

Figure 26-1

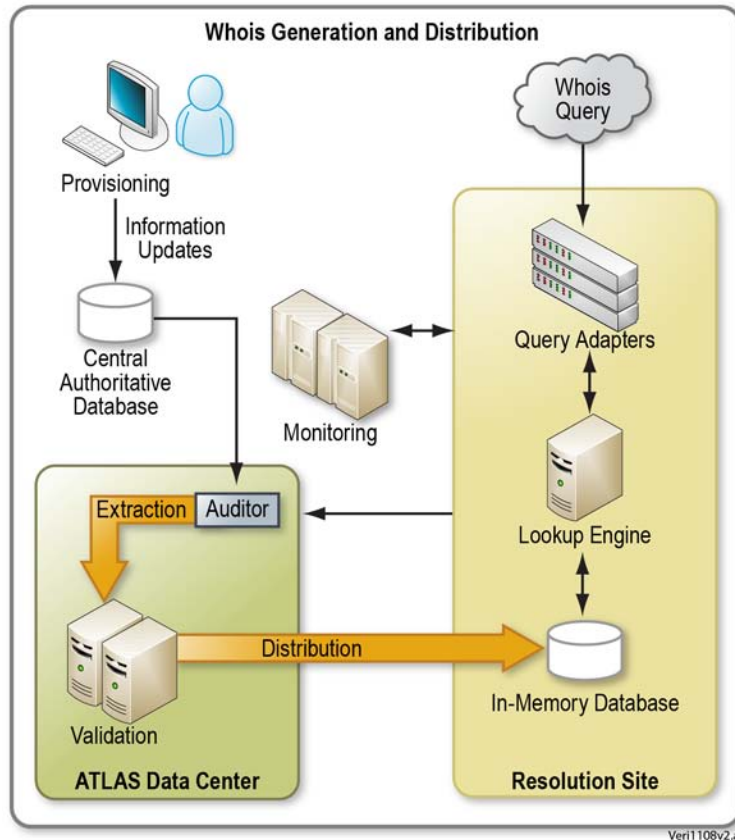


Figure 26-1: Whois Service Network Diagram. By distributing Whois service across multiple resolution sites, Whois transactions are highly available and performed with low latency.

Figure 26-2

| Component | Implementation/Configuration |
|---------------------------------------|--|
| Load Balancers | <ul style="list-style-type: none"> • Deployed as a pair for maximum availability and resilience. • Help ensure workload is evenly distributed across all systems within this gTLD resolution network. |
| Layer-3 Switches | <ul style="list-style-type: none"> • Four switches are installed in Verisign’s resolution network environment: two for front-office management, and two for back-office management. • Switches provide both routing and switching for this gTLD environment across the front-office network. |
| Terminal Servers | <ul style="list-style-type: none"> • Deployed as a pair of terminal servers to enable out-of-band management of all network hardware. • Used in the event that primary network access is unavailable at Verisign’s primary resolution sites. |
| Virtual Private Networks (VPN) | <ul style="list-style-type: none"> • Pair of VPNs installed at each of Verisign’s primary resolution sites for secure remote access to the installed systems. |
| Commodity Servers | Supporting Whois data processing needs, each commodity server consists of the following specifications: <ul style="list-style-type: none"> • Two central processing units (CPUs) |

| | |
|-------------------------|---|
| | <ul style="list-style-type: none"> • 2 – 6 gigabytes (GB) random access memory (RAM) (as dictated by the server function) • 2x73GB hard drive |
| Database Servers | Supporting Whois data processing needs, each database server consists of the following specifications: <ul style="list-style-type: none"> • 16 cores (4 x quad-core CPUs) • 64GB RAM • 5x73GB hard drive |

Figure 26-2: Whois IT and Infrastructure Resources. Verisign uses a common Whois resolution network architecture at each primary site provisioning the Whois service.

Figure 26-3

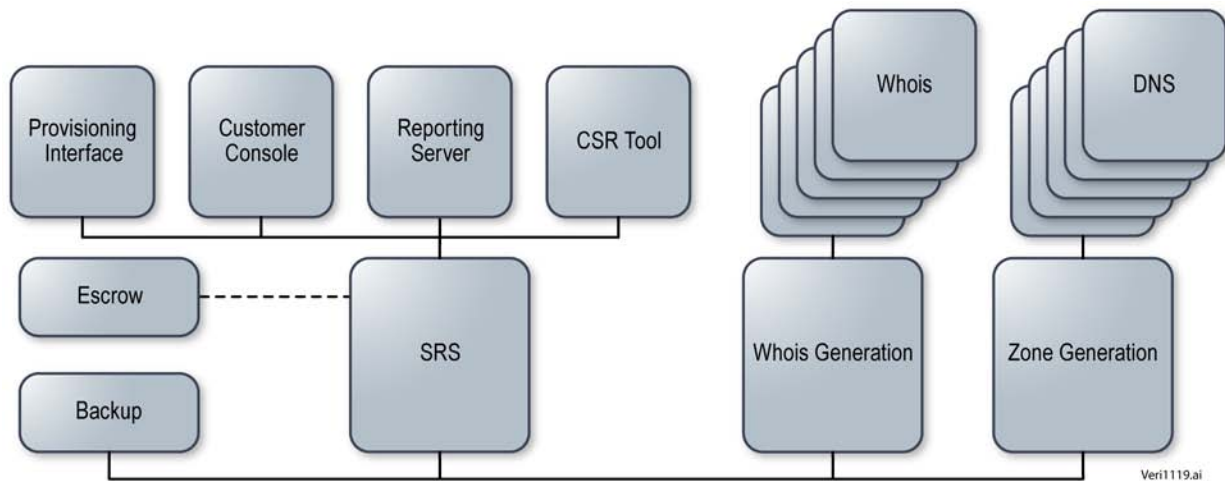


Figure 26-3: Technical Overview. Verisign's Whois services are co-located at DNS locations.

Figure 26-4

```

Domain Name Data
Query format: whois EXAMPLE.TLD
Response format:

Domain Name: EXAMPLE.TLD
Domain ID: D1234567-TLD
Whois Server: whois.example.tld
Referral URL: http://www.example.tld
Updated Date: 2009-05-29T20:13:00Z
Creation Date: 2000-10-08T00:45:00Z
Expiration Registry Expiry Date: 2010-10-08T00:44:59Z
Sponsoring Registrar: EXAMPLE REGISTRAR LLC
Sponsoring Registrar IANA ID: 5555555
Domain Status: clientDeleteProhibited
Domain Status: clientRenewProhibited
Domain Status: clientTransferProhibited
Domain Status: serverUpdateProhibited
Registrant ID: 5372808-ERL

```

Registrant Name: EXAMPLE REGISTRANT
Registrant Organization: EXAMPLE ORGANIZATION
Registrant Street: 123 EXAMPLE STREET
Registrant City: ANYTOWN
Registrant State/Province: AP
Registrant Postal Code: A1A1A1
Registrant Country: EX
Registrant Phone: +1.5555551212
Registrant Phone Ext: 1234
Registrant Fax: +1.5555551213
Registrant Fax Ext: 4321
Registrant Email: EMAIL@EXAMPLE.TLD
Admin ID: 5372809-ERL
Admin Name: EXAMPLE REGISTRANT ADMINISTRATIVE
Admin Organization: EXAMPLE REGISTRANT ORGANIZATION
Admin Street: 123 EXAMPLE STREET
Admin City: ANYTOWN
Admin State/Province: AP
Admin Postal Code: A1A1A1
Admin Country: EX
Admin Phone: +1.5555551212
Admin Phone Ext: 1234
Admin Fax: +1.5555551213
Admin Fax Ext: 4321
Admin Email: EMAIL@EXAMPLE.TLD
Tech ID: 5372811-ERL
Tech Name: EXAMPLE REGISTRAR TECHNICAL
Tech Organization: EXAMPLE REGISTRAR LLC
Tech Street: 123 EXAMPLE STREET
Tech City: ANYTOWN
Tech State/Province: AP
Tech Postal Code: A1A1A1
Tech Country: EX
Tech Phone: +1.1235551234
Tech Phone Ext: 1234
Tech Fax: +1.5555551213
Tech Fax Ext: 93
Tech Email: EMAIL@EXAMPLE.TLD
Name Server: NS01.EXAMPLEREGISTRAR.TLD
Name Server: NS02.EXAMPLEREGISTRAR.TLD
DNSSEC: signedDelegation
DNSSEC: unsigned
>>> Last update of Whois database: 2009-05-29T20:15:00Z <<<

Figure26-4: Domain Name Data Object

Figure 26-5

```
Registrar Data
Query format: whois "registrar Example Registrar, Inc."
Response format:
Registrar Name: Example Registrar, Inc.
Street: 1234 Admiralty Way
City: Marina del Rey
State/Province: CA
Postal Code: 90292
Country: USA
Phone Number: +1.3105551212
Fax Number: +1.3105551213
Email: registrar@example.tld
Whois Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
Admin Contact: Joe Registrar
Phone Number: +1.3105551213
Fax Number: +1.3105551213
Email: joeregistrar@example-registrar.tld
Admin Contact: Jane Registrar
Phone Number: +1.3105551214
Fax Number: +1.3105551213
Email: janeregistrar@example-registrar.tld
Technical Contact: John Tech
Phone Number: +1.3105551215
Fax Number: +1.3105551216
Email: johntech@example-registrar.tld
>>> Last update of Whois database: 2009-05-29T20:15:00Z <<<
```

Figure 26-5: Registrar Data Object

Figure 26-6

```
Name Server Data
Query format: whois "NS1.EXAMPLE.TLD" or whois "name server (IP address)"
Response format:
Server Name: NS1.EXAMPLE.TLD
IP Address: 192.0.2.123
IP Address: 2001:0DB8::1
Registrar: Example Registrar, Inc.
Whois Server: whois.example-registrar.tld
Referral URL: http://www.example-registrar.tld
>>> Last update of Whois database: 2009-05-29T20:15:00Z <<<
```

Figure 26-6: Name Server Data Object

Figure 26-7

| Potential Abusive Searchable Whois Risks | Verisign Risk Mitigation |
|---|---|
| <p>Single Source Data Mining</p> <p>The mining of Whois data from a single IP address conducted through manual queries</p> | <p>Access Control Lists (ACL): Implementation of an ACL at the network layer to block the offending IP address for a specified period of time; viable option given a single unique IP address</p> <p>Application Rate Limiting: Implementation of rate-limiting at the application layer to regulate the number of queries allowed from the source IP address for a specified period of time; viable option given a single unique IP address</p> |
| <p>Automated Data Mining</p> <p>Single Source: The mining of Whois data from a single IP address conducted through the use of automated scripts</p> <p>Distributed: The mining of Whois data from multiple sources/IP addresses conducted through the use of automated scripts, or, "botnets"</p> | <p>ACL and Application Rate Limiting as defined for single source data mining</p> <p>Packet Inspection: Implementation of tools that analyze the incoming "get" request to determine whether the source is a valid user or whether the request is coming from an automated script or botnet; viable option based on "get" request signature</p> <p>Completely Automated Public Turing Test To Tell Computers And Humans Apart (CAPTCHA) Techniques: Implementation of a challenge-response test prior to processing the request; viable option that limits ability to predict challenge-response; almost always requires manual interaction</p> |

Figure 26-7: Potential Searchable Whois Forms of Abuse and Mitigation. *Verisign leverages its experience supporting the .name registry to build in to the system the safeguards necessary to minimize abusive Whois practices.*