BEST PRACTICES FOR IMPROVING EXTERNAL DNS RESILIENCY AND PERFORMANCE
BEST PRACTICES FOR IMPROVING EXTERNAL DNS RESILIENCY AND PERFORMANCE

Your external DNS is a mission critical business resource. Without it, no one can reach your website, email, or web applications. Additionally, poor DNS performance translates into slow access to your website and lost customers. The cost of outages or unacceptable latency can range from a few unhappy users to millions of dollars per hour depending on the scale of e-commerce. Recent high-profile attacks leveraging the DNS to take down enterprise websites have raised awareness of DNS outages. DDoS attacks are not the only threat. External name servers operate in a hostile environment and can be brought down in a number of ways, including: server failures, network failures, natural disasters, power outages and security breaches. The following are some best practices to help organizations to improve the performance, resiliency and fault tolerance of their external DNS.

Best Practice 1

USE A HIDDEN MASTER

A hidden master is a name server that is not advertised and does not appear in any name server records. In other words, it is not known publicly on the Internet and does not answer any queries. The hidden master’s purpose is to provide zone transfers to a set of secondary name servers that are known publicly and answer queries. The benefits of a hidden master are:

- **Fault tolerance**
  Master can go down without impacting the resolution of your domain.

- **Security**
  IP address of the name server is not published, and is less likely to be hacked.

- **Easy administration**
  Reloads and restarts of the hidden master do not impact resolution of your domain.

Best Practice 2

DISABLE RECURSION ON YOUR EXTERNAL NAMESERVERS

Disable recursion on your hidden master and authoritative external nameservers. Turning off recursion reduces the vulnerability to denial of service attacks and cache poisoning, and helps improve performance.
**Best Practice 3**

**USE TSIG TO SECURE NAMESERVER TO NAMESERVER COMMUNICATIONS**

Communication between the hidden master and secondary nameservers should be cryptographically authenticated using Transaction Signatures (TSIG). TSIG is much more secure than source IP address filtering which can be easily spoofed with UDP.

**Best Practice 4**

**PLACE NAMESERVERS CLOSE TO USERS**

The latency of DNS lookups is important for your website. Long latency can translate into lost customers and revenue. Your authoritative nameservers answer queries from other nameservers on the Internet. To ensure a good user experience and fast access to your website, place your nameservers close to, or quickly accessible from the nameservers querying them. Optimally, this would involve placing nameservers in locations with good access to the Internet such as Internet Exchange Points (IXPs).

The highly recommended solution is an outsourced secondary anycast DNS service. With anycast, multiple geographically distributed nameservers share a single IP address and queries are routed to the closest nameserver. When selecting an anycast DNS secondary service, make sure the nameservers are located in IXPs that map geographically to your customers.

**Best Practice 5**

**MAKE YOUR DNS RESILIENT TO DDOS ATTACKS.**

DDoS attacks using DNS as the attack vector are on the rise. Increase resiliency to DDoS attacks with the extra query capacity and bandwidth of an anycast DNS cloud. To the world, the anycast cloud appears as a single IP address. In reality it is a network of geographically distributed nameservers. An anycast cloud is much more resilient to a DDoS attack than single unicast servers because it uses geo-location to specify what server answers a query and it has the combined capacity and bandwidth of all the servers. With anycast, the impact of an attack is isolated to the name server closest to the source(s) of the attack.
Most DDoS attacks originate offshore. When selecting an anycast DNS service ensure there are international nodes that can soak offshore attacks. An international node sinks traffic from an offshore attack while helping domestic name servers to remain unaffected.

Best Practice 6
MAKE YOUR DNS DISASTER PROOF

Use redundancy to make your external DNS disaster proof. With unicast servers, this means at least two nameservers in different locations. A better alternative is an anycast DNS cloud to provide redundancy. If a nameserver in an anycast cloud goes down, it is automatically removed from the routing tables. In this way, anycast adds redundancy and fault tolerance.

With anycast, the highest level of redundancy is achieved with two separate clouds. When compared to unicast redundancy, it is like replacing two unicast nameservers with two anycast clouds. Make sure the clouds use independent hardware and transit providers. This protects against a routing problem or transit network outage from bringing down your DNS.

Best Practice 7
USE ANYCAST DNS

Anycast has been in use for more than 10 years to provide name services for the root server on the Internet as well as many top-level domains including .CA. Anycast DNS is the optimal solution for fault-tolerance, DDoS resiliency and placing name servers close to users. For most organizations, building and managing their own anycast DNS infrastructure is too expensive and not practical. Fortunately, an anycast DNS service like D-Zone Anycast DNS can be easily added to your DNS infrastructure.
D-ZONE ANYCAST DNS SERVICE – HELPING YOU TO PROTECT YOUR BUSINESS

The D-Zone Anycast DNS Service is a secondary anycast DNS network designed for Canadian organizations or organizations serving the Canadian market.

Features at a glance:

✔ 100 per cent availability and service level agreement (SLA).

✔ 100 times over-provisioned architecture with state-of-the-art equipment and redundancy at every node.

✔ Global DNS nodes within Canada and in international Internet hubs.

✔ Local DNS nodes geographically close to, and protecting, in-region traffic from malicious activity against the DNS.

✔ Strong Canadian presence reduces the latency for Canadian visitors.

✔ Two clouds for failover redundancy and protection from DNS DDoS attacks on local nodes.

✔ Secondary service is easily added to an existing DNS infrastructure to improve its overall resilience and performance.

✔ Support for DNSSEC.

✔ Support for IPv6.

LEARN MORE

For information on ordering, finding a reseller, or becoming a reseller please contact info@d-zone.ca or visit cira.ca/d-zone.

ABOUT CIRA

The Canadian Internet Registration Authority (CIRA) manages Canada’s .CA domain name registry as a 100 per cent up time service for Canadians and Canadian organisations. In addition to stewardship over .CA, CIRA develops and implements policies that support Canada’s Internet community and the .CA registry internationally.