NETSCOUT.

nGeniusONE for SSL/TLS Certificate Monitoring

Valid SSL/TLS certificates are crucial to the functioning of all secure websites. These certificates are used to enable encryption of the data sent to and from the website, and to authenticate the identity of the website to the users, providing reassurance that the site is legitimate. If the certificate is expired, visitors to the website will receive a popup, or in some browsers even a page redirect, warning them that the certificate is invalid and they should continue at their own risk. The majority of users will close the browser window rather than continuing, sometimes redirecting to a competitor's website instead. If an underlying application relies on the validity of the certificate, the application may even fail if the certificate expires.

Monitoring the validity of certificates is thus a key part of any comprehensive web services monitoring strategy, one that is frequently overlooked by large companies as well as small. Beyond certificates, a healthy web services performance monitoring strategy should view this data in context with other information, requiring an end-to-end perspective into the health of multiple networks, servers, applications and enabling protocols that make up a web service offering.

The nGeniusONE® Service Assurance platform provides real-time visibility by analyzing all 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 require a specific skillset to operate. Powered by Adaptive Service Intelligence™ (ASI) technology, the highly scalable and patented deep packet inspection engine, the nGeniusONE platform provides IT with a comprehensive view of service performance across complex N-tier application environments. nGeniusONE enables IT teams to triage secure authentication 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.

Performance Issues Solved By nGeniusONE

nGeniusONE delivers end-to-end visibility into the performance of an integrated application environment including certificate status, server activity, service enablers, database tiers, application tiers, web tiers, and the network. As a result, nGeniusONE uncovers the full context of service anomalies contributing to slow application response times and poor user experience including:

· Expired or self-signed certificates
· Authentication failures
· Network issues
· Application issues
· Scope of end-user impact

Looking at individual components of the service delivery chain in a vacuum can delay discovery of the source of service degradations. With nGeniusONE, IT organizations benefit from having server performance metrics in context with the other service components, to rapidly identify problems and determine the root cause.

Support for Encrypted Services

In order to help IT resolve poor user experience issues, nGeniusONE relies on the power of ASI. Through continuous monitoring of all application traffic, ASI data enables nGeniusONE solution to provide a holistic view into the performance of every component that could potentially cause database performance problems. This highly structured data provides operational insights and visibility into the potential sources for service outages including web authentication failures and SSL certificate expirations. In addition to application performance, nGeniusONE also provides advanced TCP analysis to help identify any network level issues.
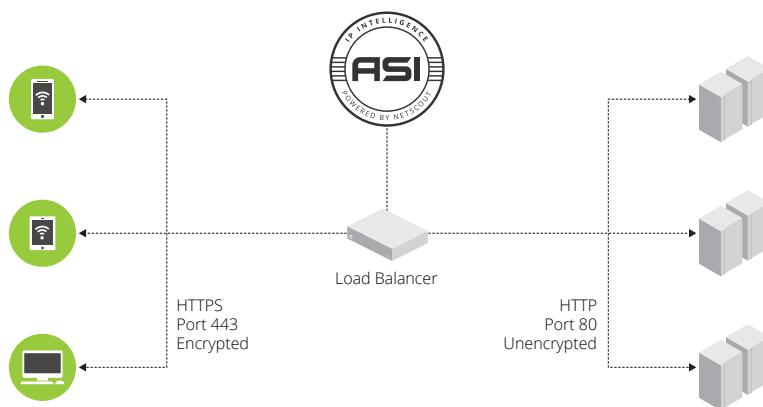

HTTPS
Port 443
Encrypted

Load Balancer

HTTP
Port 80
Unencrypted

Figure 1: Monitoring SSL/TLS certificate expiration is part of a healthy certificate management strategy.

This platform provides IT teams with an efficient top-down approach to problem identification, situation analysis, service triage, and resolution. This ultimately improves situation analysis and reduces MTTR by allowing IT to:

- Identify root cause of user authentication failures
- Discover load balancers or servers with old or missing SSL certificates
- Monitor the upcoming expiration dates of SSL certificates
- Identify if a self-signed certificate is intentional or malicious
- Manage TLS versions, ensuring the version is compliant with corporate policy

nGeniusONE provides a consistent set of service-oriented workflows to enable seamless, contextual transitioning across multiple layers of analysis. The platform facilitates efficient and informed hand-off of incident response tasks across different groups fostering IT team collaboration.

The nGeniusONE platform simplifies the challenge for IT in delivering high quality, consistent, user experience for application services by providing the following key analysis layers:

- **Service Dashboard** – The dashboard delivers real-time health status, metrics, alarms, and intelligent early warning of problems with critical business applications. IT teams can use it to quickly spot any performance issues related to a composite service including the web components, key middleware and service enablers, as well as the database servers in a single view.

- **Service Dependency Map** – The service dependency map feature provides visibility into all the dependencies among various components. This map enables IT teams to analyze the underlying states in the service environment and discover the client-server relationships and their performance.

- **Certificate Monitor** – Uniquely provides a single, consolidated view of SSL/TLS certificate status across the enterprise network. With this view in the nGeniusONE platform, IT teams have in-depth certificate and network details to troubleshoot and isolate the sources contributing to performance degradations in the most efficient manner. Available in the Certificate Monitor view is visibility into the number of certificates in use, with special callouts for certificates within 30 or 60 days of expiration, the versions of each certificate used on the server, and the number of self-signed certificates.

- **Session Analysis** – Delivers session-level analysis including ladder diagrams with hop-by-hop analysis for message exchanges between clients and servers. This view helps IT teams analyze transaction latencies. The session-level details include Certificate Name (Identity), Issuer Name, the specific expiration date, and the Client IP:Port.

- **Packet Analysis** – Enables deep-dive protocol level analysis and forensic evidence collection. Using packet analysis, IT teams get visibility into SSL versions and SNI names.

A majority of SSL/TLS performance issues can be efficiently investigated by using the Dashboard and the Certificate Monitor screens alone. However, should deep dive troubleshooting be needed, IT teams can further drill down to the Session and the Packet Analysis layers.

Benefits of nGeniusONE for Certificate Monitoring

- **Quickly and Efficiently Troubleshoot Issues** – Comprehensive service delivery platform covers all tiers including the load balancers, web, application, and database tiers, in addition to SSL/TLS Certificate analysis, enabling IT teams to efficiently research performance issues and quickly identify the root cause and reduce MTTR.

- **Manage Business Risk** – Find and update certificates before they expire, reducing risk of exposure to hackers, application failures, and loss of customers. Locate self-signed certificates, and identify if they're intentional or evidence of an attack.

- **Improve IT Team Collaboration** – Using common workflows across all application tiers, the platform improves time to knowledge by enabling collaboration between network, application, security and database teams.

- **Monitor Data, Voice, and Video Performance within a Single Solution** – Combined visibility of data, voice, and video helps organizations optimize the performance over a secure, converged IP network.

NETSCOUT.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000