

DNS Monitoring Use Cases

HANDBOOK



catchpoint™

DNS Monitoring – Why is it Important?

DNS is at the core of the world wide web. It maintains the address record of every single domain, and the DNS resolution process handles millions of requests, keeping the traffic flowing and ensuring the internet is accessible to everyone. An issue with DNS performance or availability can bring the online world to a complete standstill, so pro-actively monitoring DNS should be an indispensable part of any well-planned monitoring strategy.

Being the most critical processes of the internet, it is also the most vulnerable. Over the last decade, there have been numerous cyberattacks that have specifically targeted DNS. These attacks are yet another reason why it is absolutely necessary to monitor DNS performance. DNS monitoring is the only way to ensure resilient DNS service and to be better prepared when faced with a major DNS attack.

In this handbook, we discuss scenarios that disrupt DNS performance and how Catchpoint equips you with the right tools to prevent and mitigate DNS-related issues impacting your application.

1

Monitoring DNS Configuration

1.1 - Zone Transfers

The primary DNS server is managed by the Domain Registrar, but many organizations prefer to use a secondary DNS server. Large enterprises have their own global secondary DNS servers, but most enterprises are opting for third-party managed DNS providers such as NS1, DynDNS, or UltraDNS. These managed DNS service providers are not only cost effective, they provide scalability and security by adding redundancy to the domain's DNS configuration. It also offers user-friendly dashboards that makes the task of DNS Administrators easy and straightforward.

In a primary-secondary DNS server setup, zone transfer between these servers is required to keep the DNS records updated and relevant. Managed DNS services provide a zone transfer feature which automatically fetches the zone file from the primary DNS server and updates the secondary DNS server; this ensures that any changes to the zone file is duplicated across DNS servers.

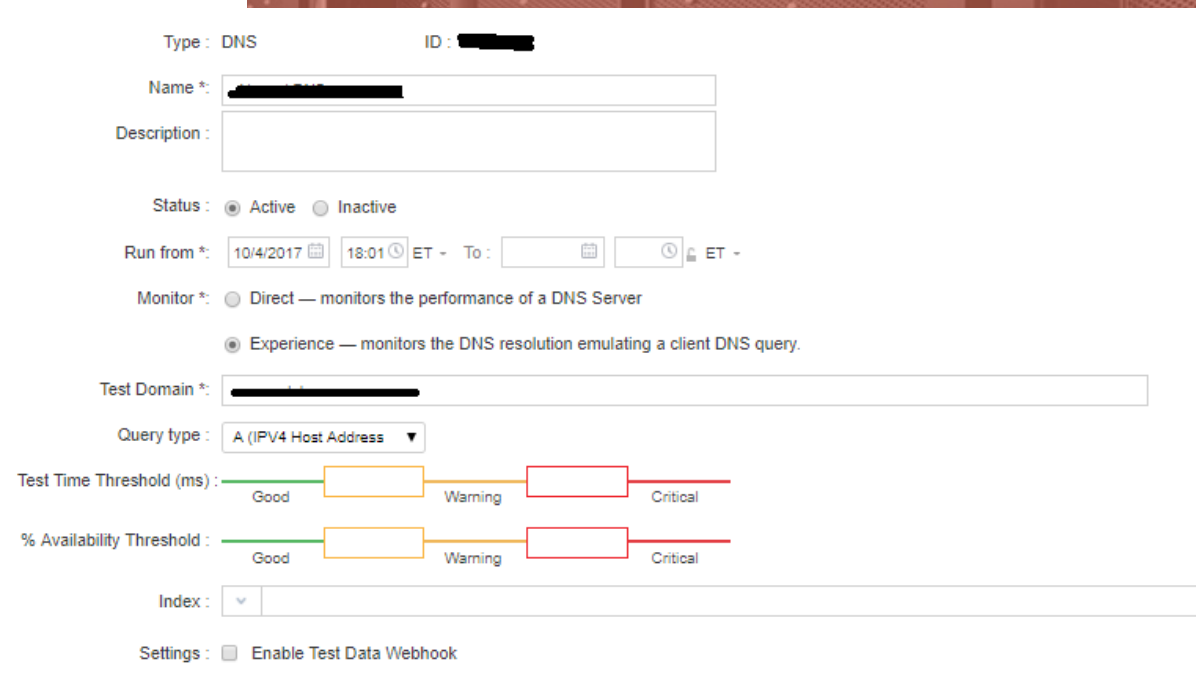
When troubleshooting DNS issues, it is important to take into account changes to the zone file. There could be instances where the DNS zone transfer may not have completed, creating a bottleneck in the DNS resolution process. In such scenarios it can be a challenge to identify whether the roadblock lies with the primary DNS or the secondary DNS server, as the DNS resolution process queries multiple servers and there are multiple query levels before the domain IP is returned.



Using Catchpoint, you can monitor zone transfers from multiple locations and from different ISPs. The different DNS test types and alerts will help you stay a step ahead so issues are tackled before they impact end users.

Analyzing the DNS performance at different locations is important when trying to decide the best point-of-presence for serving DNS requests.

In addition to monitoring zone transfers, Catchpoint gives you the tools to measure performance of private DNS servers and zones accessible via public IP address on Port 53. If private DNS records are inaccessible via a public IP address, Enterprise Nodes can be deployed on your local network or within the corporate premises for monitoring.



The screenshot displays the configuration page for a new DNS test in the Catchpoint interface. The form includes the following fields and options:

- Type:** DNS
- ID:** [Redacted]
- Name *:** [Redacted]
- Description:** [Empty text box]
- Status:** ☒ Active ☐ Inactive
- Run from *:** 10/4/2017 18:01 ET To: [Empty date/time selector] ET
- Monitor *:** ☐ Direct — monitors the performance of a DNS Server ☒ Experience — monitors the DNS resolution emulating a client DNS query.
- Test Domain *:** [Redacted]
- Query type:** A (IPv4 Host Address) [Dropdown arrow]
- Test Time Threshold (ms):** A horizontal scale with three segments: Good (green), Warning (yellow), and Critical (red).
- % Availability Threshold:** A horizontal scale with three segments: Good (green), Warning (yellow), and Critical (red).
- Index:** [Dropdown arrow]
- Settings:** ☐ Enable Test Data Webhook

1.2 - Nameserver Issues

Having more than one name server set to a particular domain name provides redundancy and works for ensuring the website's availability at all times. However, how do you ensure that all the nameservers are returning results as expected?



How Catchpoint Helps

With Catchpoint's DNS direct test, it is possible to monitor the availability and performance of each of the nameservers set for a domain. Recently, a customer was experiencing intermittent DNS failures for a web test.

A DNS Experience test showed the domain had a CNAME record for which there were four sets of nameservers being used.

- u1.*****.com
- u2.*****.com
- r1.*****.com
- r2.*****.com

Running DNS Direct test to the domain through all four of the name servers, we were able to identify the two nameservers that were unresponsive (r1/r2).

Domain *: prod-halb-nlb-a2740fbd7ae96c31.elb.us-east-1.amazonaws.com

Nodes *: Atlanta - Cogent

DNS Server *: r1.amazonaws.com
(IP address: 8.8.8.8 or hostname: ns1.site.com)

Query type: A (IPv4 Host Address)

Protocol: ☒ UDP ☐ TCP

Additional Settings: ☐ Disable Recursive Resolution

Atlanta - Cogent

Run Time: 04/06/2018 08:16:38 ET Monitor: Direct

Public URL: <https://p.catchpoint.com/ui/Entry/PW/IEnj-EU4-CT-I533-0-jVm7hFg5UI-AV0AR0-jVm7hFg5UI-EU4>

Domain: prod-halb-nlb-a2740fbd7ae96c31.elb.us-east-1.amazonaws.com

Response (ms): 2 Error: No answer or authority was received

LEVEL 1

Group 1

Address	Average Time (ms)	Bytes	Return Code	Error
205.251.192.27:53 [r1.amazonaws.com]	2	0	None	

1.3 - DNS Record Verification

Propagation of updated DNS records takes time, and verifying successful propagation is usually a waiting game that leaves your DNS performance at risk.

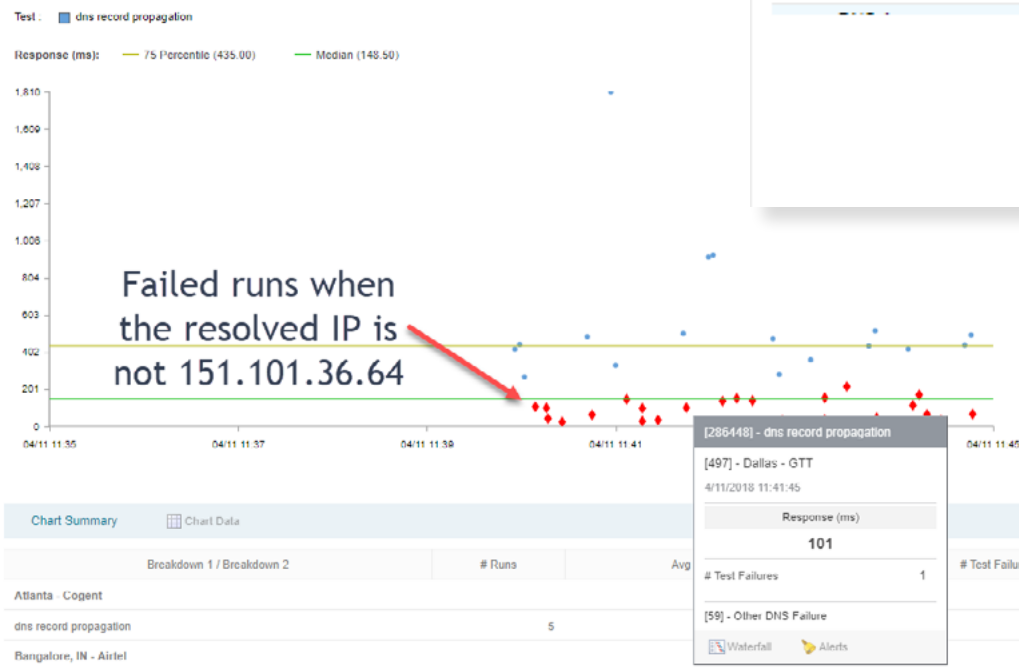
In such a scenario, you can use Catchpoint's DNS Experience test to verify successful DNS propagation globally. The test takes advantage of our globally-distributed monitoring infrastructure comprised of 600+ servers with a mix of Backbone Network, Consumer ISPs and Mobile Network locations. With this large number of test locations, you can easily identify locations that are still serving stale DNS records.



How Catchpoint Helps

Catchpoint's advanced alerting system can be configured to trigger a failure when the returned DNS record doesn't match the updated DNS record. Below is a snapshot of such a test. The test will fail if it doesn't get the IP 151.101.36.64 when resolving the DNS for the domain www.catchpoint.com from any location.

The scatterplot chart below shows the failed runs from the location where the resolved IP was different from the one specified in the alert configuration. Proactively monitoring the DNS propagation will speed up the process of identifying the nameserver with stale records.



Alert Type	Trigger
Synthetic Alert Types	Level: Last
Timing	
Test Failure	Resolved Name: www.catchpoint.com
Ping	Record Type*: A (IPv4 Host Address)
Availability	Match*: <input checked="" type="radio"/> Any <input type="radio"/> All
IP Address	Not Equal to
DNS	151.101.36.64
DNS General	TTL:
	<input checked="" type="checkbox"/> Enforce test failure when triggered on a node.

2

DNS Attacks

2.1 - DNS Flood

DNS servers hold the address details of all the domains on the Internet just like a telephone directory. When a user accesses a domain, the DNS query returns the IP address of the domain and redirects the user to the server hosting the domain. A DNS zone is a distinct portion of the domain name space in the Domain Name System. For each zone, administrative responsibility is delegated to a single server cluster.

DNS flood is a type of distributed denial of service (DDoS) attack in which the attacker targets one or more DNS servers belonging to a given zone, attempting to hamper resolution of resource records of that zone and its sub-zones.

In a DNS flood attack the offender tries to overwhelm a DNS server (or servers) with apparently valid traffic. The sudden spike in traffic taxes the server resources and impedes the servers' ability to direct legitimate requests to zone resources.






How Catchpoint Helps

During a DNS flood attack, the DNS servers will either stop responding or the query time will increase, which means the end user will spend more time waiting for the DNS resolution to complete. Catchpoint allows you to monitor the response time for a particular DNS server using DNS Direct test to identify anomalies:

Monitor *: ☒ Direct — monitors the performance of a DNS Server
☐ Experience — monitors the DNS resolution emulating a client DNS query.

Test Domain *:

DNS Server *: 
(IP address: 8.8.8.8 or hostname: ns1.site.com)

Query type :

Keeping track of the DNS response times across multiple locations will help you identify an attack as soon as it happens. This gives you the time to implement failover strategies and mitigate the impact of the attack on the end user.

2.2 - DNS Spoofing/Man in the Middle Attacks

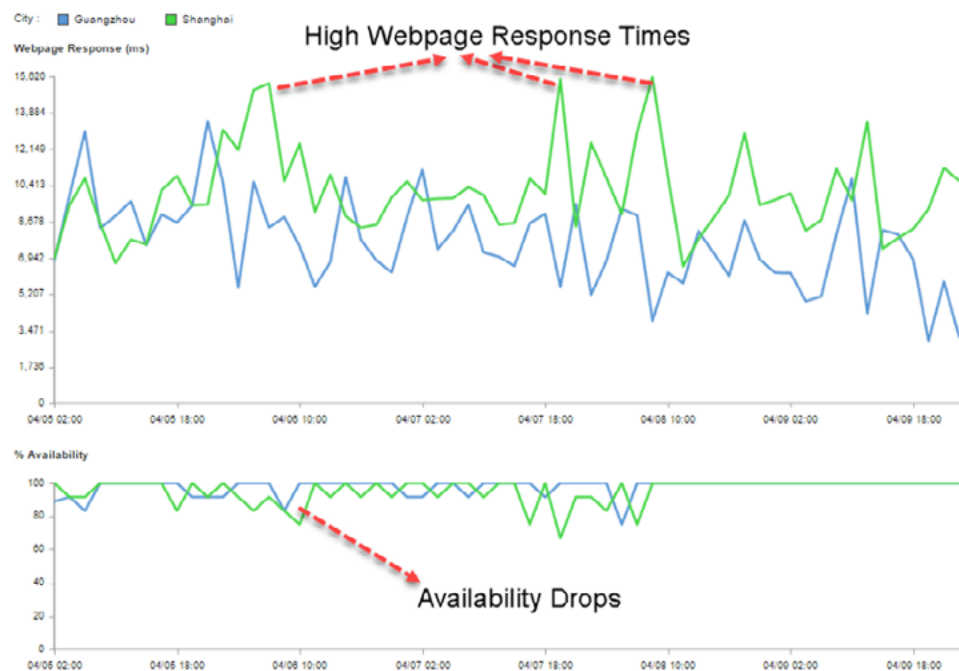
A good monitoring strategy built around DNS definitely helps uncover issues such as DNS spoofing and Man in the Middle attacks. A Man in the Middle attack, or MITM, is a situation wherein a malicious entity can read/write data being transmitted between two or more systems (usually between a user and the website they are surfing).

In a MITM attack, the attacker may use one of the many possible ways to split the TCP connection into two separate connections. One connection will be used between the client and the attacker, whereas the second connection will be used between the attacker and the web server, making the eavesdropper act like a proxy who is able to intercept data being sent between the client and the server.

Such attacks are common when it comes to HTTP because of the way the protocol is designed. HTTP works as a request/response protocol. A web browser is typically the client requesting an object, and an application or a website hosted on the web is the server responding to the request. It's easy for an Internet Service Provider (ISP) or a network administrator to run a packet sniffer such as Wireshark, Fiddler, or HTTP Analyzer on the Network and capture the traffic moving between the client and the server.



With Catchpoint's ability to set up alerts against the responses received from DNS servers, validating the responses and identifying security related issues is easier. A simple use case would be to set up DNS tests along with alerts that trigger when the IP returned after the DNS lookup is different from the expected IP range.



Recently, a customer who was using our web testing functionality to monitor their performance complained they were seeing a lot of performance issues from some of their locations in China.

Analyzing the waterfall charts helped us discover the site was under attack. The site was being redirected to random sites using a 302 temporary redirect indicating a MITM attack.

3

Benchmarking Public DNS Resolvers

A lot of our clients use a multi-DNS architecture. DNS monitoring is not exclusively for identifying performance issues. The performance data aggregated by different Catchpoint tests can also be used to benchmark DNS service providers.

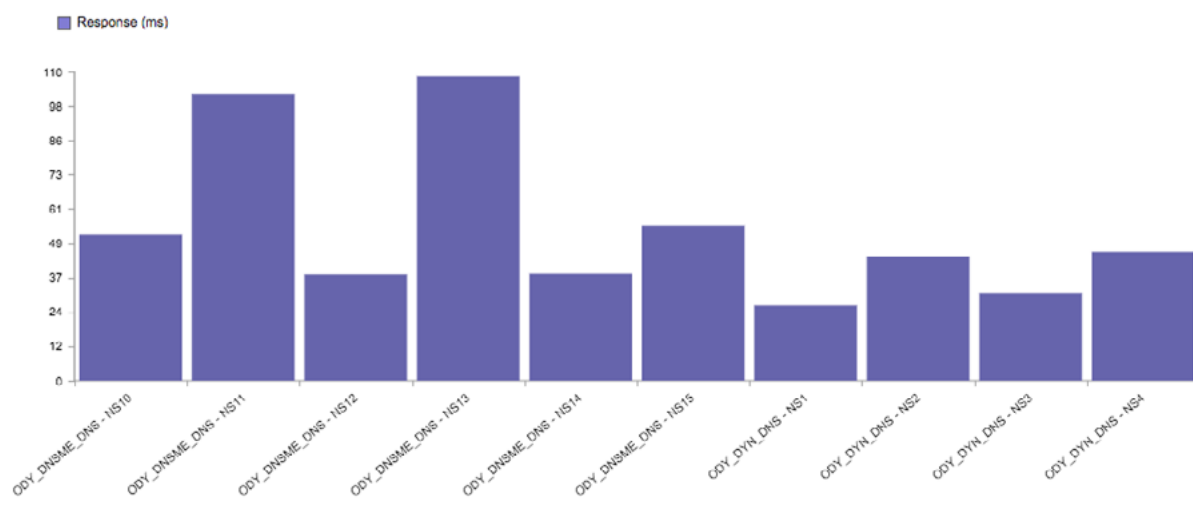
It is crucial to understand how different DNS service providers perform across different locations. With more and more enterprises moving to public DNS and the introduction of Cloudflare+Mozilla's open source DNS Resolver (1.1.1.1), the need to monitor these resolvers has become important as well.



How Catchpoint Helps

Catchpoint allows you to override the DNS resolver for real browser tests to compare and contrast the performance of different DNS resolvers and get an understanding of the performance of these resolvers.

For example: One of our clients use two different DNS Vendors: DNS Made Easy and Oracle+Dyn. Here is a comparative chart showing the performance of these vendors:



In this case, we can clearly see that DNSMadeEasy is slower when compared to Oracle+Dyn for this particular client.

Another example could be setting up Real Browser tests in Catchpoint using Google's Public DNS (8.8.8.8) and Cloudflare's Free DNS (1.1.1.1) and comparing the performance of your website and see which resolver reported better DNS time. A fast DNS can do wonders for your website performance.

4

Monitoring CDNs

The primary purpose of a Content Delivery Network (CDN) is to get content to users faster. CDNs reduce latency in the delivery chain by introducing multiple points of presence that are closer to the end user than the origin server. The CDN speeds up content delivery, the webpage loads faster, the end user gets a positive digital experience.

Many organizations are now using multiple CDN providers, so it is important to keep track of their performance. A CDN monitoring strategy is important and should account for network performance, CDN availability, content integrity, and validity.

Monitoring the CDNs on which your application depends can help you tune application performance; you can pinpoint locations where the CDN performance is degraded and you will be able to better evaluate the CDN providers you are using. Benchmarking different CDN providers will let you ensure that yours is delivering optimum performance and is not breaching SLAs.



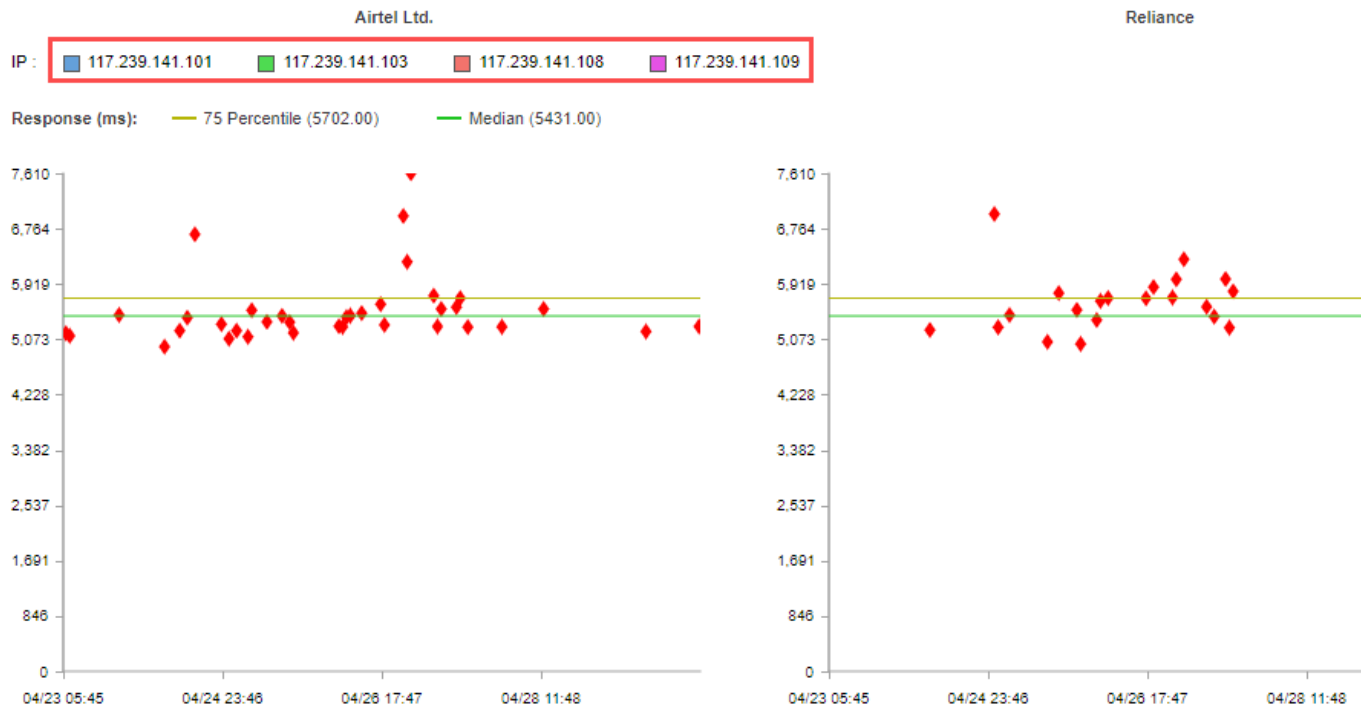
How Catchpoint Helps

Some CDNs use DNS redirection methods to redirect users to the proper edge servers, allowing faster loading of the web pages and assets. We have monitored instances where the nameservers of the CDN were slow to respond and caused performance degradation. It is important to monitor such cases; the best way to do so is using the Direct DNS test type in Catchpoint along with a combination of DNS Experience and Web tests.

Recently, Catchpoint discovered an issue with the CDN used by a major online payment gateway. This company is using a well-known CDN provider to serve their content across the globe, but their website had high DNS resolution times when accessed from India.

The DNS experience test allows you to monitor each level of DNS resolution of a domain by emulating a recursive DNS resolver without caching records. DNS experience test operate slightly different than a real user or our web monitor does to be able to identify which nameserver is problematic.

With the DNS experience test, we saw availability drop with specific ISPs. This indicates that the DNS resolution failed at some level when one of the authoritative nameservers failed to respond to the query.



The scatterplot graph above shows that the authoritative nameservers originating from the same subnet IP address fail to respond for the query when the users are coming from Airtel and Reliance.

We also used Catchpoint's DNS direct test to query the name server for a domain name directly. The CNAME provided by the CDN provider failed to respond from the authoritative nameserver whenever the user originated from Airtel and Reliance ISP.

A mixture of DNS testing helped the customer identify DNS problems that impacted a subset of users. Not all outages impact all users; knowing if even some of your end users are experiencing issues is necessary to deliver a consistent end-user experience for everyone.

5. Monitoring Multi-CDN Deployments

A multi-CDN service that combines multiple CDN providers into a single network is a common and effective way to speed up your web applications for users anywhere in the world. This strategy can also boost failover support if one of the CDNs you're using goes down. But even a multi-CDN service is not immune from performance issues. Intermittent performance drops can and do happen even with this architecture, and troubleshooting such issues should start with DNS.



How Catchpoint Helps

Let us take the example of the domain (tiqcdn.com) which has been C-Named to the multi-CDN provider "Cedexis".

Address		Average Time (ms)	
192.31.80.30:53 [d.gtld-servers.net]		0	

Query : 2-01-2f1f-0001.cdx.cedexis.net Type : A (IPv4 Host Address) Class : IN (Internet)

Authoritative Nameservers

Name	TTL	Class	Type	Info
cedexis.net.	172,800	IN (Internet)	NS (Authoritative Name Server)	flipa.cedexis.net.
cedexis.net.	172,800	IN (Internet)	NS (Authoritative Name Server)	flipd.cedexis.net.
cedexis.net.	172,800	IN (Internet)	NS (Authoritative Name Server)	flipg.cedexis.net.
cedexis.net.	172,800	IN (Internet)	NS (Authoritative Name Server)	flipm.cedexis.net.

The above query to the multi-CDN host is made, at which point the multi-CDN provider decides which CDN the request should be routed to. Routing decisions are based on real-time performance metrics captured by the provider. The decision can vary from one request to the other, which can be seen below.

Group 1 Scenario 1				
Address		Average Time (ms)	Bytes	
69.28.180.4:53 [flipd.cedexis.net]		1	0	

Query : 2-01-2f1f-0001.cdx.cedexis.net Type : A (IPv4 Host Address) Class : IN (Internet)

Answers

Name	TTL	Class	Type	Info
2-01-2f1f-0001.cdx.cedexis.net.	300	IN (Internet)	CNAME (Canonical Name for an Alias)	tags.tiqcdn.com.edgekey.net.

Akamai

The DNS Resolver will go through the process of resolving the Akamai host until it reaches the edge server that will eventually serve the content.

Scenario 2

Address	Average Time (ms)	Bytes	Return Code
69.28.180.4-53 [flipd.cedexis.net]	16	0	None

Query : 2-01-2f1f-0001.cdx.cedexis.net. Type : A (IPv4 Host Address) Class : IN (Internet)

Answers

Name	TTL	Class	Type	Highwinds
2-01-2f1f-0001.cdx.cedexis.net.	300	IN (Internet)	CNAME (Canonical Name for an Alias)	vip0x07f.ssl.hwcdn.net.

In the second scenario, as illustrated above, the DNS resolver has to go through the process of resolving this HOST again. However, in this case the nameservers of Highwinds failed to respond:

Response (ms) : 3,095 Error : The connection attempt timed out, or the connected host has failed to respond.

LEVEL 1 LEVEL 2 LEVEL 3 LEVEL 4 LEVEL 5 LEVEL 6

Group 1

Address	Average Time (ms)	Bytes	Return Code	Error	Ping Time	Packet Loss
69.16.174.10-53 [ns1.hwcdn.net]	1,501	0			*	100% (3/3)
209.187.2.10-53 [ns2.hwcdn.net]	1,501	0			*	100% (3/3)

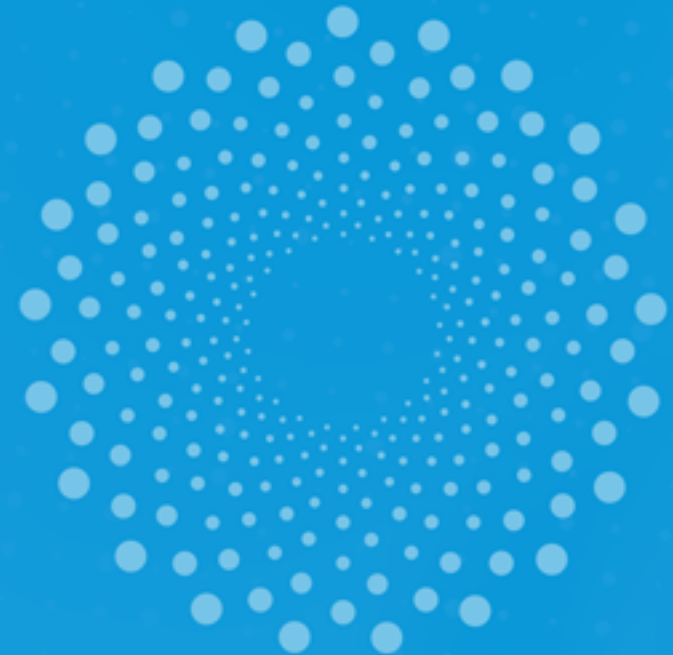
At Catchpoint, we have the option of failing a test at this point when all the available name servers fail to respond. In the real world, reattempts are made to the server if it fails the first time; the users may not see a failure, but the response times will increase significantly.

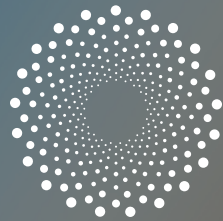
To summarize, a multi-CDN service can make your web applications faster and more reliable but is still not failsafe. Monitoring your application alone is simply not enough; DNS monitoring remains crucial.

Conclusion

At Catchpoint we are constantly helping our customers make the best use of the monitoring tools we provide. The scenarios we discussed above cover a broad range of DNS issues that can create major performance bottlenecks and impact end-user experience. DNS plays a crucial role in your web application, so monitoring your DNS infrastructure is equally crucial. Latency at any point in the DNS resolution process can quickly add up and cause a ripple effect on performance as well as user experience.

DNS Experience and DNS Direct tests can help determine what went wrong and why it went wrong. The data aggregated through these tests can also be used to benchmark third-party DNS providers as well as CDN providers. Comprehensive DNS testing must be part of your overall monitoring strategy as it can provide significant insight into your website performance.





catchpoint™

A Different Approach to Digital Experience Monitoring

Catchpoint is a leading digital experience intelligence company that provides unparalleled insight into your customer-critical services to help you consistently deliver amazing digital experiences. Catchpoint is the only performance digital experience monitoring platform that provides integrated synthetic and real user monitoring, comprehensive test types, real-time analytics, and a diverse node network to help you continuously preempt performance issues and optimize service delivery. More than 400 customers in over 30 countries trust Catchpoint to strengthen their brands and grow their businesses.

18 Smart Monitors

Real browser, multi-transaction, mobile, HTML code, API, streaming, DNS, FTP, TCP, SMTP, ping, traceroute, SSH, NTP, IMAP, web socket, MQTT and UDP.

Deepest and broadest diagnostics

100 days of object level data; 3 years of raw aggregate data.

To request a free trial, visit

<https://www.catchpoint.com/trial>

