cira

Anycast DNS Service technical architecture for top-level domains

CLASSIFICATION: SENSITIVE

Table of Contents

Executive summary

CIRA TLD Anycast is a high-performance, high-availability secondary DNS trusted by over 490 top-level domains in the gTLD and ccTLD segments – covering nearly one-third of all top-level domains in the world. CIRA offers a 100% uptime service-level-agreement (SLA) for answering DNS queries and there have been no service-impacting outages since the service went live in December of 2014.

The service architecture combines anycast technology with multiple levels of redundancy across the entire global network. For top level domains (TLDs) we offer flexible implementation options that include using your own IP blocks and hybrid clouds that combine your local nodes with CIRA's global clouds. This technical document describes various features of the architecture and how it benefits TLDs.

"The need for secondary DNS services at the TLD level has never been clearer. CIRA is thrilled with the global response to the world-class network and service we have offered through TLD Anycast."

JACOB ZACK, DNS ARCHITECT, CIRA

A global secondary DNS service for TLDs

WHAT CIRA TLD ANYCAST OFFERS:

- The necessary aggregate bandwidth, high-capacity routers and servers, global node distribution and exchange point peering to handle authoritative resolution for a top-level domain registry.
- For domain registries the kind of reporting they need to manage a TLD business.

The CIRA universal cloud

DIVERSE INTERNET BACKBONE TRANSIT THAT DESERVES ITS OWN UNIQUE DESCRIPTOR

CIRA has structured the clouds with multiple tier-1 transit providers for optimizing performance and reliability. CIRA works constantly to grow the network of thousands of peering points globally connected to the service, vastly improving network performance and resiliency

IXP connections and peering

Sites are connected to internet exchange points (IXP). In total, sites are peered with more than 8,000 networks worldwide to respond to queries in the event of a transit failure.

Redundant primaries

Fully redundant primary server clusters in two data centers with diverse network connections accessible for IPV4 and IPV6. Only one primary needs to be operational for the service to receive zone transfers and push them out to the cloud servers.

Global deployment

19 distinct points of presence in strategically placed and well-connected locations around the globe. Each location connects with diverse transit providers for internet connectivity. In addition, CIRA connects to multiple IXPs in each location with a focus on keeping DNS query traffic in the region. This design provides improved response time and improved resiliency for our customers. This architecture has been tested to ensure that local queries don't ping-pong across oceans when there is a better route.

Hybrid CCTLD DNS model

CIRA supports a hybrid cloud architecture that allows a TLD partner to own and operate nodes. TLD partners supply the IP address block for their cloud to effectively create a custom cloud. TLD partners can extend their local anycast infrastructure with CIRA's global nodes.

North America	IXP's	IXP Notes
Toronto	TORIX	#1 in Canada
Vancouver	VANIX	#5 in Canada
Miami	Equinix Miami	#12 in USA
Los Angeles	Any2 California	#2 in USA
Ashburn	Equinix Ashburn	#3 in USA
Montreal	QIX	#2 in Canada
Winnipeg	MBIX	#6 in Canada
Calgary	YYCIX	#3 in Canada

Europe	IXP's	IXP Notes
Frankfurt	DE-CIX Frankfurt	#1 in Europe #7 in Europe
London	NL-IX LINX	#3 in Europe #20 in Europe
Stockholm	Netnod Stockholm STHIX SOLIX	#32 in Europe

Asia & Oceania	IXP's	IXP Notes
Singapore	Equinix Singapore *	#1 in South Asia
Hong Kong	Equinix Hong Kong	#2 in East Asia
Tokyo	JPNAP	#3 in East Asia
Sydney	MegaIX Sydney Equinix Sydney IX Australia NSW	#1 in Oceania #2 in Oceania #3 in Oceania
Melbourne	MegaIX Melbourne IX Australia VIC	#4 in Oceania #5 in Oceania

South America	IXP's	IXP Notes
Sao Paulo 1	IX.BR Sao Paolo	#1 in South America
Sao Paulo 2	IX.BR Sao Paolo	#1 in South America
Santiago, Chile	PIT Chile	#2 in South America

Africa	IXP's	IXP Notes
Johannesburg	NAP Africa Johannesburg	#1 in Africa
Capetown	NAP Africa Capetown	#2 in Africa

Management transit

Each CIRA node has management transit that is separate from the internet backbone transit provider. The management transit is used to ensure a site is reachable in the event of a transit failure or a DDoS attack. Management transit is also used to update cloud server configuration and collect usage data. To increase security, a VPN is used to connect remote sites.

High availability DNS sites

The standard site configuration consists of a router that load balances DNS queries between multiple DNS servers. The router continuously monitors the availability of each DNS server and removes a server from the service if it is unavailable. Each site also includes a server that is used for collecting reporting data in normal operation but can also be utilized for backup or additional DNS query capacity if needed.

CIRA maintains a 100+ node remote monitoring network that is constantly monitoring our availability and response times from all over the world.

Management and configuration

PROTECTED ACCESS

CIRA provides secure, automated interfaces for the management of the network and TLD zones. CIRA uses a variety of automation tools for configuration and management. Because of the critical nature of registry services, any changes are validated in person.

DNS QUERY REPORTING

CIRA offers read-only access to a reporting portal. CIRA can also provide PCAP files to the customer for ingestion into their own systems for those that report from multiple suppliers. At each node all DNS packet data is mirrored to a dedicated server. A Parquet/PCAP file is produced every five minutes and transported to a central site over management transit where it can be pushed to a cloud repository supplied by the customer. Data collection is done out of band so it does not impact performance.

DNS LOG MESSAGE REPORTING

All log messages from the CIRA name servers that perform zone transfers into CIRA from a customer are fed into a data stack. Access to the reports on the success of zone transfers are provided to TLDs for monitoring.

DNS SOFTWARE AND HARDWARE DIVERSITY

CIRA maintains multi-platform resilience with the most recent secure versions of DNS software at all sites – including support agreements with software supplier organizations. Sites have been configured to allow rapid cut-over between applications to protect against a major zero-day event. CIRA also utilizes multiple hardware vendors to maintain hardware diversity in the same manner as we do with our DNS software. Combined, this provides protection against zero-day vulnerabilities and vendor bugs.

Protecting TLD DNS with a DDoS mitigation strategy

CIRA Anycast TLD has a 100 per cent uptime SLA for answering DNS queries. There has been no service impacting outages since the service went live in December 2014 as such, CIRA has used multiple strategies to combat the growing threat of amplified DDOS attacks.

BANDWIDTH AND QUERY CAPACITY

CIRA is continually increasing the aggregate bandwidth and query capacity of the anycast clouds.

- **Peering relationships** – With over 8,000 peers globally, CIRA continues to increase the proportion of queries that can be answered over peering rather than internet transit. Even during an attack that floods CIRA's transit, queries could still be answered over IXP peering connections. CIRA will work closely with TLDs to develop peering relationships for their regions. CIRA now has two separate third-party DDoS mitigation services, offering well over 2TB/sec of total packet scrubbing/filtering technology.

- **Packet scrubbing & filtering** - CIRA now has two separate third-party DDoS mitigation services, offering well over 2TB/sec of total packet scrubbing/filtering technology.
- **Detection and monitoring** – Early detection is critical to mitigating a DDoS attack. 24/7 monitoring with automated alerts is used to detect and respond to attacks.

MAINTAINING CONNECTIVITY AND CONTROL

Each CIRA DNS site has management transit that is diverse from the transit provider used to receive and respond to queries. In the event of an attack CIRA can maintain connectivity and control to nodes to ensure data about the attack can be collected and mitigation measures activated.

RELATIONSHIPS WITH TRANSIT PROVIDERS

CIRA maintains close relationships with transit providers. In the event of an attack, CIRA will involve transit providers to mitigate attacks closer to the edge of their networks.

Service component	Failure	Service impact	MTTR
Anycast name server	Name server fails	None	5 days
Anycast site	Complete data center failure	None	30 days to relocate data center
Anycast router	Complete router failure	None	5 days
Internet transit provider	Complete failure for internet transit provider that hits one cloud	Reduced capacity – queries answered by second cloud and IXPs	14 days to switch providers (worst case)
Anycast cloud	Large scale DDoS attack from off shore	Service impacting at international anycast sites	Depends on size, duration and type of attack and the efficacy active mitigation.

CIRA participates in our shared community

DNS-OARC CONTRIBUTOR

CIRA is an active member and contributor to DNS-OARC, including in the past and still today on relevant committees.

INTERNET ENGINEERING TASK FORCE (IETF)

CIRA has contributed to IETF efforts to standardize DNSSEC.

ICANN CCNSO, DNSSEC WORKSHOP, SSAC

CIRA is an active participant and contributor to the ccNSO workshops, ccNSO Tech Days, DNSSEC workshops and SSAC.

A shared commitment to growth

CIRA shares many technology, research and governance interests with our peers. By providing DNS to TLDs we aim to deepen collaboration in these areas, and to explore new product partnerships, including:

- DNS data research in machine learning research on PCAP.
- DNSSEC adoption via the registry operator - IETF draft protocol.
- Shared data center rack space to reduce costs and expand mutual global capacity.
- New product development such as internet performance testing and recursive services.

To get **CIRA TLD Anycast** working for your TLD,
please contact us at **cybersecurity.services@cira.ca**