KedronUK
Enterprise Management Solutions

SELECTING A NETWORK MANAGEMENT SYSTEM

A RESEARCHER'S GUIDE & RFI CHECKLIST

A VENDOR-INDEPENDENT VIEW

WHITE PAPER

KedronUK
Kern House
Stone Business Park
Brooms Road
Stone
Staffordshire
ST15 0TL

T. +44 (0) 1782 752369
sales@kedronuk.com
www.kedronuk.com

ABSTRACT & CONTEXT

This White Paper provides a vendor-independent view of the key factors that should be considered when selecting a Network Management System (NMS).

The guide is aimed at IT Professionals working within the Enterprise, Government or Education sectors who have been tasked with researching the market in order to select the best fit solution for their network.

This paper walks the reader through what can be a confusing marketplace and points out “danger points” which are often missed by companies until it’s too late. It also provides a checklist of useful requirements, which can be used for RFI and vendor comparison.

Although this paper discusses the term “Network Management”, it is appreciated that most management vendors reach into network device, server, application, traffic, storage and configuration management and therefore this paper covers requirements to monitor these multiple IT systems - using Network Management as a generic term.

THE CHALLENGE YOU FACE

WHEN RESEARCHING THE NETWORK MANAGEMENT SYSTEM MARKETPLACE THERE ARE MANY SOURCES OF INFORMATION AVAILABLE: VENDOR WEBSITES, MARKET ANALYSTS, AWARDING BODIES, COMMUNITY FORUMS AND MAGAZINE REVIEWS. ALL THIS INFORMATION CAN QUITE EASILY CONFLICT AND SERVE TO CONFUSE RESEARCHERS.

To complicate matters further, vendors market their product functionality using the same or similar terms, but when looking a little deeper, the researcher often finds what a term means for one vendor means something entirely different to the next.

For example, the term Root Cause Analysis could mean that the management software automatically has an understanding of the topology of a network and is able to send alerts only on the failure of one device that is impacting many. Or, for another product this might only be achievable via pre-configuring a series of manual rules.

As IT Professionals absorb all these information sources and the difference in perspectives, it can become very confusing and it's easy to lose sight of what their business needs.

This document will identify areas that need to be considered when investigating the deployment of a new management solution. In addition, it provides a checklist of key capabilities to use when comparing different vendors to be used within RFIs and business cases.

KEY CONSIDERATIONS

The below forms a list of key considerations that are often missed by those evaluating and selecting an NMS.

By not considering these factors, organisations can, at best, limit Return on Investment (ROI) and at worst select a system that does not function properly within their environment.

SCALABILITY & ARCHITECTURE

Some products scale to the largest global networks whilst others have inherent limitations due to their architecture or design.

The key aspect of this seems to be whether a solution has the ability to offer distributed polling of devices, reporting back to a central middleware and database. Solutions that offer this distributed or hybrid model tend to provide far greater scalability.

Vendor solutions that require polling from one central system will eventually reach the limitation of the network they are serving or of the NMS software itself.

Important questions to potential vendors:

1. Are there case studies / reference sites available for similar sized organisations?
2. What are the limitations of the vendor software you are considering? How many devices/interfaces will they support with one installation? How do they scale beyond this?
3. Does the product's ability depend on the database used as a data store for the NMS?
4. If considering a centralised deployment, how much data will the software be pulling back across your network infrastructure? Can the smaller WAN links cope?

DATA SOURCES

Dependent on which elements of infrastructure the company wishes to monitor, it is important to consider the data sources the environment can provide and a particular NMS can receive, alert and report on. Technologies to consider amongst others are:

- Flow
- SNMP
- WMI
- ICMP
- IPSLA
- QoS
- Configuration Backup
- Scripting
- SMI-S
- System Logs
- Cloud/Virtual Infrastructure API
- Critical Path
- Wire Data
- VoIP/SIP
- Synthetic User Testing

ACCESS & VISIBILITY

When selecting a solution it is important to define which access controls will be required.

Most users require there to be at least two levels of access and visibility, but it is not uncommon to require many more. Consideration should be given to who will access the system and what they should be able to do and see.

Important questions to potential vendors:

1. Are their any limitations on number of roles and users?
2. How granular is role-based access?
   (i.e. can I specify visibility by IP address range, device type, site etc.)
3. Can the user accounts and access roles be integrated into Microsoft Active Directory?

DISCOVERY PROCESS

Many systems have a discovery process that enables the system to 'onboard' the monitored devices. The capability of this process varies greatly from vendor to vendor, so it is a good idea to have in mind how much automation you want and how much manual processing you are prepared to do or pay for.

Important questions to potential vendors:

1. Is the discovery "topology aware"? Does the software understand which devices are connected to each other?
2. Is XML discovery possible, allowing automation of applying custom device definitions and measurement profiles?
3. How does the system deal with new devices added to the system? How does it keep up to date with an ever changing IT landscape?
4. Is the discovery technology based on Agent Collectors, Active Polling or Passive Listening?

VENDOR DEPENDENCY

Although device vendors often provide a management tool that will manage/monitor their own devices/platforms/applications, it is important where possible that the IT Professional can view their environment holistically in a Single Pane of Glass.

If there is a desire to use vendor specific tools: How will using multiple tools affect troubleshooting capabilities? How will the need for training and skill sets be managed across multiple platforms? Would a vendor agnostic solution or manager of managers better suit the requirement?

DEPLOYMENT & CUSTOMISATION

Some systems can cost as much again in deployment and management costs as they did to purchase in the first place. Therefore, the ease of deployment and customisation should be taken into account by the researcher.

If a tool is difficult to manage from a 'standup'/customisation and training perspective, it is not likely to stand the test of time within the business, meaning that any investment in time and financing will be wasted in the long term.

Endeavour to speak to current users of any system that you shortlist, to ascertain its viability in this area.

REPORTING

Most vendors have their own idea as to what a report is. Often it is found that the user's definition of a report does not match that of the vendor.

Important questions to potential vendors:

1. Are the reports you need now or might need moving forwards possible with the selected solution?
2. Can non-standard reports be built within the solution without requiring direct access to database or use of third party reporting packages?
3. Can reports be automated and emailed according to role?
4. Can reports be generated in multiple formats like TEXT, PDF, CSV, XML or XLS?
5. Can reports be integrated into a dashboard?

HIGH AVAILABILITY

In most environments network and application services are likely to be resilient to ensure continuity of business critical systems. In addition to this, most IT departments are required to provide reports for the board of directors demonstrating 99.99%+ availability of the landscape. Consideration should also be given to the High Availability (HA) of your monitoring tool.

Important questions to potential vendors:

1. How is HA / Redundancy / Fault Tolerance achieved?
2. What extra license costs are associated with this?
3. What additional server resources (physical/virtual) are required to implement HA?
4. How easily is this configured and maintained?
5. Does the HA solution cover all software elements and tiers of the NMS?

INTELLIGENT ALERTING

Often, monitoring solutions get ignored over time because they produce too many “false positive” alerts, damaging the user’s trust in the system. This happens either because the system’s alerting feature/functionality has been misconfigured or because it’s not sophisticated enough to cater for real life fault management scenarios.

Systems that understand service, device and test dependencies can determine the root cause of a problem and therefore prevent multiple alerts for the same issue. These types of systems are preferable, as are solutions that can alert according to job role, fault type and time of day.

Some vendors will claim to have root-cause alerting but only after the user has manually configured many rules, which is often not a practical approach for busy IT departments.

Artificial Intelligence (AI) is an emerging technology that learns what is “normal” for any given environment then makes decisions on what alerts should be raised. For larger, more complex environments with many overlapping services and platforms this approach holds a great deal of potential.

AUTOMATION

The fewer manual processes a user needs to perform, the more likely the solution is going to stay up to date with the environment, making it much more accurate at performing its task.

Opportunities for automation include:

- Scheduled Discoveries
- Database Maintenance
- Auto-Updating
- Self-Healing

VIRTUALISATION

Many companies are taking advantage of the savings, on a number of levels, that virtualisation offers. It does however present its own challenges for management and these should be considered. What was once visible now goes unseen.

An NMS that can manage both physical and virtual environments within the same platform, giving seamless visibility of your environment, is now often a key requirement for most enterprises.

Important questions to potential vendors:

1. Which virtualisation technologies and versions are supported?
2. Does the solution require that agents be deployed onto the host environment?
3. Does the solution support virtualisation platforms in the cloud?
4. Will the solution help you right-size your virtual landscape?

SDN & NFV

Software-Defined Networking (SDN) and Network Functions Virtualisation (NFV) are two distinct but complementary technologies designed to bring the following benefits to predominantly enterprise organisations:

- Increase agility
- Lower operational costs
- Easier upgrades
- Elastic infrastructure
- Cloud computation
- New business options
- Responsive services
- Improved security

However, if you intend to exploit these technologies and because of the unique and involved ways they are implemented, any NMS solution must have SDN/NFV monitoring/management capabilities built in. SDN/NFV capability is not something you can configure into a non-compliant solution.

So, you need to understand what benefits/challenges implementing this technology will bring and the potential for requiring it now or in the future before you commit.

CLOUD COMPUTING

Monitoring your Cloud environment presents new challenges especially with server-less services like AWS Lambda/Docker Containers and managed services like RDBS. Cloud services do include logging and alerting features of their own, but decisions need to be made on what is the best approach to achieve your requirements.

Then there are the more exotic services (like AWS S3, SQS, Cloud Front, Route 53, WorkSpaces etc.) that are not covered by traditional monitoring solutions. These will require some creative thinking and architecting to achieve the required levels of monitoring.

SECURITY & AUTHENTICATION

There are two elements to take into account in the area of security and authentication:

- How will access to the management system be secured?
- How will communication between the system and network device be secured?

Who will have access to the tool and what will they be allowed to do? How flexible do you need this to be? Is there a requirement for a multi-tenanted system? Will you be using TACACS or AD?

Are the network devices to be managed controlled by TACACS?

These are all questions that you will need to have answers for when it comes to choosing a management system, so that you can understand how the system can be managed within your environment and security policy. Also, can the tool actually manage the devices within your environment?

IPT/VIDEO

Voice and video transported across IP networks can have a huge impact on the overall performance of the landscape. As such the ability to monitor these technologies, in context of and alongside other services, is an increasingly important factor when selecting an NMS platform.

Tools tend to fall into two categories when monitoring IPT/Video (excluding packet capture tools which are out of scope for this paper):

- IPSLA
- Synthetic Transactions

Each have their advantages and disadvantages, so consideration should be given as to what needs to be achieved and why.

IPSLA measurements are configured on a routing device and are conducted across the chosen network segment for the given application (IPT/Video). The results are then read from the device by the management tool. Synthetic transactions are often very similar in nature to IPSLA but are configured within the management tool. They can be used to provide an end-to-end view rather than just a WAN view and don't add a processing overhead on network devices.

Another important consideration is whether the solution supports the monitoring of the following concepts/technologies which help with IPT/Video monitoring:

- VLAN
- BGP
- CB/QOS
- Call Managers
- SIP Trunks
- MOS (Mean Opinion Scores)

DUPLICATE IP ADDRESS RANGES

If a company has duplicate IP address ranges across their global estate (often occurring due to merger or acquisition) it will need to be confirmed that the chosen management tool can cope with this configuration.

INTEGRATION WITH THIRD PARTY SYSTEMS

It is often beneficial to integrate the management system with third party systems such as helpdesks, CMDBs or even other management platforms covering different perspectives.

Important questions to potential vendors:

1. How flexible and accessible is the data structure of the management tool?
2. Are there any supported APIs available for integration?
3. Are there any existing documented integrations with the chosen system?

RFI CHECKLIST

The checklist has been formulated using the above considerations as a basis to help researchers easily compare prospective vendors.

This should be used in conjunction with your own functional requirements checklist to ensure all required capabilities are captured.

Instructions

1. Enter a score of importance between 1 and 5 (1 being not important and 5 being essential) in the “Importance” column against each consideration.

2. Enter a score between 0 and 5 of how well each vendor complies with each consideration (with 0 meaning the vendor doesn’t comply at all and 5 being that it is fully compliant).

3. For each consideration, multiply the Importance score with the vendor score to provide a total. Complete this for all vendors.

4. For each vendor add the scores to provide you with a total score. The highest scoring vendor would probably best suit your requirements.

N.B. A self-calculating Microsoft Excel version of this checklist is available upon request.

RFI CHECKLIST PART 1

VENDOR 1

VENDOR 2

VENDOR 3

Consideration	Importance (1-5)	Vendor 1		Vendor 2		Vendor 3	
		Score (0-5)	Total	Score (0-5)	Total	Score (0-5)	Total
Maximum number of monitored elements per installation							
Distributed architecture option available							
Required database for optimum performance							
Relevant sized customer reference site available							
Support SNMP V2 and V3 capable							
Supports WMI							
Supports NetFlow / SFlow Monitoring (confirm versions)							
WMI capable							
TOTALS							

RFI CHECKLIST PART 2

Consideration	Importance (1-5)	Vendor 1		Vendor 2		Vendor 3	
		Score (0-5)	Total	Score (0-5)	Total	Score (0-5)	Total
Able to use common scripting languages to generate outputs for measurements							
Support SMI-S							
Ability to view and change network device configurations centrally							
Ability to report on QOS							
Virtualisation Vendor Support (specify versions)							
Limitations on number of roles and users							
How granular is role based access? (i.e can I specify visibility within roles by IP address range, device type, site etc.)							
	TOTALS						

RFI CHECKLIST PART 3

Consideration	Importance (1-5)	Vendor 1		Vendor 2		Vendor 3	
		Score (0-5)	Total	Score (0-5)	Total	Score (0-5)	Total
Is XML discovery supported?							
Are new devices discovered and automatically added to the system when installed on the network?							
Is there a list available of supported devices?							
What is the support policy for any new devices not currently covered by the solution?							
What is the approximate range of number of Professional Service days required to configure a fully functional system on a XXXXX device network							
Is the system able to produce the specified required reports?							
Are there any integration APIs for third party systems?							
		TOTALS					

RFI CHECKLIST PART 4

Consideration	Importance (1-5)	Vendor 1		Vendor 2		Vendor 3	
		Score (0-5)	Total	Score (0-5)	Total	Score (0-5)	Total
Can custom reports be created without third party reporting packages or needing to query back end database?							
Can reports be scheduled and emailed according to user role?							
Is there a supported HA option available for all solution components?							
Does this system provide topology and service-aware root cause analysis for alerting?							
Can alerts be configured according to user role, location and time of day?							
Does the system present any opportunities for automation?							
Can the solution manage duplicate IP address ranges within the same system?							
Which authentication technologies does the system support?							
TOTALS							

RFI CHECKLIST

	PART 1	PART 2	PART 3	PART 4	TOTAL
VENDOR 1					
VENDOR 2					
VENDOR 3					

CONCLUSION

SELECTING THE CORRECT NMS CAN BE A COMPLEX PROCESS AND WHAT IS IMPORTANT TO A PARTICULAR ORGANISATION WILL VARY ACCORDING TO SIZE, CURRENT TOOLS IN PLACE, PURPOSE FOR THE PROJECT, INDUSTRY, JOB FUNCTION OF THE JOB SPONSOR AND MANY OTHER FACTORS.

Researchers should always first examine what outcome they are looking to achieve and then consider what type or types of solution best suits those requirements. This will make creating a shortlist of vendors a much more efficient task.

Often the best way to move things forward for your enterprise is to engage with an experienced consultancy company who can guide you towards the correct solution to meet not only your technical but also your business needs.

KEDRONUK

Enterprise Management Solutions

KedronUK is a leading Network and Application Performance Management Consultancy.
We provide our customers with increased visibility and control across their network and application infrastructure by combining leading technology, knowledge and service.

KedronUK appreciate that although our clients have similar challenges and objectives, the obstacles they face can differ vastly from company to company and culture to culture.

We approach each client engagement as an individual project, creating unique plans for each customer, from initial discovery and scoping right through to installation, configuration, deployment and solution development.

Our services provide greater operational and security intelligence, increased productivity by reducing problem resolution times, and cost saving via automation and optimisation of IT infrastructure.

◆◆◆

KedronUK
Kern House
Stone Business Park
Brooms Road
Stone
Staffordshire
ST15 0TL

KedronUK
Enterprise Management Solutions

T. +44 (0) 1782 752369
sales@kedronuk.com
www.kedronuk.com