Infosim - WHITE PAPER

Selecting a Unified Network Management Solution: A Researcher’s Guide and RFI Check List.

Document Ref: - UNMS_ARG+RCL_JB001_RV1

Author	James Brunner – Infosim
Document Reference	UNMS_ARG+RCL_JB001_RV1
Version Number	RV1 (1st Release Version)
Issue Date	1st October 2013

Document Request – Contact: - sales@infosim.net

Contents

1 Abstract and Context

This White Paper provides a vendor independent view of the key factors that should be considered when selecting a Unified Network Management Solution (UNMS).

It 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 market place and points out "danger points" which are often missed by companies until it's too late. It also provides a useful requirements check list which can be used for RFI and Vendor comparison.

Although this paper discusses the term "Unified 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 Unified Network Management as a generic term.

2 The Challenge You Face

When researching the Unified Network Management Solution market space 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 actually when looking a little deeper, the researcher often finds what a term means for one vendor, means something entirely different to another.

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. Another product may only be able to achieve this by pre-configuring a series of manual rules which will require maintaining during the life of the tool.

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 the author believes need to be considered when investigating the deployment of a new unified network management solution. In addition it provides a check list of key capabilities to use when comparing different vendors to be used within RFI's and business cases.

3 Key Considerations

The below forms a list of key features that are often missed by those evaluating and selecting a Unified Network Management Solution.

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

3.1 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 server 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 a limitation in the network it is serving or of the UNMS software itself.

Important questions to ask potential vendors

- Are there case studies or reference sites available for similar sized organizations?
- What are the limitations of the software you are considering – how many devices or interfaces will they support with one installation and how do they scale beyond this?
- Does the product's ability depend on the database used as a data store for the NMS?
- If using a centralized deployment how much data will the software be pulling back across your network infrastructure - can my smaller WAN links cope?

3.2 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 UNMS can receive, alert and report on. Technologies to consider amongst others are:

- Flow-based (NetFlow, sFlow, jFlow etc.)
- SNMP (v1, v2c and v3)
- WMI
- ICMP
- IPSLA
- QoS
- Configuration Backup
- Scripting
- SMI-S

3.3 Access and Visibility

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

Most organizations require there to be at least two levels of access and visibility, but it is not uncommon to find situations which 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 ask potential vendors

- Are there any limitations on the number of roles or users created in the product?
- How granular is the role based access controls?
- Can you control visibility of devices by IP Address Range, Device Type, Site, etc.?

3.4 Discovery Process

Many systems have a discovery process that enables the system to 'on-board' 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 ask potential vendors

- Is the discovery process "topology aware"?
- Does the software understand how devices are connected with each other?
- Is a programmatic discovery possible allowing automation of many configuration settings such as device definitions and measurement profiles?
- How does the solution deal with new devices added to the network?

3.5 Vendor Dependency

Although device vendors often provide a management tool (usually for a fee) that will manage or monitor their own devices, platforms or applications, it is important where possible that the IT Professional can view the environment as a whole within a single pane of glass regardless of hardware vendor selected now or in the future.

Important questions to ask potential vendors

- If there is a desire to use vendor specific tools, how will using multiple tools impact on troubleshooting capabilities?
- How will training and maintenance be managed across multiple platforms?
- Would a vendor independent solution be a better fit?

3.6 Deployment and Customization

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 customization should be taken into account by the researcher.

If a tool is difficult to manage from a customization 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.

3.7 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 ask potential vendors

- Can you define the reports you need – can the solution provide powerful, flexible and simple to configure reporting?
- Can non-standard reports be built within the solution without requiring direct access to the underlying database or the use of a 3rd party reporting tool?
- Can reports be automated (creation and distribution) according to role?

3.8 High Availability

In most environments network and application services are likely to be resilient to ensure continuity of business critical systems. Consideration should also be given to the High Availability (HA) of your monitoring tool.

Important questions to ask potential vendors

- How is High-Availability/Redundancy achieved?
- What are the extra licensing costs associated with this?
- How easy is it to configure and maintain this deployment?
- Does the High-Availability/Redundancy configuration cover all elements of the NMS solution?

3.9 Intelligent Alerting

Often, monitoring systems get ignored over time as they produce many “false positive” alerts damaging trust between the system and the users.

This happens either because a systems alerting functionality has been misconfigured or because it is not sophisticated enough to cater for real life management scenarios.

Systems that can calculate ‘root cause’ of an issue and therefore prevent multiple alerts for the same fault 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.

3.10 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.

Some opportunities for platform maintenance automation include: Scheduled device and capability discovery, Automatic database maintenance and Server issue self-diagnosing and healing.

3.11 Virtualization

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

A UNMS 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 ask potential vendors

- Which virtualization technologies and version are supported on which components of a solution?
- Does the solution require that agents be deployed onto the host environment or do they remain virtualized?

3.12 IPT/Video

Voice and video transported across IP networks can have massive effects on overall IT performance. As such the ability to monitor these technologies in context of, and alongside other services is an increasingly important factor when selecting a UNMS 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 and Synthetic Transactions. Both have their advantages and disadvantages, so careful consideration should be given to what needs to be achieved and why.

IPSLA measurements are configured on routing devices 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 but increase the resource load on the devices themselves. Synthetic transactions are often very similar to IPSLA in nature but are configured within the management tool. This can provide an end-to-end view rather than just a WAN perspective and, apart from the traffic generated itself, doesn't add a resource overhead to network devices.

3.13 Duplicate IP Address ranges

If companies have 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 manage devices within this overlapping IP Address configuration.

3.14 Security and Authentication

For a Unified Network Management Solution, Security and Authentication fall into two separate areas. Firstly, how do we secure communication and access from a workstation to the management solution and secondly, how will communication and access from the solution to the devices be secured?

Important questions to ask potential vendors

- Who will have access to the management solution? What will they be allowed to do?
- How flexible are the access permissions in the solution required to be?
- Is this a multi-tenanted solution?
- Will access to the solution be controlled using an external authentication system such as TACACS, Radius or LDAP/Active Directory?
- Is access to the devices under management also controlled by an external authentication system?
- Is all workstation to management solution traffic encrypted, especially passwords?
- Does the "management solution to device" protocols supported also include encrypted standards such as HTTPS, SSH and SFTP?

3.15 Integration with 3rd Party Systems

It is often beneficial to integrate the management system with 3rd party systems such as helpdesk products, CMDBs or other management platforms covering different business perspectives.

Important questions to ask potential vendors

- How flexible and open is the data structure of the management tool?
- Are there supported AND fully documented APIs available for integration?
- Are there existing documented integrations with a chosen system already?

4 RFI Checklist

The below 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.

4.1 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 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 total scores to provide you with total score for each vendor. The highest scoring vendor would probably best suit you requirements.

4.2 The RFI Checklist

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?							
Is a relevant sized customer reference site available?							
Supports SNMP v2 and is v3 capable?							
Supports WMI?							
Supports NetFlow and/or sFlow Monitoring (please confirm versions)							
Supports device CLI interaction using Telnet, SSH etc.							
Able to use common scripting languages to generate outputs for measurements?							
Support SMI-S							
Ability to view and change network device configurations centrally							

Consideration	Importance (1-5)	Vendor 1:		Vendor 2:		Vendor 3:	
		Score (0-5)	Total	Score (0-5)	Total	Score (0-5)	Total
Ability to report on QOS?							
Virtualization Support – Vendor and version(s).							
Are there any limitations on number of roles and users?							
How granular is role based access? (i.e. can I specify element visibility by IP address range, device type, site etc.)							
Is programmatic device 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 number of Professional Service days required to configure a fully functional system on your network? Number of devices: ______________							

Consideration	Importance (1-5)	Vendor 1:		Vendor 2:		Vendor 3:	
		Score (0-5)	Total	Score (0-5)	Total	Score (0-5)	Total
Is the system able to produce the required corporate reports?							
Can custom reports be created freely without the need for 3rd party reporting packages or queries to the backend database?							
Can reports be scheduled and emailed according to user role?							
Is there a supported High-Availability 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 your system present any opportunities for process automation? Please specify.							
Which authentication technologies does the system support?							
TOTAL		__________		__________		__________	

5 Conclusion

Selecting the correct UNMS can be a complex process and what is important to a particular organization 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 short list 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 in the right direction for the correct solution that meets not only your technical but also your business's needs.

6 Resources & Further Information

Follow the links below for further information about Infosim StableNet®.

1. Infosim Web Site: www.infosim.net
2. Infosim StableNet® Videos: http://www.infosim.net/resources/videos.html
3. Infosim StableNet® Case Studies: http://www.infosim.net/resources/case-studies.html
4. Infosim StableNet® Industry Reports: http://www.infosim.net/resources/industry-reports.html
5. Infosim StableNet® Product Sheets: http://www.infosim.net/resources/product-sheets.html
6. Infosim StableNet® Request Trial: http://www.infosim.net/support/trial.html

For any additional information, demonstrations or webinar requests: http://www.infosim.net/about/contact.html

EMA Radar – Report Summary & Infosim Profile

An external report by Enterprise Management Associates® (EMA™) Radar Report for Enterprise Network Management Systems (ENMS): Q4-2012. A report summary and Infosim profile produced and written by Tracey Corbo, and Jim Frey October 2012 is available using the following link below:

http://www.infosim.net/fileadmin/user_upload/resources/industry_reports/EMA-ENMS-Q4-2012_RadarSummary-Infosim.pdf

7 About this Document

This document provides details on vendor neutral requirements that should be considered when selecting a Unified Network Management Solution. Whilst this document does not include every item that a UNMS should contain it does highlight the key features that are often missed when making this selection. It also contains a quick RFI checklist that is invaluable in this process.

7.1 About Infosim

Infosim is a leading manufacturer of automated Service Fulfillment and Service Assurance solutions for Telco's, ISP's, Managed Service Providers and Corporations. Infosim develops and markets StableNet®, the leading unified software solution for Fault, Performance and Configuration Management. StableNet® is available in two versions: Telco (for Telecom Operators and ISP's) and Enterprise (for IT and Managed Service Providers). StableNet® is a single platform unified management solution designed to address today´s many operational and technical challenges of managing distributed and mission critical IT infrastructures.

7.2 About Infosim StableNet® (Telco & Enterprise)

StableNet® Telco is a comprehensive unified management solution; offerings include: Quad-play, Mobile, High-speed Internet, VoIP (IPT, IPCC), IPTV across Carrier Ethernet, Metro Ethernet, MPLS, L2/L3 VPNs, Multi Customer VRFs, Cloud and FTTx environments. IPv4 and IPv6 are fully supported.

StableNet® Enterprise is an advanced, unified and scalable network management solution for true End-2-End management of medium to large scale mission-critical IT supported networks with enriched dashboards and detailed service-views focused on both Network & Application services.

StableNet® is a 3rd Generation highly automated Network Management System. The key differentiation of StableNet® to other legacy type Operational Support Systems (OSS) is that StableNet® is a Unified OSS system with three integrated functionalities that focus on Configuration, Fault and Performance Management, with Automated Root-Cause-Analysis (RCA). StableNet® can be deployed on a Multi-Tenant, Multi-Customer or Dedicated platform and can be operated in a highly dynamic flex-compute environment.

8 Disclaimer

This document contains information confidential and proprietary to Infosim GmbH. It shall not be disclosed by you in whole or part to any third party or to any of your employees other than those who have a need to know such information. You are not permitted to duplicate or use this document for any purpose other than its intended use.

END OF DOCUMENT