NETSCOUT.

nGeniusONE Platform for DNS

Fast Triage for Complex DNS Problems

DNS (Domain Name Service) is a critical enabling service to most enterprises, as it lets organizations perform Web-based activities, including e-mail services, cloud-based services for collaboration (e.g., Cisco WebEx® and Unified MeetingPlace®), and outsourced Software as a Service (SaaS) (e.g., SalesForce.com). When DNS performs badly, all or many of the Enterprise's services will suffer; they may be unable to update customer records, retrieve inventory information, approve staff hires, or confirm shipment of customer orders.

As so many applications are dependent on DNS, they add another layer of complexity to managing service delivery across a globally complex enterprise environment. Doing so without strong performance management visibility is exponentially more difficult. The nGeniusONE™ Service Assurance platform provides a monitoring platform for DNS, as well as the applications that depend on it, to maintain operational efficiency in today's demanding corporate networks.

The nGeniusONE platform provides real-time visibility by analyzing application traffic flows over the network. nGeniusONE leverages rich traffic-flow data for extracting performance metrics rather than relying on server agents or vendor-specific metrics and a multitude of point tools which limit analysis to a single component. Powered by Adaptive Service Intelligence™ (ASI) technology, the highly scalable and patented deep-packet inspection engine, the nGeniusONE platform provides organizations with a comprehensive view of DNS service performance across complex N-tier application environments. nGeniusONE enables IT teams to quickly triage performance issues faster which ultimately reduces Mean-Time-to-Repair (MTTR). It does this by correlating ASI data across different tiers and by providing seamless top-down workflows.

DNS Problems Solved by nGeniusONE

DNS is a protocol and service that is regularly taken for granted, until users have difficulty getting to a website or service they need.

Only then does it become a critical service for IT and Network Operations to sort out.

The nGeniusONE platform examines all applications interactions over the infrastructure to deliver holistic visibility into the performance of application tiers, network traffic, service enablers (e.g., DHCP, Active Directory/LDAP, and RADIUS), and end users to understand the full context of the service and DNS anomalies contributing to the poor user experience or application performance. With its common workflow across all tiers of a service, the nGeniusONE platform reduces the time to triage performance-impacting applications.

The nGeniusONE platform provides visibility into some of the following common DNS issues:

- **Reduce time to identify busy DNS servers** and the sessions contributing to the load to rapidly isolate a troubled server or one that may be under attack from DDOS or Malware.

- **Triage DNS errors rapidly** with easy-to-interpret performance indicators and error analysis, including common issues like IPv6 errors in IPv4 networks, causing an increase in DNS lookup traffic and poor performance of DNS to all other applications.

- **Improve analysis of global DNS environments** with breakdown and views of poorly performing servers with associated error code or latency issues.

- **Simplify troubleshooting** by addressing DNS failures that impact other business services, communities of users being affected, or particular locations that are the source of the problem by providing visibility of DNS server usage by application.
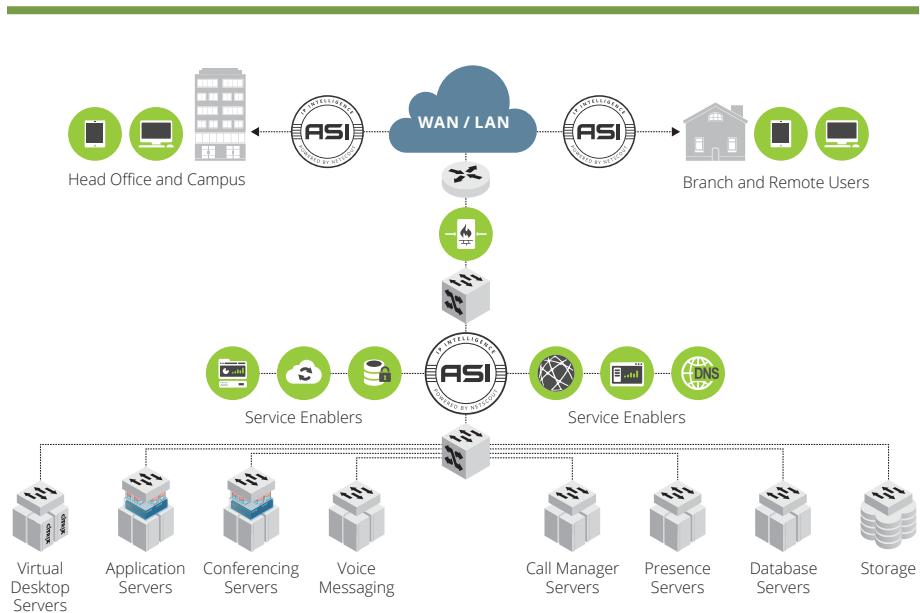

Figure 1: The nGeniusONE platform delivers cross-application tier and cross-network tier performance analytics to support end-to-end unified service delivery management.

nGeniusONE Support for DNS

In order to help IT teams address DNS performance issues, the nGeniusONE platform relies on the power of ASI. Using the efficient data organization provided by ASI, performance data can be viewed by a range of keys, such as impacted DNS server, location (community of users), etc. This enables the nGeniusONE platform to offer an efficient top-down approach to problem identification, service triage, and resolution.

nGeniusONE provides a simple view of DNS showing which users or application servers are using which DNS servers, how much strain they are putting on the DNS server in terms of both volume of traffic, and errors being generated. This allows nGeniusONE to pinpoint busy and degraded performance for specific DNS servers and simultaneously identify the users or application servers causing or suffering from the problems.

The nGeniusONE platform ultimately improves triage and reduces MTTR by:

- Isolating users causing broadcast storms due to malware on their machines looking up addresses that don't exist;
- Pinpointing servers responding with errors because they don't have the appropriate address lists;
- Identifying clients with the wrong suffixes causing them to repeatedly try to look up the wrong addresses (e.g. netscout.com);
- Discovering clients configured to use the wrong DNS Server in their environment; etc.

The nGeniusONE platform provides a consistent set of service-oriented workflows and situational analysis to enable seamless, contextual transitioning across multiple layers of analysis. This allows the nGeniusONE platform to facilitate efficient and informed hand-off of incident response tasks across the different IT groups involved in delivery of an application from one end to the other.

The nGeniusONE platform streamlines service delivery management for DNS by providing the following key analysis layers:

- **Service dashboard** delivers easy to navigate and view health performance status, and alarms for DNS, as well as dependent applications and other service enablers, so the IT organization can focus their triage efforts where needed.
- **Service dependency** visualizes the current state of the DNS and application environment by automatic discovery and mapping of client - server relationships.
- **DNS monitor** enables comprehensive analysis of DNS transactions, such as A and AAAA for IP and IPv6 lookups, PTR and NAPTR for tracking reverse DNS lookups and wildcard DNS records, and traffic analysis to identify the root cause of DNS performance issues. This specialized DNS service monitor provides holistic visibility into all DNS transaction query/response volume, their latencies, and any errors associated with the specific DNS server, as well as the affected user community.
- **Session analysis** delivers session-level analysis, ladder diagrams, with hop-by-hop transaction analysis for DNS to help identify the specific issues (e.g., with servers or proper name resolutions).
- **Packet analysis** enables deep-dive, protocol-level analysis and forensic evidence collection.

A majority of DNS issues can be efficiently triaged by the Dashboard and the DNS Monitor – Should deep dive troubleshooting be needed, IT teams can contextually drill down further and perform session and packet analysis.

Benefits of nGeniusONE for DNS

- **Triage issues quickly** – Decreases MTTR with real-time, end-to-end, comprehensive service visualization enabling IT teams to quickly research DNS issues and pinpoint the source of problems.
- **Protect customer experience** – Rapidly troubleshoot problems with key business applications that depend on DNS for service delivery to quickly restore customer facing services to quality performance.
- **Improve IT team collaboration** – Using the common nGeniusONE workflow across all application tiers, the platform improves time to knowledge by enabling collaboration between network, application, and server teams for resolving DNS problems.
- **Single solution supporting all application layers** – Allows the enterprise to monitor the performance of DNS as well as all data and voice applications and protocol enablers across the environment with a single solution.
- **Optimize available bandwidth** – nGeniusONE's visibility of network bandwidth usage provides valuable information to attribute slowdowns to the network capacity available versus slow enabling servers e.g. DNS, or slow application servers (e.g. database) in the infrastructure.
- **Combined visibility** – of data, voice, video, DNS and all other enabling services helps enterprises to optimize the environment with directed capacity upgrades.