

DATAGROUP

Micro Focus NOM (Network Operations Management) helps DATAGROUP secure and manage its networks.

Who is DATAGROUP?

DATAGROUP is one of Germany's leading IT service providers. The company designs, implements, and operates business applications and infrastructures in IT Outsourcing. IT Solutions cover services such as software development, application development, IT consulting, Robotic Process Automation (RPA), and other technologies. With over 2,000 employees, DATAGROUP is represented in all commercial German metropolises.

Secure and Predictable Internal and Client Network Management

DATAGROUP covers all IT aspects for its medium and large sized customers, including cloud enablement, leveraging Amazon Web

"We worked with implementation partner ITC. Their many years of experience in project planning and execution and their best practices helped us to implement NOM within a very short time and to achieve our goals."

JÜRGEN BÜHN

Network Management
DATAGROUP

Services (AWS) and Microsoft Azure environments. And all of this needs a secure and reliable network infrastructure.

DATAGROUP faces the challenge of operating both its internal networks and those of its customers in a secure and predictable manner. It must ensure that customers can view the status of their equipment, while at the same time ensuring complete separation from other customer environments. Devices from various vendors must be managed and monitored. A visualization of all devices and topologies is key to understanding relations and reducing MTTR (mean time to repair). Dashboards and reports are also required for both the internal network and for the individual customers. These contain not only monitoring information but also data about the performance and traffic flows of the network applications. A central management and patching of the devices and a central backup of the network configuration must also be possible.

In addition, DATAGROUP must ensure that the environment complies with their own and external security guidelines, thus ensuring security always. Another key requirement for a new solution is the ability to analyze the network environment with a detailed root cause analysis to determine what caused a failure.



DATAGROUP

At a Glance

- **Industry**
Technology
- **Location**
Germany
- **Challenge**
Management of various heterogeneous networks of many customers in a secure and proactive manner, meeting a variety of SLAs and ensuring security
- **Products and Services**
Micro Focus Network Operations Management (NOM)
- **Critical Success Factors**
 - + Reduced MTTR through root-cause analysis
 - + Automatic discovery of topology with customizable topology maps
 - + Consistent and automatic monitoring of the network infrastructure
 - + Automatic backup of all network device configuration with versioning
 - + Performance metric and traffic collection for analysis and reporting use cases

“Having one solution in Network Management that can manage fault, performance, configuration and compliance means we don’t have to spend time and budget to train staff on multiple tools.”

JÜRGEN BÜHN
Network Management
DATAGROUP

Contact us at:
www.microfocus.com

Like what you read? Share it.



NOM: One Solution for Fault, Performance, Configuration, and Compliance Management

When investigating the market, it was clear to DATAGROUP that Micro Focus Network Operation Management (NOM) has all the key features which are desired. NOM is the only network management solution that consolidates fault, performance, configuration, and compliance management. Jürgen Bühn, Network Management for DATAGROUP, comments: “Having one solution in Network Management that can manage fault, performance, configuration and compliance means we don’t have to spend time and budget to train staff on multiple tools. It also gives us a full overview of our own and customers’ environment, which always enables us to provide a clear status. The automated compliance management in NOM ensures the reliability and security of the environment continuously.”

At the beginning of the project the names of the network devices have been structured and homogenized. The new consistent naming concept facilitates the identification of customer, device role, and device location and makes it easy to handle the devices in technical tools. With this preparation the environment has been discovered and the topology has been visualized in automated topology maps (layer 2 and layer 3). The new device names helped a lot to define simple filters and accelerate the implementation. After that, the accounts were setup and the network devices were completely separated for security reasons. Immediately after discovery the continuous monitoring of the environment

takes place and first results are presented via incidents and state changes of the objects. Additionally, the configuration and compliance management are executed, and performance data are collected.

As NOM is well integrated, performance data is automatically collected and stored—no extra effort to add devices and credentials in 3rd party tools. Dashboards are used to analyze performance problems and reports can be generated and scheduled to be automatically sent to internal and external customers.

DATAGROUP can now add traffic collection which enables analysis and optimization of traffic flows through the network.

Reduced MTTR through Integrated Root-Cause Analysis

The automatic and continuous discovery ensures up-to-date information for network management.

The topology-based monitoring with the integrated root-cause analysis pinpoints the operating staff to important events. An immediate result was the identification of a faulty redundant power supply. The topology maps help to understand relations and speed up further analysis which lowers MTTR.

As devices are automatically added to the configuration management, configuration backup is done without user intervention—no more missing configuration backups or change records. The compliance of internal security requirements and external requirements like

vulnerability checks (CVEs) guarantee a reliable and secure infrastructure.

Data about performance and traffic flows enable DATAGROUP network engineers to troubleshoot performance issues, perform capacity planning, and optimize traffic flows. Finally, the introduced network device naming convention facilitates improved communication.

Mr Bühn concludes: “We worked with implementation partner ITC. Their many years of experience in project planning and execution and their best practices helped us to implement NOM within a very short time and to achieve our goals.”