: The Definitive Guide. Sebastopol, CA. O'Reilly & Associates, 2004.
- [10] The Internet Engineering Task Force. RFC 2821. Disponível em: <http://tools.ietf.org/html/rfc2821> - Acesso em: 19 Nov. 2010.
- [11] The Internet Engineering Task Force. RFC 1939. Disponível em: <http://tools.ietf.org/html/rfc1939> - Acesso em: 19 Nov. 2010.
- [12] The Internet Engineering Task Force. RFC 3501. Disponível em: <http://tools.ietf.org/html/rfc3501> - Acesso em: 19 Nov. 2010.
- [13] iRedMail - Features Overview. Disponível em: <http://www.iredmail.org/features.html> - Acesso em: 19 Nov. 2010.

-
- [14] TANENBAUM, Andrew S.. Redes de Computadores. 4. ed. São Paulo, SP: Editora Campus, 2003.
 - [15] Gouveia, Bruno. LDAP para Iniciantes. Abril de 2005. Disponível em: www.ldap.org.br
- Acesso em: 22 Nov. 2010.

Apêndice A

Documentação para instalação do servidor de e-mail

A.1 Instalação do Sistema Operacional

O sistema operacional escolhido neste projeto foi o Linux. A distribuição é o Debian Lenny em sua versão 64 bits para melhor aproveitamento dos recursos do servidor.

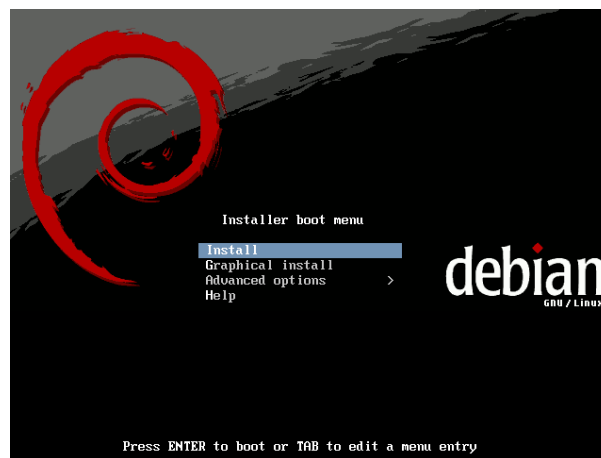


Figura A.1: Tela inicial de instalação

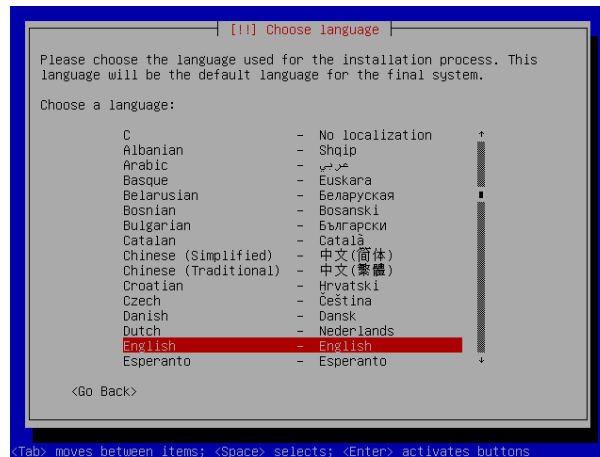


Figura A.2: Escolha do idioma do sistema

Escolher na sequência de telas as seguintes opções: *Other*, *South America* e *Brazil* respectivamente para definir a localização geográfica do servidor. Logo após, escolher o layout do teclado que será utilizado. Neste caso, a escolha foi ABNT.

O próximo passo é a de configuração de rede do sistema. Neste passo será definido o *host* da máquina e seu respectivo *domain* como mostram as figuras A.5 e A.6.

- host - *mail*
- domain - *decom.ufop.br*

Após a definição do domínio, será solicitado a escolha do *timezone* do sistema, que neste caso, é *Sao Paulo*. Veja na figura A.7.

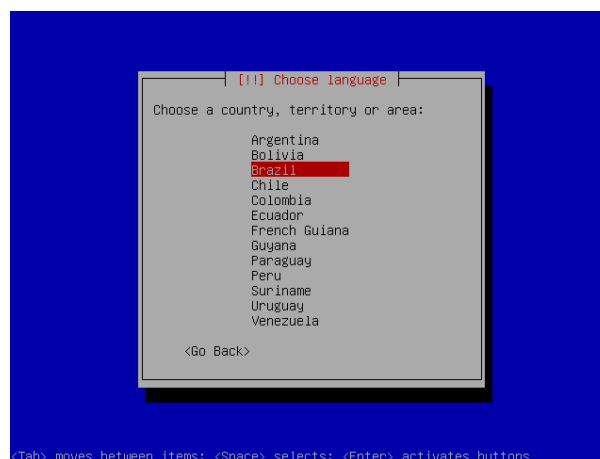


Figura A.3: Escolha do idioma do sistema

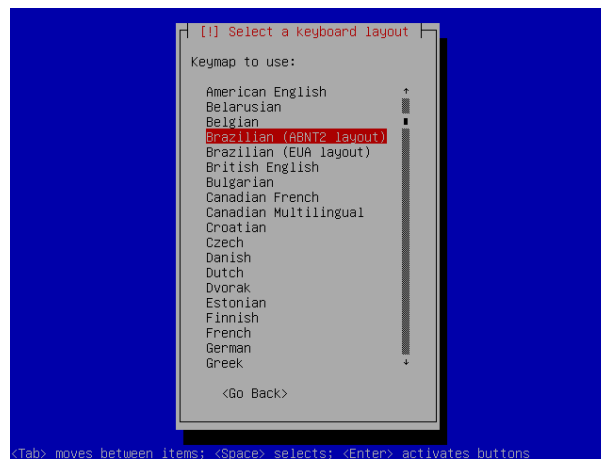


Figura A.4: Definição do Layout do teclado

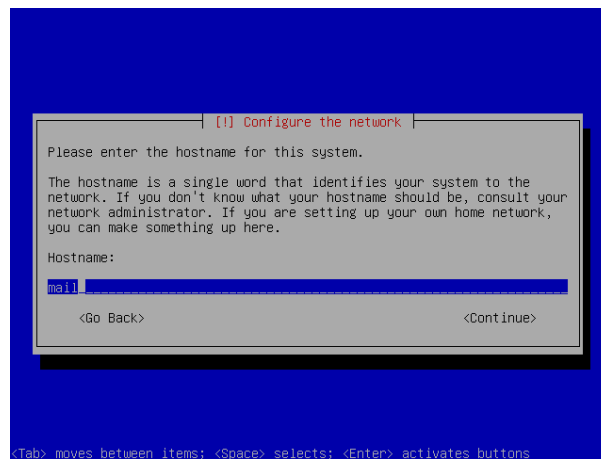


Figura A.5: Configuração do host da máquina

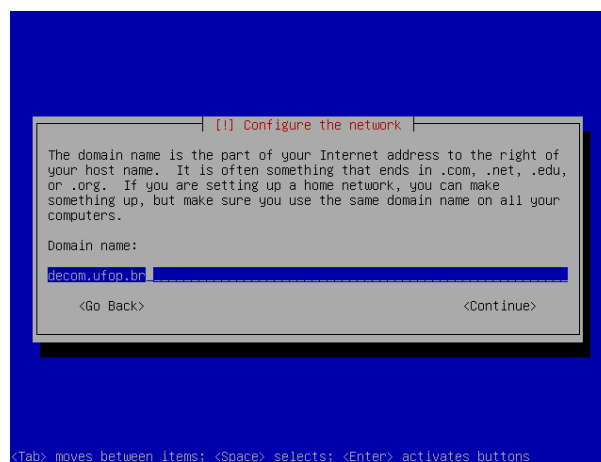


Figura A.6: Configuração do domínio

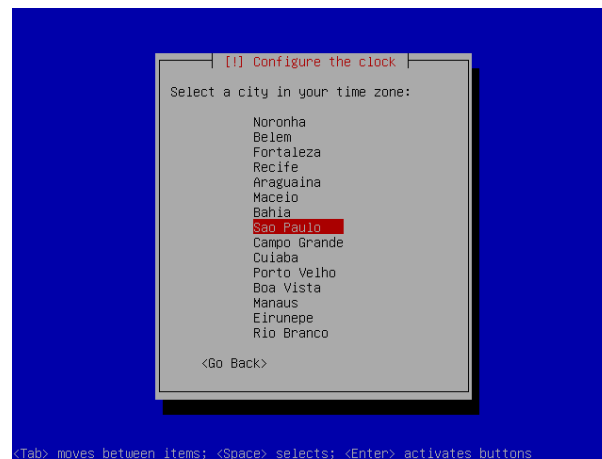


Figura A.7: Configuração do timezone do sistema

Na próxima etapa, serão configuradas as partições do sistema. Como o grande volume de dados do servidor ficará armazenado na pasta **/var**, esta terá uma partição separada com grande parte do espaço em disco. O disco será dividido da seguinte forma:

- **/** - Aproximadamente 10% do disco.
- **swap** - 4GB (quantidade de memória RAM neste caso)
- **/var** - Restante do espaço em disco

Selecione a opção manual e escolha o disco encontrado pelo sistema. Provavelmente aparecerá com o nome *SCSI...* Nas próximas telas, serão criadas as partições com a divisão informada anteriormente. Não vou entrar em muitos detalhes na criação das partições para não estender demais este manual. Na figura A.8, é apresentado um exemplo da tabela de partições criada.

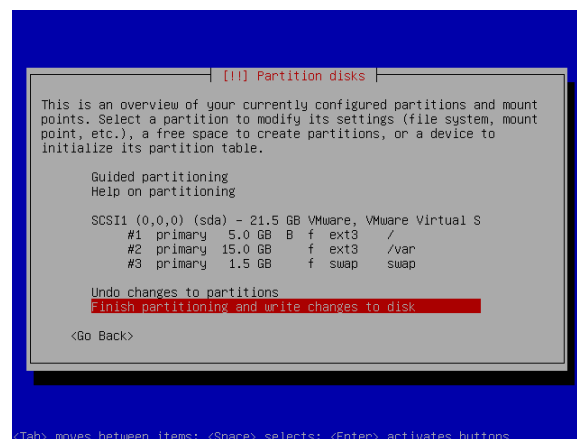


Figura A.8: Exemplo da tabela de partições criada

Depois desta etapa, é iniciada a instalação do sistema. Após o término, será solicitado a definição de senha de *root* e um nome/login para a criação de usuário comum no sistema. O próximo passo é a configuração do gerenciador de pacotes APT. Uma tela perguntando se você quer adicionar uma nova mídia como fonte de pacotes será exibida e escolha a opção *No*. Na próxima, você será questionado sobre o uso de um *Network Mirror* e deve escolher *Yes* para que o servidor não dependa apenas da mídia de instalação e possa baixar pacotes pela Internet. Uma sugestão de *mirror* seria o *debian.las.ic.unicamp.br* pois possui uma velocidade boa e sempre está disponível. Na etapa *Software selection*, escolha apenas *Standart system* para instalar apenas o básico do sistema.

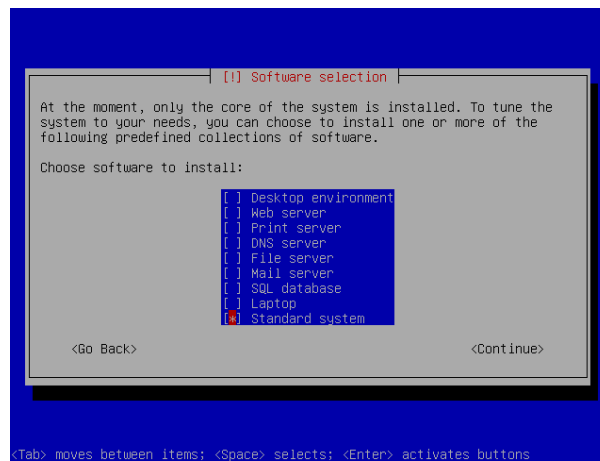


Figura A.9: Seleção de softwares a serem instalados

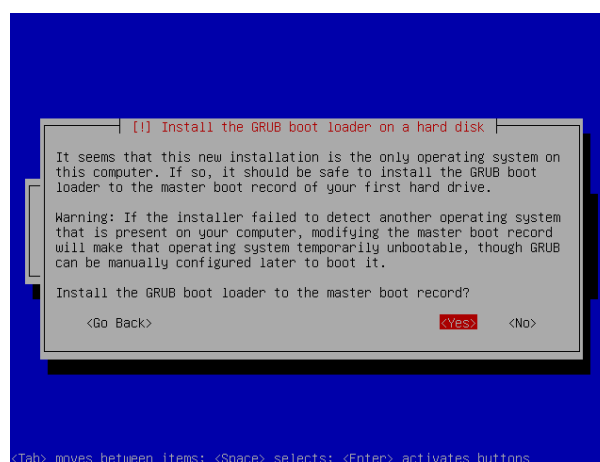


Figura A.10: Instalação do GRUB na MBR

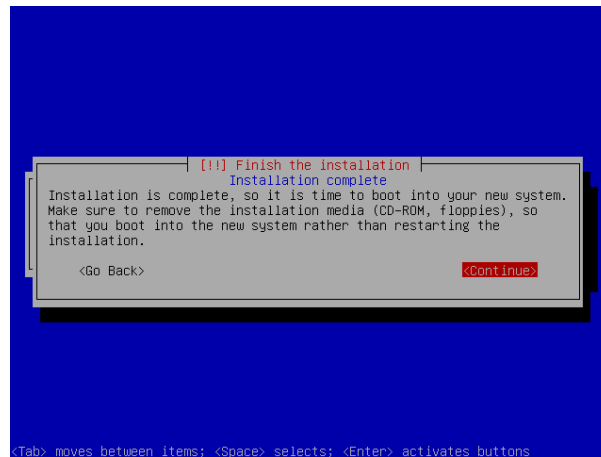


Figura A.11: Final da instalação

Após terminar a instalação, realizar os seguintes passos:

1. Instalar o OpenSSH com suas devidas dependências:
 - apt-get install ssh -y
2. Remover o *EXIM4*, MTA (*Mail Transfer Agent*) que é instalado por padrão no Debian:
 - apt-get remove --purge exim4 exim4-base exim4-config exim4-daemon-light -y
3. Alterar a porta do OpenSSH Server para 22222 por motivos de segurança:
 - vim /etc/ssh/sshd_config
 - Alterar o parâmetro *Port 22* para *Port 22222*
 - /etc/init.d/ssh restart
4. Inserir regras de firewall:
 - vim /root/firewall
 - Inserir o conteúdo da figura A.12
 - chmod +x /root/firewall
 - sh /root/firewall

```
# Limpando regras anteriores
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -F INPUT
iptables -F OUTPUT
iptables -F FORWARD

# Bloqueio de entrada e redirecionamentos
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

iptables -A INPUT -p icmp -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Liberando acesso da própria máquina
iptables -A INPUT -p all -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT
iptables -A INPUT -p all -s 200.131.25.185 -d 200.131.25.185 -j ACCEPT

# Liberando acesso SSH
iptables -A INPUT -s 0/0 -p tcp --dport 22222 -j ACCEPT
```

Figura A.12: Firewall implementado após a instalação do SO

O firewall implementado será utilizado apenas temporariamente. O firewall definitivo será o sugerido na instalação do iRedMail como será descrito na próxima seção.

A.2 Instalação dos serviços de E-mail

A.2.1 iRedMail

O primeiro passo é realizar o download do software *iRedMail* disponível em <http://www.iredmail.org/download.html>. Segue abaixo os procedimentos de instalação:

1. Fazer o download e descompactar o arquivo .bz2
 - `wget http://iredmail.googlecode.com/files/iRedMail-0.6.1.tar.bz2`
 - `apt-get install bzip2`
2. Fazer o download dos pacotes necessários para a instalação (no caso a pasta /root foi utilizada):
 - `cd /root/iRedMail-0.6.1/pkgs/`
 - `bash get_all.sh`
3. Iniciar a instalação
 - `cd /root/iRedMail-0.6.1/`
 - `bash iRedMail.sh`
4. Configuração do iRedMail (como mostrado nas figuras A.13 a A.23)
 - Definir a pasta de mensagens como /var/vmail -> Figura A.14
 - Definir a base de dados como OpenLDAP -> Figura A.15
 - Definir o sufixo do LDAP como dc=decom,dc=ufop,dc=br -> Figura A.16
 - Digitar a senha para a administração do LDAP -> Figura A.17
 - Digitar a senha para a administração do MySQL -> Figura A.18
 - Definir o primeiro domínio como decom.ufop.br -> Figura A.19
 - Digitar a senha para o login postmaster@decom.ufop.br, login de administração do domínio -> Figura A.20
 - Digitar a senha para o primeiro e-mail criado (www@decom.ufop.br) -> Figura A.21
 - Escolher os softwares a serem instalados (todos da lista) -> Figura A.22
 - Escolher o idioma pt_BR para ser utilizado como padrão no webmail (Round Cube) -> Figura A.23

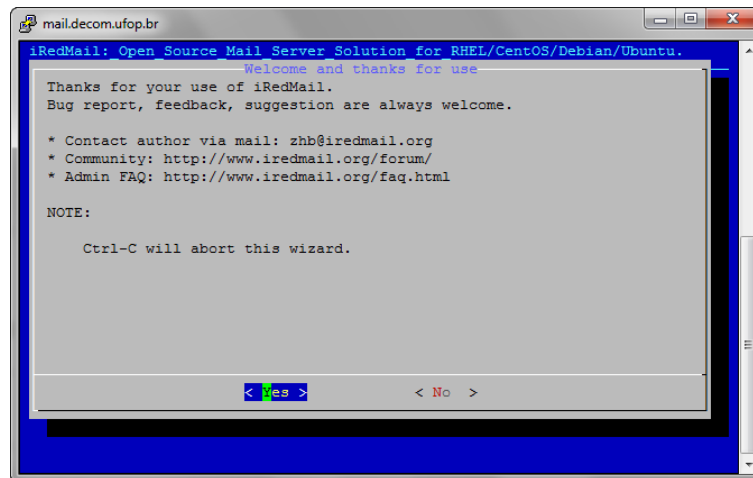


Figura A.13: Tela inicial da instalação

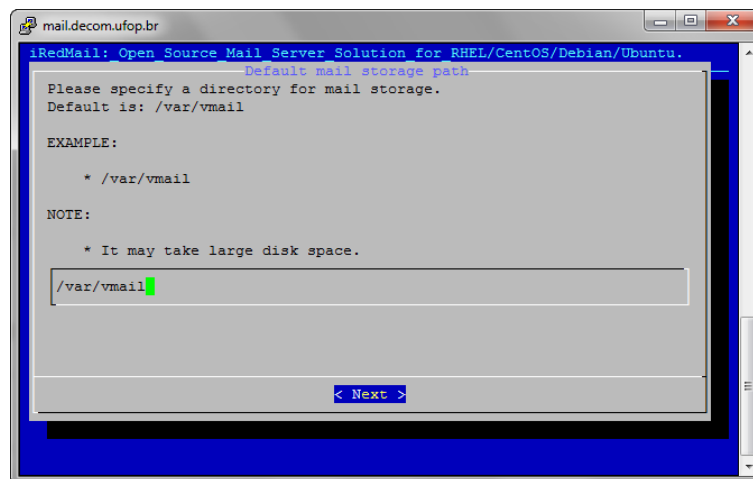


Figura A.14: Configuração da pasta de mensagens

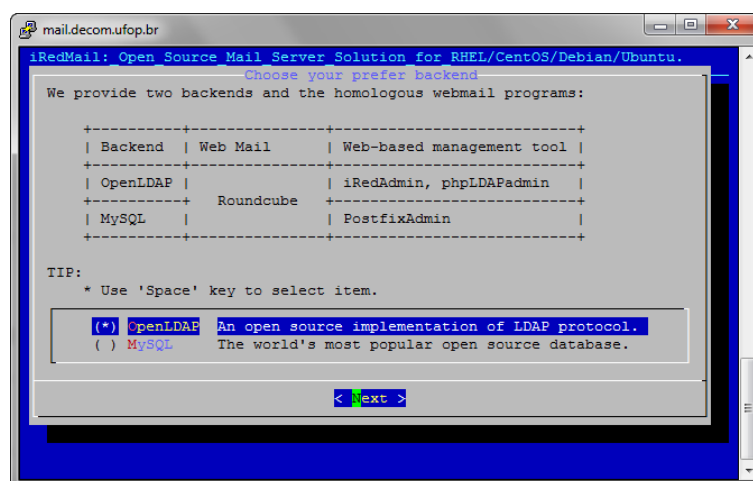


Figura A.15: Definição da base de dados

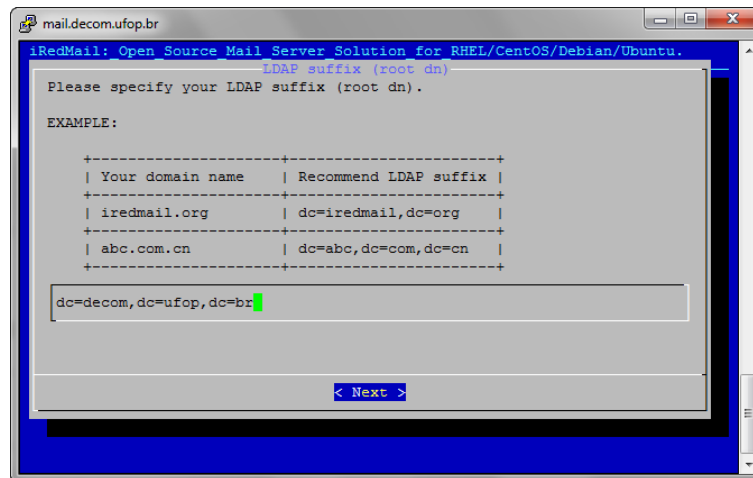


Figura A.16: Definição do sufixo da base LDAP

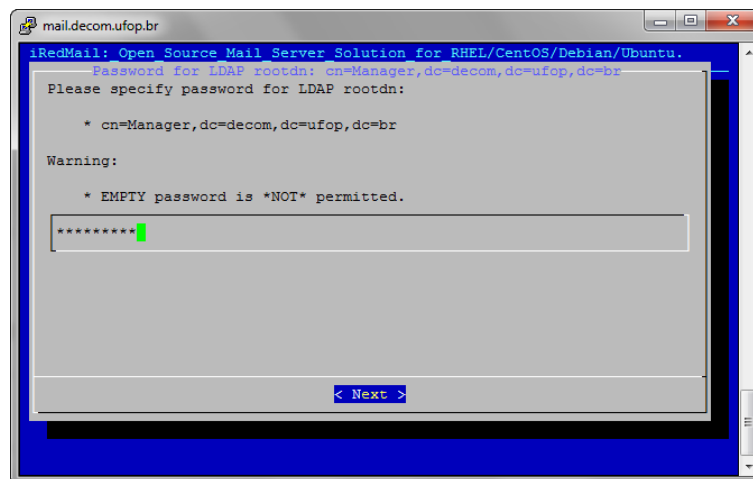


Figura A.17: Senha de administração do LDAP

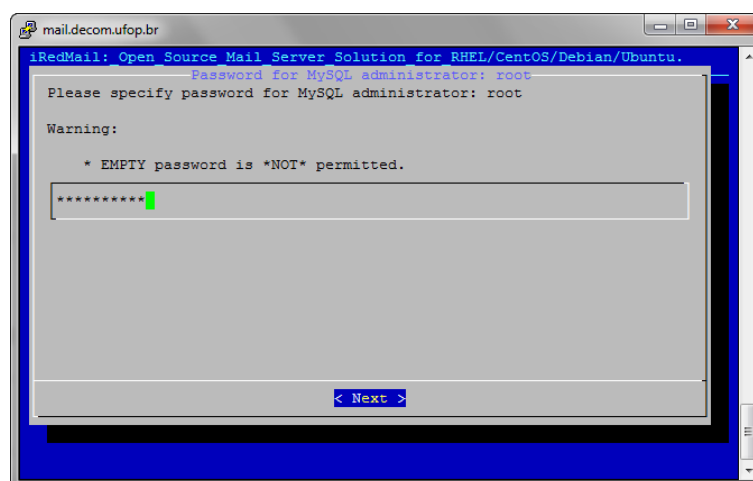


Figura A.18: Senha de administração do MySQL

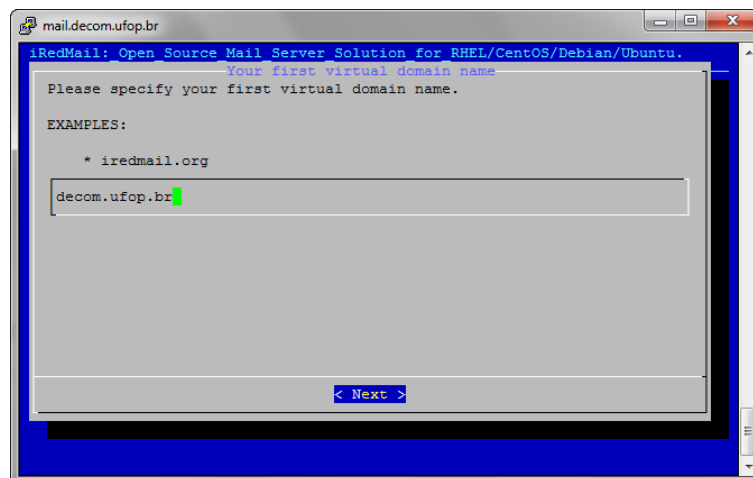


Figura A.19: Definição do domínio decom.ufop.br

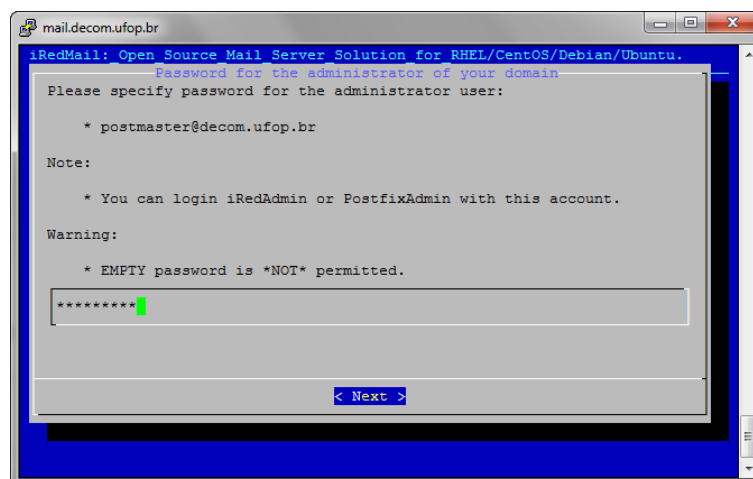


Figura A.20: Senha para o administrador do domínio postmaster@decom.ufop.br

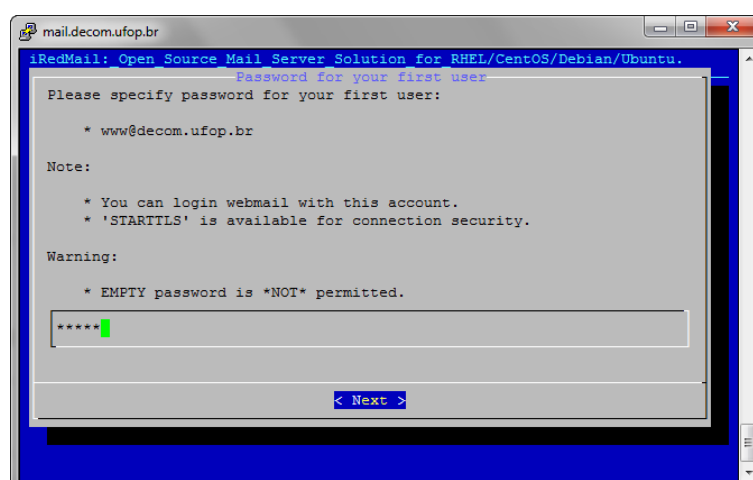


Figura A.21: Senha para o usuário www@decom.ufop.br

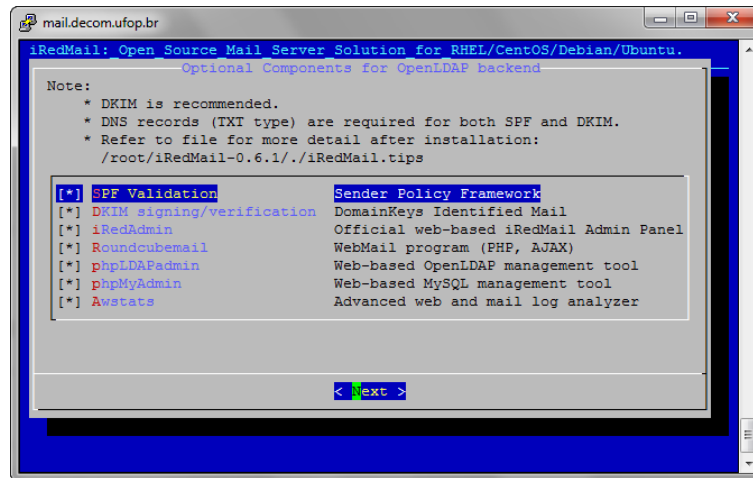


Figura A.22: Lista dos softwares

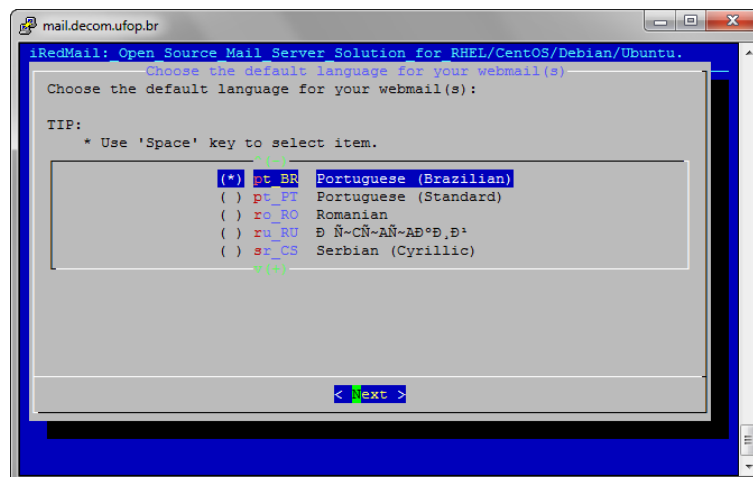


Figura A.23: Definição do idioma do webmail Round Cube

5. Instalação dos pacotes no sistema

- Nesta etapa serão instalados todos os pacotes necessários para o funcionamento do serviço de e-mail utilizando o comando *apt-get install PACOTES*
- Pacotes: *apache2 apache2-mpm-prefork apache2.2-common libapache2-mod-php5 libapache2-mod-auth-mysql php5-cli php5-imap php5-gd php5-mcrypt php5-mysql php5-ldap php5-mhash php-pear postfix postfix-pcre awstats mysql-server-5.0 mysql-client-5.0 postfix-ldap slapd ldap-utils libnet-ldap-perl postfix-policyd dovecot-imapd dovecot-pop3d amavisd-new libcrypt-openssl-rsa-perl libmail-dkim-perl clamav-freshclam clamav-daemon spamassassin altermime libmail-spf-perl python-ldap libapache2-mod-wsgi python-mysqldb python-ldap*

python-jinja2 python-netifaces python-webpy python-ldap bzip2 acl patch cron tofrodo

- Após instalação dos pacotes os arquivos de configurações dos softwares envolvidos são todos atualizados e é criado um backup no formato NOMEDOARQUIVO.DATAMODIFICACAO. Exemplo: main.cf.2010.11.10.18.50.54 (arquivo original é o main.cf).
- Responder as seguintes questões:
 - Would you like to use firewall rules shipped within iRedMail now?
File: /etc/default/iptables, with SSHD port: 22222. [Y|n] **Y**
 - Restart firewall now (with SSHD port 22222)? [y|N] **Y**
 - Would you like to start postfix now? [y|N] **Y**
- Instalação foi finalizada! Diversas informações importantes são enviadas por e-mail para o login www@decom.ufop.br, primeira conta criada pelo sistema. Para acessá-la, utilizar o webmail instalado utilizando o link da tabela A.1 e usar a senha que foi definida no processo de instalação (figura A.21).

A.2.2 Configuração das aplicações para uso de LDAP externo

Para este projeto foi necessário o aproveitamento de uma base de dados já existente no departamento de computação e todo o processo de instalação é realizado considerando uma base LDAP local. Para resolver esse problema, algumas alterações serão realizadas.

1. Postfix

No Postfix, os seguintes arquivos deverão ser alterados na pasta /etc/postfix:

- ldap_catch_all_maps.cf
- ldap_recipient_bcc_maps_domain.cf
- ldap_recipient_bcc_maps_user.cf
- ldap_relay_domains.cf
- ldap_sender_bcc_maps_domain.cf
- ldap_sender_bcc_maps_user.cf
- ldap_sender_login_maps.cf
- ldap_transport_maps_domain.cf
- ldap_transport_maps_user.cf
- ldap_virtual_alias_maps.cf
- ldap_virtual_group_maps.cf

- `ldap_virtual_mailbox_domains.cf`
- `ldap_virtual_mailbox_maps.cf`

Todos eles possuem o parâmetro `server_host = 127.0.0.1` e deverão ser alterados para `server_host = IP_DO_SERVIDOR`. Neste caso ficaria da seguinte forma: `server_host = 200.131.216.15`. Após realizar tais alterações, restartar a aplicação com o comando `/etc/init.d/postfix restart`.

2. Dovecot

No Dovecot é necessário a alteração apenas do arquivo `dovecot-ldap.conf` na pasta `/etc/dovecot`. Mudar de `hosts = 127.0.0.1:389` para `hosts = 200.131.216.15:389`. Após alteração, reiniciar o serviço através do comando `/etc/init.d/dovecot restart`.

3. OpenLDAP

O arquivo `ldap.conf` que fica na pasta `/etc/ldap/` deverá ser modificado alterando a linha `ldap.conf:URI ldap://127.0.0.1:389` para `ldap.conf:URI ldap://200.131.216.15:389`. Após alteração, reiniciar o serviço através do comando `/etc/init.d/slapd restart`.

4. RoundCube

Entrar na pasta `/usr/share/apache2/roundcubemail/plugins/password` e editar o arquivo `config.inc.php`. Nele existe a seguinte linha e deverá ser alterada da seguinte forma:

- De - `$rcmail_config['password_ldap_host'] = "127.0.0.1";`
- Para - `$rcmail_config['password_ldap_host'] = "200.131.216.15";`

5. phpLDAPAdmin

Entrar na pasta `/usr/share/apache2/phpldapadmin/config` e editar o arquivo `config.php`. Nele existe a seguinte linha e deverá ser alterada da seguinte forma:

- De - `$servers->setValue('server','host','127.0.0.1');`
- Para - `$servers->setValue('server','host','200.131.216.15');`

Com essa alteração, a base a ser acessada não será mais a local e sim a base remota. Este passo pode ser desconsiderado caso o servidor que hospeda a base tenha o phpLDAPAdmin instalado ou venha a ser instalado. Essa ferramenta é bastante importante na administração dos dados armazenados.

A.2.3 Alteração do LDAP externo para uso do serviço de e-mail

Algumas alterações no OpenLDAP do servidor do DECOM são necessárias para que o serviço de e-mail funcione corretamente. Segue abaixo os procedimentos:

1. Inserção de novos schemas no LDAP

Para o LDAP externo reconhecer a estrutura de e-mail, é necessário a inclusão de novos schemas no OpenLDAP.

- Copiar os arquivos *iredmail.schema* e *amavis.schema* para a pasta de schemas do OpenLDAP. Os arquivos encontram-se na pasta `/etc/ldap/schema/`.
- Alterar o arquivo `slapd.conf` incluindo as linhas
`include /etc/ldap/schema/iredmail.schema`
`include /etc/ldap/schema/amavis.schema`
 Atente-se pois o caminho do arquivo pode ser outro dependendo para onde foram copiados.

2. Importar arquivo LDIF gerado pela instalação do iRedMail na base externa

Após a instalação do iRedMail, é gerado um arquivo no formato LDIF com a estrutura que foi criada por ele localmente. Este arquivo encontra-se no caminho `/root/iRedMail-0.6.1/./conf/ldap_init.ldif` e deverá ser copiado ao servidor da base externa. Após copiá-lo, executar o comando `slapadd -l ldap_init.ldif` para inserir os dados na base.

A.3 Informações para acesso às aplicações

A tabela A.1 mostra os softwares utilizados para a administração do servidor. O *RoundCube* é o webmail utilizado neste projeto para que o usuário possa utilizar o seu e-mail sem a necessidade de um MUA. O *phpMyAdmin* e o *phpLDAPAdmin* são respectivamente painéis de administração de base *MySQL* e base *LDAP*. Já o *iRedAdmin*, é um painel básico de administração das contas de e-mail do servidor.

Software	URL	Acesso HTTP	Acesso HTTPS
RoundCube	http://mail.decom.ufop.br/mail/ (ou /webmail , /roundcube)	SIM	SIM
phpMyAdmin	https://mail.decom.ufop.br/phpmyadmin/ (ou /mysql)	NÃO	SIM
phpLDAPAdmin	https://mail.decom.ufop.br/ldap/ (ou /phpldapadmin)	NÃO	SIM
iRedAdmin	https://mail.decom.ufop.br/iredadmin/	NÃO	SIM

Tabela A.1: Aplicações do servidor de e-mail do DECOM.

Apêndice B

Arquivos importantes gerados no projeto e modos de uso

B.1 add_group.ldif

Este arquivo LDIF foi desenvolvido para a criação de grupos de e-mail na base do LDAP. Para utilizá-lo, basta apenas alterar o atributo *mail* com o login desejado. Segue abaixo o conteúdo do arquivo:

```
dn: mail=grupo@decom.ufop.br,ou=Groups,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
accessPolicy: domain
accountStatus: active
cn: Nome do Grupo
enabledService: mail
enabledService: deliver
mail: grupo@decom.ufop.br
objectClass: mailList
```

Comando para inserção:

```
ldapadd -f add_group.ldif -x -D "cn=Manager,dc=decom,dc=ufop,dc=br" -W
```

B.2 add_group_user.ldif

Após criação do grupo desejado, utilizar o LDIF abaixo para inserir o grupo ao usuário. O atributo *mail* deverá ser alterado para o login que deverá fazer parte do tal grupo e o atributo *memberOfGroup* deverá ter o grupo a ser adicionado ao usuário.

```
dn: mail=tassar@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
add: memberOfGroup
memberOfGroup: grupo@decom.ufop.br
```

Comando para inserir o grupo ao usuário:

```
ldapmodify -f add_group_user.ldif -x -D "cn=Manager,dc=decom,dc=ufop,dc=br" -W
```

B.3 create_mail_user_OpenLDAP.sh

Este arquivo já existe na pasta `/root/iRedMail-0.6.1/tools` e apenas os parâmetros listados abaixo deverão ser alterados (parte destacada em **negrito**). Eles são respectivamente a pasta de armazenamento das mensagens, o domínio do LDAP, o usuário administrador do LDAP, a senha do administrador do LDAP e o tamanho da caixa de mensagem padrão.

```
# -----
# ----- Global Setting -----
# -----
# Storage base directory used to store users' mail.
# mailbox of LDAP user will be:
#   ${STORAGE_BASE_DIRECTORY}/${DOMAIN_NAME}/${USERNAME}/
# Such as:
#   /var/vmail/vmail01/domain.ltd/bibby/
#   -----|=====|-----|
#   STORAGE_BASE_DIRECTORY|DOMAIN_NAME|USERNAME
#
STORAGE_BASE_DIRECTORY="/var/vmail/vmail1"

# -----
# ----- LDAP Setting -----
# -----

LDAP_SUFFIX="dc=decom,dc=ufop,dc=br"

# ----- rootdn of LDAP Server -----
# Setting rootdn of LDAP.

BINDDN="cn=Manager,$LDAP_SUFFIX"

# Setting rootpw of LDAP.

BINDPW='SENHA'

# ----- Virtual Domains & Users -----
# Set default quota for LDAP users: 104857600 = 100M

QUOTA='1048576000'
```

B.4 create_mail_users.sh

Para geração desse script, primeiramente foi necessário a realização de uma exportação de dados da base existente do DECOM. Foi utilizada a ferramenta *phpLDAPadmin* como mostram as figuras B.1, B.2 e B.3:

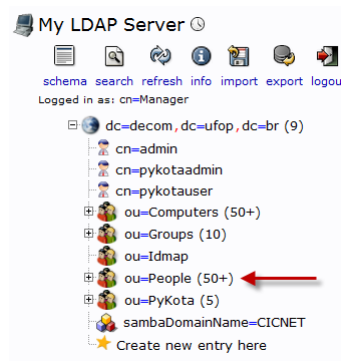


Figura B.1: Árvore LDAP do DECOM



Figura B.2: Tela após seleção do ou=People

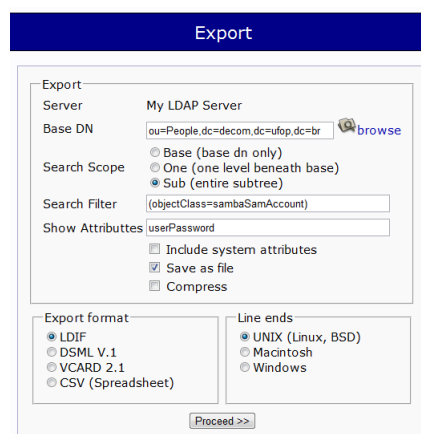


Figura B.3: Tela de exportação de dados do phpLDAPadmin

Com a base gerada, primeiramente foi utilizado o software *Terpad* para remover as quebras de linhas de cada DN gerado. Após foi realizado um filtro utilizando o comando:

```
grep -v "dn: uid=com" arquivo.ldif > arquivo_filtrado.ldif
```

Ele gera um novo LDIF removendo todos os usuários que iniciavam com *com*. Terminando esse processo, foi gerado o script para criar os e-mails de todos os logins válidos encontrados no LDAP do DECOM. O arquivo deverá ser copiado para a pasta */root/iRedMail-0.6.1/tools*.

```
sh create_mail_user_OpenLDAP.sh decom.ufop.br daniel
sh create_mail_user_OpenLDAP.sh decom.ufop.br danielgois
sh create_mail_user_OpenLDAP.sh decom.ufop.br danielmb
sh create_mail_user_OpenLDAP.sh decom.ufop.br elton
sh create_mail_user_OpenLDAP.sh decom.ufop.br ernesto
sh create_mail_user_OpenLDAP.sh decom.ufop.br fams
sh create_mail_user_OpenLDAP.sh decom.ufop.br felipesmmelo
sh create_mail_user_OpenLDAP.sh decom.ufop.br fernando.augusto
sh create_mail_user_OpenLDAP.sh decom.ufop.br fvaladares
sh create_mail_user_OpenLDAP.sh decom.ufop.br gabriel
sh create_mail_user_OpenLDAP.sh decom.ufop.br gabrielfc
sh create_mail_user_OpenLDAP.sh decom.ufop.br gilbertocm
sh create_mail_user_OpenLDAP.sh decom.ufop.br gleisson
sh create_mail_user_OpenLDAP.sh decom.ufop.br guillermo
sh create_mail_user_OpenLDAP.sh decom.ufop.br gustavo
sh create_mail_user_OpenLDAP.sh decom.ufop.br haroldo
sh create_mail_user_OpenLDAP.sh decom.ufop.br hbarbosa
sh create_mail_user_OpenLDAP.sh decom.ufop.br henrique
sh create_mail_user_OpenLDAP.sh decom.ufop.br jaderlamoia
sh create_mail_user_OpenLDAP.sh decom.ufop.br jmneves
sh create_mail_user_OpenLDAP.sh decom.ufop.br joao
sh create_mail_user_OpenLDAP.sh decom.ufop.br joaolanna
sh create_mail_user_OpenLDAP.sh decom.ufop.br joaotacio
sh create_mail_user_OpenLDAP.sh decom.ufop.br joseam
sh create_mail_user_OpenLDAP.sh decom.ufop.br joubert
sh create_mail_user_OpenLDAP.sh decom.ufop.br juliana
sh create_mail_user_OpenLDAP.sh decom.ufop.br jvdg
sh create_mail_user_OpenLDAP.sh decom.ufop.br kurumin
sh create_mail_user_OpenLDAP.sh decom.ufop.br leovale
sh create_mail_user_OpenLDAP.sh decom.ufop.br lgc
sh create_mail_user_OpenLDAP.sh decom.ufop.br loschi
```

```
sh create_mail_user_OpenLDAP.sh decom.ufop.br lucasfvr
sh create_mail_user_OpenLDAP.sh decom.ufop.br lucilia
sh create_mail_user_OpenLDAP.sh decom.ufop.br luiz
sh create_mail_user_OpenLDAP.sh decom.ufop.br marco
sh create_mail_user_OpenLDAP.sh decom.ufop.br marinalva
sh create_mail_user_OpenLDAP.sh decom.ufop.br matheus
sh create_mail_user_OpenLDAP.sh decom.ufop.br menotti
sh create_mail_user_OpenLDAP.sh decom.ufop.br messias
sh create_mail_user_OpenLDAP.sh decom.ufop.br napauria
sh create_mail_user_OpenLDAP.sh decom.ufop.br pedrohnc
sh create_mail_user_OpenLDAP.sh decom.ufop.br pietrobon
sh create_mail_user_OpenLDAP.sh decom.ufop.br red
sh create_mail_user_OpenLDAP.sh decom.ufop.br rensso
sh create_mail_user_OpenLDAP.sh decom.ufop.br ricardo
sh create_mail_user_OpenLDAP.sh decom.ufop.br romildo
sh create_mail_user_OpenLDAP.sh decom.ufop.br rreisp
sh create_mail_user_OpenLDAP.sh decom.ufop.br samuevan
sh create_mail_user_OpenLDAP.sh decom.ufop.br sdelabrida
sh create_mail_user_OpenLDAP.sh decom.ufop.br sgrasiella
sh create_mail_user_OpenLDAP.sh decom.ufop.br tarik
sh create_mail_user_OpenLDAP.sh decom.ufop.br thais
sh create_mail_user_OpenLDAP.sh decom.ufop.br thiagomac
sh create_mail_user_OpenLDAP.sh decom.ufop.br tiago
sh create_mail_user_OpenLDAP.sh decom.ufop.br toffolo
sh create_mail_user_OpenLDAP.sh decom.ufop.br wilquenio
```

B.5 modify_mail_password_users_all.ldif

Utilizando os dados do LDIF gerado na seção B.4, o LDIF desta seção foi criado para sincronizar as senhas já existentes do LDAP do DECOM aos usuários criados. Para criá-lo, foi realizada a seguinte alteração para todos os usuários:

DE:

```
dn: uid=USUARIO,ou=People,dc=decom,dc=ufop,dc=br
userPassword: {SSHA}0tt25fTd23f5bRkq3HPozZeNQxV6ei9X
```

PARA:

```
dn: mail=USUARIO@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}0tt25fTd23f5bRkq3HPozZeNQxV6ei9X
```

Segue abaixo o conteúdo do LDIF gerado:

```
dn: mail=daniel@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}0tt25fTdoqf5bRkq3HPozZeNQxV6ei9X

dn: mail=danielgois@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}23MCNGcTPgjhD250X0jqejw1+fzEn/4W

dn: mail=danielmb@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}LDxnglfyeSSWLKjqLFjd37lywihWYi9F

dn: mail=elton@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}kwxF1Xdb9ed1M2hLQ7SRS1DVKSouaVpH

dn: mail=ernesto@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}0z51UwoCic76uhxfjDca2880wXLNFFnn

dn: mail=fams@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}5Qk/tNKco2xG8R6D1F1gij1MzTF4R1A3

dn: mail=felipesmmelo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}1MrLlQyZAtDdF6+MG5JGV1k6//dvdVNC

dn: mail=fernando.augusto@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}5Yeqg4nTJbYjjSABDkAQFWGOS01xd2dn

dn: mail=fvaladares@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}QqFeo18K136eB02yph6BCYxShdNR4JSa

dn: mail=gabriel@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
```

```
changetype: modify
replace: userPassword
userPassword: {SSHA}ivm7MBExRgvFksTx1Mg4pvg2JkH+mTec

dn: mail=gabrielfc@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}M2TDKmmBtSoCNzkDEo0lyAeev52YAnbx

dn: mail=gilbertocm@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}1yX8y58IFXAGfZ9s5YNi0SWneA6ci0Zf

dn: mail=gleisson@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}RGiW2oJZx4sncNYyn8FYco+WJQVSSzRu

dn: mail=guillermo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}fYL2IQHjYrq0fVwJBRB5E+Kw8xq0z1Q1

dn: mail=gustavo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}p1Y1hif3C0spmnFatB36B2Vfo6pRVmAB

dn: mail=haroldo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}BVxzgIC52RpQ0ExyrW2+NRCfD94PE1k0

dn: mail=hbarbosa@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}eRJ7EKwwA5XL0IWHGH10X5UcFaGFKRw3

dn: mail=henrique@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}N0bHdwmVnUk/BCsqe0Nh4jVLrdxXQWtx

dn: mail=jaderlamoia@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
```

userPassword: {SSHA}T8wBI9vtQsZi3m66aL3axI++tbCdyT8v

dn: mail=jmneves@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}j3pAgWnQi/sFHNTWgCp6J8qI1AdvNMsz

dn: mail=joao@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}2ElcsQbNZgngJoZgdC/9b4hr+ThQenU5

dn: mail=joaolanna@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}KBh+jjH7R15baXiwtswF5Sqs6DJoRldV

dn: mail=joaotacio@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}Zq/bPwT507IyS+1bV5FM/pVz7U9EdXM2

dn: mail=joseam@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}Ykc6unU6UXMwLzvH1V0X4F8wfgxFympE

dn: mail=Joubert@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}cfHoV3V0wVLTbqhQV4p1ba5kZDZZNBqF

dn: mail=juliana@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}Yz5W8PnqCnaOmgoDdmIFVZqVRXF4eDVG

dn: mail=jvdg@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}wdnZJ1zipSd0j1JIv6dJ7U61xoJn+ne7

dn: mail=kurumin@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}LEXIScWQPHBH4mbCjgANsjFfED41bEtr

dn: mail=leovale@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}KZaor8RA6riBK1Qt9Qoh8LJTnZeXzG3E

dn: mail=lgc@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}8JKc1PDzY32ibIapz97wYgsf7MOQEPmr

dn: mail=loschi@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}BoqwKp2/yev8TCtsqN42zdxfbZ2Uusj9

dn: mail=lucasfvr@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}MLC3kgAtbRd4uerWBD5B0HsZXHwMdPU/

dn: mail=lucilia@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}rjdKJYgCxS04/r1U178y4KUm0TVur/kX

dn: mail=luiz@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}bdVGe4g6kBY4f2Sed8jz/KxUNQ+NBxVf

dn: mail=marco@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}p/tttholi4IB++a4JwpvcG7UGor/2plw

dn: mail=marinalva@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}2q6izSI0YufMrou/81R5uYysHpCjtpEa

dn: mail=matheus@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}CFInSH0qs0qcUsepk6Se3B8Mhu070g1j

dn: mail=menotti@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify

```
replace: userPassword
userPassword: {SSHA}djezn9Bwg9dwwEc+lsQR4dygW1E3oE1T

dn: mail=messias@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}h3LrRfTPFezUSbPek19342R37bcEfifu

dn: mail=napauria@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}N3C4jxmX0Ypuc7zwbNFd9PZpI55lbnRq

dn: mail=pedrohnc@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}0IzyCAyAlSiiq87rfhUjTkrICwQV6+uD

dn: mail=pietrobon@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}mN1lYZXBGTIYRlTkW7NAx/a1oiKNeVJa

dn: mail=red@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}h/eK1hiuCtu8eli8BNsD7ByPdW15bFgi

dn: mail=renso@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}SbErEh6gCV02YBYTyTTebSDxXwTpN4iL

dn: mail=ricardo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}u0yZFYkjeUPcOPxdiJKSHNDP3Pm6vuow

dn: mail=romildo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}1LltSsyDlBmsKlcuInu8EE3eTWAuWUZh

dn: mail=rreisp@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}VZxj4gVYPwdVJa70LGEwFbdfmwL+H3u0
```

```
dn: mail=samuevan@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}V1ZfquHqSqsdiB+RcNrXKhyPPitoMvVm
```

```
dn: mail=sdelabrida@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}rhoCn7n7drsQe/0zj9KSd2Q+d1tHT2Mu
```

```
dn: mail=sgrasiella@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}9sBJ5ZjvgID61sFa+Zdhv5DJrURQbzB0
```

```
dn: mail=tarik@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}wYm52LdVTgyv/SqL0wStLd/y7s5zgZpd
```

```
dn: mail=thais@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}CFS17bhNN46fqMCxIiz7MwmjCgUKtSj/
```

```
dn: mail=thiagomac@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}liJoYF7JXMiOXAsXvORSQxxW8l3wbcTV
```

```
dn: mail=tiago@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}z6fJT0JP4tATJqRF+qASQX0io4tuT3hl
```

```
dn: mail=toffolo@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}AkcpWUH2rUfUouYRODhxJJbQADw96sha
```

```
dn: mail=wilquenio@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
changetype: modify
replace: userPassword
userPassword: {SSHA}pJU/ufHY5/jY6lsxEEDv9IGIdW1qRDZa
```

Comando para alterar a senha dos usuários:

```
ldapmodify -f modify_mail_password_users_all.ldif -x -D "cn=Manager,dc=decom,dc=ufop,dc=br" -W
```

Apêndice C

Administração e utilização do serviço de e-mail

C.1 Criação de contas de e-mail

Para criar uma conta de e-mail, primeiramente deverá ser realizado o procedimento descrito na seção B.3. Uma conta de e-mail pode ser criada basicamente das seguintes formas:

- Através do script `create_mail_user_OpenLDAP.sh`
- Através do painel iRedAdmin

Sugiro que as contas de e-mail sejam criadas através do primeiro item pois o script já estará formatado da forma desejada e pode ser utilizado para criação de e-mails em massa facilmente.

C.1.1 Utilizando o `create_mail_user_OpenLDAP.sh`

Para criar um e-mail utilizando esse script, basta seguir os seguintes passos:

- `cd /root/iRedMail-0.6.1/tools`
- `sh create_mail_user_OpenLDAP.sh DOMÍNIO USUARIO`

O mesmo comando pode ser utilizando para criação de vários usuários:

- `sh create_mail_user_OpenLDAP.sh DOMÍNIO USUARIO1 USUARIO2 USUARIO3 ...`

Exemplo de uso:

- `sh create_mail_user_OpenLDAP.sh decom.ufop.br joao`

C.1.2 Utilizando o painel iRedAdmin

O painel iRedAdmin deverá ser acessado através do endereço informado na tabela A.1. A figura C.1 mostra a tela inicial e deverá ser utilizado o usuário e senha criado no processo de instalação.

- Login: postmaster@decom.ufop.br
- Senha: SENHA CRIADA

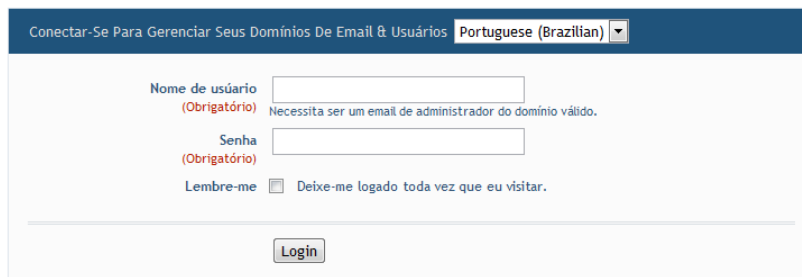
A imagem mostra a tela de login do iRedAdmin. No topo, há uma barra azul com o texto "Conectar-Se Para Gerenciar Seus Domínios De Email & Usuários" e um menu suspenso para a linguagem "Portuguese (Brazilian)". Abaixo, há campos para "Nome de usuário" e "Senha", ambos rotulados como obrigatórios. Uma mensagem de erro indica que o e-mail de administrador precisa ser válido. Há também uma opção "Lembre-me" com uma caixa de seleção e o texto "Deixe-me logado toda vez que eu visitar.". Um botão "Login" está na base.

Figura C.1: Tela inicial do painel iRedAdmin

Após autenticar no painel, será apresentada uma tela com algumas opções como mostra a figura C.2. A opção *Usuários* deverá ser selecionada.

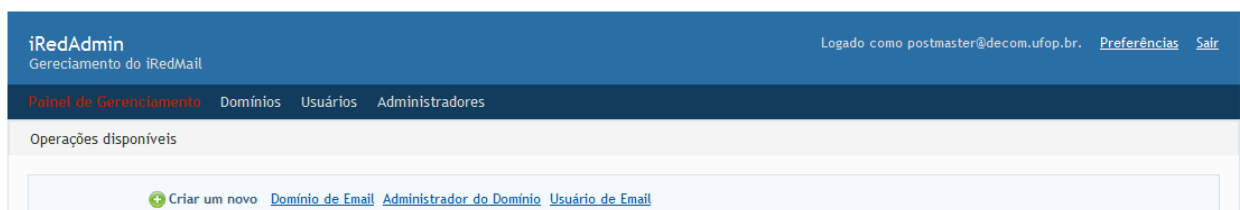
A imagem mostra a interface principal do iRedAdmin após o login. No topo, uma barra azul contém o logo "iRedAdmin", o subtítulo "Gerenciamento do iRedMail", o status "Logado como postmaster@decom.ufop.br.", e links para "Preferências" e "Sair". Abaixo, há uma barra de navegação com "Painel de Gerenciamento" em destaque, seguido por "Domínios", "Usuários" e "Administradores". A seção principal, intitulada "Operações disponíveis", contém um botão verde com um símbolo de mais e o texto "Criar um novo", seguido por links para "Domínio de Email", "Administrador do Domínio" e "Usuário de Email".

Figura C.2: Opções do painel iRedAdmin

Após entrar na opção *Usuários*, clicar em *Criar um novo usuários de Email*. A figura C.3 mostra o resultado.

The screenshot shows the iRedAdmin web interface. At the top, there's a blue header with 'iRedAdmin' and 'Gereciamento do iRedMail'. On the right, it says 'Logado como postmaster@decom.ufop.br.' with links for 'Preferências' and 'Sair'. Below the header is a navigation bar with 'Painel de Gerenciamento', 'Domínios', 'Usuários', and 'Administradores'. The main content area is titled 'Criar um novo usuário de Email'. It features a yellow warning box stating 'Nova senha necessita conter no mínimo 6 caracteres.' Below this, there are several form fields: 'Endereço de Email (Obrigatório)' with a text input and a dropdown menu showing 'decom.ufop.br'; 'Nome do usuário' with a text input; 'Cota de Email (em MB)' with a text input showing '1024'; 'Nova senha (Obrigatório)' with a text input; and 'Confirmar nova senha (Obrigatório)' with a text input and a note 'Re-digite sua senha exatamente como anteriormente'. At the bottom, there is a 'Criar' button.

Figura C.3: Tela de criação de e-mail do painel iRedAdmin

C.2 Criação de listas de e-mail

O processo de criação de lista de e-mails, foi basicamente descrito no Apêndice B. Será necessário a criação de um arquivo LDIF no seguinte formato:

```
dn: mail=LISTA@decom.ufop.br,ou=Groups,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
accessPolicy: domain
accountStatus: active
cn: NOME DA LISTA DE E-MAILS
enabledService: mail
enabledService: deliver
mail: LISTA@decom.ufop.br
objectClass: mailList
```

Após criar o arquivo, deverá ser executado o seguinte comando para inserção:

```
ldapadd -f NOMEARQUIVO.ldif -x -D "cn=Manager,dc=decom,dc=ufop,dc=br" -W
```

Este comando está considerando que o administrador do LDAP é o *cn=Manager,dc=decom,dc=ufop,dc=br* mas pode ser outro caso tenha sido criado com outro nome.

Após a criação da lista, os usuários deverão ser associados a ela através do LDIF no seguinte formato:

```
dn: mail=USUARIO@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
add: memberOfGroup
memberOfGroup: LISTA@decom.ufop.br
```

Para efetuar a inserção da lista ao usuário, o seguinte comando deverá ser utilizado:

```
ldapmodify -f NOPEARQUIVO.ldif -x -D "cn=Manager,dc=decom,dc=ufop,dc=br" -W
```

O arquivo LDIF não necessariamente precisa ter apenas um usuário. Podem ser inseridos vários em um mesmo arquivo.

```
dn: mail=USUARIO1@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
add: memberOfGroup
memberOfGroup: LISTA@decom.ufop.br
```

```
dn: mail=USUARIO2@decom.ufop.br,ou=Users,domainName=decom.ufop.br,o=domains,dc=decom,dc=ufop,dc=br
add: memberOfGroup
memberOfGroup: LISTA@decom.ufop.br
```

C.3 Utilização do serviço de e-mail

O serviço de e-mail pode ser utilizado pelo usuário de duas formas. Pode ser através de um cliente como por exemplo *Microsoft Outlook* ou através do webmail disponibilizado neste projeto (*RoundCube*).

C.3.1 Através de um cliente de e-mail

Para utilizar o seu e-mail através de um cliente de e-mail, deverão ser utilizadas as seguintes informações:

- Servidor de entrada de e-mails: *mail.decom.ufop.br*
- Servidor de saída de e-mails (SMTP): *mail.decom.ufop.br*
- Usuário: *USUARIO@decom.ufop.br*
- Senha: *SENHA DO USUARIO*
- Marcar a opção que o servidor SMTP requer autenticação

Essa configuração pode ser utilizada tanto para POP quanto para IMAP. Atentar-se a marcação da opção que o SMTP requer autenticação pois senão não será possível o envio de mensagens. O servidor está configurado para não aceitar envios sem autenticação.

C.3.2 Através do webmail

O webmail utilizado neste projeto é o *RoundCube* e pode ser acessado através do link informado na tabela A.1. A figura C.4 mostra a tela de login e deverá ser usada da seguinte forma:

- Usuário: *USUARIO@decom.ufop.br*
- Senha: *SENHA DO USUARIO*

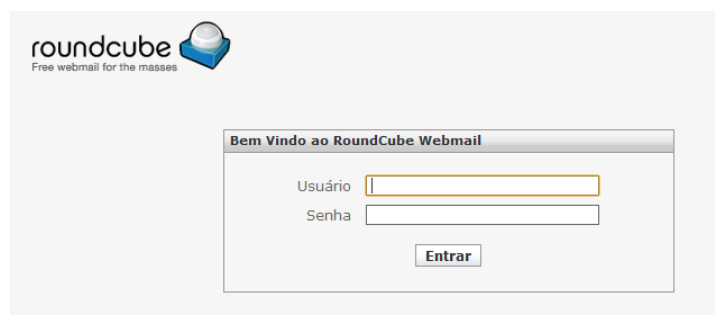


Figura C.4: Tela de login do RoundCube

Neste caso, o domínio padrão configurado é o *decom.ufop.br*. Se digitar apenas *USUARIO* também irá funcionar. A figura C.5 mostra a tela principal do *RoundCube* após autenticar com o usuário *teste*.

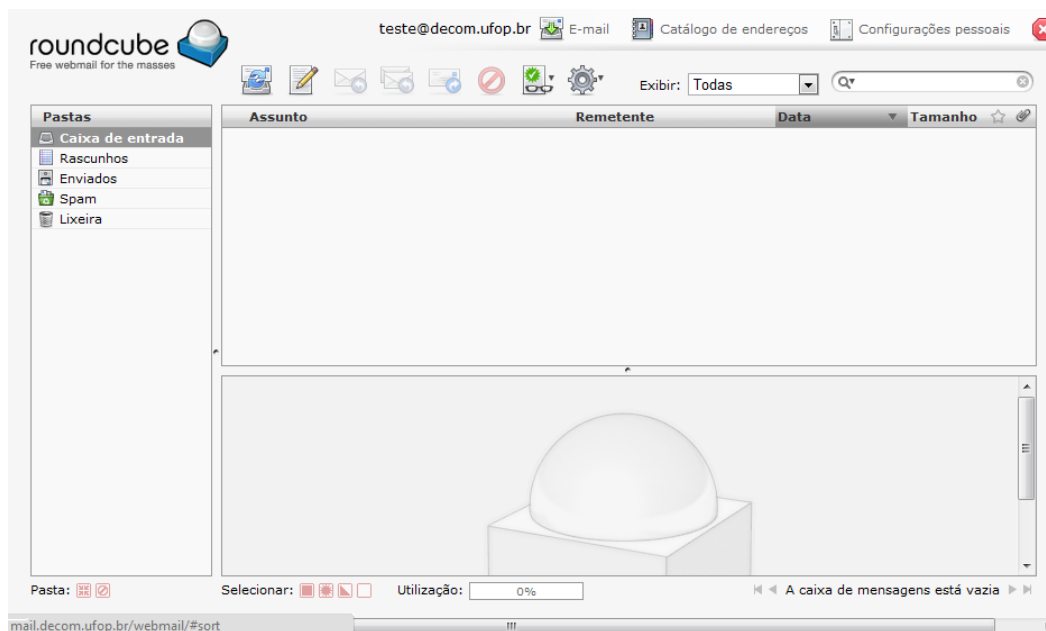


Figura C.5: Tela principal do RoundCube

O *RoundCube* possui uma interface bastante amigável e por esse motivo não detalharei como realizar operações básicas como por exemplo o envio de uma mensagem. Apenas movendo o cursor por cima dos ícones já é mostrada a sua função.

C.4 Atualização do antivírus e antispam

C.4.1 ClamAV Antivírus

A atualização do antivírus *ClamAV* é realizada através do *freshclam*. Ele é um *daemon*, ou seja, roda em *background* e realiza verificações de tempo em tempo de acordo com a configuração do arquivo */etc/clamav/freshclam.conf*. A configuração padrão é 24 verificações por dia e esta pode ser alterada substituindo o valor do parâmetro *Checks* para outro valor.

C.4.2 SpamAssassin Antispam

O antispam *SpamAssassin* é atualizado através de um agendamento diário no Linux. Existe um *Job* na pasta */etc/cron.daily* que realiza a atualização utilizando o comando *sa-update*. Para visualizar o *Job*, edite o arquivo */etc/cron.daily/spamassassin*.

C.5 Desativar o *Greylisting* do Policyd

Greylisting é um método de defesa contra spam. Um MTA quando está utilizando *greylisting* rejeitará temporariamente qualquer e-mail de um remetente não reconhecido. Se o e-mail é legítimo, o servidor de origem após um atraso tentará novamente o envio da mensagem. Em um spam são enviados milhares de e-mails e provavelmente a mensagem não será enviada novamente.

Neste servidor optei por deixar desabilitado devido ao tempo que às vezes a mensagem demora para ser recebida. Para desabilitar esse serviço, os seguintes passos deverão ser realizados:

- `vim /etc/postfix-policyd.conf`
- Alterar o parâmetro `GREYLISTING=1` para `GREYLISTING=0`
- `/etc/init.d/postfix-policyd restart`

C.6 Firewall do sistema

O *firewall* do sistema inicialmente foi implementado utilizando as regras descritas no Apêndice A na seção A.1. Após a instalação do *iRedMail*, um novo *firewall* foi aplicado no

sistema com poucas diferenças. Segue abaixo o conteúdo do arquivo */etc/default/iptables* comentado:

```
# Bloqueia pacotes de entrada e redirecionamento por padrão.
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

# Keep state.
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Libera portas - http/https, smtp/smtps, pop3/pop3s, imap/imap, ssh
-A INPUT -p tcp -m multiport --dport 80,443,25,465,110,995,143,993,587,465,22222 -j ACCEPT

# Liberando Loop device.
-A INPUT -i lo -j ACCEPT

# Liberando PING de hosts remotos.
-A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

Se for necessário qualquer alteração no *firewall*, inclua as linhas desejadas e execute o seguinte comando para aplicar as regras:

- */etc/init.d/iptables restart*