BLUECAT™ Micetro

Ensuring DNS availability across multiple DNS service platforms with BlueCat Micetro xDNS redundancy

External DNS reundancy is not as simple as it seems

When DNS is unavailable, it will appear to a user looking for a product or service online as if the website they're trying to connect to has ceased all operations. In an era where organizations are dependent on the speed and convenience of eternal connectivity, unexpected network downtime can bring enterprises to a standstill, leading to damaging losses in revenue and reputation.

The DNS challenge

DNS is the most critical aspect of any network's availability. When DNS services are halted or slowed down significantly, networks become inaccessible.

To ensure optimal network availability, many enterprises depend on top-tier managed DNS service providers for their external DNS needs. The basic requirements of an enterprise-class managed DNS service are high reliability, high availability, high performance, and effective network traffic management. However, even the most robust DNS infrastructure is not immune to outages.

Outages may be localized, during which only certain DNS servers in the network are not responding, or system-wide. Though less common, a system-wide DNS failure can take an entire business offline—the equivalent of a power failure in all its data centers. To prevent this, top-tier managed DNS systems have a great deal of built-in redundancy and fault tolerance.

Yet the danger of a single point of failure remains for enterprises that rely solely on a single-source DNS service. If no system of DNS is failure-proof, this begs the question: What should an enterprise do about it?

Using multiple DNS service providers for ultimate redundancy

DNS availability statistics for managed DNS providers show that the industry norm for uptime exceeds five nines (99.999%). This is the equivalent of about five minutes per year of downtime. However, this top line number does not provide any detail on the impact of degraded performance. Nor does it convey the cascading effect of a system-wide outage of any duration on individual enterprises.

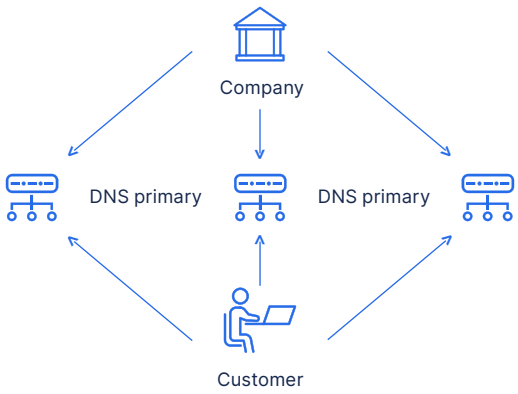
To assess the true impact of a potential loss of DNS availability, enterprises need to properly evaluate the business risk associated with relying on a sole source provider, and compare that with the cost of a second-source DNS service. What would a 30-minute DNS outage cost the business in terms of revenue loss, reputation damage, support costs, and recovery? What does it cost to maintain a second-source DNS service?

Research amongst enterprises for which online services are mission-critical generally concludes that the cost ratios are in the range of 10:1, or one order of magnitude. Put another way, the cost of one outage is roughly estimated to be ten times the annual cost of a maintaining a second service. A business would have to have a second-source DNS service for ten years to equal the cost of one major DNS outage.

Looking at the odds and costs of outages, many enterprises are opting to bring in a second, or even a third, DNS service to hold copies of critical DNS primary zones. This system of external DNS redundancy boosts DNS availability by:

- removing the danger of exposure to a single point of DNS failure

- reducing traditional primary-secondary DNS redundancy vulnerabilities, wherein secondary zones can't be changed if the primary zone becomes unavailable
- improving infrastructure resilience by hosting critical zones with multiple providers, ensuring continued service availability and change updates if one DNS service provider becomes unavailable



The risk of maintaining DNS redundancy across platforms

In theory, DNS redundancy across multiple DNS service provider platforms should be the best solution for optimal high reliability, availability, and performance. In practice, however, the complexity of tasks and risk of error involved in replicating and maintaining identical DNS zones on multiple platforms poses additional threats to DNS availability. The situation is made worse by:

- a lack of centralized views
- a lack of workflow automation
- the difficulty of coordinating multiple platform APIs

The inability to view, synchronize, and update identical zones' data simultaneously can itself lead to errors and conflicts in DNS configuration. This can result in network performance degradation or even a network outage—the very events that multi-provider DNS redundancy is intended to prevent.

Micetro xDNS makes external DNS redundancy simple

Simplified operations and maintenance

In the battle against DNS disruption, BlueCat Micetro's xDNS redundancy feature provides an abstraction level that replicates and synchronizes critical DNS primary zones across multiple DNS service provider platforms, whether they are on premises, in the cloud, or in hybrid or multicloud environments.

Micetro xDNS provides a unifed view and centralized management of DNS data, regardless of the DNS service provider platform. Network administrators and other authorized users can use xDNS to perform necessary updates to their network's DNS. Furthermore, instead of having to dig around in different DNS platforms and juggle the coordination of conflicting APIs, users can build automation with the powerful Micetro API.

Combined with the flexibility of building automation on top of Micetro, xDNS offers you the freedom to better distribute your DNS load based on zone priority, performance requirements, and accompanying costs. With xDNS, you are better equipped to steer the tiered price points of externally hosting critical high-performance or less essential low-performance zones. You can utilize the DNS service best suited to your situation at a given time.

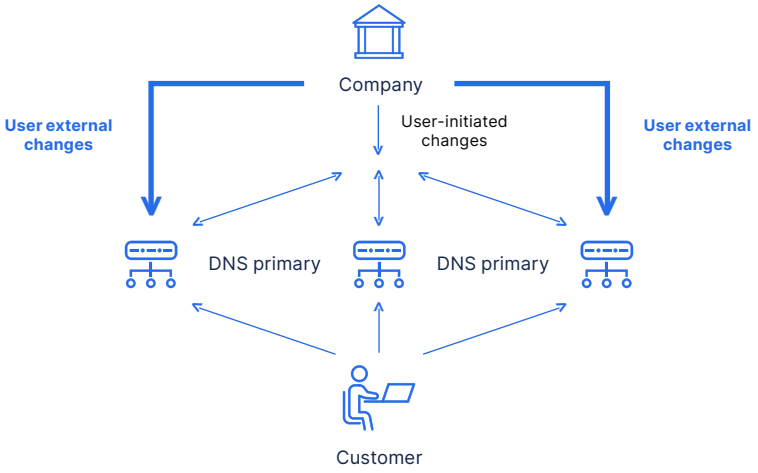
How xDNS redundancy works

Using the Micetro xDNS feature, you can create a zone redundancy group by selecting critical zones from DNS servers and services such as BIND, Windows DNS, Azure DNS, Amazon Route 53, NS1, Dyn, and Akamai Fast DNS.

Once an xDNS zone redundancy group has been created, xDNS assists the administrator with creating identically replicated zone content, resulting in multiple identical primary zones. Additional zones can be added or removed from the xDNS group as required.

All changes initiated by the user through either the Micetro UI or API will be applied to all selected zone instances in the group, as configured in the sync policy. All changes made externally to selected zones in the xDNS group will be synchronized to all zones in that particular xDNS group. However, zones that are not selected will act as 'read only.' They will only receive updates made through Micetro or when the zone itself is modified externally, such as through its corresponding cloud portal. Additionally, if DNS record conflicts arise, xDNS will alert the user and provide an option for how to resolve conflicts before the group is re-synced.

If an xDNS zone is not available for updating—for instance, if one DNS service provider experiences an outage—that zone will be marked as out of sync. Once the zone becomes available again, it will be automatically re-synchronized and will receive all updates that were made while the DNS service was unavailable.



Manage your DNS on multiple external platforms

Maintaining uninterrupted network uptime is critical to business success. Leveraging multiple managed DNS services to ensure optimal DNS redundancy is quickly becoming the clear best practice for enterprises of all sizes.

Yet DNS redundancy, a great concept on paper, is proving a daunting challenge in practice. Micetro xDNS provides a simple way for organizations to manage their DNS on multiple external platforms. Micetro automatically handles the replication and synchronization of DNS data, ensuring reliability and consistency.

Micetro xDNS takes the hard work out of maintaining external DNS redundancy. It provides the centralized views and control necessary to reduce the risk of network exposure to a single point of failure and improve network availability, reliability, and performance.

Corporate Headquarters

4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 | 1-866-895-6931

bluecat.com

Next steps

Get DNS high availability and easily maintain external DNS redundancy.

Request a free trial