The maturity model for network observability

IBM

Executive summary

Enterprises worldwide are embracing digital transformation to boost their competitiveness. By using digital technologies to power reinvented business processes, they are achieving big gains in operational agility and efficiency.

Changes of this magnitude are never easy, and digital transformations are no exception. One reason they are so challenging is that they involve making fundamental changes to how enterprises conduct businesses, putting unfamiliar digital technologies at the heart of their operations.

Then there is the complexity of the technologies involved, such as software-defined networks (SDNs), software-defined wide area networks (SD-WANs) and campuswide deployments of high-speed wifi. For enterprises that deploy them, these highly dynamic technologies create entirely new and difficult network and infrastructure management challenges.

For their digital transformations to succeed, enterprises must solve these challenges, and that requires understanding the maturity of their network observability capabilities.

To help enterprises make this assessment, IBM® SevOne® offers this maturity model with four distinct levels of maturity. The model provides a yardstick against which enterprises can compare their present status with their existing network performance management (NPM) or network observability system. It also offers suggestions for how organizations can improve their functional maturity in these areas.

Successful digital transformations don't happen overnight. They are journeys that require retooling and making incremental improvements over time. The intent of this white paper is to help enterprises begin and then successfully navigate key parts of that process.

> "Legacy NPM tools are not ready for this transformation. Only 36% of NetOps teams believe their NPM tools are fully capable of monitoring cloud networks. Also, while 91% of NetOps teams monitor their SD-WAN environment with a third-party NPM tool, only 48% of them are fully satisfied with this monitoring capability."[1]
>
> **Shamus McGillicuddy**
> Vice President of Research, Network Management
> Enterprise Management Associates, Inc.

Getting started: what to assess

The maturity of IT and network operations (NetOps) teams varies widely today, even among large organizations. At enterprises where these functions are immature, teams spend most of their time reacting to one major problem after another. At the other end of the spectrum are organizations in which these functions are more mature. Those organizations typically have much greater control over IT service assurance, which allows their IT and NetOps teams to be more focused on and responsive to the needs of the business.

Where enterprises fall on this continuum is indicated by their maturity in three areas: technology, processes and culture. To improve the maturity of their network and infrastructure management functions, enterprises must improve in three areas:

Technology
- Management tools in use
- Integration of tools within the IT and NetOps silos
- Integration of tools across all IT silos
- Technologies supported by tools

Processes
- Processes for using those tools
- Processes for collaboration within IT and NetOps
- Processes for collaboration across IT and the business

Culture
- How IT and NetOps teams define success
- How IT and NetOps view the broader technology organization
- How IT and NetOps teams view line-of-business (LOB) areas

The maturity model: supporting new network and infrastructure paradigms

As the complexity of applications and networking technologies continues to advance rapidly, monitoring them effectively has become increasingly difficult. These new environments feature physical and virtual components from multiple vendors along with resources being dynamically spun up and down on demand and in near real-time. Gathering, processing and producing useful insights from all this performance and management data—and doing it in time to be useful—requires equally responsive, scalable and agnostic monitoring and management "chops."

Vendor-specific, product-specific element management systems and traditional hardware-centric NPM tool sets weren't designed to handle today's jobs. They were fine back when network and infrastructure management meant something else. Trouble is, the requirements have changed radically, and these systems simply can no longer keep up.

Enterprises must address the growing gap between their networking power and dexterity and their ability to watch, understand and rapidly respond to activities in their environments with an application-centric approach and evolve from network performance management to network observability. The goal of the maturity model for network observability is to help enterprises make changes and improvements to close this gap.

To improve performance management in these complex environments, it helps to break down individual tasks into distinct goals, functionalities and capabilities. The maturity model for network observability describes the stages of controlled monitoring required to track, report, react to and resolve network and infrastructure performance elements comprehensively, regardless of the complexity of the network.

The maturity model helps:

- Reduce risk by closing visibility gaps
- Create stronger control of network and infrastructure performance
- Increase IT and NetOps teams' efficiency and reduce human errors
- Reduce capital expenditures (CapEx) and operating expenditures (OpEx)
- Minimize the impact of performance issues on users and customers
- Decrease customer churn

This paper provides an overview of the maturity model for network observability, detailing four distinct levels and the benefits of advancing through them. It also discusses the drawbacks and risks of leaving performance management to basic tools. Overall, it lays out a path that enterprises and service providers can follow to reach a state of optimized service delivery.

Maturity model for Network Observability

Level 1

Reactive management
Reactive “firefighting” with large collections of disparate, mostly element-centric tools results in only basic availability. New tools are added to fix specific problems but offer no solid strategic direction.

Level 2

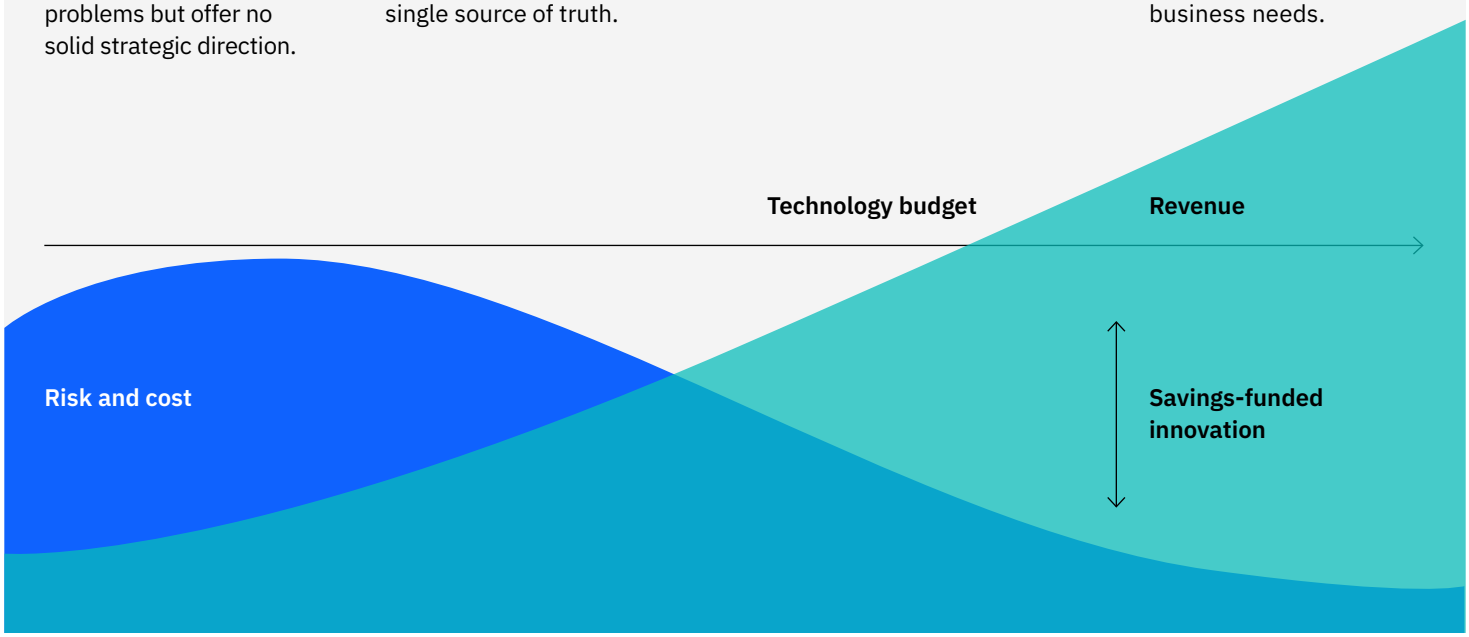
Proactive management
Teams gain more network visibility and improved response capabilities. Scalable management platforms with cross-domain data collection provide a single source of truth.

Level 3

Service-oriented management
Teams become internal service providers. They use service-level views and cross-platform processes to lower MTTR and improve decision support.

Level 4

Dynamic management
Teams use automated network management with advanced analytics. The combination enables automatic optimization of their environments to meet changing business needs.



Showing the four levels and their associated risks and costs, the maturity model for network observability can result in significant savings and increased revenue for funding innovation and growth.

The maturity model's four levels

Starting with unwieldy tool sets and limited visibility at Level 1 and proceeding through the higher levels, the maturity model describes the characteristics, advances and capabilities of each stage. Enterprises and service providers starting down the digital transformation path should use this model to help them:

- Think about their network and infrastructure management capabilities
- Assess their present functional capabilities
- Prioritize changes and upgrades they need to make to advance to the next level
- Plan for continued improvements to enable steady, upward progress through to Level 4

What's at stake for organizations that overlook or put off making these changes? Simply put, they will put the success of their digital transformation initiatives at risk and invite all the competitive issues and business challenges such failures would bring.

A smarter, more viable strategy is to plan for and start making these critical changes. Helping enterprises and service providers do that is the intent of this model. Following are the levels along with suggestions for advancing through them.

Level 1

Reactive management

At Level 1, IT and NetOps teams generally act as firefighters who move from one crisis to the next each day. Their processes are built around forwarding or escalating problems to individuals who specialize in the relevant areas. They are always playing catch up, however, because their management systems don't offer real-time views of network activity—only rearview-mirror looks at performance and availability with historical and forensic data.

Teams at this level often build out capabilities beyond the inadequate element management systems provided by their hardware vendors and implement point solutions to fix specific problems. But doing so increases both OpEx and CapEx costs without delivering what they really need: real-time network and infrastructure visibility. Without the ability to see and understand what's happening at present, these teams are always operating at a major disadvantage.

Network visibility may now reach the halfway mark, but that leaves the other half of the environment in the dark. Device polling cycles may go from five-minute intervals down to one minute when needed. However, performance data is still averaged over time, the low granularity of which negatively impacts a range of functions, such as capacity planning.

Ways to move to Level 2:

- Baseline all metrics and trigger alerts when deviations from normal performance occur.
- Correlate performance metrics with flow data to better understand consumption of resources.
- Build up interoperability and automation by integrating monitoring and management functions with AIOps and IT service management (ITSM) systems.

> "With outmoded NPM tools, the result is a NetOps team that is struggling to serve the business. EMA research found that 33% of all network trouble is detected by end users first and reported to IT. Thus, one-third of all problems are likely impacting end-user productivity and customer satisfaction before NetOps can even act on them."[1]
>
> **Shamus McGillicuddy**
> Vice President of Research, Network Management
> Enterprise Management Associates, Inc.

Level 2

Proactive management

Enterprises and service provider organizations at Level 2 have a single, unified, scalable management platform. Many of these teams also have plans to use their platforms to help them transition to more real-time monitoring capabilities and are making progress on a project-by-project basis. This enables IT and NetOps teams to create consolidated metrics for key performance indicator (KPI) monitoring. With end-to-end testing, teams get clear indications of the health of the services being provided.

Thanks to these improved monitoring capabilities, organizations at Level 2 begin to see measurable, positive changes. Costs start to decrease, staff time begins to get freed up, and a single source of truth about the infrastructure's performance emerges.

At this stage, there's end-to-end visibility of network, compute and storage resources by business unit or customer. Although teams can view both physical and virtual resources on a "single pane of glass," most infrastructure monitoring is still domain-specific. Infrastructure is well-defined, but services are not. That means IT and NetOps teams can usually restore infrastructure quickly, but it takes them longer to bring business services back online. Reporting is easier, and ad hoc or custom reports can be created dynamically because they derive from a real-time, single source of truth—thanks to the management platform.

Taking an application-centric approach is also key for level 2. Building on the end-to-end visibility for proactive management, is the need to approach network performance data from an application first perspective. IT and NetOps teams should be able to easy understand what applications are taking up bandwidth, and be able to pivot from that application usage insight to understand what specific network devices are carrying those applications. Successful IT and NetOps teams are able to ask both application and network questions of their network observability data.

At Level 2, the majority of infrastructure management is done without the need for agents or probes, significantly decreasing administrative burden. Also, at this stage, there is integration with AIOps solutions such as IBM Cloud Pak® for Watson AIOps, and ITSM solutions such as ServiceNow. This facilitates smooth transfers of information between platforms, which in turn, drive faster issue resolution.

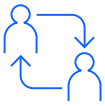
There is, however, still room for improvement at this level. For forecast needs and capacity planning, staff typically still gathers data from several sources and manually enters it into spreadsheets. The ability to scale to current monitoring demands has greatly improved, but at a cost—for gear such as high-end servers, data collectors and centralized database resources.

In general, Level 2 involves conditions that are normalized across the infrastructure. IT and NetOps teams at this level of functional maturity can be more proactive because they have greater visibility into and control over their networks and infrastructures.

Ways to move to Level 3:

- Incorporate visibility of applications and service delivery as opposed to monitoring only individual infrastructure components.
- Define, monitor and alert on custom KPIs that do not exist in the MIBs of monitored devices.

Platform

	 Level 1	 Level 2	 Level 3	 Level 4
	Reactive management	**Proactive management**	**Service-oriented management**	**Dynamic management**
Deployment	– Mostly element management tools with costly overlaps – Data collection requires stand-alone severs for each device and data type	– Unified, scalable platform addresses most monitoring needs – Point solutions still used for highly specific needs	– Hot standby and tested failover of monitoring platform – Backup solutions deployed for data protection – Uses streaming network telemetry for down to one second granularity of performance data	– Fully virtualized all-in-one monitoring platform with ability to spin monitoring capacity up or down on demand
Interoperability and automation	– Information sharing across platforms and silos is manual and slow – Air-gapped workflows hinder data transfer	– Initial integration with AIOps system such as IBM Cloud Pak for Watson AIOps – Initial integration with ITSM solutions such as ServiceNow	– Tight two-way integration with AIOps and ITSM solutions	– Use performance data to automate the network – Optimize network by feeding performance data to network automation and control systems
Scalability	– Limited ability to scale – Centralized database for all collected performance metrics slows down reporting	– Ability to scale to current monitoring demands – Questions about ability to cost-effectively scale with expanding infrastructure	– Fast reporting regardless of infrastructure size – Easily able to visually integrate existing log data with network performance data	– Provides the unlimited scalability required to handle high velocity and volume of data generated by today's modern networks

Level 3

Service-oriented management

The characteristic that distinguishes organizations at Level 3 is that their IT and NetOps teams function as internal service providers. This service orientation is enabled by monitoring and management tools that have been chosen strategically rather than on a reactive basis. Those tools have been combined to create a single, cohesive platform.

The most popular approach to the network tools integration that is the hallmark of Level 3 is implementing a fully integrated multifunctional platform.

In organizations that have achieved this level, teams have integrated various operational and support systems into their infrastructures. Service-level views and cross-platform processes ensure that reliable metrics are being used in business decision-making. This enhanced visibility unlocks other capabilities, including:

- Application- and service-delivery views of performance rather than just component monitoring
- Significant reductions in MTTR and less staff time spent on troubleshooting and issue resolution
- Automated discovery of Level 2 and Level 3 topologies, and real-time views of status and service level agreement (SLA) instrumentation, including packet loss, jitter and congestion
- Visual integration of log tools, where single clicks get staff from metrics to flows to logs within the same interface
- Proactive resolution of most issues before they impact users or customers
- Capacity planning and trending performed in a single place

Organizations know what's happening on the network, where it's happening and when it's happening—end to end. IT and NetOps strategy and operations have been streamlined and are now proactive. Visualization and analytics capture and define business impacts of IT. Workflows become more automated and are documented to capture best practices. Silos dissolve in favor of total infrastructure management, with interdependencies well understood.

Empowered by strong monitoring made possible by unified platforms, accurate and trustworthy metrics, and highly informed strategic planning, the service-centric organization emerges as a liaison to the business side. The result is a positive impact on overall business. But there's still one more threshold to cross.

Ways to move to Level 4:

- Tie alerts to multivariate analysis to spot trouble due to multiple related events.
- Incorporate service-centric status maps to create awareness of all the components required to deliver the service successfully.

Level 4
Dynamic management

Level 4 is the ultimate goal of the maturity model for network observability. With advanced, integrated platforms providing nearly 100% visibility, IT and NetOps teams gain full understanding and control of their entire infrastructures, including hybrid cloud elements and all components, both on and off premises.

At this stage, these advanced platforms enable IT and NetOps teams to focus on using resources to support and enable the business. Integrated monitoring and operational tools automate the handling of most day-to-day performance and availability problems. Their platforms can also shift resources automatically to optimize the infrastructure for changing business conditions.

Performance and management data provides insight into the business, not just infrastructure components that make up the network. With comprehensive automation and reliable real-time analytics, network and infrastructure performance undergoes continuous improvement. Staff members spend less time firefighting and more on innovating.

At Level 4, organizations leverage insights from their network observability system to automate actions of their infrastructure performance through an automation system, resulting in unprecedented levels of confidence. This allows staff members to fine-tune the particulars of their systems and implementations for continuous improvement of application and service delivery.

Both technology and business leaders understand how IT and NetOps can help make business more successful, and the two groups have a common language and frame of reference with which to communicate—all thanks to improved network observability maturity.

Push your organization forward on the maturity path

Use this framework to identify which stage of the maturity model most closely resembles your organization's present functional state. Then determine which steps your organization and your team need to take in order to improve your capabilities and begin advancing through the model.

Things to keep in mind as you start down this path include:

Monitoring tools
- Move away from element-centric and domain-centric tools.
- Focus monitoring efforts on applications and business services.

Event response
- Leave behind the firefighter mentality and always-in-a-crisis approach.
- Automate as much as possible to eliminate errors and close loops on operations.
- Turn your team's siloed specialists into domain experts who are focused on planning, optimization and business support.

Relationships with the business
- Avoid being perceived merely as a back-office cost center.
- Find ways to deliver business insights to the business, such as creating custom views and reports.
- Establish service liaisons within your team; have them learn how to speak the language of the business.
- Focus on strategic service planning to advance your organization's critically important digital transformation.

Why IBM?

IBM SevOne Network Performance Management (NPM) provides a single source of truth to help assure network performance across multivendor, enterprise, communication and managed services provider (MSP) networks.

Learn more about SevOne NPM and how it can help your organization monitor and manage the performance of both your existing and next-gen network and infrastructure resources more effectively.

> "IBM offers a new approach to network performance management with its IBM SevOne Network Performance Management solution. The IBM solution helps modern IT organizations address next-generation requirements and drive network performance through every stage of the digital transformation journey."[1]
>
> **Shamus McGillicuddy**
> Vice President of Research, Network Management
> Enterprise Management Associates, Inc.

© Copyright IBM Corporation 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
May 2024

IBM, the IBM logo, IBM Cloud Pak, and SevOne are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

1. Chart a Path to Digital Transformation with Application-Aware, AIOps-Driven Network Performance Management, EMA white paper, April 2022.