Ebook:

RETHINK DNS

ORACLE® Dyn

dyn.com 603 668 4998 @dyn

Rethink DNS

Discover smarter ways to use DNS to optimize performance, build resiliency, and manage traffic across hybrid cloud environments

Introduction:

For years, Domain Name System (DNS) solutions have functioned like a phone book for the internet. The system maintains a directory of domain names and translate them to Internet Protocol (IP) addresses. For example, when you type in a URL address, such as mycompany.com, your computer uses DNS to retrieve the website's IP address of 204.12.345.678.

DNS solutions are necessary because regardless of how memorable a URL might be, computers and other connected devices can only access a website based on its IP address. This happens every time you use a domain name, whether you are viewing websites—including links in an email or PDF—or searching for other information on the internet.

As the internet has become the dominant channel for communicating with customers, interacting with markets and delivering services, the role of the DNS has never been more strategically important. The impact of DNS has been elevated even more by the use of DNS servers to manage traffic and workloads across multiple cloud-based systems, content delivery networks (CDNs), and data center locations in an increasingly hybrid world.

Unfortunately, many organizations still rely on first-generation, often in-house DNS solutions that lack the resiliency, global scale, and advanced traffic management capabilities required to support modern hybrid cloud models.

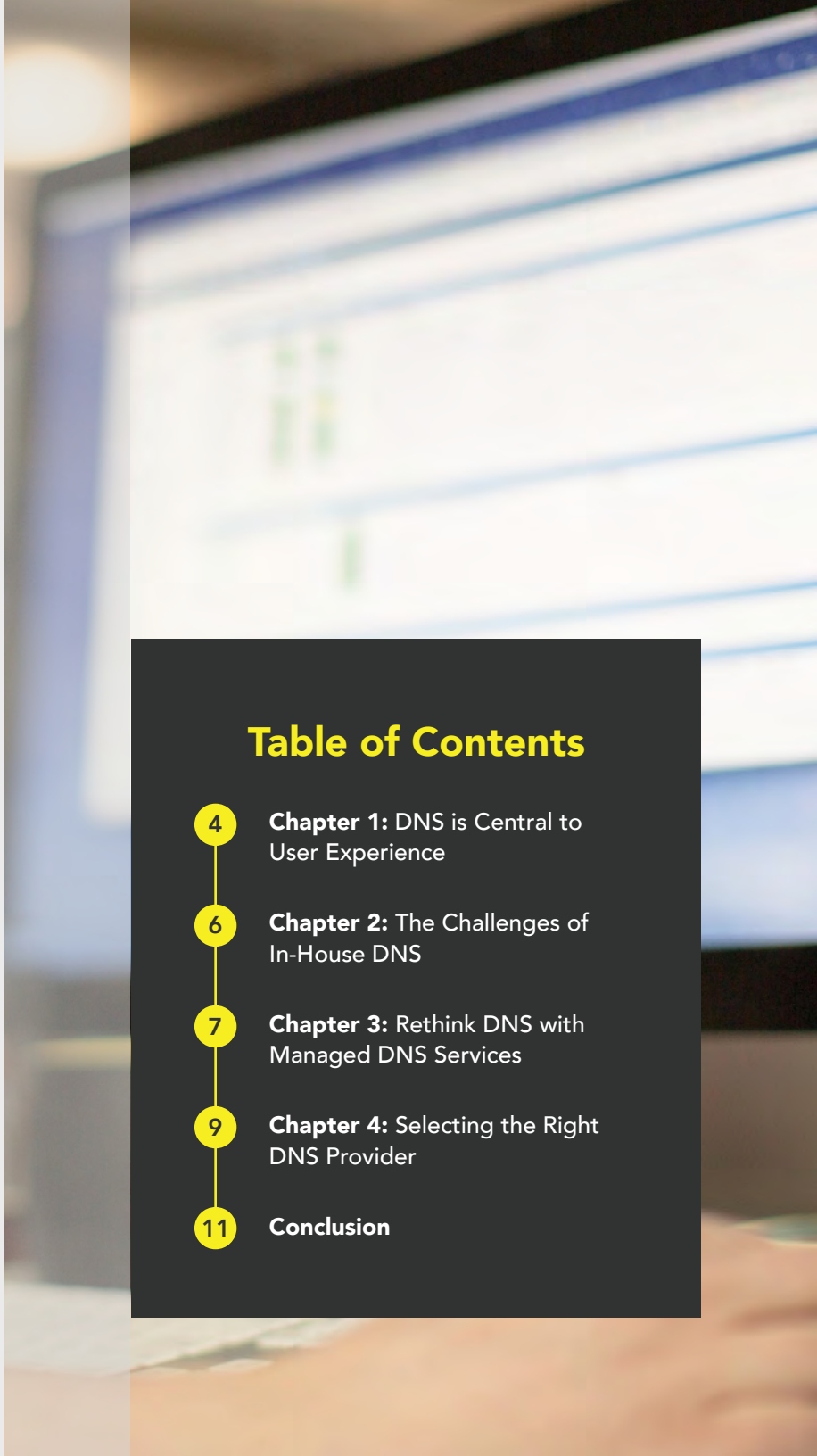


Table of Contents

That's why it's more important than ever to rethink DNS.

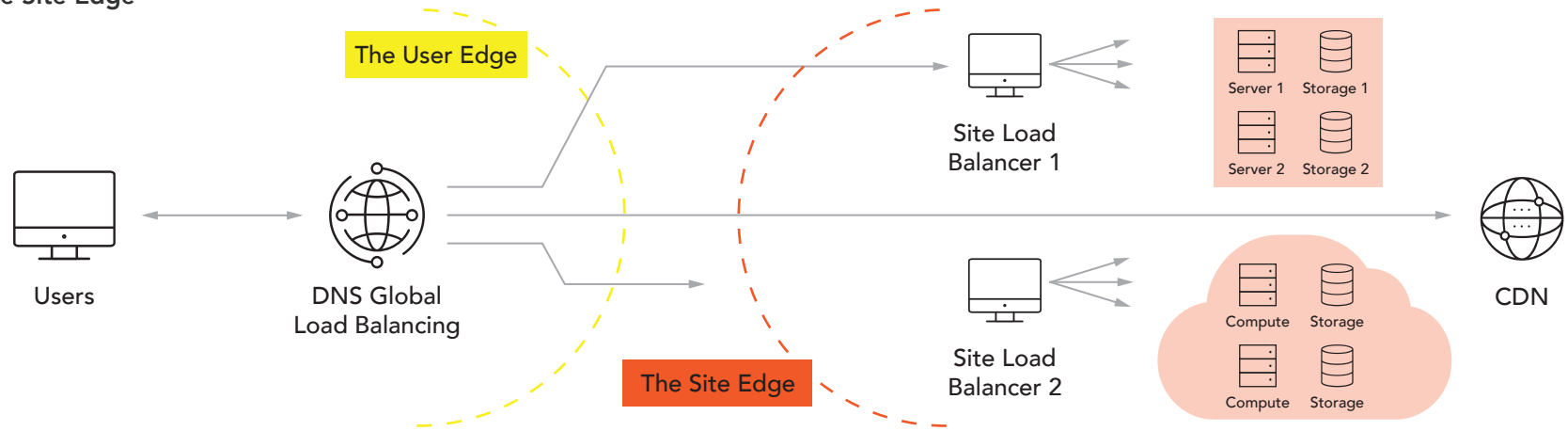
Why do you need to rethink DNS? First, it's an opportunity to rethink your DNS choices: choices around solutions, vendors and configurations that were made several years ago may no longer be optimal in today's environment. The second reason is to rethink the importance of DNS in building digital resilience, including the need for active failover and/or a secondary DNS configuration. The third reason is to rethink the value of DNS as it has evolved to be much more than simple domain name resolution.

Modern DNS with intelligent response capabilities continue to open up new opportunities for traffic steering across hybrid resources. But to take advantage, you need a "federated" approach to load balancing and traffic steering that brings together two "edges" that play key roles:

- **The user edge,** which is powered by DNS and steers user traffic to destination endpoints based on a number of policies.
- **The site edge**, which is responsible for directing traffic to the best path based upon the health of the connection and the endpoint.

When we talk about this federated architecture, we are looking at load balancing at the user and site edges operating independently. This approach applies load balancing and traffic steering policies at the appropriate layer from the user edge to the endpoint where the request is actually served.

Understanding the User Edge and the Site Edge



CHAPTER 1:
DNS is Central to User Experience

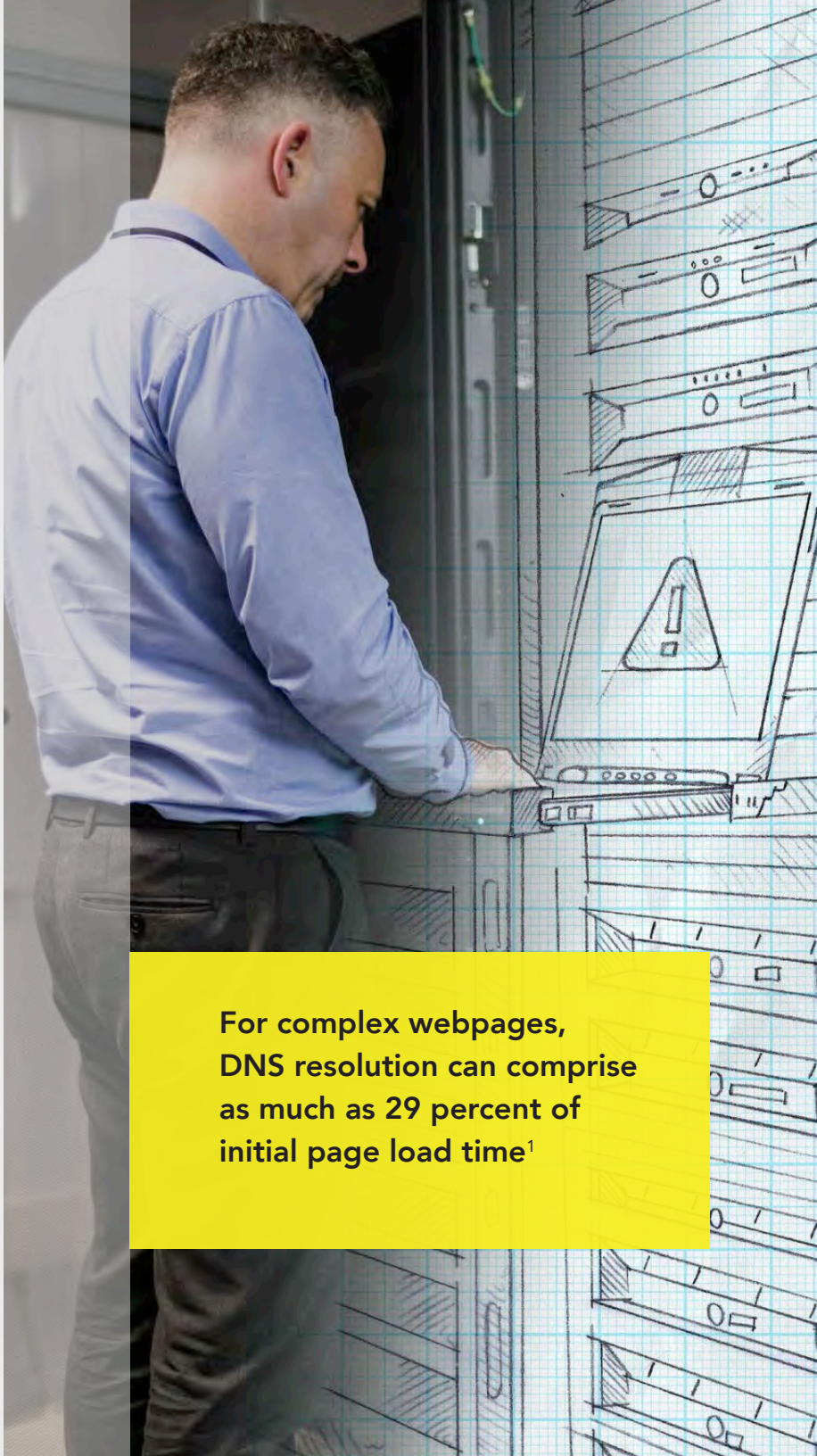
Every interaction with a website or a cloud service initiates a series of DNS queries that maps human-readable names to IP addresses, ensuring users can reach the correct destination. DNS is also about reaching cloud services (for example, in a sharded domain environment. DNS mappings are maintained in special-purpose servers called DNS nameservers. When a user (or machine) enters a URL, a DNS query is routed to a DNS nameserver containing the address mappings for your company's internet domain.

While some assets, such as online applications, content, data and services, may reside in your corporate data center, other assets might be distributed across a CDN, with still more assets residing in the cloud. DNS is responsible for steering every user to the correct source for every query.

A contemporary webpage or web application can involve dozens of DNS lookups. For complex webpages, DNS resolution can comprise as much as 29 percent of initial page load time[1].

Speed and accuracy are critical to a successful DNS strategy because queries can be slowed by internet congestion or latency. The DNS can also be impacted by infrastructure issues, network outages, or a distributed denial of service (DDoS) attack.

The scale, complexity, and volatility of the internet are increasing at a rapid pace. In addition to DDoS attacks, there are myriad outage, routing, and configuration issues that threaten to undermine the services you deliver to users. So even if DNS resolution is successful, it may lead users to an asset that's unavailable or a path with suboptimal latency.

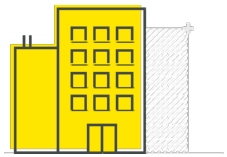


For complex webpages, DNS resolution can comprise as much as 29 percent of initial page load time[1]

1 Based on **Oracle Dyn** internal testing

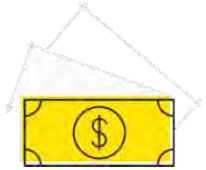
For example, route hijacks are commonplace on the internet. This is when an entity other than the owner "announces" IP space either accidentally or maliciously as part of a "man-in-the-middle" (MITM) attack. When these route hijacks occur, they can significantly affect the way internet traffic traverses the internet via peering relationships—and add unacceptable latency. Disruptions like these are the rule, not the exception. Every day, traffic on the internet is threatened by these relentless assaults on the data traveling through networks.

Conditions will only get tougher in the years to come. Research suggests that threats to DNS availability are on the rise. According to a recent Forrester Consulting study, "90% of firms experience unplanned internet downtime—and half said they experience unplanned internet downtime at least monthly. This unplanned downtime is detrimental to business operations. In fact, 68% of firms identify that a breakdown in the availability and security of their infrastructure has a considerable or catastrophic impact on their business."[2]



78%
of enterprise organizations

experience **4+**
website disruptions
per month



at an average cost of
$1,000 per minute
of downtime

"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."

– Gartner[3]

2 Forrester Consulting, "Make Edge Services an Integral Part Of Your Cloud Strategy," February 2018

3 Gartner, "If External DNS Fails, So Does Your Digital Business," Published: 25 August 2015, Refreshed: 15 September 2016

CHAPTER 2 :
The Challenges of a Default DNS

DNS is a well-established technology. Many companies have built DNS capabilities internally or purchased DNS as part of a bundle from a hosting, cloud, or Internet service provider (ISP). Too often, these approaches and solutions lack the global reach, extensive availability, and high performance of solutions designed and developed by DNS specialists.

In-house DNS solutions tend to be limited in size and scope. Most consist of a relatively small number of DNS nameservers deployed in one or two data centers. And DNS solutions offered as an "add-on" may not have the scalability or expert support required to proactively serve your business. For these reasons, relying on in-house or "add- on" DNS implementations is inherently risky and restrictive.

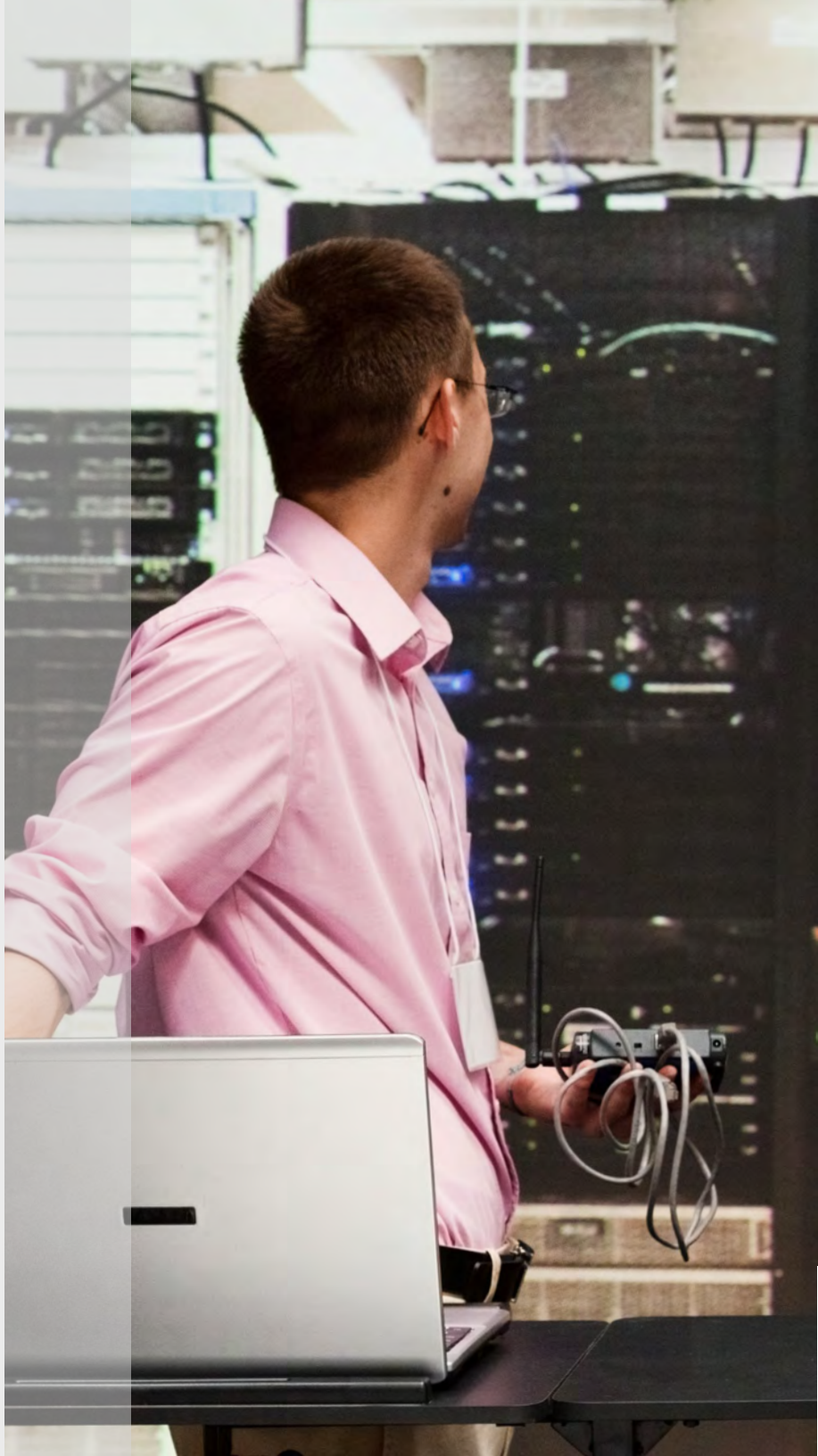
When selecting a DNS solution, it's important to be aware of:

Access – A global user base demands a global DNS solution to ensure that there is always a reachable option

Security – In-house DNS implementations are susceptible to increasingly sophisticated DoS/DDoS attacks, which can overwhelm or incapacitate nameservers

Performance – Although proximity does not always mean better performance, basic physics proves that distance adds latency. Repeated DNS lookups that travel the globe will add significant latency to your services

Implementing a large-scale, in-house DNS network requires time, money, and deep technical expertise. Unfortunately, many companies lack the financial resources to invest in the structured buildout of a global DNS infrastructure. But that's exactly what's required to improve the performance and reliability of your web-based applications and services, while providing the safeguards and support required to overcome an increasingly challenging internet environment.



Organizations need to ask whether they want to focus on building external DNS competency or focus on their core business. Every day, more companies are realizing they can achieve better business results by trusting the operation of their DNS infrastructure to a managed service provider that specializes in DNS.

While ISPs are excellent at measuring and monitoring within their network, this is often insufficient for DNS. ISPs generally have extensive monitoring for network connection and transport services, but are severely lacking in external monitoring, a key measure in DNS performance.

Because of this, ISP-based DNS is subject to regular outages that take a longer time to be identified, mitigated, or fixed. ISPs also do not typically provide service level agreements (SLAs) for DNS. Without this customer safeguard, which is designed to protect and guarantee service quality, customers are left with outages and downtime without any recourse.

CHAPTER 3:
Rethink DNS with Managed DNS Services

The strategic importance of DNS for digital business continues to escalate. But faced with the increasing volatility of the internet, growing demands from hybrid cloud, and the insufficiency of common DNS implementations, it's clearly time for organizations to rethink both how they approach DNS and the value that DNS can deliver.

In this chapter, we'll look at three ways to rethink DNS:

1. Rethink your DNS **solution** and **solution provider**
2. Rethink your DNS **resiliency**
3. Rethink your DNS for **load balancing** and **traffic steering**

Rethink your DNS solution and solution provider

When considering DNS solutions and providers, it's critical to select a DNS vendor that has mitigated major DDoS attacks at scale. While it is never easy to mitigate DDoS attacks, doing so with large, very active global customers is significantly more difficult. DNS companies operating at scale today can manage your additional traffic with minimal disruption, while smaller companies with smaller networks may not be so successful.

Rethink your DNS resiliency

Many of today's businesses live and die by the success of their digital strategies. But without the seamless functioning of their DNS active failover service, finding the path to a healthy endpoint may thwart the achievement of their continuous operations objectives.

Active failover is a DNS service that moves traffic to a healthy endpoint host in the event of degraded service. In such cases, active failover enables your website or web-based applications to remain reachable.

When the system detects an outage, traffic is automatically rerouted to an alternate, predefined endpoint—or even with multiple endpoints in succession. It ensures your traffic finds a route to a healthy location as quickly as possible.

Active failover is configured to check on service endpoint health by running HTTP, HTTPS, Ping, SMTP, TCP protocols to verify that the site is still responding. When the primary service fails to respond, traffic will be redirected to an alternate endpoint. Active Failover considers both the endpoint's ability to serve the user and the condition of the path used to reach that endpoint.

Another area to consider is what happens when it's not your site, but your primary DNS service, that suffers an outage or is attacked. Providers with a global DNS infrastructure enable you to add a secondary, global DNS service. Some organizations even deploy multiple "secondaries" to run in parallel to the primary DNS configuration, immediately resolving DNS queries if service from the primary is disrupted in any way.

Secondary DNS can also be configured to complement your existing in-house approach. One method called "Hidden Master" uses your existing DNS behind the firewall for management and configuration, and then uses a cloud-based DNS for resolving queries.

Rethink your DNS for load balancing and traffic steering

Today's network edge is increasingly important in connecting users to the digital content and web services that they need to reach. This is driving a new approach to load balancing and traffic steering that starts at the edge. Powered by DNS, edge-based global load balancing (GLB) steers user traffic to destination endpoints based on IT-defined policies.

Intelligent response means that a response to a DNS query is based on information that determines the target endpoint or the optimal network path to an available endpoint. A basic example of intelligent traffic steering is to "round-robin" traffic across multiple cloud or data center locations for load balancing.

A more sophisticated example might involve taking into account the geographic location of the user. For example, a query from London is routed to a European-based PoP, while a request from San Francisco is routed to a Western U.S.-based location. Intelligent response can also be combined with real-time internet data to layer factors such as latency, availability and security into traffic steering decisions.

What's more, these capabilities can help monitor your digital edge and DNS environment to detect and mitigate threats and anomalies—whether DDoS, routing snafus, DNS spoofing, or IP hijacks. Traffic steering can be used to shift traffic away from threats before they have a negative impact on your infrastructure.

CHAPTER 4:
Selecting the Right DNS Provider

When evaluating a managed DNS service, you need to look beyond the technical and functional aspects of the solution and consider the skills, commitment, and integrity of the service provider. It's important to understand the provider's underlying network architecture, the features and capabilities offered, and the vendor's reputation for helping its customers reach their business goals.

Avoid ISPs or CDN providers offering DNS services as a side feature. Remember, your business is at stake. You don't want to risk your reputation with a company that provides DNS services as an add-on.

Best-of-breed, managed DNS service providers should have the deep knowledge, global infrastructure, and security expertise to help you succeed. These experienced providers operate large-scale, highly resilient DNS networks that deliver superior user experience, regardless of the location of the user or the content. They utilize advanced traffic optimization and load balancing features to ensure performance and availability. And they provide 24/7 technical support to keep your operations—and your business—running around the clock.

Evaluating DNS solution providers

When reviewing DNS service providers, make sure they provide a robust IT infrastructure and architecture, along with the comprehensive offerings that are standard among top-tier providers.

Architectural Considerations:

- **Global scalability** – large-scale dynamic networks should have multiple points of presence (PoPs) placed in geographically optimal locations worldwide, such as internet exchange points (IXPs)
- **Anytime availability** – networks and equipment should include multiple power grids, flood plains and fault lines to protect against disasters; fully redundant server configurations to protect against hardware failures; and a curated mix of multiple Tier 1 transit providers

Functional Considerations:

- **Advanced traffic steering** – innovative features such as zoning, geo-load balancing, failover, and performance-based steering can maximize the responsiveness and reliability of web-based applications and services
- **Global internet visibility** – providers should help monitor and analyze real-time and historical internet performance data to optimize resiliency, availability and routing
- **Open programming interfaces** – standards-based APIs should be supported for integration with enterprise administrative systems and other DNS services
- **Rich management tools** – simple-to-use administrative interfaces can help you configure DNS records and track DNS performance and reliability
- **Support for DNS Active Failover** – providers should be able to address performance and latency issues—or in the case where you lose a site completely, the same DNS technology should be able to reroute traffic to an available endpoint. Properly configured, the failover is fully automatic.
- **Support for secondary DNS** – providers should support a variety of redundant, multiple DNS service deployment options and provide unified configuration tools for cohesively managing multiple DNS environments
- **Rapid record propagation** – providers should be able to disseminate DNS record changes in less than one minute

Conclusion

The speed, reliability, and security of your DNS infrastructure are critical to the performance of your internet applications and cloud services, the quality of the end-user experience, and the success of your business.

As you rethink your DNS strategy, remember the following:

- Make sure you have the right DNS solution in place, whether it's adding a managed or cloud-based provider to your in-house technology, or moving to a managed provider built for today's internet
- Ensure your data reaches its destination securely and efficiently by adding resiliency with an active failover service
- Consider a secondary DNS or a multiple DNS setup to avert problems in the event of a DNS service failure
- Use managed DNS to deliver the many benefits of load balancing and traffic steering

One of the quickest ways to rethink DNS is to trust your business to proven experts. Engage a provider with the deep domain expertise, global infrastructure, and security knowledge you need to achieve your goals.

Find out how Oracle Dyn solutions can benefit your organization. Learn more at: **dyn.com**

The Oracle Dyn global business unit (GBU) helps companies build and operate a secure, intelligent cloud edge. Our services help customers operate resilient, secure, and high-performance sites and applications via fully managed DNS and Web Application Security services. Dyn's solutions are backed by one of the world's most comprehensive internet performance data sets, collecting more than 200 billion internet data points daily across a global network. More than 3,500 customers rely on Oracle Dyn's edge services, including preeminent digital brands such as Netflix, Twitter, CNBC and LinkedIn. For more information, visit dyn.com.

ORACLE® Dyn

dyn.com 603 668 4998 @dyn