ChasqueMail - O e-mail da UFRGS

Alexandre Marchi, Everton Foscarini, Rui Ribeiro

Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portao K – Porto Alegre – RS

{marchi,foscarini,rui.ribeiro}@cpd.ufrgs.br

Resumo. *Este artigo apresenta o serviço ChasqueMail, que tem por objetivo proporcionar infraestrutura para troca de mensagens eletrônicas na UFRGS. O trabalho mostra informações sobre a arquitetura atual do serviço bem o arranjo de softwares que foi utilizado para sua elaboração.*

1.Introdução

O serviço de e-mail tem sua origem na ARPANET e teve sua primeira transmissão inter-institucional no inicio da década de 70 [PETER 2014]. Ao longo destas quase cinco décadas de funcionamento do e-mail, a comunidade acadêmica se beneficiou significativamente com a melhoria de interatividade apresentada por tal ferramenta. Os mais diversos projetos acadêmicos tiveram seu desenvolvimento fortemente apoiado pelo serviço de e-mail uma vez que o tempo para troca de informações entre grupos de pesquisa foi diminuído.

Na UFRGS o e-mail surgiu em 1989, com a aquisição do primeiro computador para o sistema de bibliotecas, e desde 1993 é um serviço mantido pelo CPD da UFRGS para toda a comunidade acadêmica [MARCHI 2005]. Em 2003 nasceu o ChasqueMail, a partir da migração do sistema de e-mail para ferramentas de Software Livre, permitindo que a Universidade tivesse total controle da arquitetura da sua solução de e-mail.

Com o passar dos anos o ChasqueMail teve sua arquitetura modificada, de forma a acompanhar a evolução do serviço de e-mail. Neste artigo serão apresentados os pontos principais da estrutura do serviço atual, focando nos diferenciais implementados na arquitetura da UFRGS.

2. Arquitetura do Serviço

A arquitetura do ChasqueMail foi planejada em 2003 já pensando na escalabilidade necessária para permitir o crescimento da demanda de usuários. As características que foram mantidas desde o projeto inicial foram a utilização do diretório OpenLDAP para manter o cadastro dos usuários e separação dos serviços em servidores (MTA, anti-spam, MDA, MAA). O ChasqueMail já nascia com uma arquitetura distribuida em 8 servidores físicos.

Apesar disso, a arquitetura do serviço de e-mail tem se transformado com o passar dos anos, impulsionado pela virtualização dos servidores e pela possibilidade de criar máquinas virtuais com perfil dedicado a uma atividade especifica. Em 2014 o ChasqueMail conta com 18 servidores que desempenham funções diversas, sendo 17 GNU/Linux e 1 Windows 2008R2 [MICROSOFT 2010]. A Figura 1 apresenta uma topologia resumida do ChasqueMail, apresentando os principais serviços e

seus relacionamentos.

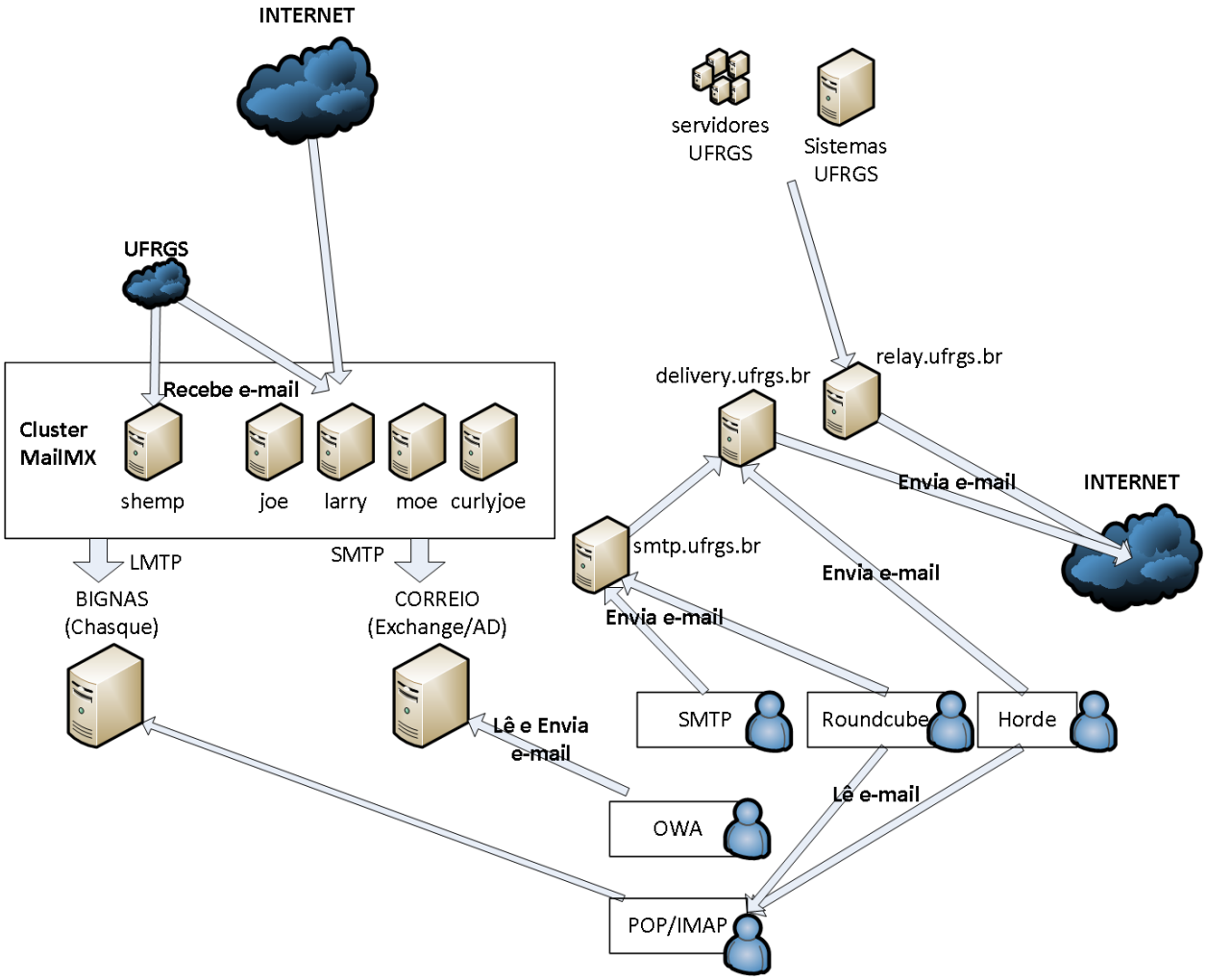

Figura 1. Arquitetura do ChasqueMail em 2014

2.1. Recebimento de E-mail

O recebimento de e-mails do ChasqueMail é tratado por um conjunto de servidores postfix [POSTFIX 2014] configurados com o perfil MailMX. Esses servidores são totalmente independentes, e o balanceamento é feito pelo anúncio no DNS conforme pode ser visto na Figura 2.

```
~$ dig mx ufrgs.br +short
10 shemp.ufrgs.br.
20 moe.ufrgs.br.
20 larry.ufrgs.br.
20 curlyjoe.ufrgs.br.
20 joe.ufrgs.br.
```

Figura 2. Consulta DNS relativa aos servidores MX da UFRGS

O cluster MailMX emprega diversas técnicas para diminuir a incidência de *Spam* (mensagens não solicitadas) nas caixas de entrada dos usuários. Exemplos:

- FakeMX - MX de maior prioridade que rejeita conexões
- RBL - Listas de bloqueio de IPs
- Greylist - Bloqueio temporário de IPs
- Checagem SPF
- Verificação de existência de domínio remetente
- ClamAV utilizando SpamAssassin, pyzor, razor
- Regras personalizadas para SpamAssassin

A maioria das técnicas empregadas para recebimento de e-mail no Cluster MailMX são amplamente divulgadas nos fórums, sites de documentação e listas de discussão sobre o assunto, mas algumas delas foram personalizadas para o nosso ambiente.

- FakeMX - O servidor MX falso recebe as mensagens enviadas pelos servidores de e-mail da rede interna da Universidade. Dessa forma o tráfego interno é sempre priorizado, contando com um servidor dedicado.
- Regras personalizadas para SpamAssassin
    - Garantir que mensagens geradas na rede da UFRGS não sejam marcadas como Spam
    - Definição de regras locais de bloqueio/marcação como Spam a partir de análise estatística das mensagens recebidas
    - Bloqueio de mensagens de Phishing bancário ou para roubo de senhas

A partir do recebimento das mensagens pelo cluster MailMX, elas são verificadas pelo antivirus, anti-spam e são entregues para um dos servidores de caixas postais.

2.2. Servidores de caixa postal

Na configuração atual, o software Postfix dos servidores MailMX está configurado para verificar em uma consulta ao OpenLDAP se o destinatário de uma mensagem é uma conta válida. O OpenLDAP também pode informar ao Postfix que o destinatário ou domínio está vinculado ao Exchange corporativo da UFRGS, repassando a consulta para o ActiveDirectory.

As caracteristicas atuais dos serviços de caixa postal são:

- ChasqueMail - dovecot 2.2
    - Contas pessoais e departamentais
    - Toda a comunidade acadêmica e administrativa
    - Vinculadas às pessoas ou unidades acadêmicas/administrativas
    - Entre 2GB e 20GB de armazenamento, crescimento sob demanda
    - Acesso IMAP, POP3 e Webmail Roundcube
- Microsoft Exchange 2010
    - Contas corporativas pessoais ou impessoais
    - Reitoria, CPD e outros órgãos administrativos
    - Vinculadas à atividade profissional executadas nos órgãos
    - 2GB de armazenamento
    - Acesso via Outlook e OWA

2.3. Saída de E-mail

A saída de e-mails na UFRGS é composta por diversos níveis de filtragem. Tal abordagem foi implementada para permitir o controle de fluxo de e-mails e diminuir a incidência uso não legítimo da infraestrutura, como para envio de *Spam* ou *phishing* após o roubo de credenciais de nossos usuários. O descontrole acerca do uso indevido pode fazer com que os servidores de e-mail passem a compor listas de bloqueios que são amplamente utilizadas, por exemplo SpamCop, Spamhaus, entre outras.

A UFRGS possui diversos sistemas de informação que demandam o envio não autenticado de envio de mensagens, como Moodle, Portal de Serviços, sistema de matrícula, sistema de tickets, entre outros. O serviço *relay.ufrgs.br* foi criado com o objetivo de permitir o envio de mensagens sem autenticação, com forte controle de fluxo e alertas para coibir abusos e/ou tentativas de falsificação de remetentes.

O serviço *relay.ufrgs.br* é baseado no software Postfix, e utiliza o postfwd [KESSLET 2014] para efetuar controle de taxa de mensagens enviadas por remetente e endereço IP de origem.

- postfwd- analisa a taxa de envio de e-mails em função do IP de origem.
- clamsmtpd - verifica a presença de virus nas mensagens.
- postfix - verifica se a mensagem não é uma resposta a um phishing.
- opendkim - assinatura criptográfica de headers da mensagem.

Para os usuários do serviço de e-mail bem como para os sistema que não possuem restrição quanto a autenticação, a UFRGS possui o serviço de *relay* autenticado. Este serviço é sub-dividido em dois outros serviços: *smtp.ufrgs.br* e *delivery.ufrgs.br*.

Ao enviar uma mensagem de e-mail, o usuário a submete ao *smtp.ufrgs.br*. Este serviço, diferentemente do *relay.ufrgs.br,* exige que o usuário esteja autenticado, alem disso implementa o controle de taxa de mensagens enviadas por remetente e exige que os endereços que constam na mensagem estejam bem formados. Após fazer tais verificações o *smtp.ufrgs.br* encaminha as mensagens ao *delivery.ufrgs.br.*

Ao receber uma mensagem, o *delivery.ufrgs.br* verifica o controle de taxa de mensagens enviadas em função do endereço de e-mail do remetente autenticado. Esse controle permite criar um ponto de retenção das mensagens caso ocorra o roubo de uma senha de usuário. Na sequência é verificada a presença de vírus na mensagem (clamsmtpd), que é seguida pela verificação de resolução de DNS (postfix) e por fim um filtro de respostas a *phishings* (postfix). Percorridas as verificações, a mensagem é então assinada (DKIM) e enviada ao destino.

Na Figura 3 é possível ver com maior riqueza de detalhes o sub-sistema de envio de e-mails e as aplicações que são responsáveis pelo processamento das mensagens. A esquerda está representado o *relay* não autenticado (*relay.ufrgs.br*) e a direita o *relay* autenticado (smtp.ufrgs.br e delivery.ufrgs.br).

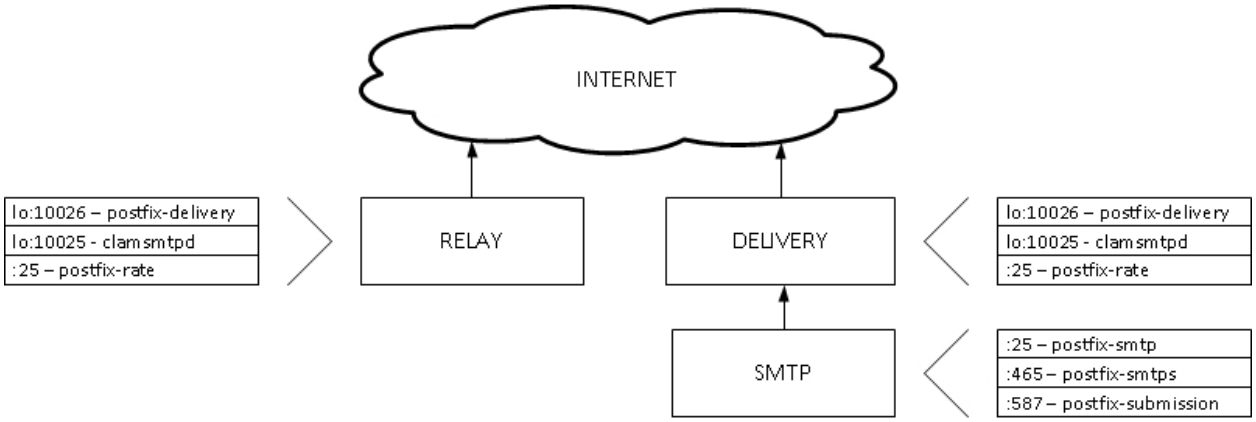

Figura 3. Sub-sistema de saída de e-mails

2.4. ChasqueWebmail

O ChasqueWebmail é a interface webmail recomendada para os usuários do ChaqueMail. Para implementar o ChasqueWebmail foi utilizado o software livre RoundCube, com algumas personalizações para adequar ao ambiente da Universidade:

- Verificação de débitos no sistema de bibliotecas - Gera aviso aos usuários
- Criação de identidades de e-mail vinculadas aos endereços válidos para cada usuário
- Autenticação por nome de login, e-mail ou apelido
- Geração de listas de bloqueios de remetentes (blacklist) integradas ao dovecot/Caixa Postal
- Configuração de mensagem de ausência (vacation) integrada ao dovecot/Caixa Postal

Essas funcionalidades foram implementadas através de *plugins* do RoundCube, que permitem a extensão de funcionalidades sem a necessidade de intereferir no código da aplicação, o que facilita a atualização do Roundcube.

A figura 4 exibe a página de configuração da mensagem de ausência, que foi implementada a partir de uma extensão do plugin ManageSieve que é distribuído juntamente ao código fonte do RoundCube.

Algumas caracteristícas do RoundCube foram cruciais para a escolha por este software para implementar o Chaque Webmail:

- Interface limpa e intuitiva
- Configurações simplificadas
- Ativamente desenvolvido pela comunidade
- API bem definida
- Biblioteca de plugins bem estabelecida

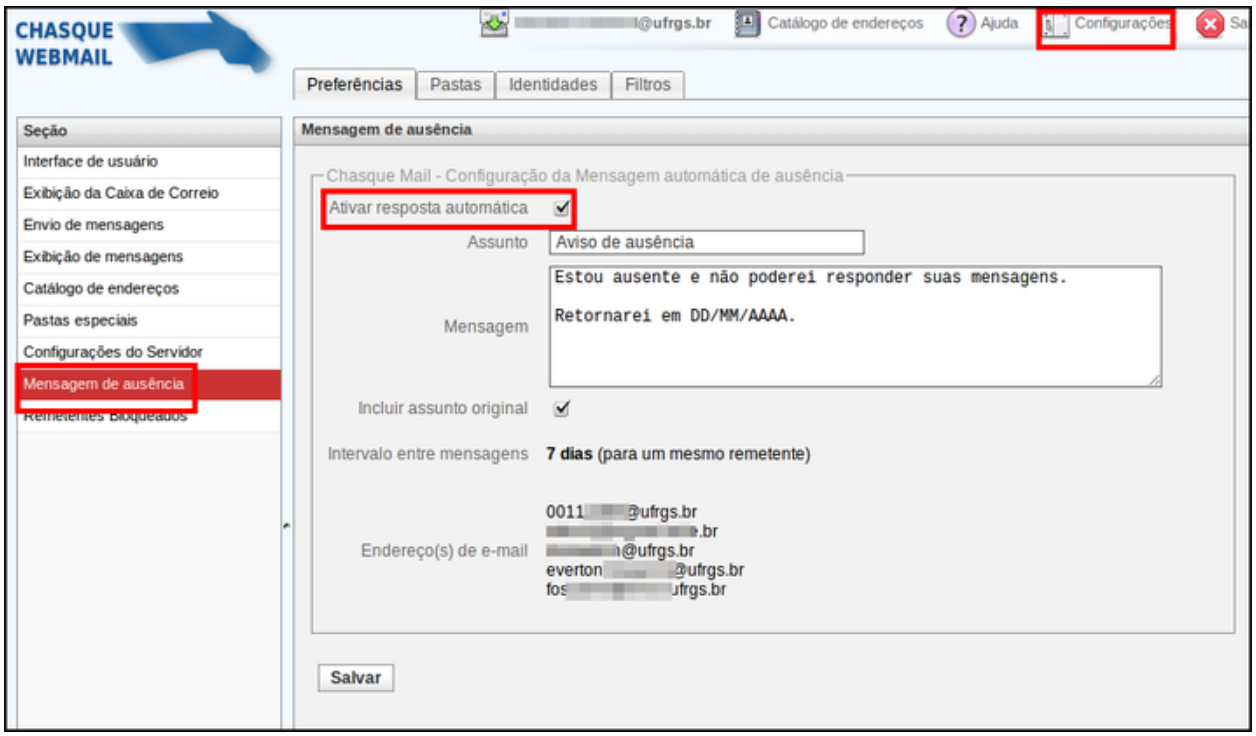

Figura 4: Configuração da mensagem de ausência

3. Considerações finais

O sistema de e-mail da UFRGS vem evoluindo ao longo dos anos buscando atender as demandas de funcionalidade, segurança, qualidade do *anti-spam* e espaço de armazenamento dos usuários. A cada iteração temos buscado criar uma arquitetura cada vez mais escalável e resiliente, de forma a permitir o crescimento da infraestrutura de acordo com o aumento do número de usuários e de mensagens armazenadas.

Apesar disso a evolução dos *softwares* e protocolos pressiona os administradores do serviço a buscar melhorar ainda mais a infraestrutura, e algumas das tecnologias que precisam ser implementadas nas próximas atualizações do serviço são o uso de TLS/DANE para transporte de e-mail, DMARC para filtrar/rejeitar mensagens e a replicação completa dos servidores de caixas postais do Chasque via dsync (dovecot).

O ChasqueMail é uma marca consolidada entre os usuários da UFRGS, e a manutenção da qualidade desse serviço é um dos pontos focais da administração do CPD da UFRGS.

Referências

KESSLER, Jan Peter (2013) http://postfwd.org/. Acesso em 11 de junho de 2014.

MARCHI, Alexandre et al. Chasque: o correio eletrônico da UFRGS migrando para o software livre. Fórum Internacional do Software Livre, 2005. Porto Alegre. Disponível em http://www.lume.ufrgs.br/handle/10183/69885

Microsoft (2010) http://www.microsoft.com/brasil/servidores/windowsserver2008/r2/default.mspx. Acesso em 11 de junho de 2014.

PETER, Ian (2014) http://www.nethistory.info/History%20of%20the%20Internet/email.html. Acesso em 11 de junho de 2014.

Postfix Project (2014) thttp://www.postfix.org/. Acesso em 11 de junho de 2014.