Consolidating network performance monitoring tools

A business case for financial services

IBM

Consolidating network performance monitoring (NPM) tools is an effective way for financial services enterprises to save costs and resources. By using a modern NPM system, they can eliminate redundant tools and their maintenance contracts along with resources needed to sustain them. When consolidating to a new platform, they can avoid obstacles by choosing a solution that addresses pain points of individual staff and departments. The end result is a reduction in capital expenditures (CapEx) and operating expenses (OpEx), a related decrease in risk and a streamlined path to improved troubleshooting and less downtime.

Too many performance monitoring tools?

Of all the major business sectors, few depend on the performance of their IT infrastructure more than financial services. Any disruption of service — even a fraction of a second — can result in major cost impacts on both the enterprise and its customers. The use of numerous disparate monitoring tools is common throughout the industry, including using tools from the blending of two or more IT infrastructures due to mergers and acquisitions or siloed monitoring towers.

Although the goal of performance monitoring is to keep everything up and running efficiently, the proliferation of point solution tools is having the opposite effect. Too many can slow down operations, with devastating effects.

How many performance monitoring tools are too many? Isn't it time you considered the benefits of NPM tool consolidation?

This white paper examines why consolidation of performance monitoring tools is critical for the financial services industry, what obstacles exist to achieving that goal and how to choose a monitoring platform that's right for your enterprise.

"Although many network management tools are multifunction solutions that address a variety of use cases and workflows, EMA has long found that most network operations teams use large, fragmented toolsets ... the network team has anywhere from 4 to 15 tools. It is very rare for a network team to have fewer than four tools."[1]

Shamus McGillicuddy
Vice President of Research, Network Management
Enterprise Management Associates, Inc.

The benefits of tool consolidation

Consolidating NPM tools can yield a host of benefits beyond the basic cost savings achieved by the elimination of overlapping functionality and redundant maintenance contracts:

– **CapEx reduction.** Tool consolidation can reduce the high costs of the hardware needed to support individual tools. It can also soften the investment through realized cost savings.

– **OpEx reduction.** Cutting back on the resources needed to support duplicative monitoring features from multiple vendors can yield significant savings in operating costs by optimizing efficiencies and streamlining operations.

– **Improved responsiveness to line of business (LOB).** LOB requests from the types of internal departments that financial services deal with — wealth management, capital markets, retail, wholesale banking, asset management, insurance and so on — depend on transparency from the infrastructure team. Consolidating tools allows financial services firms to respond more quickly and with full transparency to LOB requests.

– **Collapsing IT silos and data sources.** By reducing the number of people required to support multiple tools, consolidation frees resources and staff for other pursuits. Fewer people administering tools means there will be more staff developing innovative solutions to increase revenue and customer satisfaction.

– **Improved MTTR.** Reducing the number of tools can minimize the mean time to repair (MTTR) by giving troubleshooters a single source of truth to investigate and speeding up identification of the root causes behind issues.

– **Risk reduction.** Consolidation can mitigate risk before issues arise, thereby minimizing the possibility of service disruption and resultant user impact. Improved visibility in infrastructure management leads directly to a clearer understanding of when performance may impact the customer base.

– **Faster time to market with new services.** Consolidating tools allows you to deploy new services quickly, all in one place. From implementing desktop services to setting up branch offices, consolidation aids in application migration and establishes before-and-after baselines to help analyze the impact of change in the environment.

Consolidating network performance monitoring tools

How to overcome resistance and choose the right NPM system

From a leadership perspective, tool consolidation isn't an easy decision because you'll likely encounter initial resistance among the ranks, especially from those who will lose their favorite tools. This resistance stems from three main personnel-related sources:

– Staff in traditional independent IT silos have their own tools, like them and want to keep them.
– Managers have their longtime favorite tools and reports.
– Mergers and acquisitions staff bring their own tool sets and are reluctant to give them up.

Non-personnel impediments can be even more daunting. Existing tools may be tightly integrated into larger relationships and other platforms, such as integration management, AIOps and fault systems, reporting solutions and more. A new NPM must match or supersede existing individual functionality, such as NetFlow or capacity measurements. Plus, the costs of breaking ties with vendors who supply product-specific tools may significantly inhibit change.

You need to develop a groundswell around the resistance by demonstrating to others that the change will be good for everyone. And the best way to get others to champion the changeover is to choose the right NPM system for your organization. If you do, the team should come around pretty quickly. Why, you ask? A change that is right for your organization will reduce both costs and risk while introducing a wealth of new functionality. In the aftermath of a wise choice, staff will welcome the improved troubleshooting that will make their jobs easier while also reducing MTTR.

The right NPM system is the one that best addresses your main pain points. It should have a small hardware footprint, be able to handle tremendous scale, reduce the number of application instances — which will save money and reduce administration costs — and be able to visualize and easily pivot between metric, flow, and third-party log data in a single system. It should also provide access to the application programming interface (API) for no additional cost and support for leading next-generation software-defined networks (SDNs) while delivering rapid device certification of new technologies for Simple Network Management Protocol (SNMP) polling, so teams can monitor new devices in the network quickly.

In short, the right NPM system is a single source of truth that improves functionality and solves monitoring problems your current tools cannot.

It will be difficult to replace 100% of monitoring tasks, but the right platform can get you most of the way there. The remaining tasks are often best accomplished by individual point tools. These point solutions are clearly essential in some cases. However, you can also use the overview from a next-generation NPM system to alert you to changes that may need to be examined and addressed by specific point solutions.

Remember: There's no need to consolidate all the tools all at once. Executing conversion in stages frees up employees to pursue new technologies and vendors and helps them become accustomed to the new platform.

Rationale for changing to a monitoring platform

Identifying the pain points in your current performance monitoring platform — or collection of tools — is the first step in determining what improvements you'll need. Cost savings and risk reduction are always incentives for change, especially when you need new hardware or have identified security vulnerabilities. But any one of the six areas of concern outlined on the next page can help justify changing to a comprehensive NPM system.

To make the business case in your organization, look to your individual LOB. Attach the solution to an issue and then get into the specifics of solving the problem. For example, trade and brokerage firms need polling at rates unavailable with traditional tools, and they also want to be able to visualize metrics associated with network latency. Retail banks need a single page view of the infrastructure to identify bottlenecks. The value of knowing application traffic and end-to-end performance applies to all sub-verticals in finance.

Consolidating network performance monitoring tools

Six pain points for the financial services industry

1. **Optimum performance.** Financial services firms require optimum performance from their network to support online transactions, especially when involved in high-velocity trading, which scans dozens of public and private marketplaces simultaneously and processes millions of orders per second.

2. **Availability of online business.** The financial sector rarely conducts business by phone, opting instead for the internet. Insurance claims processing, retail bank access and stock trades are all supported by the network. Hence, availability of these real-time interactions with the public directly impacts revenue.

3. **Consolidation.** Mergers and acquisitions over the past 15 years have resulted in mass consolidation of the financial services market. Today, financial services organizations must deal with data center consolidation. A side effect of mergers is a plethora of performance monitoring tools brought by the different IT teams. A single NPM system can eliminate many of these tools and their redundant functionalities and overlapping maintenance contracts.

4. **Complexity of global networks.** Top investment banks are global entities with data centers across many geographies that support dozens of LOBs. They require an NPM that can support massive scale distributed across their branch offices and data centers.

5. **SDNs.** The use of software-defined networking across the wide area network (WAN) and in the data center poses new monitoring challenges to many organizations. SNMP is typically not the standard protocol for these next-generation networks. Retrieving performance data from SDNs often requires use of APIs interfacing with software-defined control systems or vendor-supplied management tools.

6. **Security and distributed-denial-of-service (DDoS) attacks.** DDoS attacks that target online banking portals and credit card payment gateways pose a tremendous threat to financial services firms and the security of their customer data. Performance monitoring can confirm service availability.

Reliable reports support business decisions and offer insights based on key performance indicators (KPIs) you define. An effective NPM system will collect any time series data, regardless of source, and seamlessly integrate it with other metrics, such as SNMP and IP service level agreements (SLAs). You'll want the capability to view any metric down to one-second granularity, with zero degradation to the speed of reports, no matter the size of your monitored domain.

Perhaps your organization wants to optimize network performance to meet application delivery SLAs and reduce risk, or to increase competitive standing through technology. Or maybe you need to provide LOB visibility into the delivery of network services to ensure timely understanding of current outages.

These performance monitoring "upgrades" are possible and often necessary. But they will happen only when you replace an unrelated set of tools with a comprehensive NPM system.

Consolidating network performance monitoring tools

The urgency for consolidation versus the initial cost

Changing to a new NPM system is not without cost. Even when ROI is substantial, initial cost justification is mandatory. When weighing the cost, consider what you're currently paying in ongoing professional services fees to get your existing software to do what you need it to do, or to integrate disparate systems. Your existing professional services and integration costs could be unnecessarily high.

In addition to the benefits of a comprehensive NPM already noted, there's another urgency to consolidating tools: You need to replace homegrown tools before you lose the people who know how to use them. And instead of spending several worker days every month pulling together data from that collection of discreet vendor tools you currently use, think about the ease of doing it all at once, automatically, with the right platform. Is it worth the risk to wait until two of the ten people you've been using to do this monthly labor-intensive task leave the organization? Besides the gap left behind, there are the demands of hiring and training new people.

Lastly, think about the urgency to consolidate tools in this way. A problem is occurring, something new, an incident you haven't seen before. Rather than configuring five tools to identify the parameters of the issue, wouldn't you rather employ one comprehensive NPM that lets you discover what's wrong? You could be troubleshooting the case much faster by using one NPM system to create extraordinary reaction speed for your organization.

A solution to consider

When seeking a performance monitoring platform that will help your organization in many ways, including tool consolidation, IBM® SevOne® Network Performance Management (NPM) is an obvious choice.

SevOne NPM has extensive experience helping all segments of the financial services industry. To cite a handful:

— When a high-profile network outage halted trading on a major stock exchange, SevOne NPM helped ensure such a disruption would not reoccur.

— When a global investment bank approved a global IP SLA architecture project to install shadow routers in each global data center, it ran a fully meshed latency and jitter monitoring configuration across multiple quality of service (QoS) queues with SevOne NPM as the core monitoring and reporting tool.

— A leading investment firm specializing in wealth management used SevOne NPM integration of SNMP and NetFlow to provide better visibility between utilization and top consumers across international WAN links, including connectivity to exchanges.

— A corporate bank needed a single solution that could scale to support its 55,000-device global network and provide a truly global view across all geographical operations centers around the world. Specifically, it was drawn to SevOne NPM's 10-day device certification, high availability, efficient data collection for all the devices in a sub-minute polling cycle, and fast reporting to replace overnight reports.

— A large retail bank used the SevOne NPM solution's metric-to-flow capability to identify and stop antivirus updates that were being pushed during the business day, saturating bandwidth and impacting the performance of branch applications.

Enterprises in the financial services industry that want to replace multiple monitoring systems with a consolidated system need look no further than SevOne NPM. Those that want an aggregation point for multiple types of data can benefit from its flexibility in creating dashboards and reports that incorporate various data types.

When you manage a global network, you never know what might go wrong. Ask yourself: Do I have visibility into everything? You can't let the sheer volume of machine data on your network dictate what you will and won't monitor. SevOne NPM was purpose-built to handle massive amounts of data, providing speed at scale. The best way to ensure 100% availability of business-critical apps and services is to monitor everything. Then create baselines for that data, define alerts and report on any performance deviation.

Your networks don't operate on a minute-by-minute basis. So why monitor them that way? Financial services firms — especially those that operate or access trade networks — require sub-minute polling to detect issues that may temporarily disrupt services. Those issues typically go unnoticed at traditional polling cycles, leaving you in the dark about what's going on with your infrastructure.
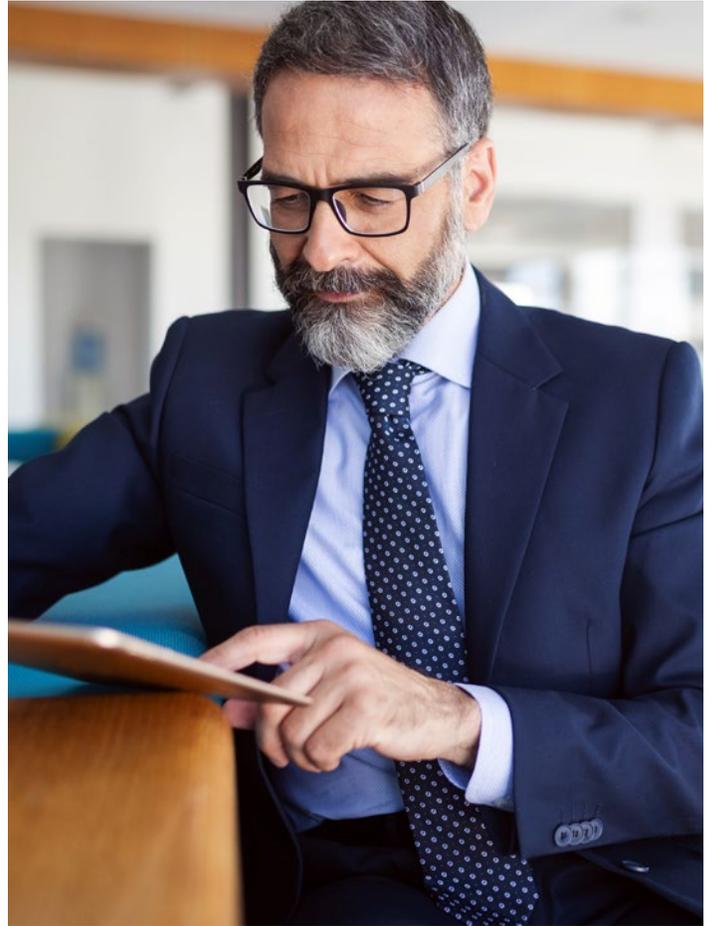
One of the greatest assets of SevOne NPM is its ability to combine multiple monitoring functions into a consolidated offering with a single pane of glass for viewing all key performance metrics. This greatly improves troubleshooting. A single source of truth eliminates finger-pointing and blame games and gets the team to work at once, with resolution of the issue in record time.

Isn't it time to put IT tools to work for you instead of the other way around?

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.

Consolidating network performance monitoring tools

1. Network Management Megatrends 2022: Navigating Multi-Cloud, IoT,
    and NetDevOps During a Labor Shortage, EMA Research Report Summary,
    April 2022.