

# Assuring VPN Business Continuity and Remote Services Availability

This NETSCOUT Use Case focuses on how information technology (IT) teams are able to assure high-quality customer service delivery for their remote Call Center Agents (CCAs) using the nGeniusONE Service Assurance platform and nGenius solution, with this narrative focusing on one contact center services provider as an example.

While the nGeniusONE platform and nGeniusPULSE workflows described here are relatively straightforward, their real-world value grew exponentially in the days following COVID-19's arrival, with the majority of this CCA's business now relying on VPN and remote business service platforms to support call center service delivery to commercial, government, technology, and other enterprise customers.

The NETSCOUT best-practices described here may well apply to other enterprise and government IT teams occasionally finding themselves in similar circumstances, as they tackle enterprise technology environment changes in response to the remote workforce realities.

## Performance Issue

Companies around the world confronted complex challenges with the arrival of COVID-19. They faced local and national government "shut-down" directives that sent home non-essential employees to reduce the spread of the coronavirus. This led to corporations implementing business continuity plans (BCPs) to ensure customer service and revenue for corporate survival. For those organizations with employees working in centralized buildings using workstations to answer calls and support service requests, this meant IT teams needed to quickly address business continuity issues occurring across multiple fronts, including:

- Procuring, imaging, securing, and deploying new laptops, as well as factoring how the sudden surge in VPN traffic impacted service delivery
- Assuring their CCAs could remotely access customer and partner platforms to assure Contact Center performance in compliance with negotiated service level agreements (SLAs)

After procuring and imaging the laptops, the IT team also had the important task of assuring CCAs could securely access their own Contact Center applications and business service platforms, as well as those of their clients. As part of this process, the IT team deployed several large Dynamic Host Configuration Protocol (DHCP) IP address pools. Shortly after provisioning, the CCAs began reporting poor performance when using their laptops to log into Remote Access / VPN Services. With these newly established VPN DHCP IP ranges, the IT team found it was no longer able to correlate CCA performance to the customers they were tasked with supporting.

## Impact

When the only interaction a customer has with a business is via the contact center, it is essential that the experience is flawless. Depending on the type of business, the impact to the customer can be minor or severe. To the business, these disruptions can have a similar range of impacts, from an annoyed customer, to loss of significant amount of revenue, to reputational damage.

In this case, prior to the pandemic, CCAs were associated with their clients by local area network (LAN) subnet, making customer service more complete, thorough, and swift. With the LAN no longer part of the everyday remote delivery environment, the IT team needed to quickly troubleshoot this remote performance issue to enable the CCAs to deliver voice and video services to their customers.

## Troubleshooting

The IT team turned to their contracted NETSCOUT® Remote Site Engineer (RSE) to make several nGeniusONE® configuration changes and run nGeniusPULSE synthetic tests that addressed the VPN visibility and real-time monitoring issues, with these high-level fixes factoring the use of:

- nGeniusONE Site Definitions for the VPN DHCP Pool
- nGenius®PULSE for Remote Access Portal Availability Testing

In the troubleshooting workflow, the RSE first established nGeniusONE Site Definitions and Remote Services for remote access, with this sequential process including:

- Site Definitions for Remote Access Subnets, including Defining Subnets in nGeniusONE
- Setting relevant InfiniStreamNG® (ISNG) appliance interface's vifn\_ mode to some variant of Site Mode
- Associating the newly created Sites to corresponding ISNG interfaces
- Creating network service(s) based on the sites
- Adding the network service to the nGeniusONE Enterprise Service Domain Hierarchy

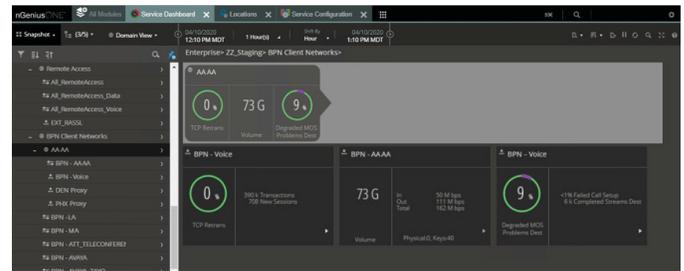
Next, the NETSCOUT RSE created nGeniusPULSE synthetic transactions from internet-connected nGeniusPULSE nPoints to external remote access URLs, which enabled nGeniusPULSE monitoring of availability and performance of remote access services. With this workflow, the RSE used some key capabilities offered by the nGeniusPULSE solution, including:

- Identifying URLs of public-facing Remote Access URL(s) (e.g., sslvpn.netscout.com)
- Creating Web Test(s) in nGeniusPULSE Administration pages to test those URL(s)
- Creating a Business Service comprised of those Web Tests
- Drilling into nGeniusPULSE test results to examine any performance issues, such as inability to resolve hosts

With nGeniusPULSE synthetic testing identifying the connection issues at hand, as well as verifying availability of Remote Access VPN gateways, the RSE's troubleshooting workflow transitioned to applying those findings to properly associate CCAs (who were intermingled on VPN DHCP Agents) to their assigned client or business partner network (BPN) resource.

This workflow first involved the RSE defining nGeniusONE Sites for clients. The RSE then defined nGeniusONE network services for particular clients. As a result of the immediately preceding nGeniusONE Site Definition exercise, the RSE was then able to designate an nGeniusONE Network service to a particular client or business partner.

As a result of the RSE's workflows, the IT team now had access to high-level nGeniusONE Service Dashboard views configured specifically for real-time monitoring of their CCAs' assigned clients and BPNs they access, as exhibited in Figure 1.



**Figure 1. nGeniusONE Service Dashboard view, configured for real-time monitoring of a specific client's voice service environment.**

## Remediation

With the IT team using the RSE-provided nGeniusONE visibility and analysis improvements, they were able to change the VPN DHCP agent configurations to properly associate CCAs to their assigned client or business partner network resource. This enabled the CCAs to deliver business-as-usual call support to their designated clients and technology partners.

## Summary

The use of in-place NETSCOUT smart visibility solutions and performance analytics and RSE resources enabled this IT team to successfully troubleshoot client-impacting service delivery issues at a critical time, all without the need to deploy additional tools in an already-transitioning remote environment. This enabled the IT team to:

- Quickly execute on their organizational BCP
- Maintain quality end-user experience for their at-home CCAs
- Deliver prompt, complete customer care during the pandemic

Additionally, the IT team and the company benefited from the additional Return on Investment from their NETSCOUT implementation.

**NETSCOUT**

**Corporate Headquarters**  
NETSCOUT Systems, Inc.  
Westford, MA 01886-4105  
Phone: +1 978-614-4000  
www.netscout.com

**Sales Information**  
Toll Free US: 800-309-4804  
(International numbers below)

**Product Support**  
Toll Free US: 888-357-7667  
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: [www.netscout.com/company/contact-us](http://www.netscout.com/company/contact-us)