

Managed DNSSEC Validation

February 2010

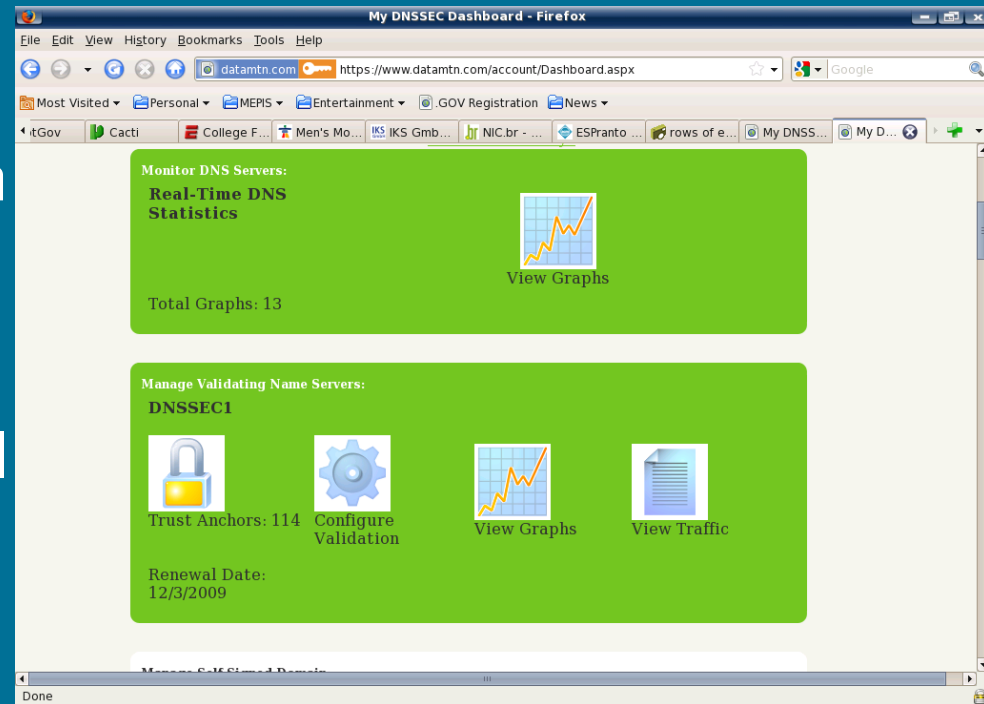
DNSSEC Validation Challenges

- Trusted Key Selection and Rotation (daily)
- 27,000+ (4,300+) signed zones now, growing to 27,000,000
- Monitor server use and validation failures
- Internal and External DNSSEC Configuration



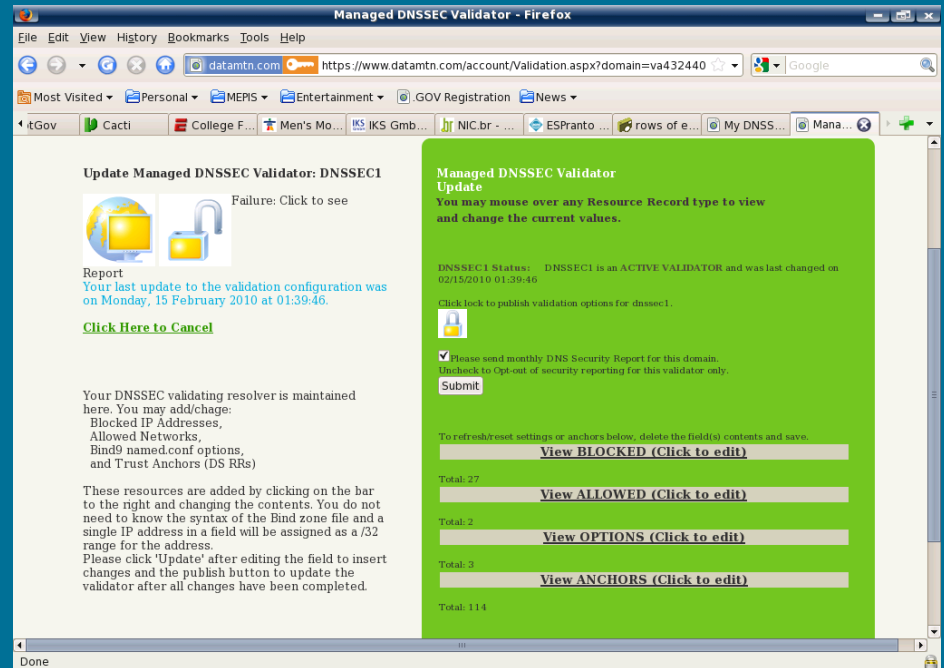
DMS – Managed DNSSEC Validation

- Hosted Validators using latest Bind9 engine
- Hardened SecureMepis HVT OS (virtual machine on Cloud Computing)
- DMS Cloud Operations Centers across USA
- Web App for Agency control
- \$45/validator/month
- GSA Schedule (credit card purchase)



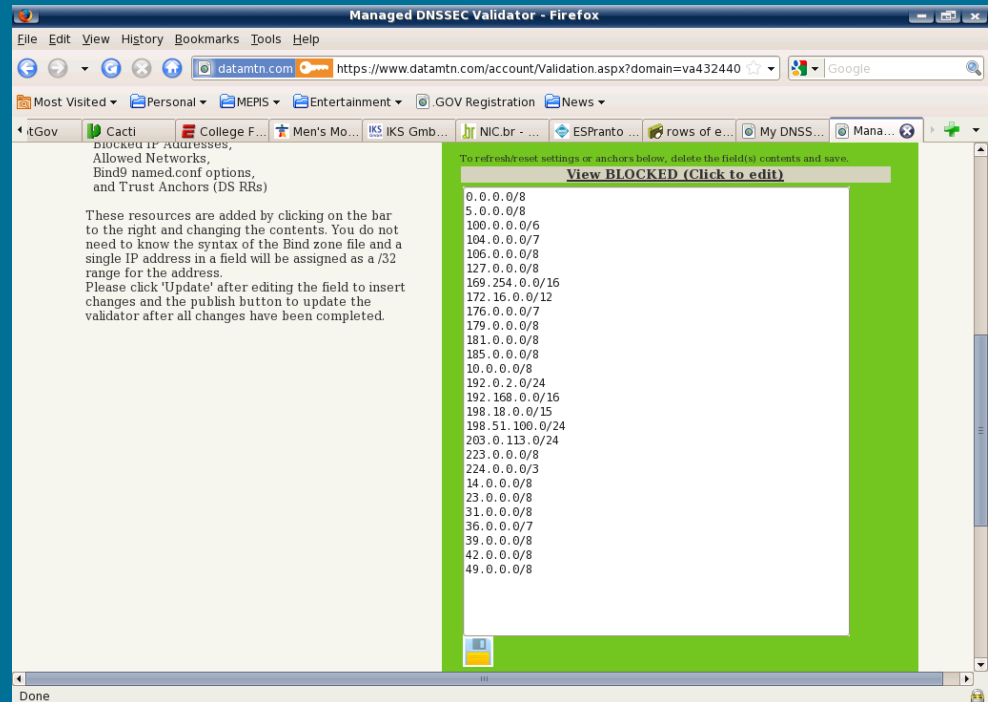
Managed Validation Control

- Test Trusted Keys
- Block unwanted networks
- Allow internal and/or external nets
- No Training required
- < 1 hour Automated Deployment



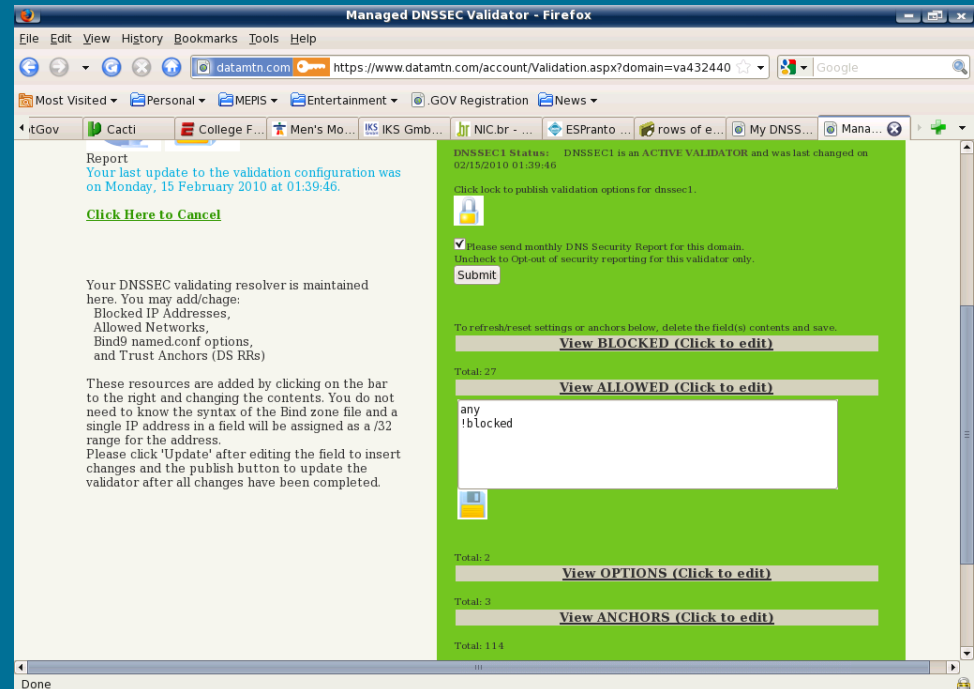
MV – Blocked Networks

- Defaults to best practices/FISMA compliance
- Dynamically update and release with single click
- SSL Web connection to Admin Console



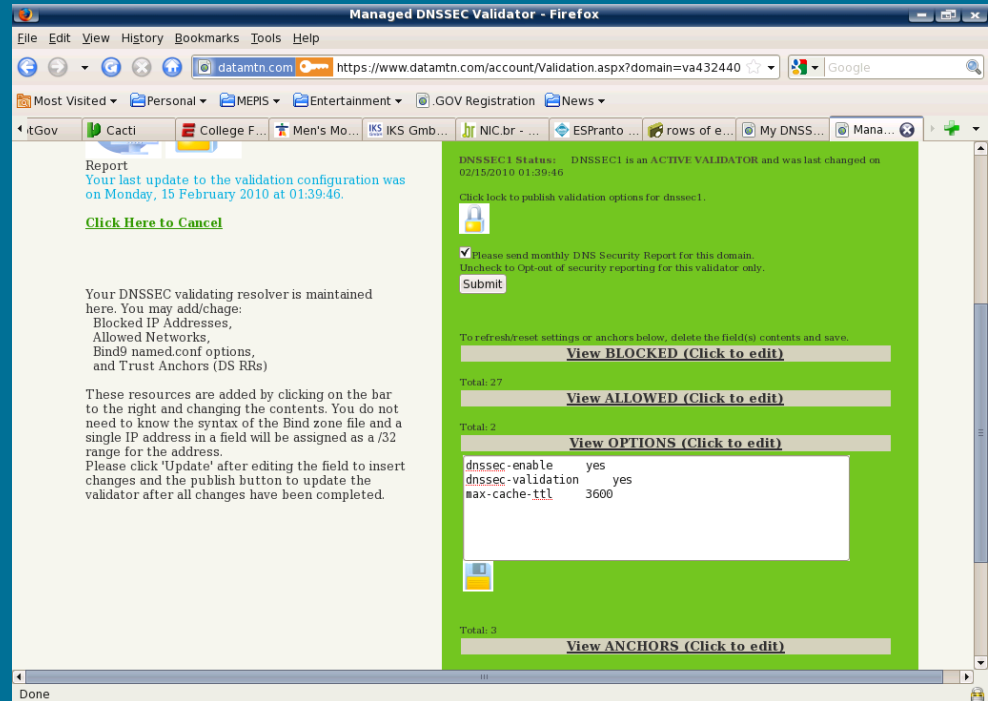
MV – Allowed Networks

- Set allowed IPs and IP ranges for validation
- Can use Agency legacy DNS servers as Forwarders
- All traffic and queries are logged and graphed
- Monthly Security Reporting for FISMA CMP is included



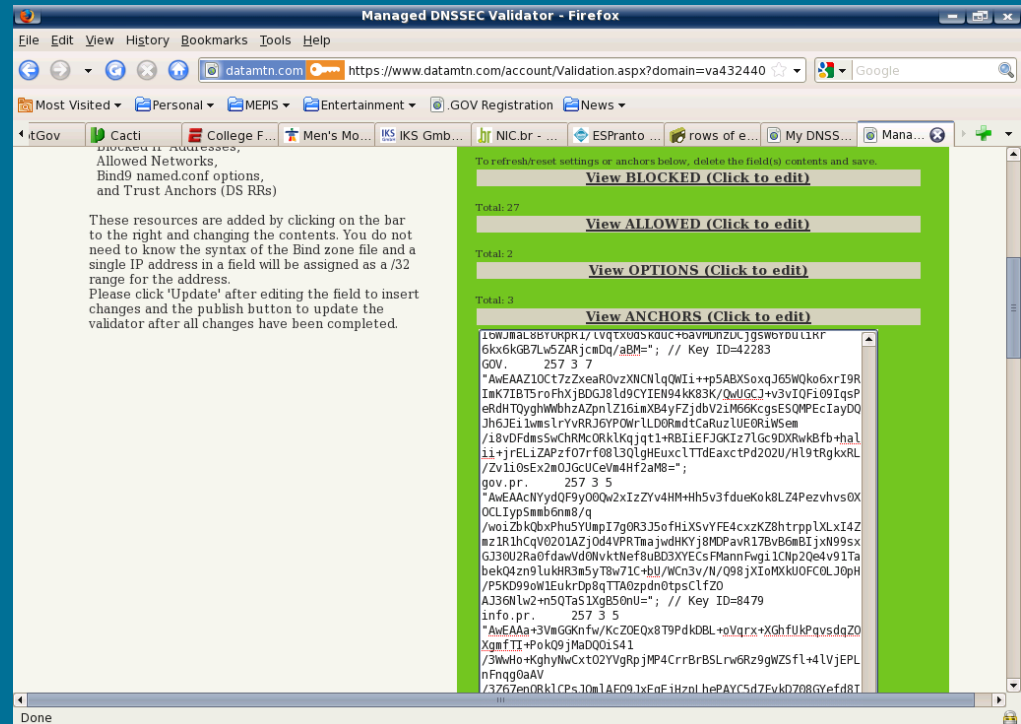
MV – Bind9 Options

- Enable/Disable DNSSEC for testing/deployment and emergency purposes
- Immediately publish and reload options with a single click
- Automated Admin Email notification of changes to DNS Security Options



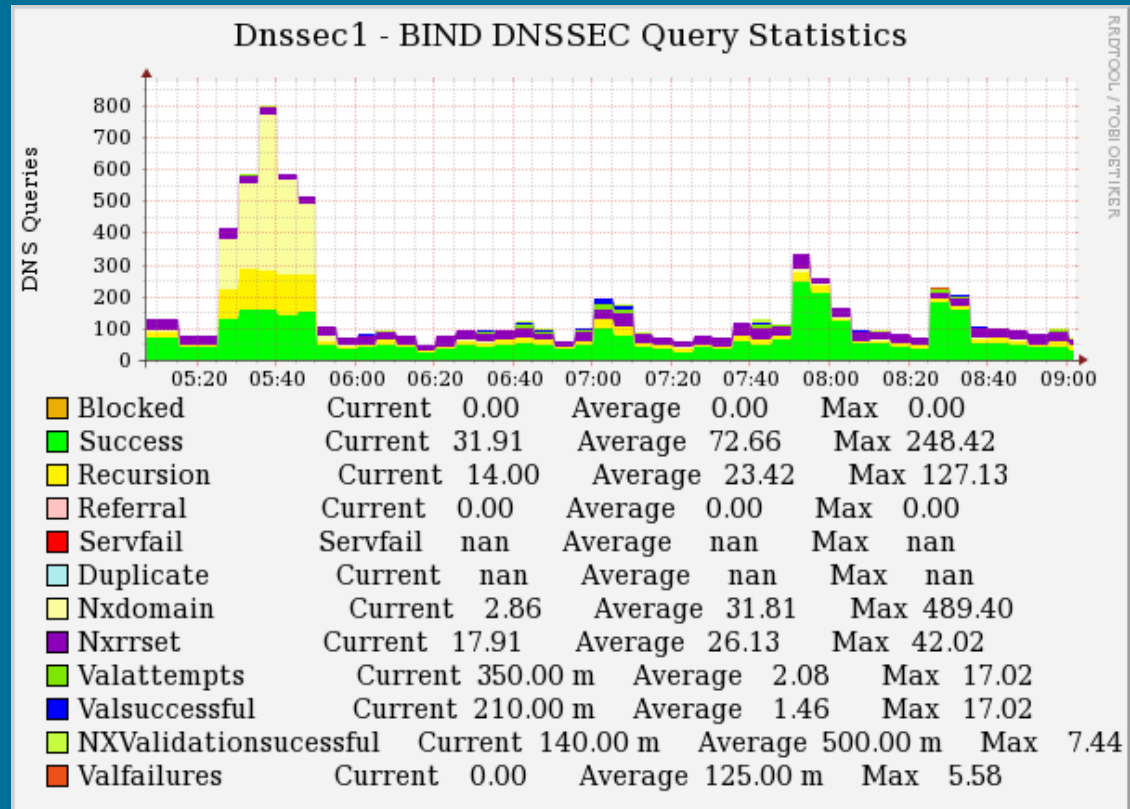
MV – Trusted Key Management

- DMS cleans and corrects broken islands
- Update to latest keysets with a single click
- Add or remove keysets desired for your organization
- 27,000 domains under DNSSEC and growing



MV – Real-Time Monitoring

- Real-time Monitor/Graphing of DNS Activity
- Private Cloud Access to Traffic and Queries



MV – Query Details

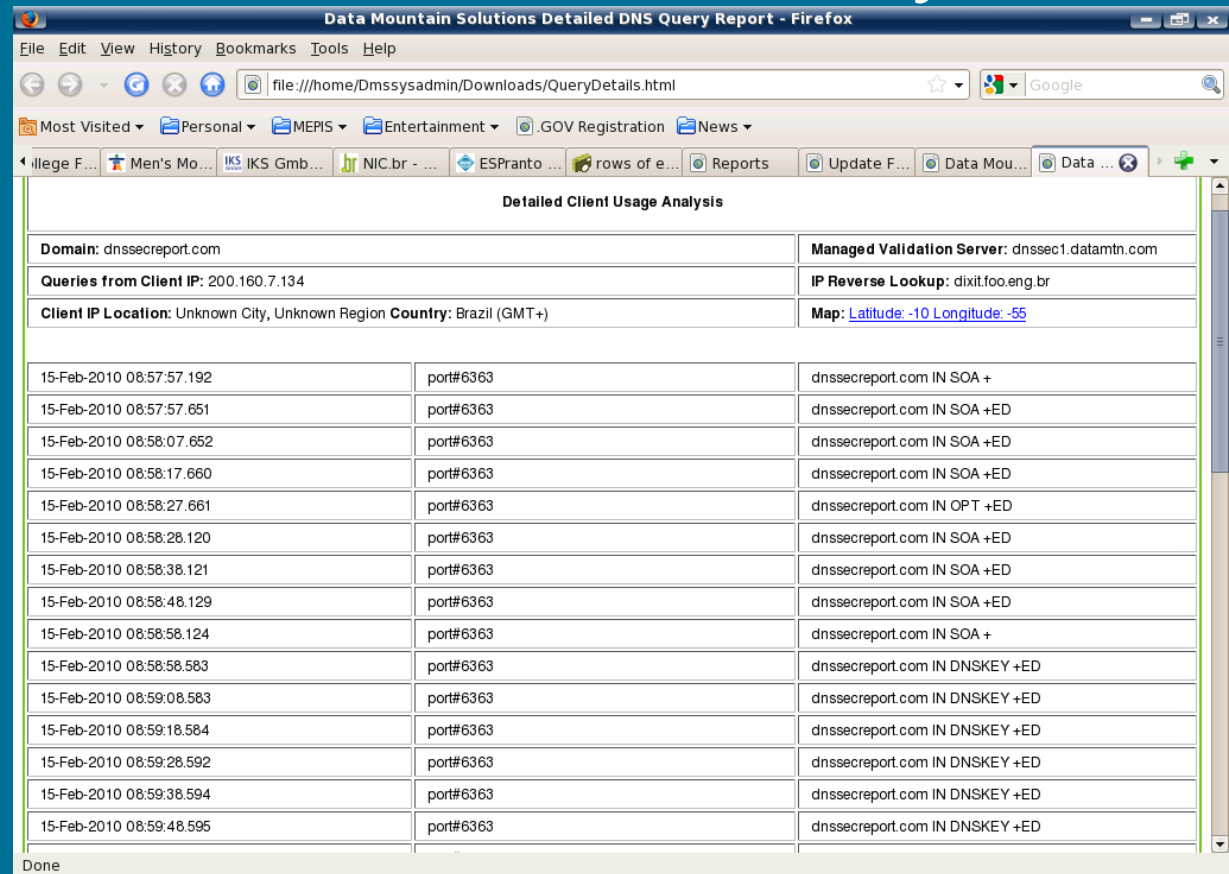
- Private Capture/Archive of DNS Activity
- Single-click Reporting and Raw Data Export

The screenshot shows a web browser window titled "Reports - Firefox" displaying the "Show Client DNS Queries" page on datamtn.com. The page includes a search form with fields for Start Date, End Date, Client Name, Client IP, and Authoritative Name Servers, along with a "Filter Server" dropdown and an "Only IPv6 Queries" checkbox. Below the form is a "Search Results" table with columns: Customer Domain, Server Name, Client IP, Detailed Info, Client Name, Query Count, and DNS Query Date. The table contains 30 rows of data, showing various domains like dnssecreport.com and client names like dixit.foo.eng.br.

Customer Domain	Server Name	Client IP	Detailed Info	Client Name	Query Count	DNS Query Date
dnssecreport.com	dnssec7	200.160.7.134	whois	dixit.foo.eng.br	25	15-Feb-10 09:15
dnssecreport.com	dnssec7	206.204.217.155	whois	dnssec2.datamtnsol.com	1	15-Feb-10 09:15
dnssecreport.com	dnssec11	200.160.7.134	whois	dixit.foo.eng.br	3	15-Feb-10 09:15
dnssecreport.com	dnssec11	216.239.58.94	whois	dixit.foo.eng.br	1	15-Feb-10 09:15
dnssecreport.com	dnssec12	200.160.7.134	whois	dixit.foo.eng.br	3	15-Feb-10 09:15
dnssecreport.com	dnssec12	204.168.112.69	whois	dnssec1.datamtnsol.com	1	15-Feb-10 09:15
dnssecreport.com	dnssec14	200.160.7.134	whois	dixit.foo.eng.br	3	15-Feb-10 09:15
dnssecreport.com	dnssec14	209.85.228.94	whois	dixit.foo.eng.br	1	15-Feb-10 09:15
dnssecreport.com	dnssec14	206.204.217.155	whois	dnssec2.datamtnsol.com	1	15-Feb-10 09:15
dnssecreport.com	dnssec10	200.160.7.134	whois	dixit.foo.eng.br	3	15-Feb-10 09:15
dnssecreport.com	dnssec10	74.125.114.94	whois	vx-out-f94.1e100.net	1	15-Feb-10 09:15
dnssecreport.com	dnssec10	74.125.86.94	whois	dixit.foo.eng.br	1	15-Feb-10 09:15
dnssecreport.com	dnssec12	200.160.7.134	whois	dixit.foo.eng.br	32	15-Feb-10 09:00
dnssecreport.com	dnssec12	65.55.238.17	whois	dixit.foo.eng.br	1	15-Feb-10 09:00
dnssecreport.com	dnssec14	200.160.7.134	whois	dixit.foo.eng.br	39	15-Feb-10 09:00
dnssecreport.com	dnssec14	207.46.200.36	whois	dixit.foo.eng.br	1	15-Feb-10 09:00
dnssecreport.com	dnssec14	74.125.78.94	whois	ey-out-f94.1e100.net	1	15-Feb-10 09:00
dnssecreport.com	dnssec14	209.85.128.94	whois	fk-out-f94.1e100.net	1	15-Feb-10 09:00
dnssecreport.com	dnssec7	200.160.7.134	whois	dixit.foo.eng.br	17	15-Feb-10 09:00
dnssecreport.com	dnssec9	200.160.7.134	whois	dixit.foo.eng.br	33	15-Feb-10 09:00
dnssecreport.com	dnssec9	152.85.8.33	whois	exeuntcha2.tva.gov	2	15-Feb-10 09:00

MV – Query Details (more)

- Detailed Port/Query analysis from Client IPs
- Integrate data into Blocked IP/IDS system



Data Mountain Solutions Detailed DNS Query Report - Firefox

File Edit View History Bookmarks Tools Help

file:///home/Dmssysadmin/Downloads/QueryDetails.html

Most Visited Personal MEPIS Entertainment .GOV Registration News

illeg F... Men's Mo... IKS IKS Gmb... NIC.br - ... ESPranto ... rows of e... Reports Update F... Data Mou... Data ...

Detailed Client Usage Analysis

Domain: dnssecreport.com	Managed Validation Server: dnssec1.datamtn.com
Queries from Client IP: 200.160.7.134	IP Reverse Lookup: dixit.foo.eng.br
Client IP Location: Unknown City, Unknown Region Country: Brazil (GMT+)	Map: Latitude -10 Longitude -55

15-Feb-2010 08:57:57.192	port#6363	dnssecreport.com IN SOA +
15-Feb-2010 08:57:57.651	port#6363	dnssecreport.com IN SOA +ED
15-Feb-2010 08:58:07.652	port#6363	dnssecreport.com IN SOA +ED
15-Feb-2010 08:58:17.660	port#6363	dnssecreport.com IN SOA +ED
15-Feb-2010 08:58:27.661	port#6363	dnssecreport.com IN OPT +ED
15-Feb-2010 08:58:28.120	port#6363	dnssecreport.com IN SOA +ED
15-Feb-2010 08:58:38.121	port#6363	dnssecreport.com IN SOA +ED
15-Feb-2010 08:58:48.129	port#6363	dnssecreport.com IN SOA +ED
15-Feb-2010 08:58:58.124	port#6363	dnssecreport.com IN SOA +
15-Feb-2010 08:58:58.583	port#6363	dnssecreport.com IN DNSKEY +ED
15-Feb-2010 08:59:08.583	port#6363	dnssecreport.com IN DNSKEY +ED
15-Feb-2010 08:59:18.584	port#6363	dnssecreport.com IN DNSKEY +ED
15-Feb-2010 08:59:28.592	port#6363	dnssecreport.com IN DNSKEY +ED
15-Feb-2010 08:59:38.594	port#6363	dnssecreport.com IN DNSKEY +ED
15-Feb-2010 08:59:48.595	port#6363	dnssecreport.com IN DNSKEY +ED

Done

MV – WHOIS Details

- Immediate mapping/lookup of DNS sources
- International crossref into ICANN regions

Data Mountain Solutions WHOIS Results - Firefox

File Edit View History Bookmarks Tools Help

https://www.datamtn.com/account/whois.aspx?whois=200.160.7.134

Most Visited Personal MEPIS Entertainment .GOV Registration News

cti College F... Men's Mo... IKS IKS Gmb... NIC.br - ... ESPranto ... rows of e... Reports Update F... Data ...

WHOIS Information 200.160.7.134


% Joint Whois - whois.lacnic.net
% This server accepts single ASN, IPv4 or IPv6 queries

% Brazilian resource: whois.registro.br

% Copyright (c) Nic.br
% The use of the data below is only permitted as described in
% full by the terms of use (<http://registro.br/termo/en.html>),
% being prohibited its distribution, comercialization or
% reproduction, in particular, to use it for advertising or
% any similar purpose.
% 2010-02-15 12:31:52 (BRST -02:00)

inetnum: 200.160.0/20
aut-num: AS22548
abuse-c: FAN
owner: Ncleo de Informao e Coordenao do Ponto 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: 20100212 AA
nslastaa: 20100212
nserver: b.dns.br
nsstat: 20100212 AA
nslastaa: 20100212
nserver: c.dns.br

Device IP Address registered in: Brazil GMT-4
Location: Unknown City, Unknown Region
Latitude: -10 Longitude: -55



View Larger Map

Done

DNSSEC Bundles

- (1) Managed Validation + Full Service = \$120/month (addl Auth domains = \$75/mo)
- (2) Managed Validation + Full Service = \$165/month (addl Auth domains = \$75/mo)
- US GOV DNSSEC and FISMA DNS Compliance in less than 1 hour!

DNSSEC Bundles

- (1) Managed Validation + Full Service = \$120/month (addl Auth domains = \$75/mo)
- (2) Managed Validation + Full Service = \$165/month (addl Auth domains = \$75/mo)
- US GOV DNSSEC and FISMA DNS Compliance in less than 1 hour!