


A man with a beard, wearing a dark sweater over a plaid shirt, is standing in profile, writing on a large whiteboard. The whiteboard has some faint red and black writing on it, including the words "ReThink DNS". The background is a brick wall. The overall image has a dark, semi-transparent overlay.


EBook:

MANAGED DNS EVALUATION GUIDE

Understanding What Matters Most
When Selecting Managed DNS

ORACLE® + Dyn

 dyn.com

 603 668 4998

 @dyn

Managed DNS Evaluation Guide

Understanding What Matters Most When Selecting Managed DNS

Introduction

DNS is central to the performance and reliability of your internet applications and cloud services. Extended DNS outages or slow DNS performance can lead to customer dissatisfaction, a tarnished brand and lost revenue. This guide explains how a cloud-based DNS service can help you improve business results and provides guidelines for choosing a managed DNS service provider.

1 Gartner, If External DNS Fails, So Does Your Digital Business, Refreshed: 15 September 2016

In this guide you will learn:

- +
- The critical role DNS plays in the user experience.
- +
- The advantages of a cloud-based managed DNS service.
- +
- Key criteria for evaluating a managed DNS service provider.
- +
- The added benefits of a secondary DNS service.

“DNS is mission-critical to all organizations that connect to the Internet. DNS failure or poor performance leads to applications, data and content becoming unavailable, causing user frustration, lost sales and business reputation damage.”

– Gartner¹

Why DNS Matters

Every user’s first interaction with your website begins with a series of DNS queries. The Domain Name System (DNS) is a distributed internet database that maps human-readable names to IP addresses, ensuring users reach the correct website when entering a URL. DNS mappings are maintained in special-purpose servers called DNS nameservers. When a user enters your company’s URL, a DNS query is routed to a DNS nameserver containing the address mappings for your company’s internet domain.

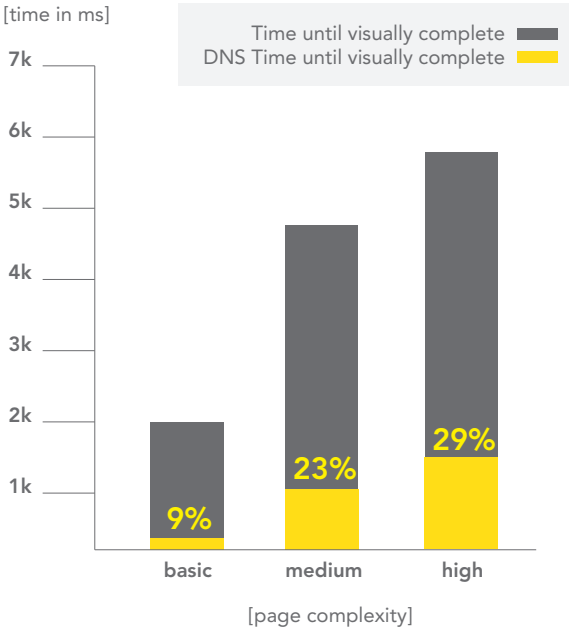
Your online applications and digital content may be scattered across the internet. Some assets might reside in your corporate data center, some might be distributed across a CDN and some might reside in the cloud. DNS is responsible for steering users to the correct source.

DNS performance and availability are central to the user experience. A **contemporary webpage** can involve dozens of DNS lookups. For complex webpages, DNS resolution can comprise as much as 29% of initial page load time.² (see chart on next page)

If DNS query responses are slow because of internet congestion or latency the user experience will be impaired (and users may abandon your site). Worse still, if your DNS infrastructure is unreachable because of equipment problems, network outages or a DDoS attack, users may not be able to access the data and content on your site—regardless of where it resides.

2 Based on Dyn internal testing





The 4X Rule

A common rule of thumb is that you need at least 4X bandwidth capacity to withstand even a medium-size DDoS attack. So a company with a 10GB pipe into the data center would need 40GB of capacity. Recent volumetric DDoS attacks have been increasing in size so even 40GB will not be enough for large-scale attacks.

Managed DNS Services Deliver Superior User Experiences

Many businesses are constrained by in-house DNS solutions that are limited in size and scope. Most in-house DNS implementations consist of a relatively small number of DNS nameservers deployed in one or two data centers. Relying on a small-scale DNS implementation is inherently risky and restrictive. Concerns include:

- **Availability constraints** – If your DNS implementation is unreachable for any reason (disasters, equipment failures, network outages) users may not be able to access your website or web-based applications—regardless of where your content or services are hosted.
- **Security vulnerabilities** – In-house DNS implementations are susceptible to DoS/DDoS attacks. Hackers can impair your DNS service by overwhelming or incapacitating your nameservers. Most corporate IT organizations lack the time and resources to keep pace with ever-evolving and increasingly sophisticated security threats.
- **Performance limitations** – Most in-house DNS implementations include a small number of nameservers deployed in a limited number of sites many hops away from most global users.

You can improve the performance and reliability of your web-based applications and services by implementing a large-scale DNS network, with geographically distributed nameservers. But designing, operating and safeguarding a global DNS network is a resource intensive, expensive and time-consuming proposition. You can achieve better business results by trusting the operation of your DNS infrastructure to a managed service provider that specializes in DNS. Better still, you can free up valuable IT staff and budget to focus on core business initiatives, instead of underlying IT infrastructure.

Managed DNS Services Deliver Superior User Experiences

Not all DNS services are the same. When evaluating a managed DNS service you should carefully consider the technical and functional aspects of the solution as well as the skills and commitment of the service provider. Best-of-breed managed DNS service providers have the global infrastructure and deep DNS and security expertise to ensure your success. They operate large-scale, highly resilient DNS networks that deliver superior user experiences across the world. They offer advanced traffic steering and load balancing features to ensure high performance and availability. And they employ full-time DNS experts and offer 24x7x365 technical support to help you keep your operations running smoothly around the clock.

Beware of ISPs or CDN providers offering DNS services as a side business. Choose a dedicated provider that offers DNS as its primary business and makes the capital and personnel investments necessary to ensure your success.

3 NOTE: Because it is the most prevalent form of multi-DNS configuration, “Secondary DNS” is also the prevailing term of art. However, there are some multi-DNS configurations in which there is are technically no “Secondary” DNS servers (e.g. Primary-Primary) or where the “secondary” service is primarily responsible for resolving queries (hidden master).

Optimize Performance and Availability with a Secondary DNS Service

Whether you are currently using an in-house DNS solution or a managed DNS service, you can improve the overall performance, security and reliability of your internet applications and cloud services by adding a “secondary DNS”³ service to your IT environment. Some organizations may even deploy multiple “secondaries,” or a multi-DNS configuration. Operating in an active-active capacity, secondary DNS services run in parallel to the primary and resolve DNS queries if service from the primary is disrupted, thereby ensuring business continuity.

A secondary DNS configuration is a great way to protect and extend your previous DNS infrastructure investments. You can evaluate, pilot and implement a redundant DNS service without introducing risk or disrupting your current DNS infrastructure. There are several multi-DNS configurations in use today, each with different advantages depending on your needs and network. Read Dyn’s High Availability DNS white paper to learn more about these patterns.

Learn more – Read our white paper: [High Availability DNS Reduces Downtime Risk and Improves End-User Experience](#)

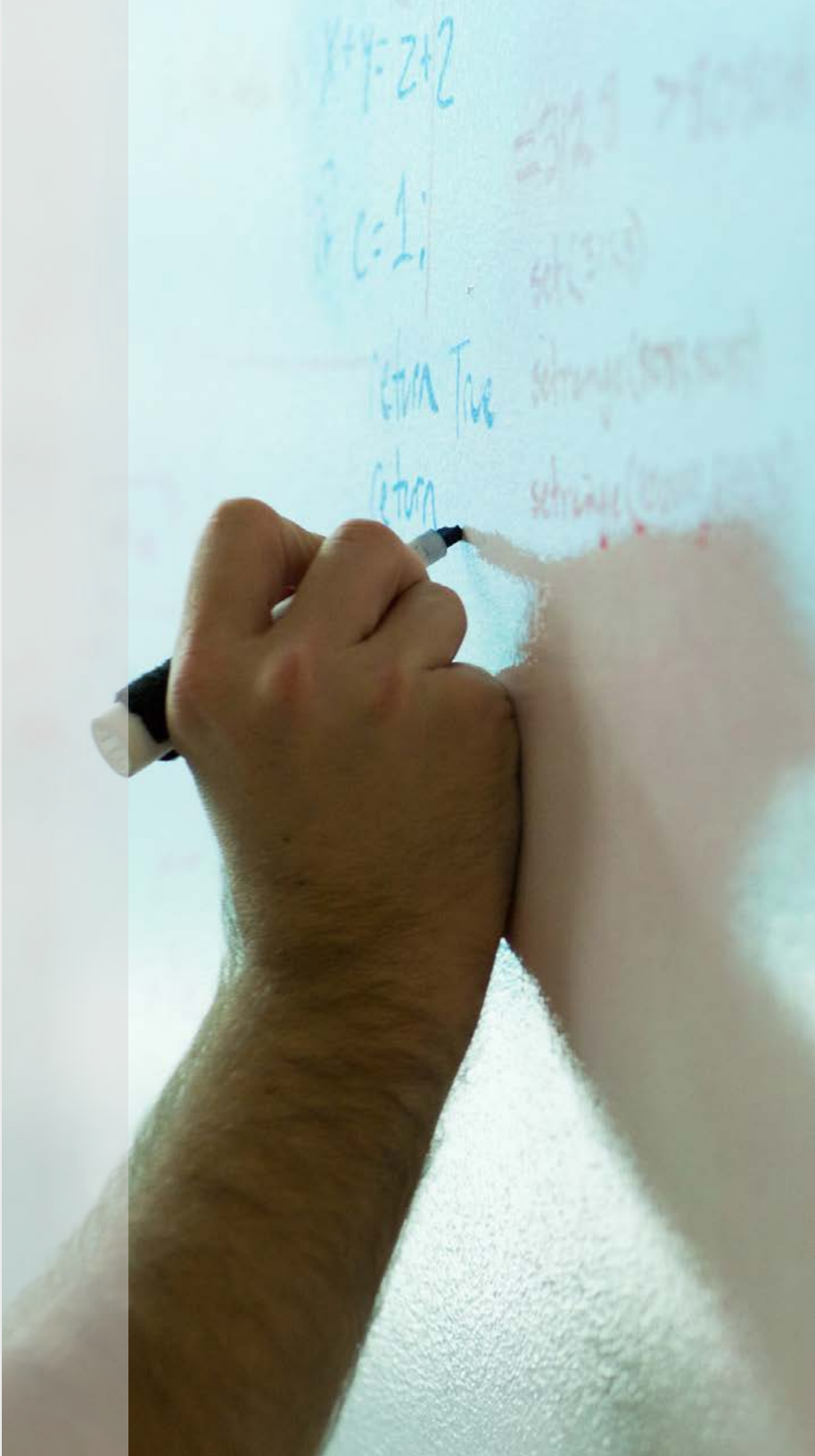
Managed DNS Service Evaluation Criteria

When evaluating a managed DNS service provider be sure to consider the provider's underlying network architecture, the features and capabilities of the service, and the service provider's acumen and business focus.

Architectural Considerations – Choose a service that delivers global scalability, performance and resiliency.

- **Global scalability** – Best-of-breed DNS service providers operate large-scale anycast networks with multiple PoPs across the world located in geographically optimal locations, such as internet exchange points (IXPs). Global anycast networks accelerate DNS resolution by automatically steering DNS queries to the “nearest” nameserver⁴. In addition, leading DNS service providers connect directly to Tier 1 internet transit providers, minimizing internet transmission and propagation delays.
- **High availability** – Leading DNS service providers operate out of geographically distributed PoPs on separate power grids, flood plains and fault lines to protect against disasters. They leverage fully redundant active/active DNS constellations for global reliability, employ fully redundant server configurations to protect against hardware failures and leverage a curated mix of multiple Tier 1 transit providers at each PoP for resilient connectivity.

4 Technically speaking, the BGP routing protocol employed in the IP network directs the user to the DNS nameserver with the lowest hop count.



Functional Considerations – Pick a provider that supports an extensive collection of advanced DNS features and capabilities.

- **Advanced traffic steering** – Leading DNS providers offer innovative features such as zoning, geo-load balancing, failover and performance-based steering⁵ to maximize the responsiveness and reliability of web-based applications and services.
- **Global internet visibility** – Best-of-breed providers collect and analyze real-time and historical internet performance data to optimize resiliency, availability and routing.
- **Open programming interfaces** – Leading providers offer standards-based APIs for integration with enterprise administrative systems and other DNS services.
- **Rich management tools** – Best-in-class providers offer simple-to-use administrative interfaces for configuring DNS records and tracking DNS performance and reliability.
- **Support for secondary DNS** – Look for a provider with a proven track record interoperating with other DNS services. Leading providers support a variety of redundant, multi-DNS service deployment options and provide unified configuration tools for cohesively managing multi-DNS environments.
- **Rapid record propagation** – Best-in-class providers disseminate DNS record changes in less than a minute.

“Without properly functioning external DNS, Internet-based resources may ‘disappear’ without warning. For enterprises with Web and cloud-based applications and content, external DNS solutions offer reliability, performance and traffic management beyond that of traditional opensource-based solutions.”

– Bob Gill, Gartner Inc.⁶

5 With geo load balancing, users are distributed across endpoints to optimize performance. With performance-based steering, the DNS service automatically directs users to the most efficient endpoint based on geography, current internet conditions or endpoint performance.

6 Gartner, If External DNS Fails, So Does Your Digital Business, Refreshed: 15 September 2016

Service Provider Considerations – Seek out a provider with a dedicated focus on DNS, with a demonstrated record of success, a prominent customer base, and a strong investment commitment.

- **Extensive customer base** – Choose a DNS service provider with a long history successfully powering large enterprises that run their businesses on the internet. Best-of-breed providers count large e-commerce sites, video and content providers, social networking sites and global corporations and web properties as their customers.
- **World-class DNS experience and support** – Best-in-class DNS service providers focus on DNS, making the extensive capital and staffing investments necessary to ensure your success. They employ full-time DNS experts and offer 24x7x365 technical support via phone and email to help you keep your web presence running smoothly around the clock. They offer a variety of support plans and SLA options, and provide onboarding, vprofessional services and training options to help you get up to speed quickly.
- **Strong security expertise** – Choose a provider with a proven history of resilience in the face large-scale and/or complex DDoS attacks, under full load, with large customers. Best-in-class DNS service providers employ a variety of security measures to establish trust and defend against threats. They retain dedicated security experts who closely monitor industry trends and continuously update data center systems and practices to protect against malicious attacks. And they proactively engage in DDoS testing, vulnerability assessment and mitigation planning to manage risk and minimize downtime.
- **Deep industry involvement** – Look for a provider that is actively involved in the internet community in general and the DNS community in particular. Best-of-breed DNS providers drive industry standards and maintain strong relationships with users, vendors and other providers to foster innovation, resolve interoperability challenges and defuse security threats.



Five Questions to ask a DNS Service Provider

On the surface, many managed DNS solutions may appear similar. Many exploit large-scale anycast networks and offer load balancing and traffic steering capabilities. But when it comes to network design, functional depth, and DNS expertise, not all services are the same.

Ask these five simple questions to identify a provider that delivers best-in-class reliability and performance:

- 1 What is the average global DNS response time delivered by your service?
- 2 What is the average propagation time for DNS record changes?
- 3 Do you intelligently steer traffic based on real-time global internet reachability and performance data?
- 4 Do you leverage multiple Tier 1 Transit Providers per PoP to ensure high availability and minimize internet latency?
- 5 Do you serve a large, global customer base with extreme internet application performance requirements?

Conclusion – Make the Right Choice

DNS speed and reliability are fundamental to the performance of your internet applications and cloud services—and essential to your business. You can improve user experiences and boost business results with a cloud-based managed DNS service. But not all managed DNS services are the same. Be sure to choose a service provider that lives and breathes DNS. Best-in-class managed DNS service providers deliver the worldwide DNS infrastructure, experience and resources to ensure your success.

Rethink DNS.

Oracle Dyn is global business unit (GBU) focused on critical cloud infrastructure. Dyn is a pioneer in DNS and a leader in cloud-based infrastructure that connects users with digital content and experiences across a global internet. Dyn's solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC. Adding Dyn's best-in-class DNS and email services extend the Oracle cloud computing platform and provides enterprise customers with a one-stop shop for infrastructure as a service (IaaS) and platform as a service (PaaS).

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. 1006

ORACLE® + Dyn

🏠 dyn.com

☎ 603 668 4998

🐦 @dyn