Defesa de “Projeto Final” (U.C. 21095)

“Sistema de Servidor Pessoal de E-mail”

Ricardo Ferreira da Conceição Dias Marques
(Estudante n.º 1100281)
1100281@estudante.uab.pt / uab@ricmarques.net

Universidade Aberta
Departamento de Ciências e Tecnologia (DCeT)
Licenciatura em Informática
dezembro de 2016

UNIVERSIDADE AbERTA
www.uab.pt

Agenda

- Objetivo Principal do Projeto
- Funcionalidades pretendidas
- Tarefas realizadas
- Componentes de *software* da solução
- "*Zone file*" do domínio "uabdemo.info"
- Modelo de Dados dos domínios, mailboxes e aliases
- Modelo de Dados da Funcionalidade Adicional
- Implementação da Funcionalidade Adicional
- Algumas *screenshots* relevantes
- Objetivos atingidos
- Oportunidades futuras de melhoria
- Siglas usadas nesta apresentação
- Modelo (*template*) usado nesta apresentação
- Referências Bibliográficas

Objetivo Principal do Projeto

- Montar, num computador (**servidor**) com Sistema Operativo **Linux**, um sistema de **e-mail** bastante funcional, para o uso pessoal de um utilizador que queira administrar o seu próprio servidor de e-mail.

Funcionalidades pretendidas

- Envio de e-mail por **SMTP** com **cifra** do canal de **transporte**.
- Receção de e-mail via **IMAPS**, protocolo que **cifra** o canal de **transporte**.
- Suporte a **múltiplos domínios** de e-mail.
- Suporte a **múltiplas *mailboxes* e *aliases*** (permitindo **reencaminhamento** de mensagens para domínios internos ou externos), com **informação das *mailboxes* e *aliases*** registada **em Base de Dados.**
- Interface web (***Webmail***) com certificado digital ativo para que as comunicações sejam feitas por **HTTPS** (*Hyper Text Transfer Protocol Secure*) para **identificação do servidor** e **cifra do canal de transporte**.
- **Funcionalidade proposta pelo Professor Orientador**: *reporting* automático no sistema de email que permita monitorizar entregas de documentos em resposta a um e-mail enviado a um grupo de pessoas. O sistema deveria permita criar um **relatório** em qualquer momento, que indique o **número e percentagem de respostas** recebidas, **com e sem ficheiros anexos.** Esse relatório deveria também **indicar quem do grupo de destinatários ainda não respondeu** ao pedido (e eventualmente permitir a criação de um email de reforço apenas para esses).

Tarefas realizadas

- Escolhida a *Digital Ocean como* fornecedor de VPS para usar, como servidor da solução, uma máquina virtual alojada remotamente.
- A *Digital Ocean* usa o termo "*Droplets"* para designar as máquinas virtuais que aloja. Foi escolhido o tamanho mais pequeno e barato para a *Droplet*: 1 processador virtual, 512 MB RAM, 20 GB Disco (SSD) .
- Escolhido a "imagem" base com Sistema Operativo Linux (CentOS 6.8).
- Registado o domínio "**uabdemo.info**", usando o *registrar* "GoDaddy.com" e criados os registos necessários de DNS
- Executadas algumas operações de *hardening* de segurança (como seja configurações de *firewall* por *software* via "iptables")
- Gerado par de chaves pública e privada RSA, criado um CSR e instalado o certificado (assinado pela CA da StartSSL) no Apache e Dovecot
- Instalados e configurados os componentes de *software* necessários, na VM
- Criadas as Bases de Dados "**dbvmail**" (associadas aos domínios de e-mail, *mailboxes* e *aliases*), "**dbmailings**" (associada à Funcionalidade Adicional proposta pelo Professor Orientador) e do Roundcube ("**roundcubemail**") e as contas associadas de utilizador.
- Desenvolvido código Perl e PHP para implementar a Funcionalidade Adicional.

Componentes de *software* da solução

- Máquina virtual alojada na ***DigitalOcean*** *(*empresa fornecedora de serviços VPS / IaaS) com “imagem” de Sistema Operativo Linux (**CentOS 6.8**)
- *Software* servidor de Envio de E-mail (MTA): **Postfix** (versão 2.6.6)
- *Software* servidor de Receção de E-mail: **Dovecot** (versão 2.0.9)
- *Software* de Webmail: **Roundcube** (versão 1.0.9)
- *Software* servidor HTTP para suporte ao Webmail: **Apache** (versão 2.2.15)
- Linguagem de *scripting* Web para suporte ao Webmail e ao requisito adicional proposto pelo Professor Orientador: **PHP** (versão 5.3.3)
- Software servidor de Base de Dados (para suporte à Base de Dados de mailboxes/aliases, ao Webmail e à funcionalidade adicional): **MySQL** (versão 5.1.73)
- Linguagem de *scripting* para a funcionalidade adicional: **Perl** (versão 5.10.1)

“Zone file” do domínio “uabdemo.info”

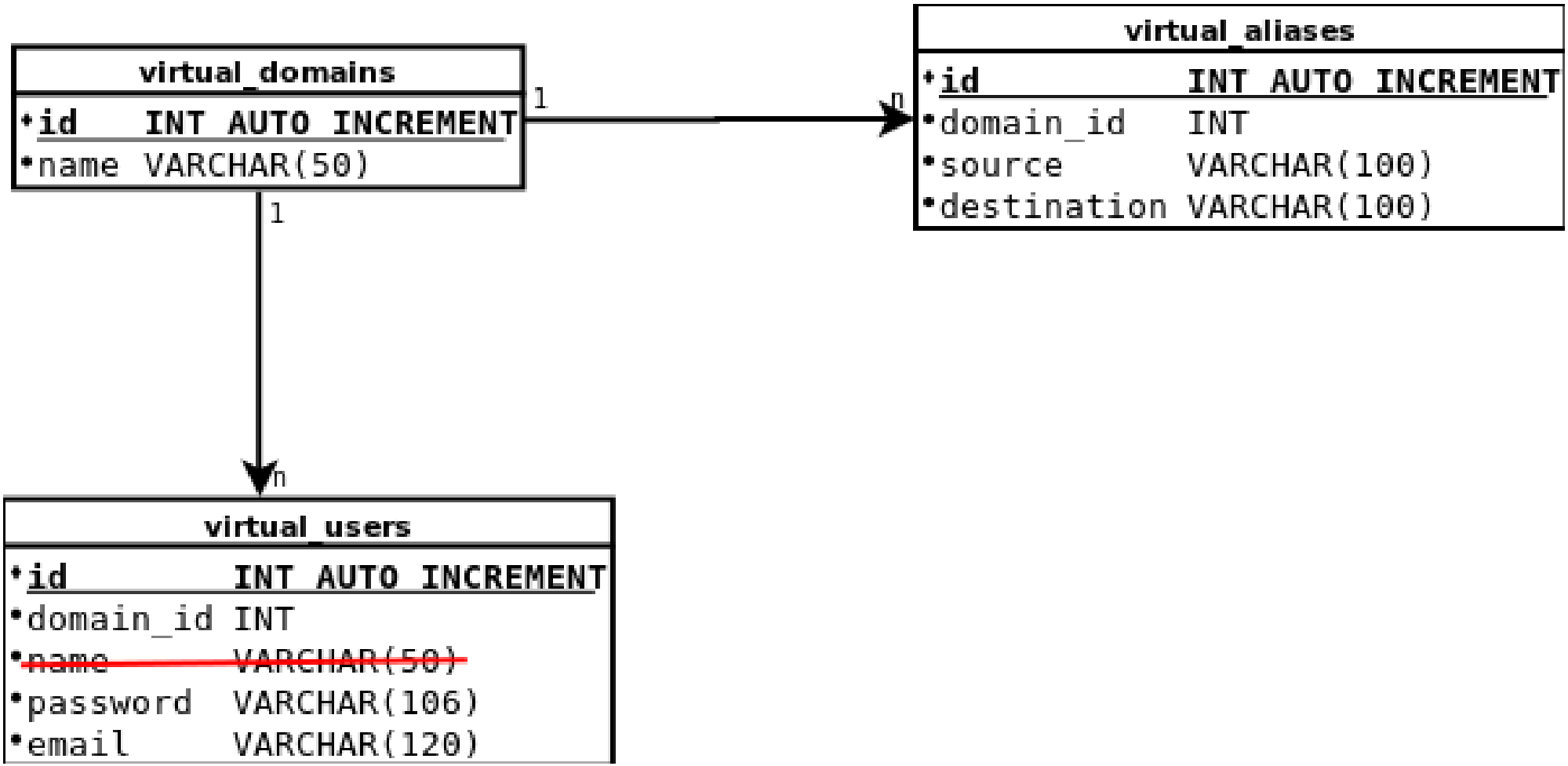
$ORIGIN uabdemo.info.
$TTL 1800
uabdemo.info. IN **SOA** ns1.digitalocean.com. hostmaster.uabdemo.info. 1477782678 10800 3600 604800 1800
uabdemo.info. 1800 IN **NS** ns1.digitalocean.com.
uabdemo.info. 1800 IN **NS** ns2.digitalocean.com.
uabdemo.info. 1800 IN **NS** ns3.digitalocean.com.
uabdemo.info. 1800 IN **A** 138.68.131.28
machine2.uabdemo.info. 1800 IN **A** 138.68.131.28
www.uabdemo.info. 1800 IN **A** 138.68.131.28
mail.uabdemo.info. 1800 IN **A** 138.68.131.28
uabdemo.info. 1800 IN **MX** 10 mail.uabdemo.info.
webmail.uabdemo.info. 1800 IN **A** 138.68.131.28
uabdemo.info. 1800 IN **TXT** v=spf1 mx -all

(“*Zone File*” copiado do final da configuração realizada através da *interface Web* da *Digital Ocean* para criação de registos DNS disponível em: https://cloud.digitalocean.com/domains/uabdemo.info)

Instalação / Configuração do Postfix

- A versão do Postfix que vem com o repositório do CentOS não inclui suporte para MySQL. Por isso, foi desinstalada a versão que vinha instalada de base e foi instalada a versão que está disponível no repositório **CentOSPlus** que, essa sim, inclui suporte para MySQL.
- Para a instalação e configuração do Postfix, foram usados, como base / referência, os seguintes tutoriais:
- https://www.digitalocean.com/community/tutorials/how-to-configure-a-mail-server-using-postfix-dovecot-mysql-and-spamassassin
- https://www.linode.com/docs/email/postfix/email-with-postfix-dovecot-and-mysql

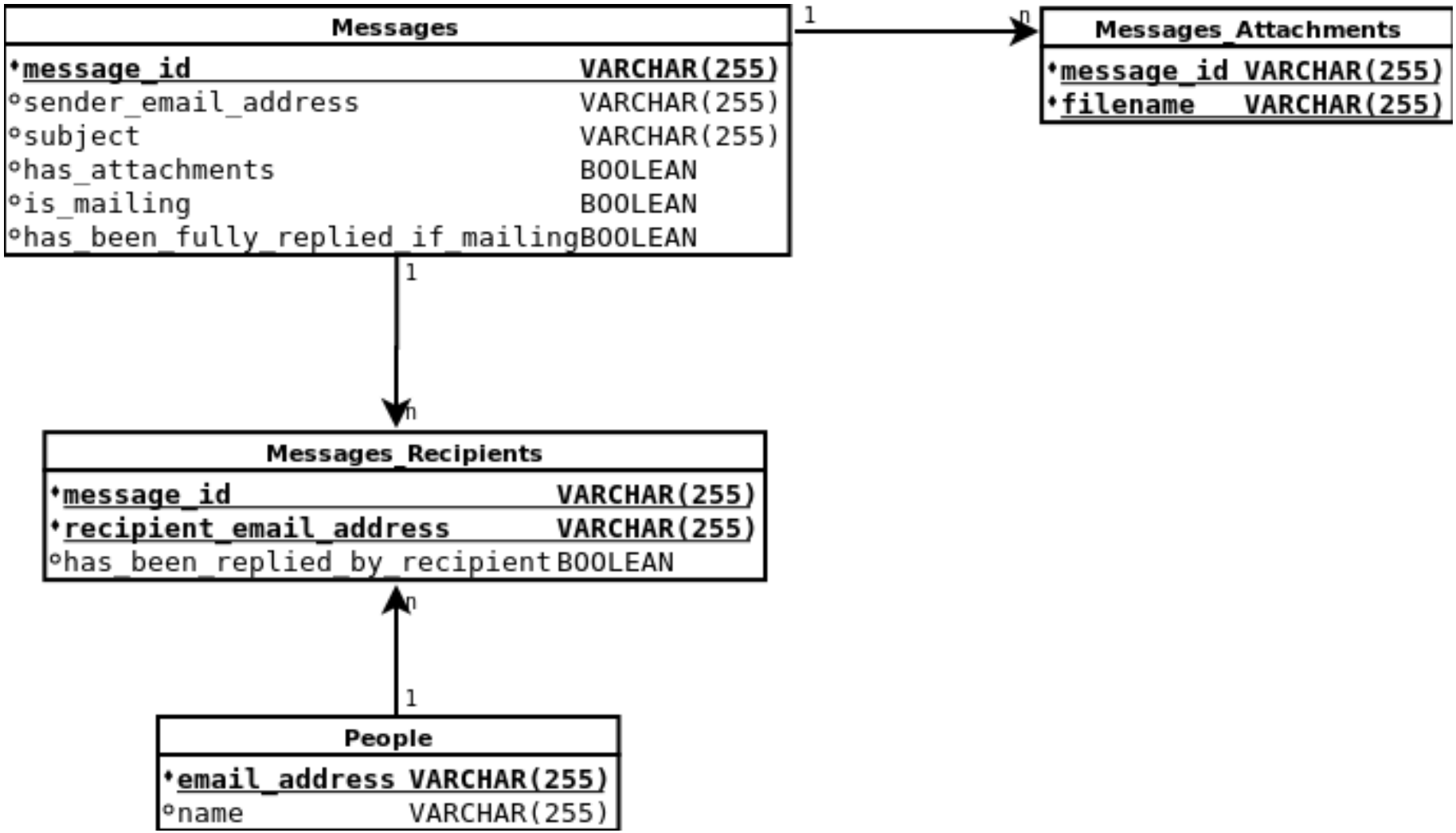
Modelo de Dados dos domínios, *mailboxes* e *aliases*



Base de Dados "**dbvmail**"

Schema criado a partir das instruções DDL disponíveis em:
https://www.digitalocean.com/community/tutorials/how-to-configure-a-mail-server-using-postfix-dovecot-mysql-and-spamassassin

Modelo de Dados da Funcionalidade Adicional



Base de Dados “**dbmailings**”

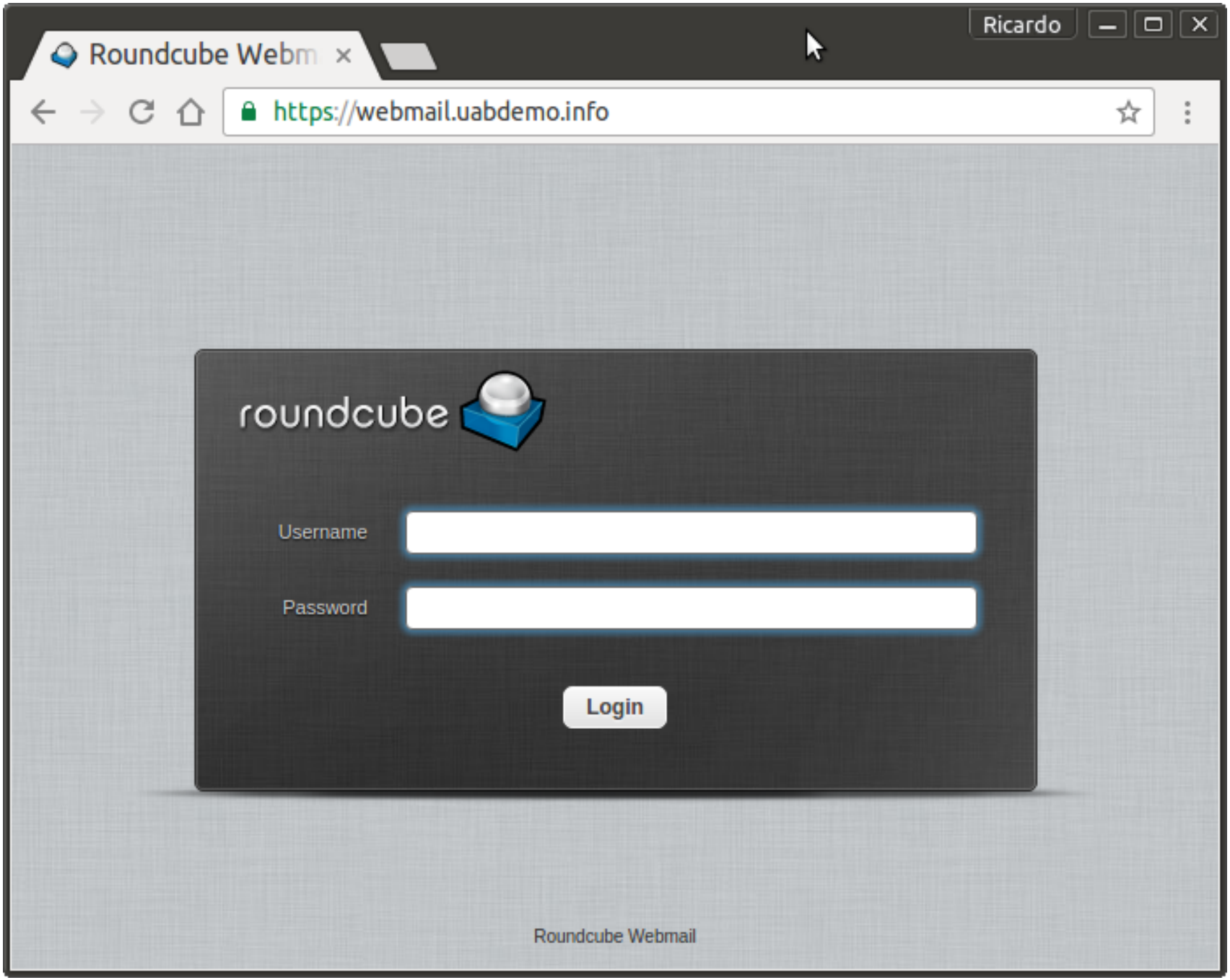
Implementação da Funcionalidade Adicional

- Um dos campos que tem particular importância numa mensagem de e-mail é o "**Message-ID**" (que é apresentado como "message_id" no Modelo de Dados desenhado). Conforme indicado no RFC 5322, em particular na secção "*3.6.4. Identification fields*", esse campo de "Message-ID", embora opcional, é (fortemente) recomendado e, caso exista, terá de ser único.
- Criado um programa/script em **Perl** que executa o processamento/parsing das mensagens presentes na **pasta "INBOX" de uma *mailbox* de *mailings*** (associada ao endereço mailings@uabdemo.info) e que **guarda, numa base de dados MySQL** ("dbmailings"), a meta-informação processada.
- A opção pela linguagem Perl deveu-se à:
  - Experiência prévia com a linguagem ;
  - Existência de vários módulos, no chamado CPAN, para o acesso programático a *mailboxes* através do protocolo IMAP (módulo **Mail::IMAPClient**) ; de extração de endereços de e-mail (**Email::Address**) ; de "descodificação" de cabeçalhos de mensagens (**MIME::EncWords**), etc...
- Para mostrar a meta-informação processada ao utilizador, foi criada um programa/**página web** na linguagem de programação **PHP**, que **lê** a informação da **base de dados MySQL** e a **mostra ao utilizador**.
- A página de Relatório dos Mailings pode ser consultada no URL https://www.uabdemo.info/mailings.php

Código Perl e PHP

- Observação dos ficheiros que foram desenvolvidos com código:
  - **Perl**: “**messages_metadata_parser_to_db.pl**”
  - **PHP**: “**mailings.php**”

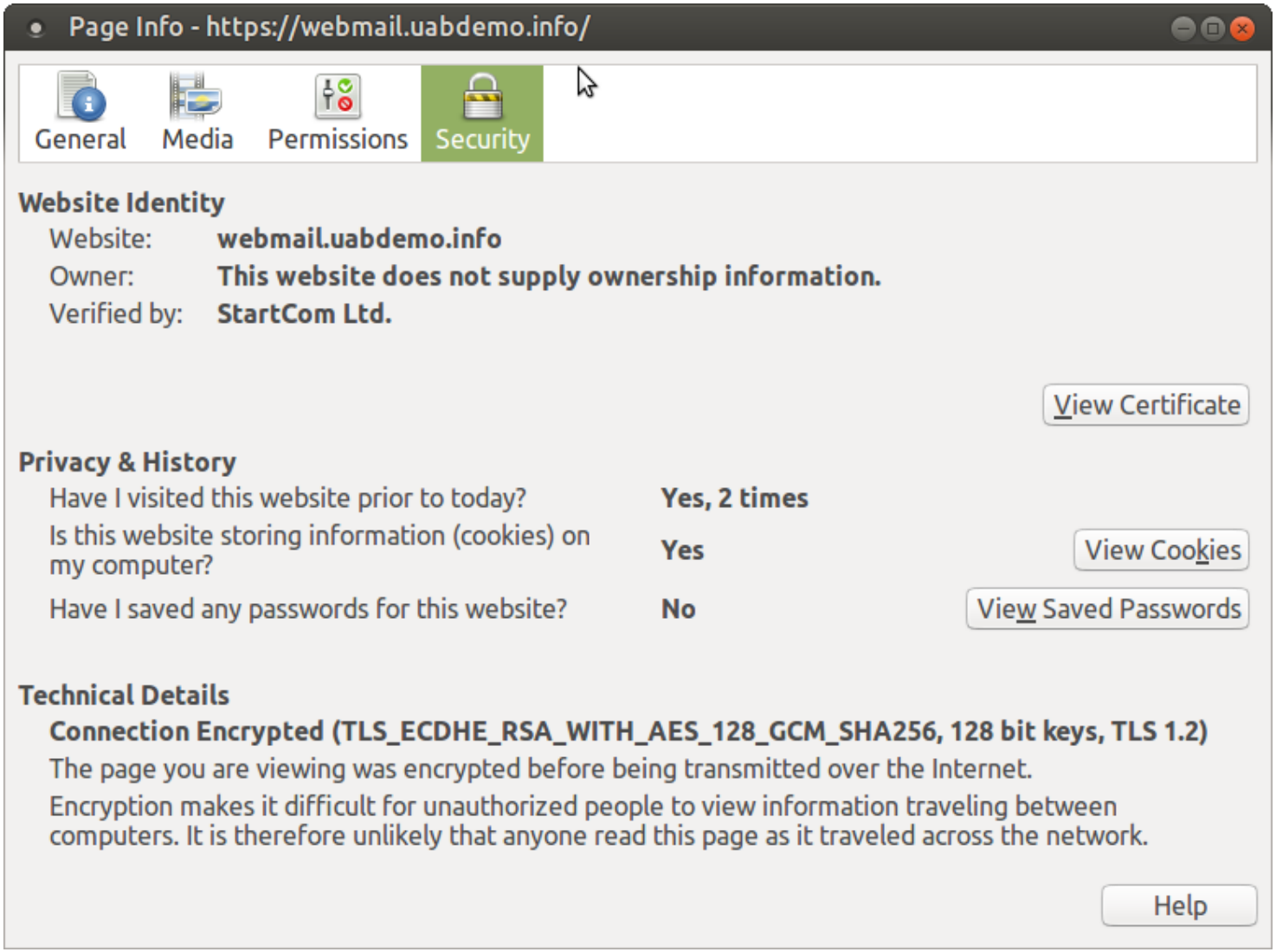
Página de Login do Roundcube Webmail



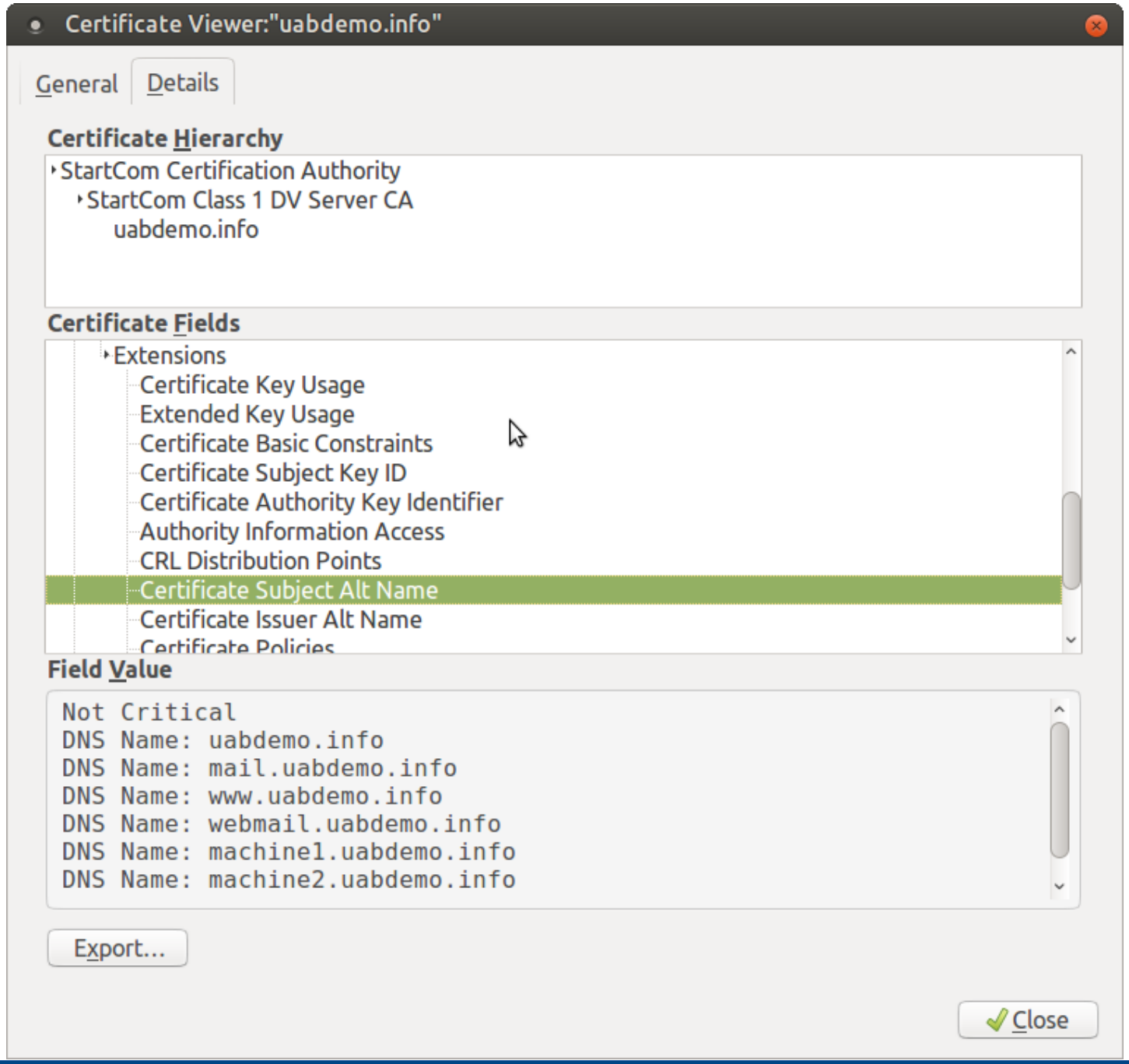
Configuração do Apache para uso do Certificado

```
[root@machine2 ~]# cd /etc/httpd/conf.d/
[root@machine2 conf.d]# vim ssl.conf
[root@machine2 conf.d]# cat ssl.conf
# RICARDO
# 8-Oct-2016
# Section created for SSL VirtualHosts (vhosts)
Listen 443
LoadModule ssl_module modules/mod_ssl.so
NameVirtualHost *:443
<VirtualHost *:443>
    SSLEngine On
    SSLCertificateFile /etc/pki/tls/certs/uabdemo.info.crt
    SSLCertificateKeyFile /etc/pki/tls/private/uabdemo.info.key
    ServerName www.uabdemo.info
    DocumentRoot /var/www/vhosts/www.uabdemo.info/html
    <Directory /var/www/vhosts/www.uabdemo.info/html>
        AllowOverride All
    </Directory>
</VirtualHost>
<VirtualHost *:443>
    SSLEngine On
    SSLCertificateFile /etc/pki/tls/certs/uabdemo.info.crt
    SSLCertificateKeyFile /etc/pki/tls/private/uabdemo.info.key
    ServerName webmail.uabdemo.info
    DocumentRoot /var/www/vhosts/webmail.uabdemo.info/roundcubemail
    <Directory /var/www/vhosts/webmail.uabdemo.info/roundcubemail>
        AllowOverride All
    </Directory>
</VirtualHost>
```

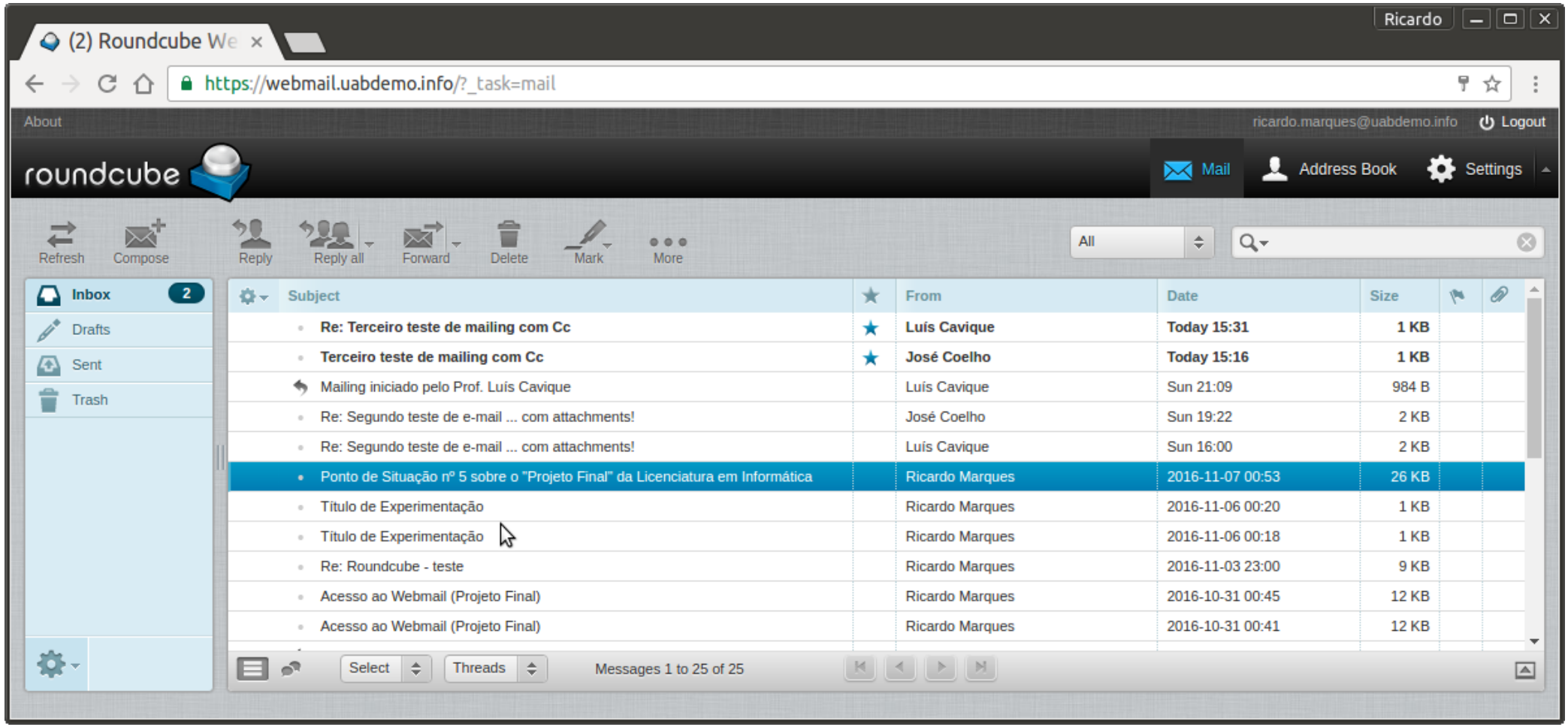
Certificado SSL / TLS, visto no *browser* (1 de 2)



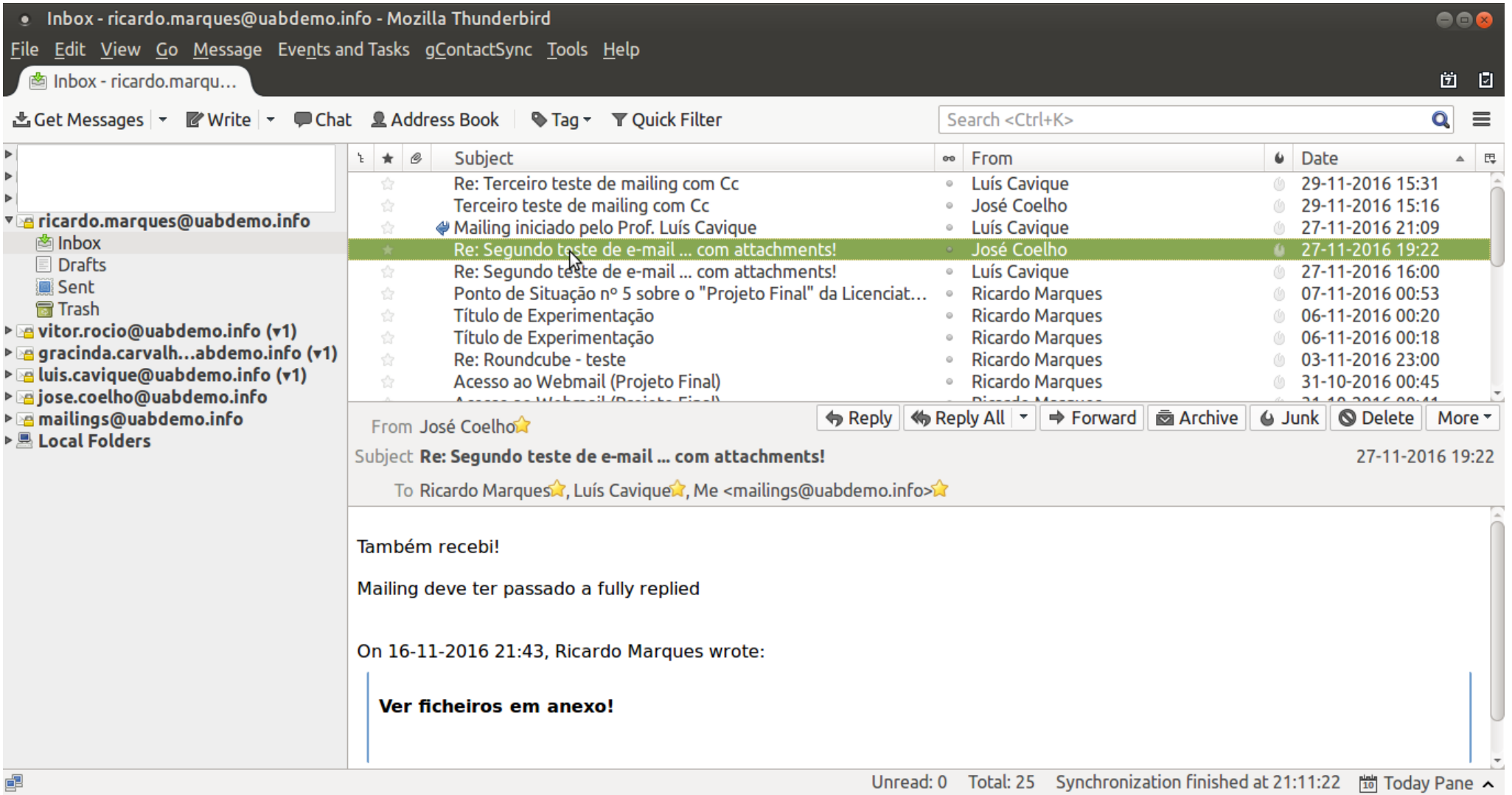
Certificado SSL / TLS, visto no *browser* (2 de 2)



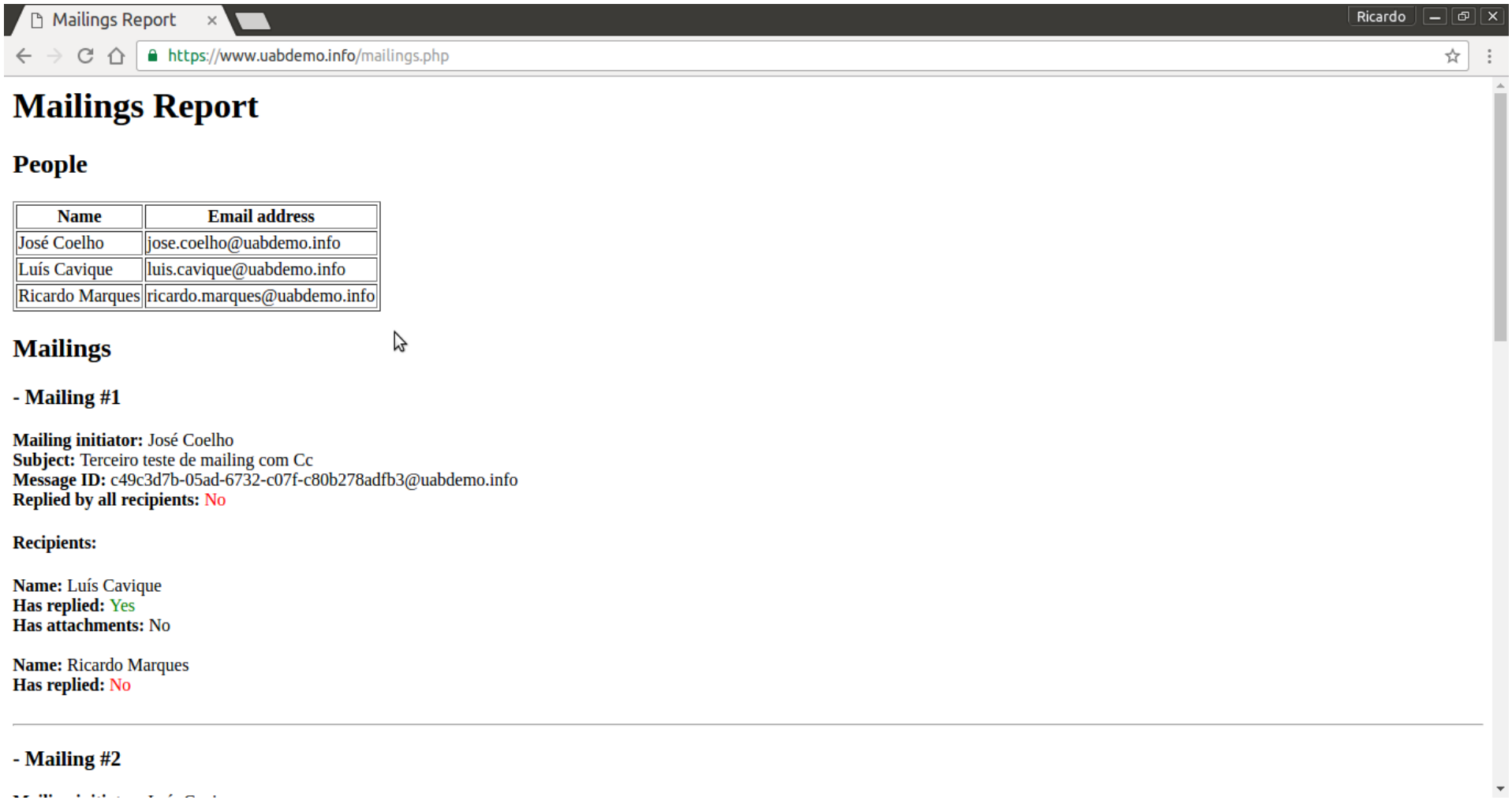
Página da Inbox consultada no Webmail



Mail (Inbox) consultado no Mozilla Thunderbird



Página de report de Mailings (Funcionalidade Adicional)



Objetivos atingidos (1 de 2)

- “Envio de e-mail por SMTP com cifra do canal de transporte.”
- “*Receção de e-mail via IMAPS (Internet Message Access Protocol over SSL), com cifra do canal de transporte.*”
- “*Suporte a múltiplos domínios de e-mail*” - Sistema preparado para suportar múltiplos domínios de e-mail, mas apenas registado e testado um domínio (uabdemo.info), por limitações de tempo e para evitar custos de registo de outros domínios.
- “*Suporte a múltiplas mailboxes e aliases (permitindo reencaminhamento de mensagens para domínios internos ou externos), com informação das mailboxes e aliases registada em Base de Dados.*” - Realizada configuração necessária, mas não testada a funcionalidade de *aliases*/reencaminhamento.
- *“Interface web (Webmail) para leitura e envio de e-mail, com certificado digital ativo para que as comunicações sejam feitas por HTTPS (Hyper Text Transfer Protocol Secure) para identificação do servidor e para cifrar o canal de transporte.”* - Usada **CA** *da* ***StartSSL*** (https://www.startssl.com/) para assinar o ***CSR*** gerado. Escolhida a variante gratuita “*StartSSL Free*”.

Objetivos atingidos (2 de 2)

- "*Funcionalidade proposta pelo Professor Orientador: Criar uma funcionalidade de reporting automático no sistema de email que permita monitorizar entregas de documentos como resposta a um pedido (...)*" - Este objetivo foi conseguido, embora com várias limitações:
  - Necessário a execução manual do programa Perl para refrescar a Base de Dados;
  - *Interface web sem* elementos de *design* gráfico, não interativa e não integrada com o Webmail;
  - Não foram testados *mailings* com vários indicadores/prefixos de resposta no início do assunto;
  - Não foi tratada a possibilidade de *mailings* diferentes com o mesmo assunto, nem a possibilidade de um mesmo utilizador ter vários endereços de e-mail.
  - No entanto, a informação pretendida é devidamente compilada e apresentada na página, permitindo uma gestão mais eficaz dos pedidos e respetivas respostas efetuadas por *email*.

Oportunidades futuras de melhoria (1 de 2)

- Automatizar a instalação e/ou configuração de alguns dos componentes de software do sistema.
- Registar vários domínios e testar o sistema com vários domínios.
- **Criar uma *interface* para criar contas de utilizador e alterar as *passwords* respetivas**
- Definir e testar aliases / forwarding
- Configurar um sistema de anti-spam como o SpamAssassin, incorporando também filtros bayesianos.
- Instalar e configurar um software anti-vírus no servidor de e-mail (como, por exemplo, o ClamAV) integrando-o com o Postfix
- Implementar o backup via "mysqldump" para garantir que os backups são consistentes, no que diz respeito às Bases de Dados (quer da Base de Dados “dbvmail”, quer da Base de Dados “dbmailings”).

Oportunidades futuras de melhoria (2 de 2)

- Sobre a funcionalidade proposta pelo Prof. Orientador, existem oportunidades para trabalhos futuros:
  - Integrar, de alguma forma, o servidor de e-mail com o programa Perl criado de forma a que a receção de uma mensagem na caixa de mailings invoque automaticamente o programa Perl para refrescar a informação na Base de Dados.
  - Mover, para uma pasta da mailbox de mailings fora da “INBOX”, as mensagens já guardadas na Base de Dados MySQL de mailings, para reduzir o volume de mensagens que o programa tem de processar em cada execução.
  - Criar uma interface web com design gráfico apelativo e funcionalidades mais interativas e, se possível, integrá-lo com o sistema de Webmail.
  - Testar e tratar situações de mensagens com assuntos que tenham mais do que um indicador/prefixo de resposta no início do assunto.
  - Suportar a possibilidade de uma mesma pessoa ter vários endereços de e-mail.

Siglas usadas nesta apresentação

- CA – *Certificate Authority*
- CPAN – *Comprehensive Perl Archive Network*
- CSR – *Certificate Signing Request*
- DDL – *Data Definition Language*
- HTTP – *Hypertext Transfer Protocol*
- IaaS – *Infrastructure as a Service*
- IMAPS – *Internet Message Access Protocol over SSL*
- MTA – *Mail Transfer Agent*
- SMTP – *Simple Mail Transfer Protocol*
- SSL – *Secure Sockets Layer*
- TLS – *Transport Layer Security*
- VPS – *Virtual Private Server*

Modelo (*template*) usado para esta Apresentação

- Para esta apresentação foi usado (e ligeiramente adaptado) o seguinte / modelo (*template*) que está disponível numa Licença de Domínio Público (*Public Domain*):
- ***University Course Material Template 1.0***
  http://templates.libreoffice.org/template-center/university-course-material-template

Referências Bibliográficas

Bradner, S. (1997). RFC 2119 – *Key words for use in RFCs to Indicate Requirement Levels*. IETF, março 1997. https://tools.ietf.org/html/rfc2119

Coulouris, G. et al. (2011). *Distributed Systems: Concepts and Design*. 5th Edition, Addison Wesley Longman.

Crocker, D. (1982). RFC 822 – *Standard for the format of ARPA Internet Text Messages*. IETF, agosto 1982. https://tools.ietf.org/search/rfc822

Kitterman, S. (2014). RFC 7208 – *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.* IETF, abril 2014. https://tools.ietf.org/html/rfc7208

Mockapetris, P. (1987a). RFC 1034 – *Domain Names – Concepts and Facilities.* IETF, novembro 1987. https://tools.ietf.org/html/rfc1034

Mockapetris, P. (1987b). RFC 1035 – *Domain Names – Implementation and Specification*. IETF, novembro 1987. https://tools.ietf.org/html/rfc1035

Resnick, P. (2001). RFC 2822 – Internet Message Format. IETF, abril 2001. https://tools.ietf.org/search/rfc2822

Resnick, P. (2008). RFC 5322 – Internet Message Format. IETF, outubro 2008. https://tools.ietf.org/search/rfc5322

Svistunov, M. et al. (2016). *Red Hat Enterprise Linux 6 Deployment Guide - Deployment, Configuration and Administration of Red Hat Enterprise Linux 6*. Red Hat, 2016. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/

Wong, M. & Schlitt, W. (2006). RFC 4408 – *Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.* IETF, abril 2006. https://tools.ietf.org/html/rfc4408

Defesa de “Projeto Final” (U.C. 21095)

OBRIGADO!

“Sistema de Servidor Pessoal de E-mail”

Ricardo Ferreira da Conceição Dias Marques
(Estudante n.º 1100281)
1100281@estudante.uab.pt / uab@ricmarques.net

Universidade Aberta
Departamento de Ciências e Tecnologia (DCeT)
Licenciatura em Informática
dezembro de 2016

UNIVERSIDADE AbERTA
www.uab.pt