

# Click21 - Embratel

## um caso de sucesso

**Marco Antonio P D'Andrade**  
mda@click21.com.br



## Apresentação

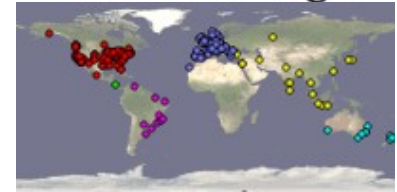
**Marco Antonio P D´Andrade**

- ★Auto-didata
- ★Atual lider do grupo Rio Perl Mongers
- ★Atuando desde 2001 na Gerencia de Servidores Internet da Embratel, sendo que nos ultimos 2 anos focado no desenvolvimento de ferramentas para aprovisionamento de serviços.
- ★Represento o grupo de usuarios de Perl do Rio de Janeiro

**As informações aqui prestadas de responsabilidade pessoal, baseado em experiências e opiniões próprias.**

***Não representam a posição ou opinião da Embratel ou Click21 e não vinculam a imagem destas empresas com o grupo que participo.***

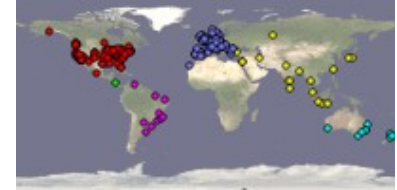
## Motivação pessoal



Trabalho com programação desde 89, quando tive contato com programação em Cobol e Clipper, as quais aprendi por cartões de referencia, pois não dispunha de outras fontes de informações.

Até 93 havia reunido e desenvolvido uma extensa biblioteca de funções em Clipper, através troca de necessidades e soluções com um grupo de 4 amigos, que por varios meses foi motivo de muito orgulho, porém como ela não foi compartilhada, a partir de 96, acabou sendo esquecida em um disquete, sem nenhum novo uso desde então.

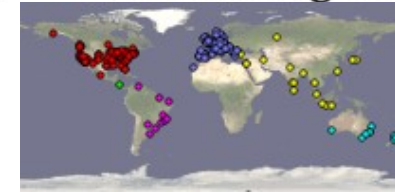
# Objetivos



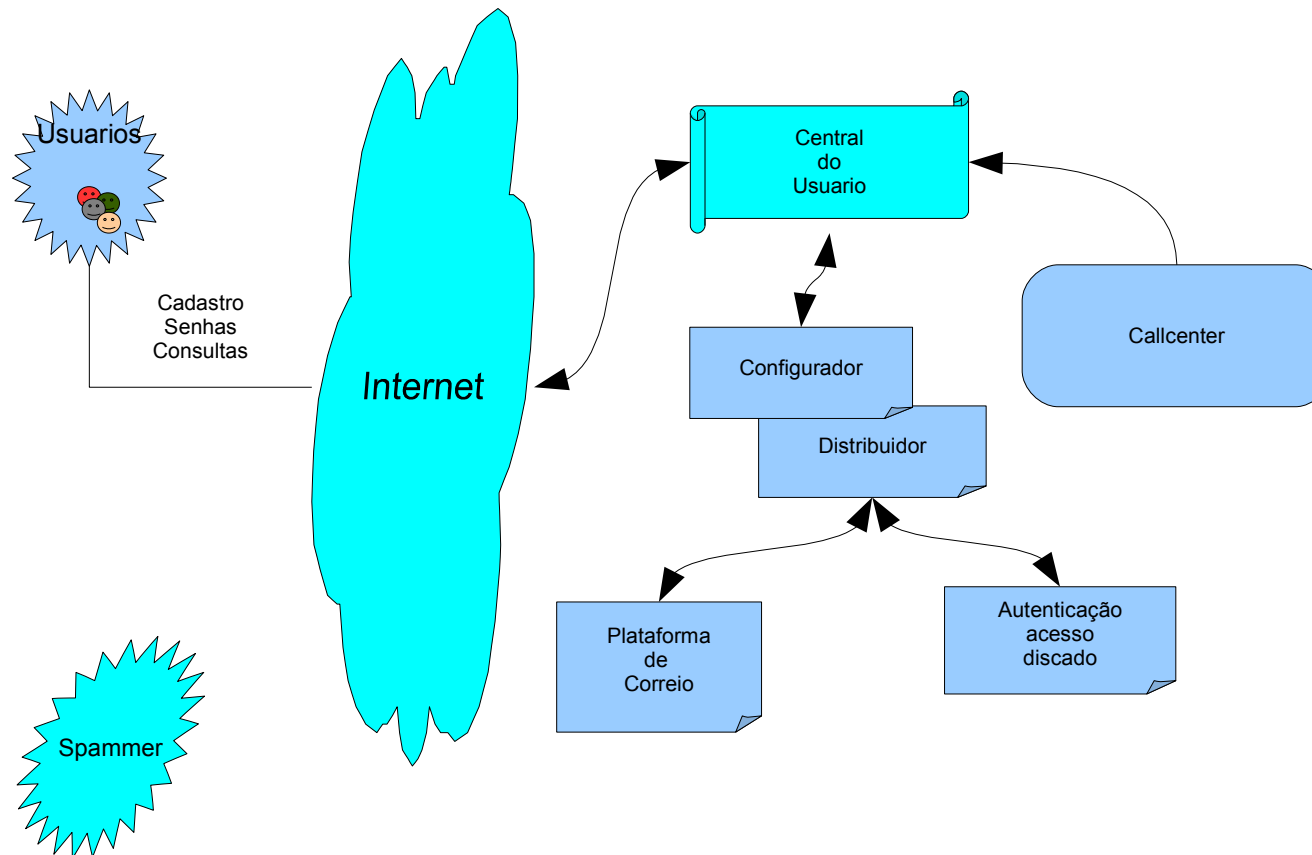
Apresentar alguns aspectos técnicos, dificuldades e soluções utilizadas no projeto Click21, focadas nos projetos em que estive envolvido.

## Ferramentas a serem apresentadas

- **Configurador** – provisionamento de usuarios
- **MailFlow** – defesa contra abusos no serviço
- **Mailgraph** – ferramenta utilizada para gerenciar fluxo de mensagens



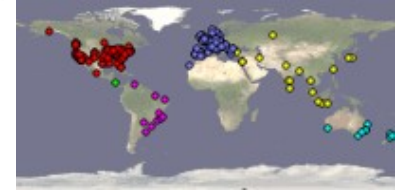
## Configurador – provisionamento de usuarios



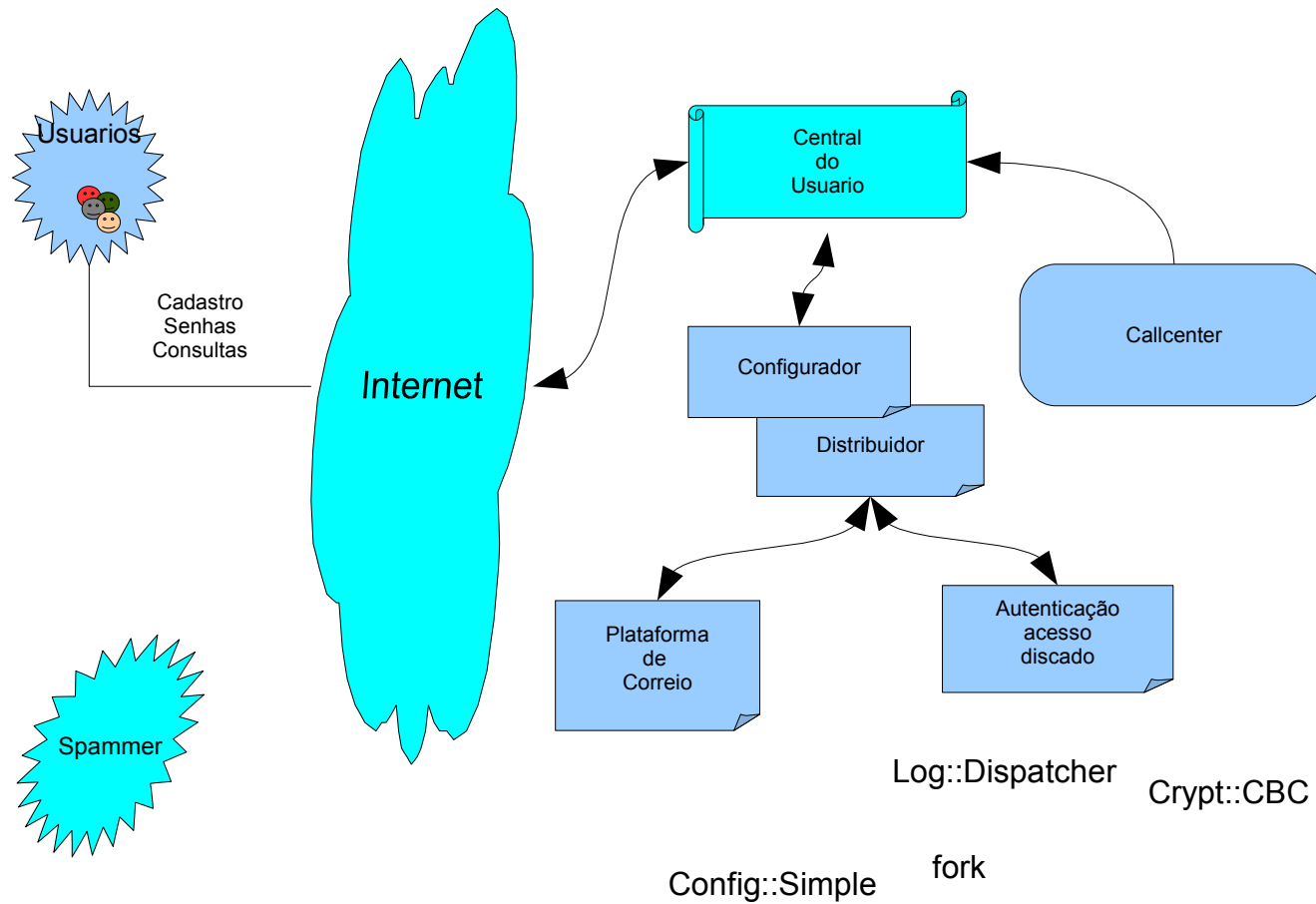
Configurador  
Desenvolvido em Perl,  
utilizando módulos já  
disponíveis com  
customização mínima,  
focando na solução.

Em uso desde 2003

Facilidade na  
implementação de novas  
requisições



# Configurador – provisionamento de usuarios

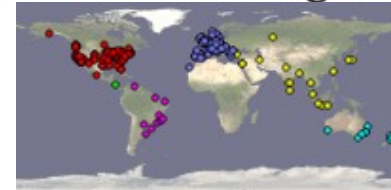


Configurador  
 Desenvolvido em Perl,  
 utilizando módulos já  
 disponíveis com  
 customização mínima,  
 focando na solução.

Em uso desde 2003

Facilidade na  
 implementação de novas  
 requisições

## MailFlow – defesa contra abusos no serviço



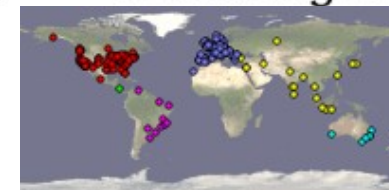
Ferramenta desenvolvida internamente, a partir do processamento de Logs de correio, focado no bloqueio de abusos identificáveis, sempre buscando manter o serviço inalterado para os usuários.

A tática foi automatizar acessos a identificação de padrões de envio de mensagens indesejadas

Processa em média 5GB de logs de SMTP diariamente, próximo a 20 milhões de linhas

O bloqueio de abusos de spammers, foi uma das técnicas empregadas para a redução do número de mensagens de spam recebidas

# MailFlow



## Defesa contra abusos no serviço

Aug 4 08:28:49 mail1 postfix/smtpd[13109]: 46E0BAB8E5: client=mail.viatrafego.com.br[207.44.182.69]  
Aug 4 08:28:50 mail1 postfix/cleanup[11111]: 46E0BAB8E5: message-id=<20050804132547.B53974BB2ED@mail.viatrafego.com.br>  
Aug 4 08:28:50 mail1 postfix/qmgr[28827]: 46E0BAB8E5: from=<informativo@affinato120.com.br>, size=10127, nrcpt=1 (queue active)  
Aug 4 08:28:51 mail1 postfix/virus-filter[23105]: 46E0BAB8E5: crm=SPAM Sender=informativo@affinato120.com.br cid=0 rcpts=1 data=-6.2877  
file=none, size=10004  
Aug 4 08:28:51 mail1 postfix/pickup[21271]: 8BFA4ABD14: uid=501 from=<informativo@affinato120.com.br>  
Aug 4 08:28:51 mail1 postfix/cleanup[22078]: 8BFA4ABD14: message-id=<20050804132547.B53974BB2ED@mail.viatrafego.com.br>  
Aug 4 08:28:51 mail1 postfix/pipe[20218]: 46E0BAB8E5: to=<lbordignonn@click21.com.br>, relay=clamav, delay=2, status=sent (dummy)  
Aug 4 08:28:51 mail1 postfix/qmgr[28827]: 46E0BAB8E5: removed

Aug 4 08:10:59 mail1 postfix/smtpd[14428]: 7409CAC637: client=unknown[200.206.214.11], sasl\_method=LOGIN, sasl\_username=calei70@click21.com.br, status=sent (click21.com.br) (queue active)

Aug 4 08:10:59 mail1 postfix/cleanup[17710]: 7409CAC637: message-id=<20050804111059.7409CAC637@mail1.click21.com.br>

Aug 4 08:11:00 mail1 postfix/qmgr[28827]: 7409CAC637: from=<calei70@click21.com.br>, size=427, nrcpt=1 (queue active)

Aug 4 08:11:52 mail1 postfix/virus-filter[31436]: 7409CAC637: crm=GOOD Sender=calei70@click21.com.br cid=1276766 rcpts=1 data=-2.5487 size=4

53

Aug 4 08:11:53 mail1 postfix/pickup[31404]: 408B3AB70B: uid=501 from=<calei70@click21.com.br>

Aug 4 08:11:53 mail1 postfix/cleanup[24503]: 408B3AB70B: message-id=<20050804111059.7409CAC637@mail1.click21.com.br>

Aug 4 08:11:53 mail1 postfix/qmgr[28827]: 408B3AB70B: from=<calei70@click21.com.br>, size=544, nrcpt=1 (queue active)

Aug 4 08:11:53 mail1 postfix/pipe[29717]: 7409CAC637: to=<criolo70@gmail.com>, relay=clamav, delay=54, status=sent (dummy)

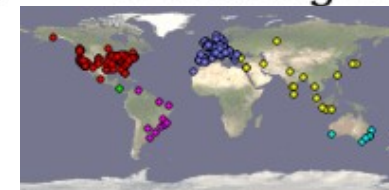
Aug 4 08:11:53 mail1 postfix/qmgr[28827]: 7409CAC637: removed

Aug 4 08:11:54 mail1 postfix/smtp[10920]: 408B3AB70B: to=<criolo70@gmail.com>, relay=gmail-smtp-in.l.google.com[64.233.185.27], delay=1, sta

tus=sent (250 2.0.0 OK 1123153914 34si554517wra)

Aug 4 08:11:54 mail1 postfix/qmgr[28827]: 408B3AB70B: removed

# MailFlow



## Defesa contra abusos no serviço

```
# UNKNOWN LOCAL
if ( $t =~ /User unknown in local recipient table/ ) {
    $QU->add_reject( time => $time, ip=> $ip, id => 'local', );

# RATE LIMIT
} elsif ( $t =~ /Sender address rejected: message rate/ ) {
    $QU->add_reject( time => $time, ip=> $ip, id => 'rate', );

# DOMAIN NOT FOUND
} elsif ( $t =~ /Sender address rejected: Domain not/ ) {
    $QU->add_reject( time => $time, ip=> $ip, id => 'domain', );

# ENVIO SEM LOGIN
} elsif ( $t =~ /not logged in/ ) {
    $QU->add_reject( time => $time, ip=> $ip, id => 'not_logged', );

# TENTOU OUTRO USER (spammer incompetente!)
} elsif ( $t =~ /not owned/ ) {
    $QU->add_reject( time => $time, ip=> $ip, id => 'not_owned', );

# * SENDER
} elsif ( $t =~ /Sender address rejected:/ ) {
    if ( $t =~ /spf.pobox/ ) {
        $QU->add_reject( time => $time, ip=> $ip, id => 'spf', );
    } elsif ( $t =~ /Access denied/ ) {
        $QU->add_reject( time => $time, ip=> $ip, id => 'sender:denied', );
    } else {
        $QU->add_reject( time => $time, ip=> $ip, id => 'sender*', );
    }
}

# RELAY NEGADO
```

```
Aug 4 08:10:5
sasl_extern
br
Aug 4 08:10:5
Aug 4 08:11:0
Aug 4 08:11:5
2.5487 size=4
53
Aug 4 08:11:5
Aug 4 08:11:5
Aug 4 08:11:5
Aug 4 08:11:5
Aug 4 08:11:5
Aug 4 08:11:5
delay=1, sta
tus=sent (250 2.0.0 OK 1123153914 34si55451/wra)
Aug 4 08:11:54 mail1 postfix/qmgr[28827]: 408B3AB70B: removed
```

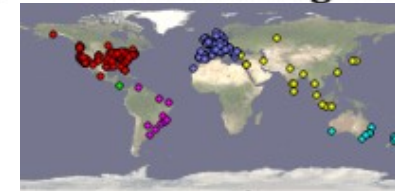
```
viatrafego.com.br>
rcpt=1 (queue active)
cid=0 rcpts=1 data=-6.2877
```

```
viatrafego.com.br>
status=sent (dummy)
```

```
1 (queue active)
us=sent (click21.com.br)
```

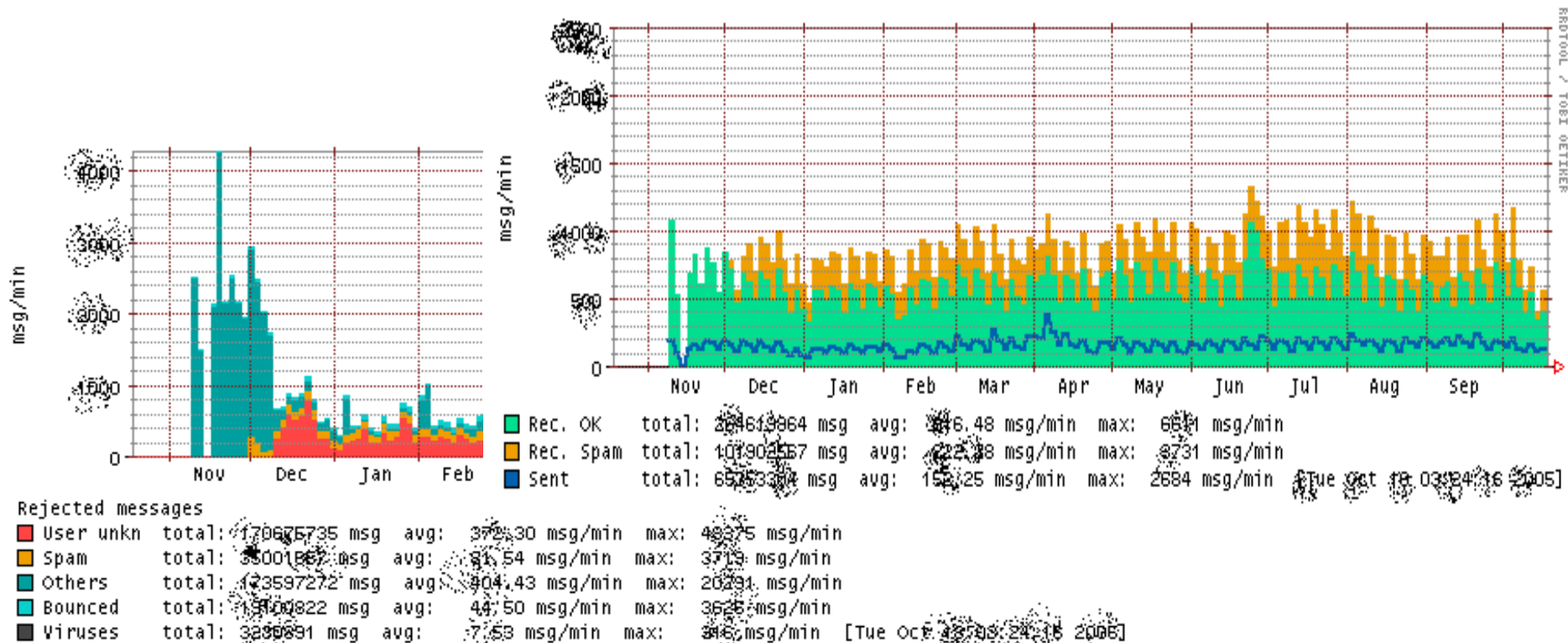


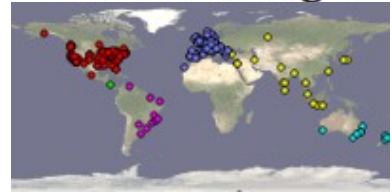
# Mailgraph



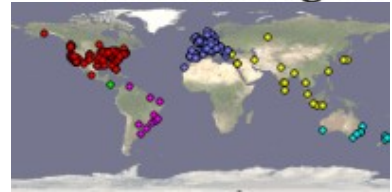
## Ferramenta utilizada para gerenciar fluxo de mensagens

Apesar de não haver tempo para detalhar, acredito que não seria justo não destacar esta ferramenta como um sensor de efeito das medidas



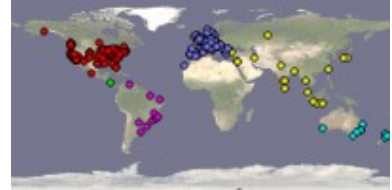


**Duvidas**



**F I M . . .**

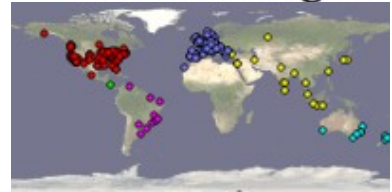
Mas novos projetos e idéias estão a caminho



**F I M . .**

Os comportamentos de uso de smtp estão mudando !!

Se até vermes evoluem  
porque não os spammers ??



**F I M . .**

Os comportamentos de uso de smtp estão mudando !!

**Se até vermes evoluem  
porque não os spammers ??**