RDAP: O novo protocolo de WHOIS

Darío Gómez, dario @ lacnic.net

O Que é o WHOIS?

- Ferramenta de pesquisa na base de dados dos registros de internet
  - Blocos IPv4 e IPv6
  - Sistemas Autônomos
  - Pontos de Contato
  - Organizações
- Protocolo definido pela RFC 3912 (Set. 2004)
- Serviço histórico dos registros de Internet e nomes de domínio
- Protocolo de visualização dá informação

lacnic

Importância do WHOIS

- Serviço fundamental dos registros regionais e nacionais
- CERTs – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
- Fonte de informação para organizações e pessoas
- Automatização de sistemas

Como funciona o WHOIS?

- Esquema simples de pergunta/resposta
- Baseado no protocolo TCP/IP (Porta 43)
- Diferentes formatos de resposta
- Projeto Joint Whois
- Cliente Linha de comandos o web

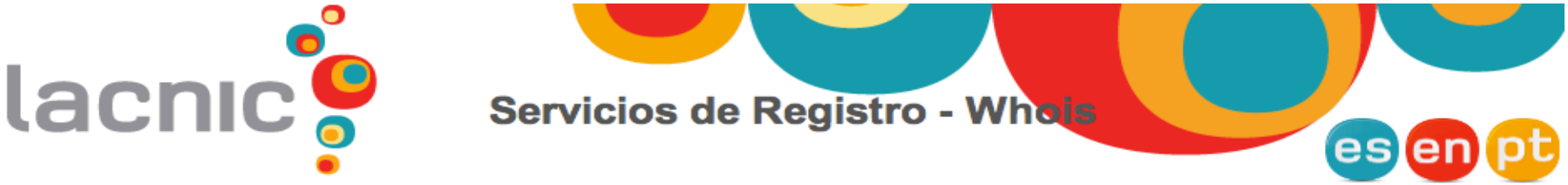
```
client                                server at whois.nic.mil

open TCP    ---- (SYN) ------------------------------>
            <---- (SYN+ACK) -------------------------
send query  ---- "Smith<CR><LF>" -------------------->
get answer  <---- "Info about Smith<CR><LF>" ---------
            <---- "More info about Smith<CR><LF>" ----
close       <---- (FIN) ------------------------------
            ----- (FIN) ------------------------------>
```

Como funciona o WHOIS?

```
BR-MacBook:~ dariogomez$ whois -h whois.lacnic.net DAG16
 % LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2013-05-20 12:43:48 (BRT -03:00)

nic-hdl:     DAG16
person:      Dar?o G?mez
e-mail:      dario@LACNIC.NET
address:     Rmbla Re?blica de M?xico, 6125,
address:     11400 - Montevideo -
country:     UY
phone:       +598  26042222 [4126]
created:     20110121
changed:     20121204

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.

BR-MacBook:~ dariogomez$
```

lacnic

Como funciona o WHOIS?



Whois

BUSCAR

```
 % LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2013-05-20 17:01:53 (BRT -03:00)

nic-hdl:     DAG16
person:      Darío Gómez
e-mail:      dario@LACNIC.NET
address:     Rmbla Reública de México, 6125,
address:     11400 - Montevideo -
country:     UY
phone:       +598  26042222 [4126]
created:     20110121
changed:     20121204

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.
```

Limitações do atual WHOIS

- Não ha um formato das respostas
- Não é possível o processamento automático
- Internacionalização dos dados
- Criação de extensões
- Serviços diferenciados
- Políticas de privacidade

Como funciona o novo RDAP?

- Serviços semânticos sobre o protocolo HTTP 1.1
- Baseado na tecnica REST
- Modelo de dados extensível das respostas
- Padronização das respostas (XML/JSON)
- Rate Limit
  - 100 querys cada 5 minutos
  - 1000 querys cada 60 minutos
- Serviço de API Keys

lacnic

Como funciona o novo RDAP?

BETA restful WHOIS

Entity

Handle	DAG16
Names	Darío Gómez
Address	Rmbla Reública de México 6125 []
City	Montevideo
Country	UY
Postal Code	11400
Emails	dario@lacnic.net
Phones	office 598 26042222 [4126]
Registration Date	20110121
Last Changed Date	20130520
Last Changed By	

lacnic

Como funciona o novo RDAP?


```
{
    "names":["Darío Gómez"],
    "roles":[""],
    "handle":"DAG16",
    "postalAddress":[
        "Rambla Rep. Mexico 6125 []",
        "Montevideo",
        "UY",
        "11600"],
    "emails":["dario@lacnic.net"],
    "phones":{
        "office":["598 2 6042222 []"],
        "fax":[],
        "mobile":[]
        },
    "remarks":[],
    "registrationDate":"20080125",
    "lastChangedDate":"20110512",
    "lastChangedBy":null,
    "entities":[],
    "links":[{
        "value":"http://restfulwhoisv2.labs.lacnic.net/entity/AIL",
        "href":"http://restfulwhoisv2.labs.lacnic.net/entity/AIL",
        "rel":"self"
        }]
}
```

```
▼<entity>
  <handle>DAG16</handle>
  <names>Darío Gómez</names>
  <roles/>
  <postalAddress>Rmbla Reública de México 6125 []</postalAddress>
  <postalAddress>Montevideo</postalAddress>
  <postalAddress>UY</postalAddress>
  <postalAddress>11400</postalAddress>
  <emails>dario@lacnic.net</emails>
 ▼<phones>
    <office>598 26042222 [4126]</office>
  </phones>
 ▼<links>
    <value>http://localhost:8080/rdap/entity/DAG16</value>
    <rel>self</rel>
    <href>http://localhost:8080/rdap/entity/DAG16</href>
  </links>
  <registrationDate>20110121</registrationDate>
  <lastChangedDate>20130520</lastChangedDate>
</entity>
```

RDAP - Processamento automático

```python
import json
import urllib2

def procesar (func, param):
    url = "http://rdap.labs.lacnic.net/rdap/" + func + "/" + param +"/"

    req = urllib2.Request(url)
    req.add_header('Accept', 'application/json')

    data = json.load(urllib2.urlopen(req))

    print "Meu nome é ",json.dumps(data['names']), " e meu email é ", json.dumps(data['emails'])
```

```
BR-MacBook:~ dariogomez$ python whois_client.py entity ail
Meu nome é  ["Arturo Servin"]  e meu email é  ["ipadmin@LACNIC.NET"]
```

lacnic

RDAP - Internacionalização

- Não ha uma especificação do jogo de caracteres
- Cada banco de dados tem o seu codificação
- Não ha uma estandardização do formato das respostas
- O grupo do IETF (WIERDS) esta trabalhando na padronização

RDAP - Internacionalização

```
BR-MacBook:~ dariogomez$ whois -h whois.lacnic.net B
 % LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purpos
%  and to assist persons in obtaining information ab
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use thi
%  only for lawful purposes.
%  2013-05-20 18:00:20 (BRT -03:00)

owner:       Comite Gestor da Internet no Brasil
ownerid:     BR-CGIN-LACNIC
responsible: Frederico A C Neves
address:     Av. das Na??es Unidas, 11541, 7? andar
address:     04578-000 - S?o Paulo - SP
country:     BR
phone:       +55 11 91190304 []
owner-c:     CGB
created:     20020902
changed:     20130309

nic-hdl:     CGB
person:      Comite Gestor da Internet no Brasil
e-mail:      blkadm@NIC.BR
address:     Av. das Na??es Unidas, 11541, 7? andar
address:     04578-000 - S?o Paulo - SP
country:     BR
phone:       +55 19 9119-0304 []
created:     20020902
changed:     20061004
```

Entity

Handle	BR-CGIN-LACNIC
Names	Comite Gestor da Internet no Brasil
Roles	registrant
Address	Av. das Na??es Unidas 11541 [7? andar]
City	S?o Paulo
Country	BR
Postal Code	04578-000
Phones	office 55 11 91190304 []
Registration Date	20020902
Last Changed Date	20130309
Last Changed By	
autnum	See related autnum
inetnum	See related inetnum

lacnic

RDAP – API Keys

- Identificar usuarios ou programas que accesam ao serviço
- Código único gerado
- Permissões de acesso a dados ou funções do serviço
- Parámetro ?apikey=axdnu123as
  - Exemplo: http://rdap.labs.lacnic.net/restfulwhois/entity/dag16?apikey=axdnu123as

RDAP – O futuro do protocolo

- Padronização definitiva das respostas
- Definição de políticas de segurança e privacidade
- Ligação com outros sistemas
  - RPKI
  - Solicitude de Recursos
  - Outros
- Melhorar a internacionalização
- Rediretor Joint Whois

Informações e Participação

- LACNIC Labs: http://labs.lacnic.net/site/restful-whois
- Weirds Working Group: http://datatracker.ietf.org/wg/weirds/charter/
- Implementação do ARIN: https://www.arin.net/resources/whoisrws/index.html
- Implementação do RIPE: https://labs.ripe.net/ripe-database/database-api/api-documentation

www.lacnic.net/pt/web/lacnic/documentos-tecnicos-whois

labs.lacnic.net/site/restful-whois

dario @ lacnic.net

@daro_ua

OBRIGADO!