SEG12 - Semana 1 - Sessão 11

Francisco Marcelo, Marcelo Karam e Felipe Scarel

06-08-2018

Correio Eletrônico — SMTP

As atividades desta sessão serão realizadas na máquina virtual *Server_Linux*.

Neste capítulo iremos realizar a configuração da primeira parte de um serviço de correio eletrônico: o envio e recebimento de emails entre domínios através do protocolo *Simple Mail Transfer Protocol* (SMTP). Iremos instalar e configurar o Postfix, uma dos servidores SMTP *open source* mais populares do mundo. Juntamente com o Postfix iremos instalar também o Cyrus SASL, um programa que provê módulos de autenticação plugáveis para verificarmos usuários e senhas via acesso cifrado, com criptografia TLS.

1) Instalação do servidor SMTP Postfix

Antes de instalar o Postfix, temos que corrigir alguns aspectos da nossa instalação atual. Como você se recorda da sessão 7 — DNS e NFS, configuramos a máquina *Server_Linux* com o nome de domínio `servidor.empresa.com.br`, no IP 192.168.0.10. Da mesma forma, inserimos uma entrada fictícia no DNS para uma máquina `email.empresa.com.br` no IP 192.168.0.15, que não existe em nossa topologia de rede.

Já que vamos instalar o Posfix + Cyrus na máquina *Server_Linux*, temos que apontar o nome `email.empresa.com.br` para o IP 192.168.0.10.

Contudo, não podemos tomar o caminho mais fácil, que seria criar um registro de *alias* `CNAME` do nome `email.empresa.com.br` para o nome `servidor.empresa.com.br` — a RFC 2181, seção 10.3 (https://tools.ietf.org/html/rfc2181) proíbe uso de `CNAME` para apontamentos `MX`, exigindo que esses apontamentos sejam feitos diretamente por registros `A`.

Isso exige uma série de alterações ao registro direto do domínio `empresa.com.br`, no arquivo `/etc/bind/db.empresa.com.br`, que fica como se segue:

```
$TTL 86400 ; (1 day)
$ORIGIN empresa.com.br.
@         IN    SOA           email.empresa.com.br. admin.empresa.com.br. (
                2018081200    ;Serial (YYYYMMDDnn)
                14400         ;Refresh (4 hours)
                1800          ;Retry (30 minutes)
                1209600       ;Expire (2 weeks)
                3600          ;Negative Cache TTL (1 hour)
)

@         IN    NS            email.empresa.com.br.

@         IN    MX      10    email.empresa.com.br.

email     IN    A             192.168.0.10
cliente   IN    A             192.168.0.20
windows   IN    A             192.168.0.25

meusite   IN    CNAME         email
pop       IN    CNAME         email
servidor  IN    CNAME         email
smtp      IN    CNAME         email
www       IN    CNAME         email
```

Da mesma forma, surge um problema também na resolução de registros reversos do domínio. Não é recomendado que haja múltiplos apontamentos `PTR` para o mesmo endereço IP, sob pena de obter respostas diferentes em duas *queries* DNS distintas. Vamos alterar o registro reverso no arquivo `/etc/bind/db.0.168.192`, deixando-o assim:

```
$TTL 86400 ; (1 day)
$ORIGIN 0.168.192.in-addr.arpa.
@         IN    SOA           email.empresa.com.br. admin.empresa.com.br. (
                2018081200    ;Serial (YYYYMMDDnn)
                14400         ;Refresh (4 hours)
                1800          ;Retry (30 minutes)
                1209600       ;Expire (2 weeks)
                3600          ;Negative Cache TTL (1 hour)
)

@         IN    NS            email.empresa.com.br.

@         IN    MX      10    email.empresa.com.br.

10        IN    PTR           email.empresa.com.br.
20        IN    PTR           cliente.empresa.com.br.
25        IN    PTR           windows.empresa.com.br.
```

Agora, vamos testar. Reinicie o serviço `bind` e verifique se o DNS que responde pelo domínio

empresa.com.br é, de fato, a máquina email.empresa.com.br:

```
# systemctl restart bind9.service

# dig -t NS empresa.com.br

; <<>> DiG 9.9.5-9+deb8u15-Debian <<>> -t NS empresa.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35860
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;empresa.com.br.                        IN      NS

;; ANSWER SECTION:
empresa.com.br.         86400   IN      NS      email.empresa.com.br.

;; ADDITIONAL SECTION:
email.empresa.com.br.   86400   IN      A       192.168.0.10

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Aug 12 14:50:45 -03 2018
;; MSG SIZE  rcvd: 79
```

De igual forma, verifique o registro reverso do IP 192.168.0.10, que deve retornar o nome email.empresa.com.br. Finalmente, o nome servidor.empresa.com.br torna-se agora um *alias* do CNAME email.empresa.com.br.

```
# nslookup 192.168.0.10
Server:         127.0.0.1
Address:        127.0.0.1#53

10.0.168.192.in-addr.arpa       name = email.empresa.com.br.

# nslookup servidor.empresa.com.br
Server:         127.0.0.1
Address:        127.0.0.1#53

servidor.empresa.com.br canonical name = email.empresa.com.br.
Name:   email.empresa.com.br
Address: 192.168.0.10
```

Ainda falta alterar os registros locais de nomes, nos arquivos /etc/hostname, /etc/mailname e /etc/hosts. Altere-os como mostrado a seguir:

```
# cat /etc/hostname
email

# cat /etc/mailname
email.empresa.com.br

# cat /etc/hosts
127.0.0.1                       localhost
127.0.1.1    email.empresa.com.br email
192.168.0.10 email.empresa.com.br email

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Finalmente, reinicie a máquina *Server_Linux*. No próximo login, o nome mostrado pelo *prompt* do shell deve ser `USERNAME@email:~$`.

```
# reboot

(...)

$ ssh aluno@192.168.0.10
You have new mail.
Last login: Sun Aug 12 18:00:53 2018 from 192.168.0.254
aluno@email:~$
```

Isso feito, podemos começar a atividade. Instale o Postfix + Cyrus SASL na máquina *Server_Linux* (pacotes `postfix`, `sasl2-bin` e `mailutils`). Em seguida, reconfigure o Postfix (comando `dpkg-reconfigure postfix`) de acordo com as informações da tabela abaixo:

Tabela 1. Configurações do Postfix

Parâmetro	**Valor**
Tipo geral de configuração de e-mail	Site da internet
Nome de e-mail do sistema	email.empresa.com.br
Destinatário das mensagens para root e postmaster	Em branco
Outros destinos para os quais deve aceitar mensagens	email.empresa.com.br, localhost.empresa.com.br, empresa.com.br, localhost
Forçar atualizações síncronas na fila de mensagem	Não
Redes locais	127.0.0.0/8, 192.168.1.0/24, 172.16.0.0/24, [::ffff:127.0.0.0]/104, [::1]/128

Parâmetro	Valor
Usar procmail para entrega local	Sim
Limite de tamanho da caixa postal	0
Caractere de extensão de endereço local	+
Protocolos de internet para usar	Todos

Crie um par de chaves RSA de 4096 bits e validade de dois anos para permitir conexões TLS ao seu servidor, com chave pública em `/etc/ssl/certs/smtpd.crt` e chave privada em `/etc/ssl/private/smtpd.key`. Feito isso, configure o Postfix, editando o arquivo `/etc/postfix/main.cf`, e:

- Habilite criptografia TLS em conexões oriundas dos clientes, de forma opcional;
- Use as chaves assimétricas criadas acima para implementar a cifragem TLS;
- Habilite autenticação SASL dos tipos PLAIN e LOGIN, comunicando-se com o *daemon* `saslauthd` do Cyrus — deve-se consultar a base de usuários locais via PAM para autenticação.

Atente-se para o fato de que, por padrão, o Postfix opera dentro de um ambiente `chroot`. Será necessário editar opções padrão do `saslauthd` no arquivo `/etc/default/saslauthd` para adaptar-se a esse cenário. Mais além, adicione o usuário do `postfix` ao grupo `sasl` para permitir comunicação entre os dois *daemons*.

Ao final do processo, use o comando `telnet` para testar a configuração realizada, logando no servidor SMTP com usuário `aluno` e senha `rnpesr` pelo método PLAIN.

2) Envio e recebimento de mensagens por *telnet*

Vamos agora testar o envio de mensagens usando o comando `telnet`, diretamente a partir do servidor SMTP. Este teste visa averiguar o funcionamento do servidor de e-mail sem a influência de configurações de clientes de e-mail (*Mail User Agents* — MUA).

Conecte-se ao servidor SMTP por `telnet` com um usuário qualquer existente na base local de usuários ou LDAP e envie email para outro usuário usando os comandos `MAIL` e `RCPT TO` do SMTP. Logue na conta do destinatário e verifique que a mensagem foi recebida.

3) Análise do log de envio

Envie uma nova mensagem de email usando o `telnet`, e monitore ao mesmo tempo o arquivo `/var/log/mail.log` por alterações. Responda, apontando a excerto do log que identifica a informação:

- Qual é o IP de origem da conexão SMTP?
- Qual o nome do usuário que efetuou login?
- Qual o endereço do destinatário da mensagem?
- Qual o método de entrega da mensagem para a caixa do usuário?