White Paper

MaaS and CaaS

Monitoring As A Service
Compliance As A Service

ARGENT

Introduction

An effective way to increase IT efficiency is to move to the MaaS monitoring model. With the right choice of vendor this provides extensive cost savings and at the same time increases operating efficiencies of the always-understaffed IT department.

MaaS means different things to different people; this Argent white paper will explain some of the more common and popular approaches.

The Traditional Model

The best way to view the future is to start by examining the past. The traditional model of monitoring was an all-in-house affair: one or more monitoring products would be bought, and after some little time, and often more than a little pain, the products would be up and running, all happily monitoring their assigned hardware or software resources. When something bad happened, the assigned monitoring product would display a message on its own GUI and, upon noticing this alert, the in-house employee would take corrective action.

Often the benefit of a specialized monitor for a particular portion of the infrastructure was offset by the inefficiency of employees being forced to view multiple screens, often on different hardware platforms. In addition, the in-house employee needed to learn and use entirely different operational motifs for the different products from different vendors for different parts of the environment, no single pane of glass.

Worst of all, one or more in-house employees would be needed to watch the multiplicity of screens; larger companies could afford to create specialist Network Operations Centers or NOCs, but small and medium-sized companies were forced to use a crude ad hoc approach that was both expensive and often times ineffectual.

The MaaS Model

While MaaS vendors' approaches vary in detail and in cost, there are many commonalities.

The most significant difference between the traditional approach and MaaS is that the in-house employees are replaced with trained specialists whose sole job is to monitor various clients' environments. This is essentially a Super-NOC for a range of clients. So instead of an in-house employee noticing an issue has arisen, it will be the vendor's specialists.

A critical requirement with leading MaaS vendors is **Universality** – it is useless to outsource monitoring to a vendor if the vendor cannot monitor all the critical software and hardware resources. To do so would be to have the worst of both worlds – paying a MaaS vendor while still having to use in-house employees.

All MaaS vendors always *claim* they have this Universality, but this is the second most important point to verify when reviewing MaaS vendors. There is a sample checklist in Appendix A of this White Paper, taken from a real-world MaaS implementation completed by Argent in 2012. While every customer's needs are different, this checklist can be used as a starting point.

Alerting Management Protocol (AMP)

The most important aspect of the MaaS model is the vendor's experience in creating the Alerting Management Protocol (AMP). Events that are tracked by the MaaS vendor vary widely, from the benign to the critical.

An example of a benign issue is when a production SQL Server machine falls below 20% disk free space; an example of a critical issue is when the same production SQL Server machine falls below 2% disk free space. In the first case, a simple email is typically sufficient. In contrast, in the second case, the customer's employees need to be gotten out of bed, as the production SQL Server machine is about to fail.

Which introduces the next point – one that is actually an extension of the Alerting Management Protocol, namely, who corrects?

Argent strongly recommends that the MaaS model be just that: a model of outsourcing the monitoring to an experienced vendor. **The actual correction of the error conditions reported by the MaaS vendor must only be done by the customer's employees. To have the MaaS vendor take corrective action is far too dangerous.** The purpose of MaaS is to efficiently outsource the prosaic, but critical, day-to-day monitoring of the entire infrastructure; it is not to take over the complete control of the monitored infrastructure. To do so would be tantamount to outsourcing everything.

A clear line has to be drawn between monitoring and correcting. The purpose of the Alerting Management Protocol is to clearly define the steps to be taken, and the escalations to be implemented when an event occurs, so there are no 'misunderstandings' and no fingerpointing.

While time consuming, it is critical that a complete Alert Management Protocol be created for each and every monitored event. This is where MaaS most often fails or fails to deliver to its fullest potential: corners are cut and this results in completely avoidable confusion.

CaaS Model

CaaS is another of the ever-growing family of 'aaS' acronyms. In this case it is *Compliance* as a Service. Ever more stringent compliance rules and regulations are second only to moving to the cloud as challenges faced by CIOs. Worldwide, governments are promulgating more and more rules and these greatly increase the workload of the already pressed IT department. A simple example is retention of Windows Event Log files. Many regulations in various countries mandate that these files be retained so they can be reviewed by external auditors. While the numbers of years to retain the event log files varies from country to country, this simple requirement is actually a major pain.

One increasingly popular approach is to offload the archiving of these compliance files to the cloud, or more specifically to a CaaS vendor who can handle all the day-to-day archiving and retrieval of this critical compliance data. The failure to meet these compliance laws can be harsh – HIPAA fines often range in to the millions of dollars – Cignet Health was fined $4,300,000; CVS was fined $2,200,000, and these are just two of the HIPAA fines.

So as part of the base MaaS, CaaS should be very seriously considered as well – monitoring, compliance, and alerting are interrelated. As such all three need to be viewed as a single project, not as three different and discrete parts of the IT puzzle.

About Argent

Argent's worldwide headquarters are located at 100 Wall Street in the heart of Manhattan's financial district. With over two decades of experience and 2,500 customers worldwide, Argent solves customers' automation, compliance, and monitoring problems in over 30 countries. For more information please see Argent.com.

Appendix A – Sample Real-World Checklist

The following is a brief, general-purpose, checklist that can be used as a basis for reviewing MaaS and CaaS vendors. This is based on one Argent customer's needs, and as such is an excellent real-world baseline.

This file is available as a Word file at:
http://help.Argent.com/Argent_Maas_CaaS_Checklist.doc

MaaS – Monitoring as a Service

Internet and Intranet

- Worldwide monitoring of performance of external web sites and intranets
- IIS
- Apache

Software

- Siebel
- Stellant
- Active Directory
- Symantec
- Backup
- SAP
- Oracle
- Exchange 2007/2010
- SQL Server 2005/2008/2012
- Production file transfers

Physical Resources

- Temperature of server room
- Humidity of server room
- Server room air conditioning filters
- UPS backups
- Swipe card access stations
- CCTVs

Servers

- AIX servers
- Solaris servers
- Windows servers
- iSeries machines

SNMP

- Cisco routers and switches
- Juniper routers and switches

CaaS – Compliance as a Service

General Requirements

- 256-bit encryption
- Standard PK zip compression
- Dual location data pathing
- Two-phase commit
- Local compression and encryption
- Automatic push-out deployment
- Custom filters available in WMI, PowerShell, and VBScript

Secure Server Farms

- AIX servers
- Solaris servers
- HP-UX servers
- Linux servers
- Windows servers
- iSeries machines

Windows Event Logs

- Ability to reset and purge after completion of two-phase commit

SYSLOGs

- Universal support – SNMP routers and switches as well as Linux and Unix

Application Logs

- Support of ASCII and UNICODE