



nie.br

Núcleo de Informação
e Coordenação do
Ponto BR

cgi.br

Comitê Gestor da
Internet no Brasil

registro.br cert.br cetic.br ceptro.br ptt.br ceweb.br



IMPLANTAÇÃO DE RDAP NO REGISTRO.BR

Frederico Neves
Rafael Dantas Justo



nic.br

WHOIS DEFINIÇÃO

WHOIS DEFINIÇÃO

- Criado em 1982 (usuários ARPANET)

WHOIS DEFINIÇÃO

- Criado em 1982 (usuários ARPANET)
- Protocolo texto simples (chave e valor), feito para **humanos**

WHOIS DEFINIÇÃO

- Criado em 1982 (usuários ARPANET)
- Protocolo texto simples (chave e valor), feito para **humanos**
- Serviço de diretórios para obter informações de contato

whois -h whois.registro.br registro.br

```
domain:      registro.br
owner:       Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:     005.506.560/0001-36
responsible: Demi Getschko
country:     BR
owner-c:     FAN
admin-c:     FAN
tech-c:      FAN
billing-c:   FAN
nserver:     a.dns.br
nsstat:      20151201 AA
nslastaa:    20151201
nserver:     b.dns.br
nsstat:      20151201 AA
nslastaa:    20151201
nserver:     c.dns.br
nsstat:      20151201 AA
nslastaa:    20151201
```

whois -h whois.registro.br 200.160.0.0/20

```
inetnum:      200.160.0/20
aut-num:      AS22548
abuse-c:      FAN
owner:        Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:      005.506.560/0001-36
responsible:  Demi Getschko
country:      BR
owner-c:      FAN
tech-c:       FAN
inetrev:      200.160.0/20
nserver:      a.dns.br
nsstat:       20151201 AA
nslastaa:     20151201
nserver:      b.dns.br
nsstat:       20151201 AA
nslastaa:     20151201
nserver:      c.dns.br
nsstat:       20151201 AA
nslastaa:     20151201
```


whois -h whois.registro.br 22548

```
aut-num:      AS22548
owner:        Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:      005.506.560/0001-36
responsible:  Demi Getschko
country:      BR
owner-c:      FAN
routing-c:    FAN
abuse-c:      FAN
created:      20011016
changed:      20130306
inetnum:      200.160.0/20
inetnum:      2001:12ff::/32
as-in:        from AS3549 100 accept ANY
as-in:        from AS16735 100 accept ANY
as-out:       to AS3549 announce AS22548
as-out:       to AS16735 announce AS22548
```

whois -h whois.registro.br P1

```
provider:      NICBR (1)
providern:     Núcleo de Informação e Coordenação do Ponto BR
providerid:    005.506.560/0001-36
responsible:   Frederico A C Neves
css-email:     hostmaster@registro.br
css-website:   http://registro.br/
css-phone:     11 55093500
provider-c:    FAN
created:       20060623
changed:       20130516

nic-hdl-br:    FAN
person:        Frederico Augusto de Carvalho Neves
e-mail:        fneves@registro.br
created:       19971217
changed:       20150803
```

whois -h whois.registro.br FAN

```
nic-hdl-br:  FAN  
person:      Frederico Augusto de Carvalho Neves  
created:     19971217  
changed:     20150803
```

WHOIS UTILIDADES

- Identificar um phishing
- Entrar em contato com responsáveis
- Geração dos relatórios dos CERTs

Problema 1: Nome dos campos

```
# whois 173.194.118.110
OrgName:      Google Inc.
OrgId:        GOGI
Address:      1600 Amphitheatre Parkway
City:         Mountain View
StateProv:    CA
PostalCode:   94043
Country:      US
```

```
# whois 200.160.2.3
owner:        Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:      005.506.560/0001-36
responsible:  Demi Getschko
country:      BR
```

Problema 2: Encoding

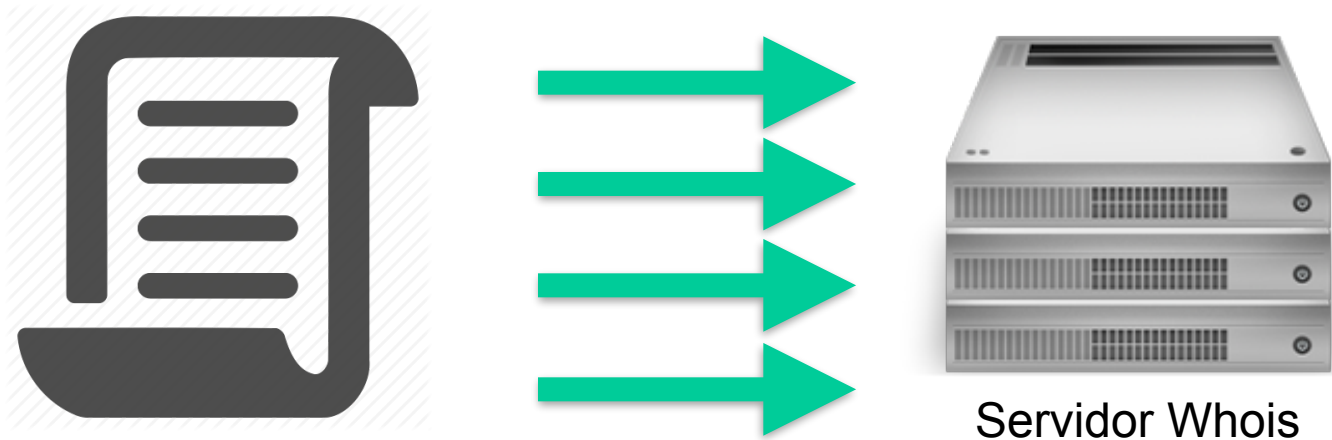
UTF-8

```
# whois 200.160.2.3
owner:      N?cleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:    005.506.560/0001-36
responsible: Demi Getschko
country:    BR
```

ISO-8859-1

```
# whois 200.160.2.3
owner:      Núcleo de Inf. e Coord. do Ponto BR - NIC.BR
ownerid:    005.506.560/0001-36
responsible: Demi Getschko
country:    BR
```

Problema 3: Rate Limit



Acesso condicionado exclusivamente ao endereço de origem da consulta

Problema 4: Quem consultar?



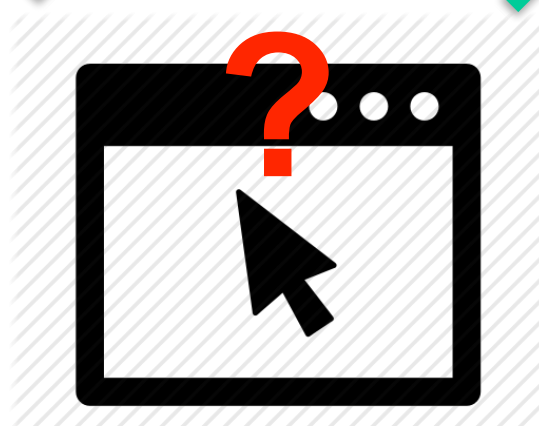
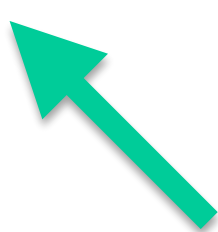
Servidor Whois



Servidor Whois



Servidor Whois



Problema 4: Quem consultar?

IANA Whois

```
# whois -h whois.iana.org exemplo.com.br  
refer:          whois.registro.br  
  
domain:         BR
```

DNS

```
# dig +short br.whois-servers.net  
whois.nic.br.  
registro.br.  
200.160.2.3
```



<http://github.com/whois-server-list/whois-server-list>

WHOIS PROBLEMAS

- Falta de padronização

Nome e semântica dos campos, encoding e busca de servidores
(bootstrap)

- Autenticação

Permitir "rate limit" diferenciado para clientes autenticados

TENTATIVAS IRIS (2005)

Internet Registry Information Service

- RFC 3981 - 3983; RFC 4992
- Solução utilizando XML
- Complexo (transporte beep/xpc, schemas, namespaces, ...)
- Cliente dedicado
- Não compensava o investimento

```
<domain
  authority="iana.org" registryType="dregl"
  entityClass="domain-handle" entityName="example-com-1">
  <domainName>example.com</domainName>
  <domainHandle>tcs-com-1</domainHandle>
  <nameServer
    iris:referentType="host"
    authority="iana.org" registryType="dregl"
    entityClass="host-handle" entityName="research7" />
  <nameServer
    iris:referentType="host"
    authority="iana.org" registryType="dregl"
    entityClass="host-handle" entityName="nsoll84" />
  iris:referentType="registrationAuthority"
  authority="com"
  registryType="dregl"
  entityClass="contact-handle"
  entityName="VGRS" />
</registrat
  iris:referentType="registrationAuthority"
  authority="iana.org" registryType="dregl"
  entityClass="contact-handle" entityName="dbarton" />
</domain>
```

IETF WEIRDS (2013)

- **Objetivo:** Criar um substituto simples para o WHOIS
- Inspirado nas soluções do IRIS e nos serviços RESTful

WHOIS do ARIN

RDAP

Registration **D**ata **A**ccess **P**rotocol

2015

RDAP

CARACTERÍSTICAS

- RFC 7480 - 7485
- Padronização (nome e semântica dos campos e bootstrap)
- Interface REST (HTTP/HTTPS)
- Content-Type: application/rdap+**JSON**
- Autenticação
- Extensões!

RDAP INTERFACE REST

- Utiliza o protocolo HTTP para executar ações nos recursos
- Suporte a múltiplos idiomas
(Accept-Language)
- Suporte a múltiplos encodings
(Accept-Charset)
- Redirecionamentos
Cabeçalho HTTP Location e códigos 3xx
- Stateless

RDAP INTERFACE REST

Recurso	URI	Exemplo
Domínio	/domain/<FQDN>	/domain/registro.br
Titularidade, Provedor, Usuário	/entity/<ID>	/entity/05506560000136 /entity/P1 /entity/FAN
Autonomous System	/autnum/<ASN>	/autnum/22548
Bloco IP	/ip/<ip> /ip/<ip>/<cidr>	/ip/200.160.2.3 /ip/200.160.0.0/20
Ajuda	/help	

RDAP AUTENTICAÇÃO

- Acesso condicionado padronizado
- Autenticação HTTP básica ou por digest
RFC 7235
- Certificado TLS X.509
- Autenticação Federada (draft RDAP OpenID)
Mesma autenticação para múltiplos servidores RDAP

RDAP JSON

<https://rdap.registro.br/domain/nic.br>

```
{
  "objectClassName": "domain",
  "handle": "nic.br",
  "ldhName": "nic.br",
  "nameservers": [
    {
      "objectClassName": "nameserver",
      "ldhName": "a.dns.br",
    },
    {
      "objectClassName": "nameserver",
      "ldhName": "b.dns.br",
    },
  ],
  ...
}
```

RDAP EXTENSÕES



Extensão RDAP.br
<http://registro.br/rdap>

<https://rdap.registro.br/entity/P1>

```
{
  "objectClassName": "entity",
  "handle": "P1",
  "publicIds": [
    {
      "type": "cnpj",
      "identifier": "05.506.560/0001-36"
    }
  ],
  "nicbr_customerSupportService": {
    "nicbr_email": "hostmaster@registro.br",
    "nicbr_website": "http://registro.br/",
    "nicbr_phone": "11 55093500"
  },
  ...
}
```

RDAP BOOTSTRAP



IANA Server

Client



RDAP BOOTSTRAP

exemplo.com.br?

Client



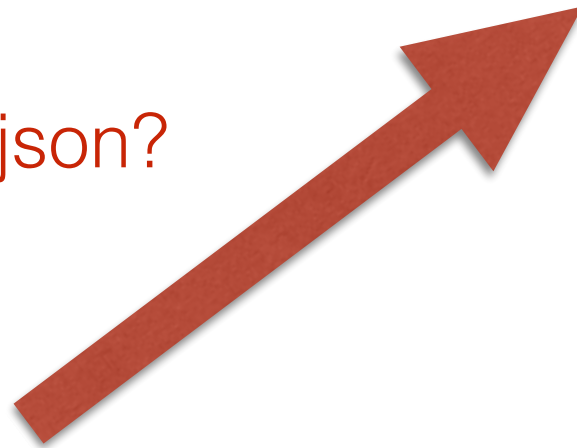
IANA Server

RDAP BOOTSTRAP

dns.json?

IANA Server

Client



RDAP BOOTSTRAP

```
{
  "description": "RDAP bootstrap file for Domain Name System registrations",
  "publication": "2015-12-04T00:09:31Z",
  "services": [
    [
      [
        "br"
      ],
      [
        "https://rdap.registro.br/"
      ]
    ]
  ]
}
```

IANA Server

Client



RDAP BOOTSTRAP



IANA Server

Client



RDAP Brasil



RDAP ADOÇÃO

- NIC.br
<https://rdap.registro.br>
- APNIC
<https://rdap.apnic.net>
- ARIN
<https://rdap.arin.net/registry>
- LACNIC
<https://rdap.lacnic.net/rdap>
- NIC.cz
<https://rdap.nic.cz>

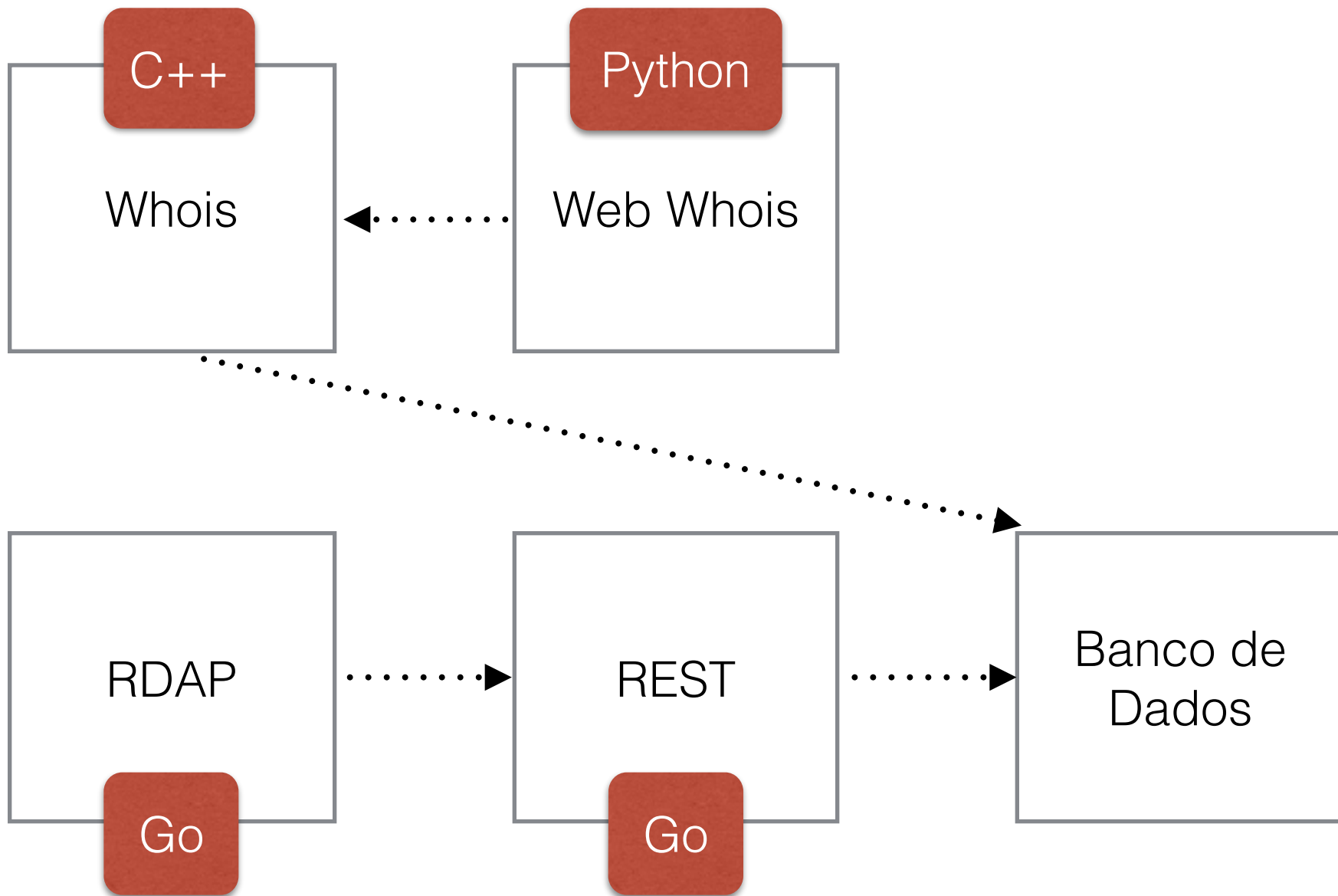
RDAP CLIENTES

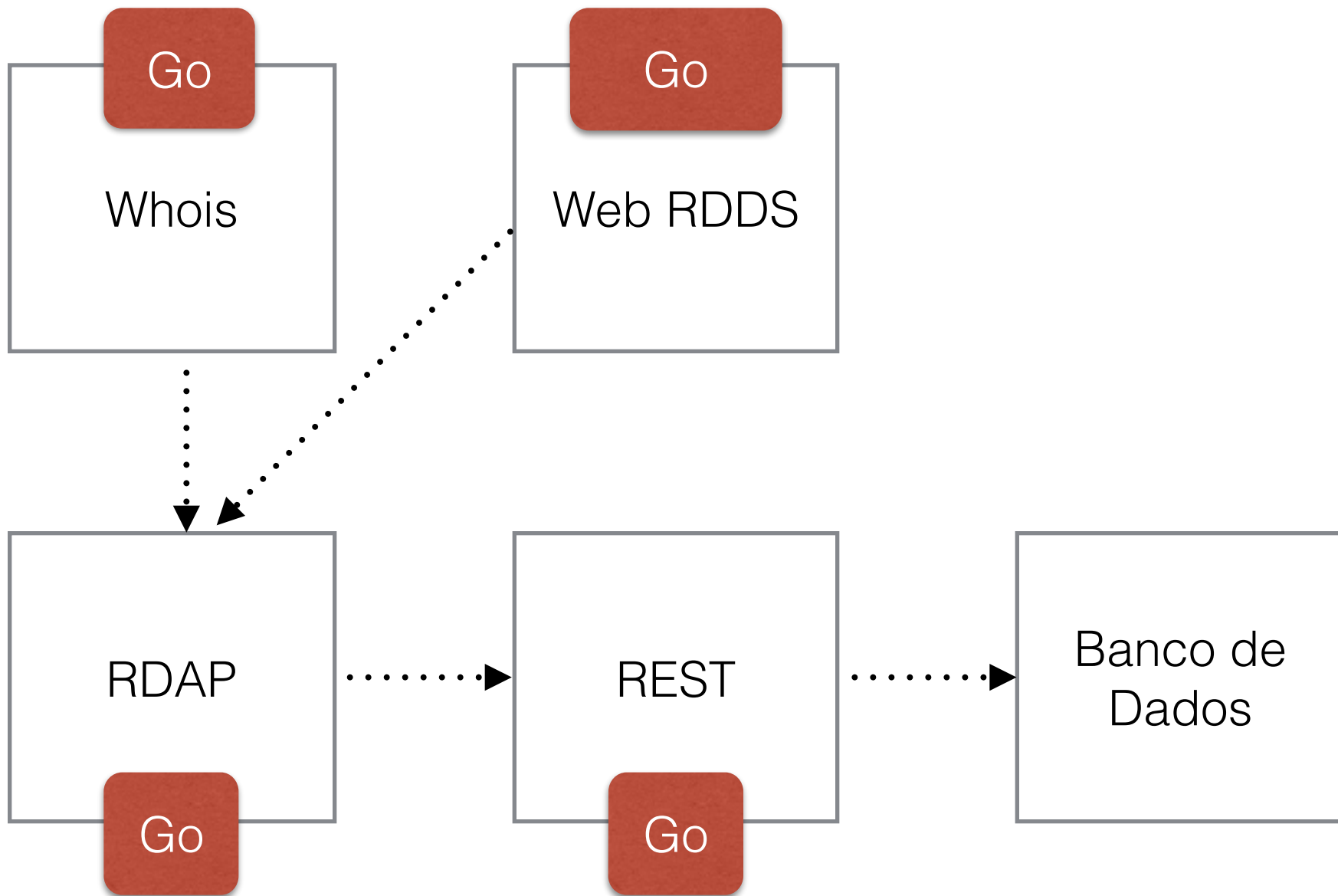
- <https://github.com/arineng/nicinfo> (Ruby)
- <https://github.com/gitpan/rdapper> (Perl)
- <https://github.com/cnnic/rdap> (Java)
- <https://github.com/DNSBelgium/rdap> (Java)
- <https://github.com/registrobr/rdap-client> (Go)

RDAP BIBLIOTECAS

- <https://github.com/arineng/nicinfo> (Ruby)
- <https://github.com/gitpan/rdapper> (Perl)
- <https://github.com/cnnic/rdap> (Java)
- <https://github.com/DNSBelgium/rdap> (Java)
- <https://github.com/registrobr/rdap-client> (Go)

Arquitetura RDAP .br





Obrigado

www.registro.br

 fneves@registro.br

10 de Dezembro de 2015

nic.br **cgi.br**

www.nic.br | www.cgi.br