

Visibility to Troubleshoot Production Applications in Factories with Omnis Smart Edge Monitoring

Manufacturers rely on their globally distributed factories to take orders, build and assemble products, and ship finished goods to local distributors and customers. Unplanned network and application downtime in manufacturing plants can dramatically impact a factory's ability to produce products, deliver on committed schedules, and attain daily quota targets. Any network or application degradations or outages need to be avoided or identified and resolved rapidly to ensure continuous operation.

Issue

Critical applications used in factories include Manufacturing Execution Systems (MES), Computer-Aided Design and Computer-Aided Manufacturing (CAD/CAM), Supervisory Control and Data Acquisition (SCADA) systems, Customer Resource Management (CRM) applications, and Plant Floor Performance Management Systems (PFS), any of which could impact manufacturers should issues occur. Many of these solutions operate with the main application servers in a private data center or in the cloud with local clients in the factories (e.g., CAD/CAM and PFS), while others, depending on their function, may operate principally within the factory itself (e.g., MES).

In this case, the PFS application that was used to specify feature options for the equipment, evaluate the building and assembly of the product, perform quality checks at the end of production, and track required repairs was experiencing intermittent problems. Design specifications are provided through this application from application servers in one of the main headquarters data centers, over MPLS, to the factory closest to the order for assembly. Timely production execution for these orders is expected.

Impact

Intermittent problems in PFS application performance will slow production, and if severe enough, could impact plant quotas and delivery commitments. The more it happens, the greater the backlog could become. At some point, if left unresolved, it could impact customer service, distributor relations, and overall corporate revenue.

Meanwhile there is also an employee impact in the local plant staff with loss of productivity, as well as on corporate IT staff losing time attempting to pinpoint the source of the problem with little or no success. IT needed a way to improve their time to knowledge (MTTK), reduce time lost to finger-pointing among their staffs at headquarters and the factories, as well as with their third-party MPLS vendor.

Troubleshooting

The manufacturer's factories were in over 100 locations, all with MPLS WAN links from their small local data centers to communicate with the corporate data centers in the United States, as well as with cloud and Software-as-a-Service (SaaS) applications, such as Google Cloud, and all needing similar visibility for service assurance.

With the assistance of their premium service engineer (PSE) from NETSCOUT®, the IT team developed a visibility plan for monitoring the network and application infrastructures with nGeniusONE® Service Assurance (nGeniusONE) solution in each of the factory data centers.

nGenius® Packet Flow Switches (PFS) were deployed to tap key segments in the local plant data center to send copies of network traffic to monitoring appliances. These include InfiniStreamNG® (ISNG)

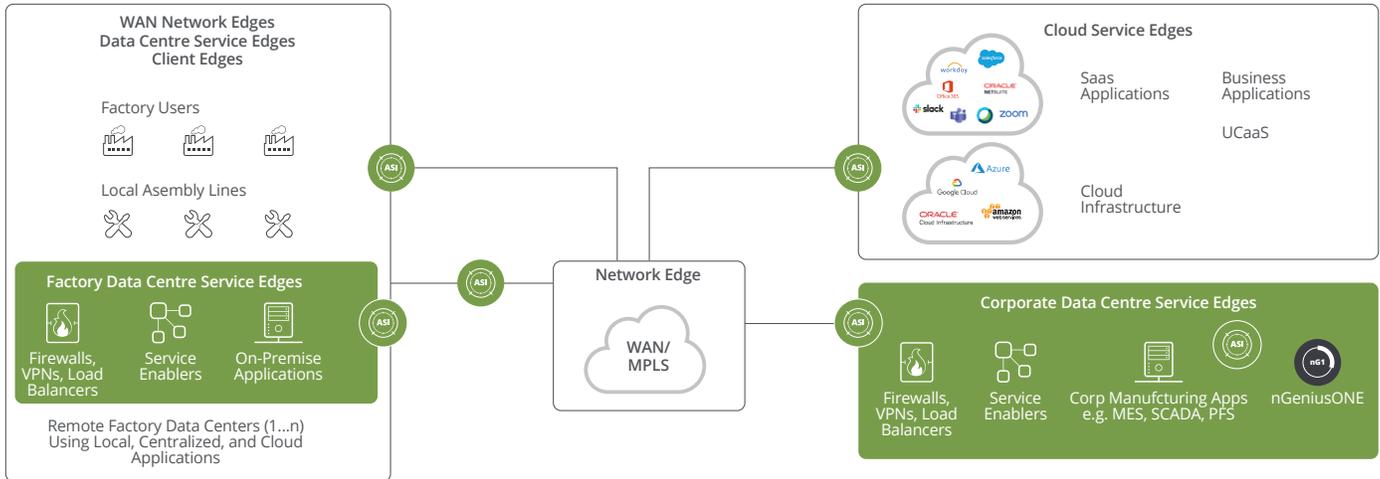


Figure 1: Complex, manufacturing network environments, with multiple remote factories, and centralized, local, and cloud application services, typically have gaps in visibility at client, network, and service edges, where technology domains exist. Ensuring efficient end-through-end visibility for service assurance requires comprehensive visibility across those unmanaged domains.

appliances at the WAN Network Edge (where the MPLS link connects, traffic domains change, and packets are transferred to a third-party. Additional ISNGs were installed in the factory Data Center Service Edge, where the network core carries the highest traffic volume and critical server farms are located (Figure 1).

The smart data from the ISNG appliances in the plants are being analyzed using the nGeniusONE centrally located in the manufacturer’s headquarters. The IT staff, along with the NETSCOUT PSE, have configured meaningful dashboards and workflows to address of the complex issues the factory personnel have been grappling with, specifically for the PFS service experiencing intermittent delays.

For the factories experiencing the delays and disruptions in their PFS service, the pressing issue was finding the source and correcting the issue to establish seamless operation of this essential system. With drill downs to link utilization (Figure 2) and traffic details (Figure 3) for the PFS application, they quickly diagnosed a QoS mismatch. All the ingress PFS traffic coming from the corporate data center, over the MPLS link, into the factory carried an outbound assignment of 26, which was correct. Deemed a latency-intolerant service, it had a priority delivery QoS class assignment. However, all egress PFS traffic being handed off from the factory data center to the MPLS provider had a QoS assignment of 0.

This proved what the MPLS provider had stated throughout the troubleshooting efforts. That is, the QoS assignment was not an issue created in their network. It was with the manufacturer’s own network.

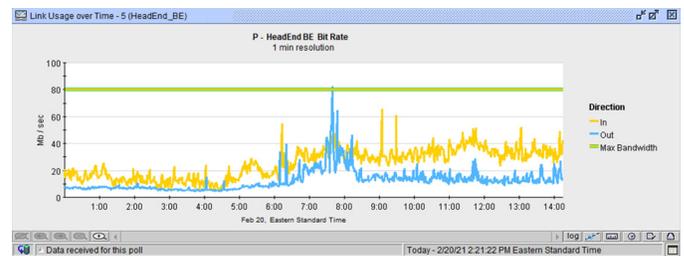


Figure 2: Link usage for the PFS application inbound and outbound at the factory

Remediation

With the new ISNGs in the local plant, it was determined a network switch at the plant was not applying the proper QoS classification. Configuring that local plant switch correctly solved this issue and restored high-quality, reliable performance for the critical PFS application at the factory.

| Location | Packets Total | Volume Total (bytes) |
|---|----------------|----------------------|
| INFAD03#4 B_MPLS_Plant_Tap_ID-202 PFS P Assembly | 311 20K | 242 22M |
| INFAD03#4 B_MPLS_Plant_Tap_ID-202 PFS | 311 20K | 242 22M |
| INFAD03#4 B_MPLS_Plant_Tap_ID-202 PFS P Assembly QoS level 26 | 168 37K | 226 69M |
| INFAD03#4 B_MPLS_Plant_Tap_ID-202 PFS P Assembly QoS level 0 | 142 83K | 15 52M |
| INFSDC05#4 S ASE-Plant ID-101 ALL | 729 | 491 65K |
| INFSDC05#4 S ASE-Plant ID-101 ALL P Assembly | 729 | 491 65K |
| INFSDC05#4 S ASE-Plant ID-101 ALL P Assembly QoS level 0 | 729 | 491 65K |
| INFSDC01#4 B_PLANT_MPLS_TAP PFS ID-211 P Assembly | 143 | 45 42K |
| INFSDC01#4 B_PLANT_MPLS_TAP PFS ID-211 P Assembly QoS level 0 | 143 | 45 42K |
| INFSDC01#4 B_PLANT_MPLS_TAP PFS ID-211 | 143 | 45 42K |
| INFAD02#3 E_Plant_TAPAHDSM02_Tap3 ID-229 PFS ALL P Assembly | 32 | 22 49K |
| INFAD02#3 E_Plant_TAPAHDSM02_Tap3 ID-229 PFS ALL P Assembly QoS level 0 | 32 | 22 49K |
| INFAD02#3 E_Plant_TAPAHDSM02_Tap3 ID-229 PFS ALL | 32 | 22 49K |
| Total | 936 31K | 728 33M |

Figure 3: Evidence that all the PFS traffic within the local plant was tagged with a QoS 0 assignment but the traffic coming into the factory from headquarters was configured properly with the QoS 26 priority assignment.

Summary

This use case highlights the power of Omnis™ Smart Edge Monitoring to gain visibility at several network and data center service edges in a corporate network. Locations where domains, packet formatting, or control of the conversations change are ideal areas to add visibility to improve MTTK and mean-time-to-repair (MTTR). Omnis Smart Edge Monitoring is best able to deliver comprehensive analysis and detail from the edges along the broader enterprise network path to determine more precisely why a problem exists and pinpoint where the degradation is occurring.



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