POSTFIX

Otimizando para Alto Tráfego

Humberto Sartini
http://web.onda.com.br/humberto

Palestrante

Humberto Sartini

- Analista de Segurança do Provedor Onda S/A
- Participante dos projetos:
  - Rau-Tu Linux (http://www.rau-tu.unicamp.br/linux/)
  - HoneypotBR (http://www.honeypot.com.br/)
- Participante do:
  - IV Fórum Internacional de SL (Porto Alegre – 2003)
  - Conferência Internacional de SL (Curitiba - 2003)

Tópicos

- Instalação PCRE
- Instalação Postfix
- Configuração Básica
- Configuração de envio e recebimento
- Bloqueio através do Cabeçalho e Corpo
- Restrição de envio por usuários
- Outros comandos
- Ferramentas Postfix

Instalação PCRE

- O PCRE (Perl Compatible Regular Expression) é necessário devido a utilização de Expressões Regulares nas checagens do Cabeçalho e Corpo do E-mail

- Versão 2.08

http://www.pcre.org

Instalação PCRE

```
tar xzvpf pcre-2.08.tar.gz
cd pcre-2.08
make
make install
```

Instalação Postfix

- O Postfix é um dos mais completos, robustos e seguros servidores de e-mails.

- Versão 2.0.18

http://www.postfix.org

Instalação Postfix

Alguns passos são necessários antes da instalação do Postfix, iremos “preparar o terreno”.

- Criação de Grupo
  groupadd postdrop

- Criação de Usuários
  adduser -s /bin/false postfix

Instalação Postfix

- É necessário renomear os arquivos do Sendmail, para que haja compatibilidade.

mv /usr/sbin/sendmail /usr/sbin/sendmail.OFF
mv /usr/sbin/newaliases /usr/sbin/newaliases.OFF
mv /usr/sbin/mailq /usr/sbin/mailq.OFF
chmod 755 /usr/sbin/sendmail.OFF
chmod 755 /usr/sbin/newaliases.OFF
chmod 755 /usr/sbin/mailq.OFF

Instalação Postfix

tar xzpvf postfix-2.0.18.tar.gz

cd postfix-2.0.18

make

make install

(ou “make upgrade” para atualização)

Instalação Postfix

Paramêtros de instalação (1/4)

- Diretório Raiz (Padrão)

install_root: [/]

- Diretório usado durante a instalação (Padrão)

tempdir: [/tmp/postfix-2.0.18]

- Diretório de instalação dos arquivos de configuração (Padrão)

config_directory: [/etc/postfix]

- Diretório onde ficará o daemon (Padrão)

daemon_directory: [/usr/libexec/postfix]

Instalação Postfix

Paramêtros de instalação (2/4)

- Diretório onda ficará ferramentas do Postfix (Padrão)

command_directory: [/usr/sbin]

- Diretório de armazenamento de e-mails (Padrão)

queue_directory: [/var/spool/postfix]

- Caminho do "sendmail", para compatibilidade (Checar caminho)

sendmail_path: [/usr/sbin/sendmail]

- Caminho do "newaliases", para compatibilidade (Checar caminho)

newaliases_path: [/usr/bin/newaliases]

Instalação Postfix

Paramêtros de instalação (3/4)

- Caminho do "mailq", para compatibilidade (Checar caminho)

mailq_path: [/usr/bin/mailq]

- Usuário utilizado pelo Postfix (Padrão)

mail_owner: [postfix]

- Grupo utilizado pelo Postfix (Padrão)

setgid_group: [postdrop]

- Diretório do Manual do Postfix (Padrão)

manpage_directory: [/usr/local/man]

Instalação Postfix

Paramêtros de instalação (4/4)

- Diretório de examplos do Postfix (Alterado)

sample_directory: [/etc/postfix] /etc/postfix/sample

- Diretório do README (Padrão)

readme_directory: [no]

Pronto !!!

O Postfix está instalado !!

Configuração Básica do Postfix

Temos dois arquivos principais de configuração:

- master.cf

  Gerencia número de processos e serviços .

- main.cf

  Parâmetros de configuração, são mais de 280.

Configuração Básica do Postfix

• Diretório de Fila
queue_directory = /var/spool/postfix

• Diretório de Comandos
command_directory = /usr/sbin

• Diretório de Daemon
daemon_directory = /usr/libexec/postfix

• Usuário do Postfix
mail_owner = postfix

• Hostname do servidor
myhostname = servidor.meudominio.com.br

Configuração Básica do Postfix

• Dominio do servidor
mydomain = meudominio.com.br

• Qual o completo após o @ do e-mail
myorigin = $mydomain

• Qual interface responde pelo Postfix
inet_interfaces = all

• Destinos válidos
mydestination = $myhostname, localhost.$mydomain, $mydomain

• Confia somente no host (Class / Subnet / Host)
mynetworks_style = host

Configuração Básica do Postfix

• Dominio do servidor
mydomain = meudominio.com.br

• Resposta para usuários não encontrados
unknown_local_recipient_reject_code = 500

• Rede que serão liberadas para Relay
mynetworks = 127.0.0.0/8, 192.168.0.0/24
#mynetworks = $config_directory/mynetworks

• Arquivos com alias
alias_maps = hash:/etc/aliases

• Formato da Caixa de E-mail (Mailbox / Maildir)
home_mailbox = Mailbox

Configuração Básica do Postfix

• Diretório de Armazenamento de E-mails

mail_spool_directory = /var/spool/mail

• Tamanho da caixa do usuário (50 Megas)

mailbox_size_limit = 51200000

• Tamanho máximo da mensagem (10 Megas)

message_size_limit = 10240000

• Banner do servidor SMTP

smtpd_banner = $myhostname - Servidor de E-mail

• Nível de debug

debug_peer_level = 2

Configuração Básica do Postfix

• Parâmetros para o debug

```
debugger_command =
    PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
    xxgdb $daemon_directory/$process_name
$process_id & sleep 5
```

• Caminho do Sendmail

```
sendmail_path = /usr/sbin/sendmail
```

• Caminho do Newaliases

```
newaliases_path = /usr/bin/newaliases
```

• Caminho do Mailq

```
mailq_path = /usr/bin/mailq
```

Configuração Básica do Postfix

- Grupo do Postfix

setgid_group = postdrop

- Diretório do Manual

manpage_directory = /usr/local/man

- Diretório de Exemplos

sample_directory = /etc/postfix/sample

Configuração de envio e recebimento

Esses parâmetros visam melhorar a segurança do servidor e combater o Spam

- Número máximo de destinatários no mesmo e-mail
smtpd_recipient_limit = 100

- Respeita RFC 821 - MAIL FROM e RCPT TO
strict_rfc821_envelopes = yes

- Ativo checagem de helo
smtpd_helo_required = yes

Configuração de envio e recebimento

• Desabilita VRFY
disable_vrfy_command = yes

• Listas de RBL
maps_rbl_domains = relays.ordb.org, list.dsbl.org, dun.dnsrbl.net, spam.dnsrbl.net

Obs.: Utilizar com cuidado as listas, pois algumas bloqueiam e-mails do Brasil. Mais informações em: http://www.dnsstuff.com

Configuração de envio e recebimento

- Restricão do cliente - Após o aceite da conexao SMTP

```
smtpd_client_restrictions =
   # Checa conteúdo do CLIENT_ACCESS
   check_client_access hash:/etc/postfix/client_access,
   # Permite "mynetwork"
   permit_mynetworks,
   # Permite conteudo do ACCESS
   hash:/etc/postfix/access,
   # Quando não há entrada PTR do IP
   reject_unknown_client,
   # Bloqueio comando para forçar entrega
   reject_unauth_pipelining,
   # Bloqueia IP's listados em RBL
   reject_rbl_client maps_rbl_domains
```

Configuração de envio e recebimento

- Restricão durante comando HELO/EHLO

```
smtpd_helo_restrictions =
   # Permite "mynetwork"
   permit_mynetworks,
   # Quando não é informado o hostname
   reject_invalid_hostname,
   # Quando não existe entrada DNS A ou MX
   reject_unknown_hostname,
   # Quando o hostname não apresenta hostname válido
   reject_non_fqdn_hostname,
   # Bloqueio comando para forçar entrega
   reject_unauth_pipelining,
   # Bloqueia IP's listados em RBL
   reject_rbl_client maps_rbl_domains
```

Configuração de envio e recebimento

- Restricão aplicada no MAIL FROM

```
smtpd_sender_restrictions =
   # Permite "mynetwork"
   permit_mynetworks,
   # Permite conteudo do ACCESS
   check_sender_access hash:/etc/postfix/access,
   # Bloqueio quando não existe entrada DNS A ou MX
   reject_unknown_sender_domain,
   # Quando o hostname não apresenta hostname válido
   reject_non_fqdn_sender,
   # Bloqueio comando para forçar entrega.
   reject_unauth_pipelining
```

Configuração de envio e recebimento

- Restricão aplicada no RCPT TO

```
smtpd_recipient_restrictions =
   # Permite "mynetwork"
   permit_mynetworks,
   # Permite conteúdo do ACCESS
   check_sender_access hash:/etc/postfix/access,
   # Bloqueia quando não existe entrada DNS A ou MX
   reject_unknown_recipient_domain,
   # Quando o hostname não apresenta hostname válido
   reject_non_fqdn_recipient,
   # Bloqueio comando para forçar entrega
   reject_unauth_pipelining
```

Configuração de envio e recebimento

- Arquivo /etc/postfix/access

```
joaozinho@123.com.br      E-MAIL REJEITADO
123.com.br                DOMINIO REJEITADO
/^postmaster@/            OK
/^abuse@/                 OK
```

- Arquivo /etc/postfix/client_access

```
200.200.200.200    RELAY
100.100.100        554 SPAMMER NETWORK
150.100.100.100    554 SPAMMER HOST
dsl.telesp.net.br  554 SPAMMER NETWORK
```

Bloqueio através do Cabeçalho e Corpo

- Bloqueio por Assunto

Adicione a linha abaixo no main.cf

```
header_checks = pcre:/etc/postfix/header_checks
mime_header_checks = $header_checks
nested_header_checks = $header_checks
```

Bloqueio através do Cabeçalho e Corpo

- Conteúdo do /etc/postfix/header_checks

/^Subject: Trabalhe em casa/ REJECT SPAMMER
/^To: joao@trabalheemcasa.com.br/ REJECT
/^Subject:.*V.agr.\?*./ REJECT Email rejeitado
/^Subject:.*FIQUE RICO.*./ REJECT Email rejeitado
/^Content-(Type|Disposition):.*(file)?name=.*\.(com|lnk|bat|scr|chm|hlp|hta|reg|shs|vbe|vbs|wsf|wsh|pif)/ REJECT Email rejeitado, devido a um arquivo .${3} em anexo

Bloqueio através do Cabeçalho e Corpo

- Bloqueio por Conteúdo

  Adicione a linha abaixo no main.cf

```
body_checks = pcre:/etc/postfix/body_checks

# Verifica os 50 K inicais
body_checks_size_limit = 51200
```

Bloqueio através do Cabeçalho e Corpo

- Conteúdo do /etc/postfix/body_checks

/^Content-(Type|Disposition):.*(file)?name=.*\.(com|lnk|bat|scr|chm|hlp|hta|reg|shs|vbe|vbs|wsf|wsh|pif|exe)/ REJECT Email rejeitado, devido a um arquivo .$ {3} em anexo
/^.*decidaservencedor.kit.net*/ REJECT Spammer.
/^RSLxwtYBDB6FCv8ybBcS0zp9VU5of3K4BXuwyehTM0RI9IrSjVuwP94xfn0wgOjouKWzGXHVk3qg$/ DISCARD VIRUS(sobig.f)
/^(UEsDBAoAAAAAA(.....KJx\+eAFgAAABYAA|...Nz|K4)|ApIAUCZKAEAD\/bJpmiwQBPQl6AEAS 85pmm7ZH8gqwAO4sKimaZqmoJiQiICapmmaeHBoYFhQzWCf)/ DISCARD VIRUS (W32/Mydoom@MM)

Bloqueio através do Cabeçalho e Corpo

- Algumas opções

REJECT [texto opcional]

Rejeita a mensagem e retorno erro para o remetente

OK

Aceita a mensagem

IGNORE

Ignora a mensagem sem reportar mensagem para o remetente

DISCARD [texto opcional]

Ignora a mensagem

Restrição de envio por usuário

As vezes é necessário bloquear o envio de e-mail de determinados usuários e para isso fazemos:

/etc/postfix/main.cf:

```
smtpd_recipient_restrictions =
    hash:/etc/postfix/usuarios_restritos
    ... outros parametros ...
```

Restrição de envio por usuário

/etc/postfix/main.cf:
smtpd_restriction_classes = dominios_restritos
dominios_restritos =
   check_sender_access hash:/etc/postfix/dominios_restritos, reject

/etc/postfix/usuarios_restritos:
    usuario1@meudominio.com.br   dominios_restritos
    usuario2@meudominio.com.br   dominios_restritos

/etc/postfix/dominios_restritos:
  dominio1.com.br   OK
  dominio2.com.br   OK
  dominio3.com.br   OK

Restrição de envio por usuário

Depois de criar os arquivos é necessário rodar os comandos:

postmap /etc/postfix/usuarios_restritos
postmap /etc/postfix/dominios_restritos
postfix reload

Outros comandos

• Todos os e-mails que chegam irão para e-mail abaixo
always_bcc = email@meudominio.com.br

• Tamanho da mensagem de erro
bounce_size_limit = 50000

• Tamanho máximo do HEADER aceito
header_size_limit = 102400

• Entrega de e-mails para mesmo destino
smtp_destination_concurrency_limit = 20

• Entrega de e-mails para mesmo destino - remoto
default_destination_concurrency_limit = 20

• Entrega de e-mails para mesmo destino - local
default_destination_recipient_limit = 50

Outros comandos

- Tempo de reenvio de mensagem em fila
fast_flush_refresh_time = 12h

- Tempo de deleção de mensagem em fila
fast_flush_purge_time = 1d

- Tempo de mensagem em fila
maximal_queue_lifetime = 240m

As variavéis de tempo válidas são:

s -> segundos (seconds)
m -> minutos (minutes)
h -> horas (hours)
d -> dias (days)
w -> semanas (week)

Ferramentas do Postfix

- Postalias

  Comando necessário para criar a base dos Alias. Substituto do "newaliases". O arquivo padrão dos Alias é /etc/postfix/aliases

  Ex.: postalias /etc/postfix/aliases

- Postmap

  Comando necessário para criar a base hash. Substituto do "makemap".

  Ex.: postmap /etc/postfix/access

- Postlog

  Utilizado para enviar logs, muito útil em scripts

  Ex: postlog -p (info|warn|error|fatal|panic) -t Titulo "Texto"

Ferramentas do Postfix

- Postcat

  Comando para ler o conteúdo de e-mail quando estiver na fila. Digita-se "mailq" e através da coluna "Queue ID" obtêm os dados.

-Queue ID- -Size- -Arrival Time- -Sender/Recipient-
A44BD17D18* 359 Wed Feb 25 22:32:24 root@meudominio.com.br
joazinho@seila.com.br

35C2317D13 359 Wed Feb 25 22:29:03 root@meudominio.com.br
(Name service error for name=seila.com.br type=MX: Host not found, try again)
joazinho@seila.com.br
-- 1 Kbytes in 2 Requests.

Ex: postcat /var/spool/postfix/active/A/A44BD17D18
Ex: postcat /var/spool/postfix/deferred/3/35C2317D13

Ferramentas do Postfix

- Postconf

  Ferramenta de configuração do Postfix. Modifica o arquivo /etc/postfix/main.cf. Alguns parâmetros:

  postconf (Mostra todas os parâmetros)
  postconf -n (Mostra os parâmetros não padrão)
  postconf -e parametro=valor (Adiciona no final)

- Postsuper

  Ferramenta de manutenção da fila do Postfix

  Deletando e-mail especifico da Fila:
  postsuper -d 35C2317D13

  Deletando todos os e-mails da Fila:
  postsuper -d ALL

Ferramentas do Postfix

- Postfix (start|stop|reload|abort|flush|check)

Start -> Inicia Postfix
Stop -> Para Postfix
Reload -> Rele as configurações
Abort -> Para o Postfix no ato
Flush -> Força o reenvio dos e-mails na fila
Check -> Verifica Sintaxe dos arquivos

Scripts

```
#!/bin/bash
nice -n -20 mailq | grep $1 | awk {'print
$1'} | cut -f1 -d '*' > lista

while read line
    do
        `postsuper -d $line`
    done < ./lista
```

Utilização: ./script texto

Contato

- Através do site ou e-mail

http://web.onda.com.br/humberto

humberto@onda.com.br