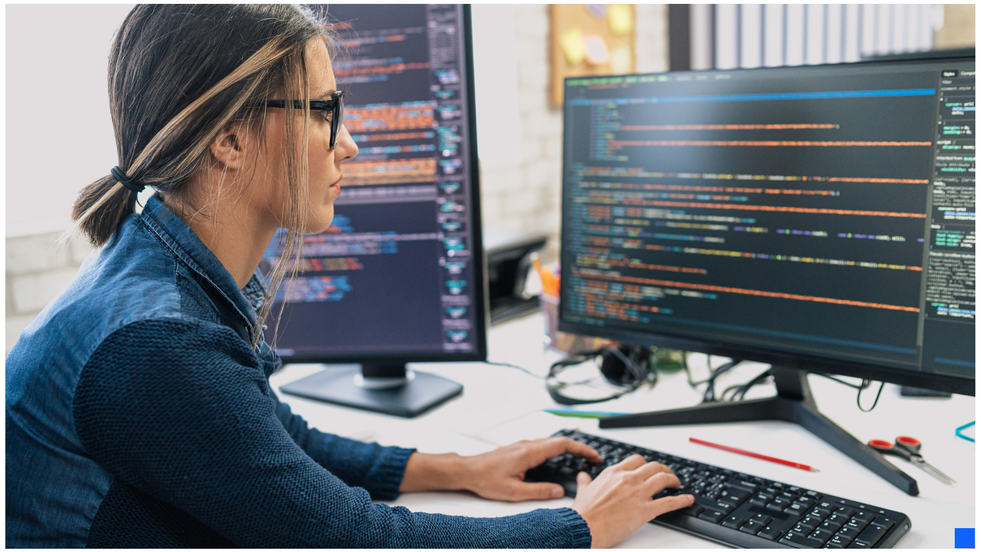
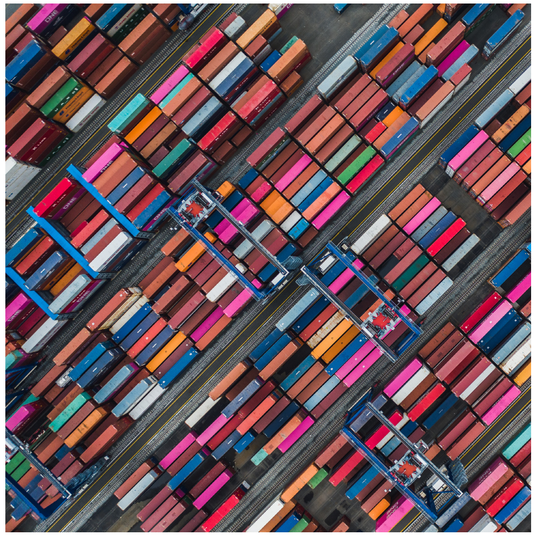
Improving network resilience at scale with IBM NS1 Connect

Contents



01

Introduction



Why is ensuring network reliability so complicated?

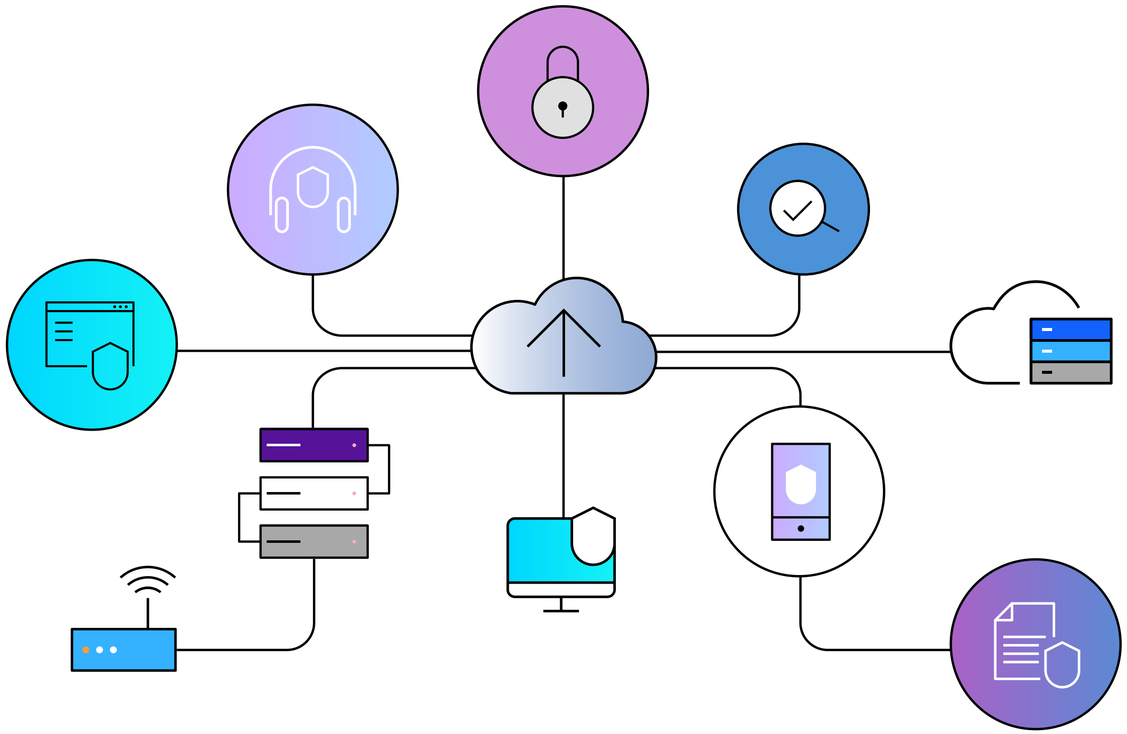
In today's digital age, resilience in business technology is more critical to business continuity than ever. The ability to keep customers, partners and employees securely connected to websites and external applications at all times is paramount to business success. 34% of enterprises,[1] for example, report that an hour of downtime can cost them more than $1 million. That hour of downtime today means lost sales, employee productivity and more. Since network and application infrastructure are foundational to business technology, they need to be highly reliable and adaptable to disruption. Without a resilient network, companies face risks like poor user experience, potential data breaches, or outages and other issues.

To meet this challenge, leading organizations invest in flexible, diverse and redundant IT infrastructure. For example, IBM research found that companies furthest along in digital transformation initiatives make full use of multicloud/hybrid cloud architectures, with 25% of the enterprise's applications deployed on the cloud.[2] They're also leveraging multiple new and emerging technologies supported by the cloud.

Of course, increasing infrastructure complexity comes with management challenges. When coupled with a rise in large-scale network outages, cybercriminal activity and even natural disasters, most companies today are at risk of experiencing an issue that knocks key applications and websites offline. In a digital-first world, this can mean you're effectively closed for business—resulting in lost revenue, customer churn and damages to brand reputation.

However, investments in foundational infrastructure that can often go overlooked—like external authoritative DNS—can improve overall network reliability in the face of disruptions and even help companies realize other gains.

IBM research found that companies furthest along in digital transformation initiatives make full use of multicloud/ hybrid cloud architectures, with 25% of the enterprise's applications deployed on the cloud.[2]



02

The role DNS plays in improving reliability

Look to the “backbone of the internet” to ensure more resilient, reliable connections to applications and websites

As the connection point between any company and its customers, the domain name system (DNS) plays a vital role in resilience. Even when all of an organization’s core systems are up and running, if there’s no way to access those systems through a customer-facing website, the company is “offline” for all intents and purposes.

Therefore, it is critical for your authoritative DNS solution to be reliable and performant to help ensure high availability of websites and applications. To meet this bar, authoritative DNS needs to:

- Have scalable capacity to meet unexpected spikes in traffic
- Include redundancy and failover mechanisms
- Mitigate downtime from service outages by proactively steering application traffic away from unhealthy endpoints
- Enable automation of routine maintenance

Legacy, on-premises authoritative DNS solutions struggle to provide reliable connections at the speed and scale needed today. To combat this, companies are modernizing by switching to a managed or SaaS-based DNS service. Managed DNS service providers run authoritative servers on behalf of their customers and are experts in delivering this mission-critical service with global servers built for reliability and performance.

Most managed DNS providers enable features needed to provide resilience at a global scale: better reporting, API automation, traffic management and other features hard to achieve in a self-operated system. IBM® NS1 Connect provides not only these “table stakes” features expected from a managed DNS provider, but also more sophisticated features that can help improve resilience.

Capacity and coverage at scale

Meet unexpected changes in traffic patterns without missing a beat

Outsourcing authoritative DNS gives companies immediate access to massive network scale that would be cost prohibitive to build and maintain internally. This scale can help mitigate a common cause of outages or performance issues: unexpected traffic spikes that exceed the capacity of your authoritative DNS solution. There are many events that can cause this type of spike in traffic: for example, a dramatic and unexpected surge in legitimate traffic, or a misconfiguration error.

A more concerning cause for traffic spikes is a distributed denial of service (DDoS) attack. In a DDoS attack, malicious actors will attempt to overwhelm a DNS server with queries to take it offline. DDoS attacks can target different layers of DNS architecture, but all tend to share the same playbook of overwhelming the target with traffic. If successful, the traffic renders the server—and therefore any connected websites or applications—inoperable. Typically, “botnets,” or remotely controlled, hacked computers, are used to flood the targeted server. DDoS attacks are one of the more common cyberattacks, so if your company has fallen victim to one before you’re not alone.

IBM® NS1 Connect offers the capacity and scale needed to absorb dramatic traffic spikes and continue to answer every DNS query promptly with:

- Overbuilding and auto scaling, which can absorb the volume of a typical DDoS attack
- Vastly overpositioned PoPs that you can steer queries to when under extreme duress
- Global architecture designed to improve availability and decrease latency

Of course, bad actors are continuously adjusting and adapting attack techniques. Another benefit of outsourcing to a managed provider is that it removes the burden on your internal team to keep up with a rapidly changing landscape.

“We haven’t had any issues at all with uptime when there is a DDoS attack. When we have been the subject of an attack, NS1 has been up and stable for us, as well as performant. On top of that, it has been able to provide us with pretty good details of what kinds of attacks we have been subject to and what NS1 was doing at the time. Even if we are undergoing DDoS attacks, NS1 will still serve DNS for us.”

Link to full review here.

11%

DDoS attacks represented 11% of all cybersecurity attacks in 2021 for a cross-section of industries, IBM research finds.

04

DNS redundancy for when disaster strikes

Avoid single points of failure within critical infrastructure, without adding management complexity

When DNS fails, or is taken down in an attack, the websites, applications and online services that depend on it effectively disappear from the internet, taking revenue and brand reputation down with it. That's why companies focused on building network resilience will avoid a single point of failure within authoritative DNS by implementing a secondary, separate IBM® NS1 Connect infrastructure.

Implementing DNS redundancy can be achieved with IBM® NS1 Connect in two ways:

- Adding IBM® NS1 Connect Dedicated DNS, a separated, redundant DNS layer that sits alongside Managed DNS
- Using IBM® NS1 Connect Managed DNS as a primary or secondary provider alongside another DNS provider

IBM® NS1 Connect Dedicated DNS is a single-tenant, physically and logically separate anycast network that seamlessly synchronizes with your Managed DNS network providing redundancy without increasing management overhead.

Or, if you have multiple DNS providers, you may prefer an architecture that supports a dual-provider DNS configuration. IBM® NS1 Connect Managed DNS can be configured as either the primary or secondary provider. We also support toolkits like octoDNS and Terraform to make it easier to manage multiple DNS providers.

05

Minimize the effect of outages on your end users

Avoid service deprecations and outages with automated traffic steering

It's best practice to avoid single points of failure—especially within critical IT infrastructure—through diverse and redundant architectures. Many organizations have implemented redundant systems to mitigate the impact of an outage on critical business operations.

What they may or may not have in place, however, is the automated mechanism that redirects traffic to those redundant systems when an issue arises. Your application delivery environment can change quickly, and without automated routing policies you are still vulnerable to outages or downtime.

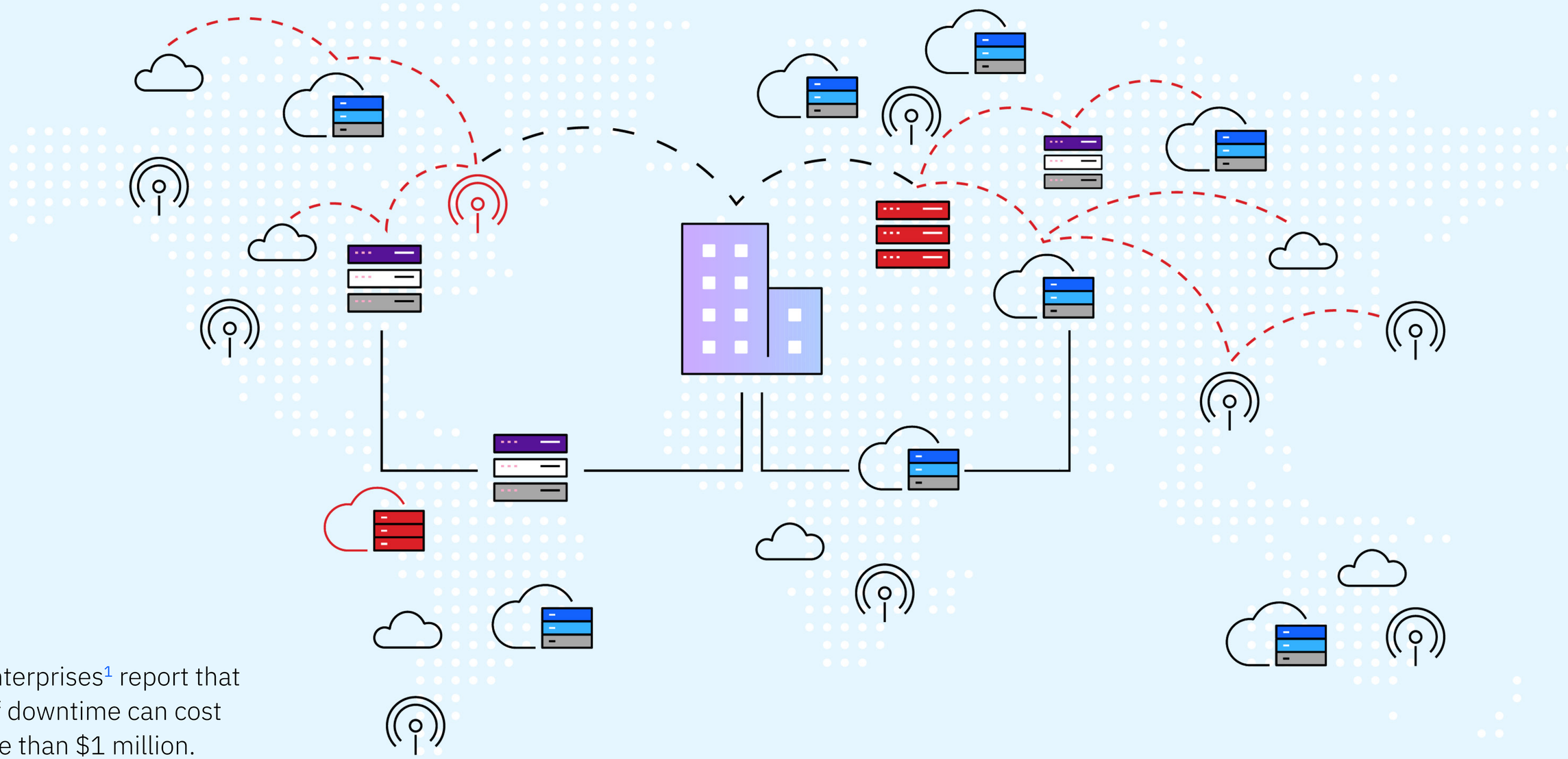
IBM® NS1 Connect's sophisticated traffic steering technology uses the power of DNS to automatically reroute traffic between service providers in the event of a network service disruption. While the capabilities are sophisticated, managing traffic steering on IBM® NS1 Connect is pretty straightforward. Automated traffic steering logic paired with endpoint health monitors enables you to seamlessly divert traffic around outages to avoid service deprecations and maintain maximum performance levels even when crises hit.

With a wide range of options for traffic steering, from simple geolocation-based options to sophisticated logic based on real user monitoring (RUM) data, IBM® NS1 Connect enables you to optimize how you route traffic across your network for a variety of use cases beyond failover mechanisms.

For example, multicloud and multi-CDN deployments add the flexibility and scale you need to ensure reliability, though managing commits with various providers can quickly become complicated. IBM® NS1 Connect's traffic steering capabilities can also be used to optimize end-user experience while taking into cost commits across vendors in multicloud and multi-CDN deployments.

18%

Companies furthest along in their cloud journey dedicate about 18% of IT budget to cloud spend, according to IBM research.[1]



34% of enterprises[1] report that an hour of downtime can cost them more than $1 million.

06

Embrace automation

Minimize DNS configuration errors and streamline routine maintenance

As your IT infrastructure grows in size and complexity, so does the work required to manage your infrastructure. Mistakes happen when trying to keep up with this work through manual processes. Sometimes a simple “fat finger” error can redirect traffic to a dead end. Sometimes a configuration that looks fine in a test environment doesn’t work in production. Protecting against these honest mistakes is just as important as protecting against nefarious actors.

Automating routine maintenance can minimize the likelihood of “fat finger” errors, but legacy authoritative DNS solutions make it challenging to move away from manual processes. BIND, for example, doesn’t have an API and wasn’t built to support any form of automation. DIY architectures usually aren’t built to support standard automation platforms like Ansible or Terraform. It’s near impossible to orchestrate DIY architectures using third-party tools.

IBM® NS1 Connect’s high-performance and API-first technology stack allows for automation and integrations with tools you are already using. This empowers your teams to do their best work by integrating with popular DevOps tools and applications like Ansible and Terraform. Customers leverage our robust API to automate builds, production deployments and testing environments. Additionally, routine network maintenance can be handled automatically, increasing the efficiency of your team.

“NS1 has greatly reduced DNS maintenance work in our organization... For instance, to deploy a new region...it would take a lot of very manual work to add records. Now we can just Terraform it. That process has gone from taking the relatively long period of an entire day to being able to Terraform, apply, and be done with it.”

Valentino Volonghi
CTA at a tech vendor
Full review can be found here.

07

Conclusion

Keeping end users reliably connected to your applications and websites is a business priority; if your digital presence is offline, you're essentially "closed for business." Ensuring high reliability and availability is challenging given the complexity of underlying application delivery environments, but IBM® NS1 Connect can help address some of the most common reasons for an outage or service deprecation—and give you the tools to do much more with authoritative DNS. Visit ibm.com/products/ns1-connect to see how our solutions enable you to streamline DNS management, optimize application performance, get targeted, actionable DNS traffic data and more.

About IBM® NS1 Connect
IBM® NS1 Connect provides premium managed DNS and advanced traffic steering solutions delivered as-a-Service, to make connections faster and more reliable. That's why companies around the world depend on us to optimize their network traffic, identify network performance-impacting problems and lower costs, so they can deliver the optimized experiences their users expect online.

1. Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs $300,000+; 34% of Companies Say One Hour of Downtime Tops $1Million, ITIC, 16 May, 2019.

2. IT Organization Benchmark Report - Key Findings, IBM, 18 January, 2024.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2024