NETSCOUT nGeniusONE and nGeniusPULSE to Support Combined Joint All Domain Command and Control Multi Domain Operations Efforts

Submitted By:

COL(Retired) Gerald H. Miller, Jr.

Senior Global Account Manager, U.S. Army NETSCOUT Systems

11 May 2021

NETSCOUT

Introduction

Today, the military has multiple systems for transmitting data directly from one computer to another – machine to machine – over radio and landline, but each focuses on a specific function, like navigation, logistics, or artillery planning - and they don't connect with other systems in the same service, let alone with those of other services. This challenge is a decades old problem. The challenge is further exacerbated when we bring Coalition interoperability requirements into the equation. All Services and Agencies need to look at "seams, gaps and overlaps" as they implement the new strategy for All Domain Ops". Either directly, or indirectly, C5ISR (Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance) cannot happen without the network. We are confident that NETSCOUT Systems' nGeniusONE and nGeniusPulse products will support the Joint and Army efforts to effectively support Combined/Joint All Domain Command and Control and Multi Domain Operations Requirements.

nGeniusONE

nGeniusONE monitors for availability, performance and health issues and provides near real-time awareness of service-impacting issues. Additionally, nGeniusONE provides intuitive repeatable triage workflows that contain actionable application-centric and network-centric analytics derived from IP packets whether they be in the cloud, on prem, or in a hybrid environment. nGeniusONE enables you to proactively monitor any application service your organization delivers or uses, and rapidly triage issues, collaborate between teams, and validate remediation efforts.

As digital communication is exchanged between clients and application-services, it can become impaired or impeded by anything along the path that either transports the communication or provides required services or data. But regardless of what causes an issue or where it occurs, the result is the same – delivery of critical data is delayed.

Because mission success frequently depends on the timely delivery of digital data, or digital packages, the military needs an impartial overarching tool that's capable of analyzing communication within any environment and proactively exposing anomalies regardless of how or where they were caused. This is exactly what the nGeniusONE service-assurance platform was purpose-built to do – to proactively expose communication issues within any environment by continuously inspecting live IP data- packets.

There is no better source than live IP data-packets, or simply Live Data, for detecting communication issues between clients and application-services because Live Data is the communication. By leveraging the actual communication and inspecting **every** OSI layer, nGeniusONE can: measure performance of all service-interactions; monitor application-layer health in many applications; and monitor application availability.

As nGeniusONE collects vital details about each service's performance, health, and availability, it evaluates the information to determine whether it meets the criteria for sending alert notifications. This process happens in near real-time, making nGeniusONE an early-warning-system for service issues. Once you're aware of an issue, you can rapidly triage it using nGeniusONE's built-in powerful workflows. These workflows, which are only a few levels deep, contain a wealth of actionable information that's presented in easily understood views. Each workflow also provides access to the inspected IP data packets that are stored at the point of inspection.

The same workflows that you use for triage can also be used to validate the effectiveness of steps taken to remediate an issue. Also, they enable teams to easily collaborate on issues because everyone can see the same data, regardless of where the data resides on the network.

NETSCOUT achieves this powerful capability through our patented deep packet inspection software, Adaptive Service Intelligence (ASI). ASI produces smart data analytics in real time and runs on our InfiniStreamNG (hardware appliance) and vSTREAM (software). These products can be deployed in any cloud, virtual or physical environment. The smart data produced by ASI enables consistent and continuous high-resolution monitoring for any application including UC, and those developed in-house, to enable proactive and rapid triage of service-impacting issues and the production of meaningful and actionable reports.

ASI has a major role in the nGeniusONE platform because it enables all capabilities, including the vital ability to provide continuous high-resolution monitoring of all IP-based applications. To enable ASI to fulfill its role, NETSCOUT designed it to operate on both hardware- and software-based platforms that can be embedded wherever monitoring is needed, whether it be within a cloud-based or on-premises application-hosting environment, or at the network’s perimeter, or at remote offices and sites. It is vitally important to have ASI embedded at each of these locations.

Monitoring within an application-hosting environment enables nGeniusONE to monitor East-West communication, detect issues with applications in the back-end, expose dependencies between applications, and monitor communication from these locations to applications that are hosted within environments you don’t, or can’t monitor. Monitoring at the network’s perimeter and at remote sites enables nGeniusONE to monitor site-to-site communication, to isolate with specificity where IP packets were either altered, dropped, or delayed.

All smart data that’s produced by every ASI platform is made available to a central nGeniusONE server that provides a single-pane window in which users can view and triage monitored applications from the perspective of any single ASI inspection-point and from the perspective of multiple inspection-points simultaneously. Also, NETSCOUT recognizes that our Smart Data can be useful in other platforms, so we support data-feeds to big-data lakes and direct, but occasional, data- extraction via a REST API.

nGeniusPULSE

nGeniusPULSE is another product that will support an integrator’s role in effectively and efficiently administering the Army Enterprise Application Modernization and Migration to Commercial Cloud requirements. nGeniusPULSE actively validates that important applications and services are accessible and usable from end-user locations. It leverages synthetic tests, emulates end-user actions, and performs network tests that are sent automatically, intelligently, and continuously 24x7x365.

nGeniusPULSE monitors the service-delivery infrastructure and leverages data-polling methods that collect health-and-performance metrics from network devices and servers, both virtual and physical. This holistic approach to monitoring enables you to proactively detect problems from the perspective of end-users, even when users are not on-site. This methodology also rapidly pinpoints a problem's source and scope and will easily validate the effectiveness of remediation efforts.

When describing nGeniusONE, we stated that mission success frequently depends on the timely delivery of digital data, or packages, and we described how nGeniusONE excels at monitoring live communication and enabling you to rapidly triage issues. While assuring application services in this manner is vital, it's also important to ensure that critical services are accessible and usable at the moment they're needed. Critical digital data can't be delivered if the sender, whether it be an end-user or a device such as a sensor, can't connect to a service and get logged in or registered. This is where nGeniusPULSE can help.

nGeniusPULSE contains two distinct but complementary capabilities that combine to provide end-to-end visibility into issues affecting the end-user experience. The first capability involves testing services both automatically and continuously, 24x7. These tests emulate actions that end-users or sensors would take, such as connecting to a service and then logging in or registering, and they originate from end-user or sensor locations to ensure that nGeniusPULSE captures the true end-user experience. The second capability involves monitoring the availability, health, and performance of your service-delivery infrastructure by leveraging polling methods such as SNMP, WinRM and ICMP. nGeniusPULSE's holistic approach to monitoring reduces any organization's troubleshooting-time by enabling them to easily correlate service issues with infrastructure issues.

nGeniusPULSE's service-tests originate from a component within the platform called an nPoint. The physical version of nPoint is a compact 5x5-inch platform that can fit anywhere. A virtual version of nPoint is also available that can be installed on Windows and Linux systems. The physical nPoint is used primarily for persistent testing while the virtual nPoint is used primarily for ad hoc testing. However, either nPoint can fulfill either role. Both nPoints have the same capability when it comes to the type of test that can be performed. Earlier, I described a quick example of end-user actions nPoints can emulate, but it can emulate almost anything a user can do, including making VoIP calls. An nPoint can also perform network tests to measure bandwidth, latency, and jitter and although many tests are already built-into nGeniusPULSE, custom Python-based tests can be added.

From an infrastructure monitoring perspective, (SNMP and WinRM polling, and a VMware API), nGeniusPULSE can collect health-and-performance metrics from these elements of the service-delivery infrastructure:

- Servers (Windows and Linux) to monitor Uptime, CPU, Memory, Disk Usage and I/O
- Network I/O-Network Devices (Routers, Switches, Firewalls) to monitor Uptime, CPU, Memory, Interface Status, Utilization
- Wi-Fi Infrastructure (Wireless LAN Controllers, Access Points, Radios) to monitor Uptime, CPU, Memory, Interface Status, Channel Utilization, Retry Rate, Error Frame Rate
- VMware Infrastructure (Hypervisors, Virtual Machines) to monitor Uptime, CPU, Disk Latency and I/O, Network I/O and Packet Drops, Top VMs

Finally, from a proactive monitoring perspective, nGeniusPULSE provides two methods to enable you to proactively monitor for issues, one of which involves receiving alert notifications via emails and SNMP traps when issues meet appropriate criteria. The other involves monitoring a live dashboard.

nGeniusPULSE provides two dashboards, one that enables you to monitor by service, for example a VoIP service, and one that enables you to monitor by location. The Sites Overview dashboard enables users to monitor by location. Regardless of which dashboard you use, you'll easily recognize from the color-coding which locations or services are experiencing issues and how severe those issues are. Also, all issues are exposed in the dashboard even if they don't meet the criteria for triggering an alert, and a contextual workflow where you can investigate the issue is always one-click away.

Conclusion

C2 and Mission Command, Air Power, whatever term you want to use for the functions that our military provides is enabled by Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance. The mission enabling data, services and applications that support C5ISR is useless if the network that transports said enabling data, services and applications is not visible, available, assured, and secured, and shareable. That is NETSCOUT's wheelhouse regardless of the transport medium (SATCOM, IP Radio, Tropo, TADIL Links, Cable, Terrestrial Microwave, Cellular, etc.). Those mediums are simply diverse mediums over which to transport the data, services and applications that enable mission command and the CJADC2 effort. They are all mediums for transporting critical sensor data. This imperative also rings true regardless of whether the user is a DOD or Coalition warfighting commander, or a CEO of a major commercial IT Service Provider that we support today like AT&T, Verizon, Lumen Technologies, etc. providing services to the DoD.

Mission success of all Services and Agencies and Coalition Partners is fully dependent upon the strength, security and scalability of their network. Employing sensors and operational effectors in service and domain agnostic ways dramatically shortens the time it takes to engage multiple relocatable targets. Compressing time to knowledge enables greater speed and agility of decision making to attack and maneuver faster than our adversary can operate. Moving toward true "multi-domain operations" will require capabilities that are "application ingestion agnostic".

So, to make CJADC2 more than just another acronym like NCW, or SOA we must solve the time problem that enables the Joint and Coalition Forces to accelerate attack and maneuver faster than the adversary can operate. We believe this acceleration is one of the central animating requirements behind and Combined Joint All Domain Command and Control (JADC2), and Comply to Connect, and Army TITAN, and Army and Air Force EITaaS, and Unified Communications, and more. This evolution will require capabilities that are "application ingestion agnostic" so we are able to see the network to defend the network - and we must do so faster than our adversary! We must get inside of our adversary's OODA Loop faster than they can get into ours. We must implement and integrate at the network level across the Strategic, Operational and Tactical layers over a Network that is visible, assured, and secured. All Services and Agencies are alike in one respect - they are all "network dependent". Now, more than ever, we must be able to see the network to exploit and defend the network and we think you agree that we must do so faster than our adversary.

Execution of the new DoD programs demands that look for as many existing common network denominators as possible. We must focus on fully implementing, and most importantly, integrating them into a network capable of sharing critical sensor data, Services and Applications controlled by CONOPS comprised of Joint and Coalition SOPs, TTPs, Tailored Response Options (TROs), and clearly defined roles, responsibilities, functions and tasks on Echelon.

NETSCOUT will help the DoD get to the ABMS-JADC2-Multi Domain Operations end state faster by using products that are already heavily implemented and integrated across the Services and Agencies.

NETSCOUT can help CJADC2 and many more emerging programs that are moving from Service Centric to Joint to help DoD get to the end state faster and smarter by using products and solutions that are already heavily implemented across the Services and Agencies:

- Our presence cuts down on initial implementation costs- less Rip and Replace!
- Reduces total cost of ownership
- Reduces time and cost of training the Airmen, Soldiers, Sailors, Marines, GS and Contractor workforce
- Supports standardization of CONOPS, SOPs, TTPs, TRAs and TROs
- Standardizes views in real time of the health and performance of the networks data, services and applications.

We believe the introduction of the concept of integration of the NETSCOUT products that already exist across the DoD Services and Agencies as a “Common Denominator” to support PROACTIVE network health, performance and cybersecurity monitoring for the relevant data, services, and applications across the Joint All Domain C2 environment is certainly something to be explored, can help the DoD get to their end zone faster, and is definitely value added.