OVUM

The Power & Payback Of Unified Monitoring

CA Unified Infrastructure Management: The IT Monitoring Solution for the Digital Enterprise

(Formerly known as CA Nimsoft Monitor)

Written by: Michael Azoff

Published September, 2014, © Ovum

MANAGEMENT SUMMARY

KEY CHALLENGES FOR IT OPERATIONS

Monitoring IT operations is made costly and inefficient due to the presence of multiple, complex monitoring solutions. These legacy systems have a silo view of the IT environment creating unnecessary complications when trying to resolve infrastructure and availability issues. While system administrators are attempting to resolve these problems the customers and their business are suffering. For hosting providers there is the threat that customers will walk to cloud outsourcers. There is therefore a need for a single solution that can provide timely support for new applications and technologies, to help reduce IT operational costs and complexity, and to put customer need at the center of operations.

In addition there is the problem of managing remote data centers, whether as a managed host provider or an enterprise with locations in remote regions of the globe. IT operations require a monitoring solution that is easy to manage and configure, with new system components added remotely into live systems – as simple as plug and play. A multi-tenant system is also ideal for managed host providers, making the task of managing customers cost effective, exploiting virtual environments.

The cost to the business of not monitoring can be substantial, but in order for the tools to achieve the benefits of monitoring the tools must be easy to use and configure to meet business requirements, such as reports and KPIs.

THE BENEFITS OF CA UNIFIED INFRASTRUCTURE MANAGEMENT (CA UIM)

CA UIM satisfies the above needs of IT operations, and has the following key features:

- Single console unified monitoring across diverse devices and applications.
- Multi-tenant architecture with subscription based licensing.
- On-premise solution or hosted by a CA Technologies partner.
- Designed for large enterprises and managed hosting service providers.
- Plug-and-play probes can be added for specific monitoring of applications and packages, or generic ones used for custom applications.
- Exceptional scaling: a single polling engine/server can monitor 50k end items (to be extended to 100k).
- Suitable for monitoring legacy, non-standard devices and applications.

Representative large enterprise and managed service provider case studies in this report outline how CA UIM has been implemented to ensure organizations are able to gain transparency into IT infrastructure and applications, and thereby reduce IT operations costs.

© Ovum. This White Paper is a licensed product and is not to be photocopied

INTRODUCTION

IT DOWNTIME DIRECTLY IMPACTS REVENUE

Businesses today rely on IT to a greater extent than ever before, for example with e-commerce the physical outlets of traditional retailers and many financial services have turned into Internet-based businesses. Monitoring the health of its IT infrastructure has therefore become a core activity for the business as a whole, impacting mission critical service delivery and revenue streams. Downtime is no longer just an inconvenience for back office staff, it equates to immediate loss of customers and revenue, and impacts reputation. Industries with the highest downtime costs include healthcare, financial services, and transportation.

The highest cost factors in downtime incidents are now due to business disruption and loss of revenue; a worst case scenario may see a business wiped out as a result of downtime impact. An unplanned downtime incident of a typical data center can cost as much as $0.5million. On this basis the cost to prevent outages and downtimes is less than the cost to monitor and prevent outages in the first place. Therefore investing in the health monitoring of IT applications, services, and infrastructure has a ROI within a year in use.

The key monitoring activities for ensuring the good health of IT infrastructure cover servers, applications, databases, storage, and networks. CA UIM spans all these elements, and specifically for applications the coverage is synthetic testing for application availability and response time measurement.

Modern monitoring solutions alert key stakeholders with messages to their preferred personal devices, and they ensure that any unusual events and behavior in the IT infrastructure are investigated before serious outcomes disrupt services. In addition, the capability to track all metrics in real-time reduces the risk of sampling signals and missing essential information. New generation monitoring solutions are designed to be easy and intuitive to use and help reduce the cost and complexity of keeping IT infrastructure functioning.

BUSINESSES NEED UNIFIED MONITORING

There is a diverse range of IT equipment, systems, and components that make up the modern data center, and this diversity only increases through merger and acquisition activity. Typically systems administrators end up with a collection of monitoring tools that cover different patches of the environment with little integration between them. In order to maximize the benefits of monitoring, a unified view that spans across the IT environment is recommended. This allows correlations of metrics and signals to be evaluated across the data center to detect complex issues that would otherwise not show up in purely localized monitoring equipment. Unified monitoring also simplifies the burden on system administrators who need to keep abreast of IT health issues and frees them to perform other work, making best use of automation. For MSPs, unified monitoring is taken a degree further, with monitoring of multiple customer sites on a single unified console. These different aspects are explored in the next section.

© Ovum. This White Paper is a licensed product and is not to be photocopied

PERSPECTIVES OF IT MONITORING USERS

THE MANAGED SERVICE PROVIDER

The multi-tenant architecture of CA UIM allows a MSP to display monitoring content for multiple customers within a single CA UIM installation. For example, in Figure 1 a MSP based in Dallas has 500+ customers, two of whom are shown, one based in London and another in Sydney. The MSP installs CA UIM in the primary data center and a client hub at each remote site, inside the customer's firewall. All data at the customer site is packed in a secure manner and relayed back to the primary system in the MSP HQ. The database stored in the primary site is multi-tenanted so the client only sees its users via the connection. The MSP can give its customers user logins to the solution and they will have no knowledge that the solution is also monitoring different customers. CA UIM provides the necessary technology to create SSL tunnels as part of the solution, there is no need for a third-party VPN solution, or domain controllers.

The MSP can add customers to the existing primary hub without needing to contact CA Technologies; CA UIM licensing is easy to manage via the cloud and based on the number of probes deployed. There is no concurrent user access restriction to the portal dashboard, instead it is wide open. This makes it easy for the customer to align monitoring costs and for CA Technologies to recovers those costs.

Case Study: Managed Service Provider

A European-based managed service provider offers four service pillars: ITSM, High Availability, Capacity Planning, and Unified Monitoring. This MSP is used in the public sector and the systems it monitors, for example the tax revenue collection operations, can impact many millions of people. The typical customer is a large organization, such as government ministry, telecom, or manufacturer.

The typical failures experienced include unrecoverable errors such as due to hardware failures from mechanical parts wear and tear. Another major factor impacting data centers in the EU region is due to new energy savings regulations. As a result, new power systems are being deployed which are poorly implemented causing power related failures.

This MSP is using CA UIM as the main monitoring solution and also the consolidating, unified view tool to which other tools connect. One benefit is that CA UIM supports many legacy and non-standard pieces of equipment, which reduces the maintenance costs, as only one monitoring solution is required, and supports the SLAs.

The ROI can run into millions as the prevention or early detection of a server going down in, say, the tax collecting operation, can impact revenue by millions of euros. Such customers are on a 5 nines availability agreement – this translates to 50 minutes unplanned downtime per year.

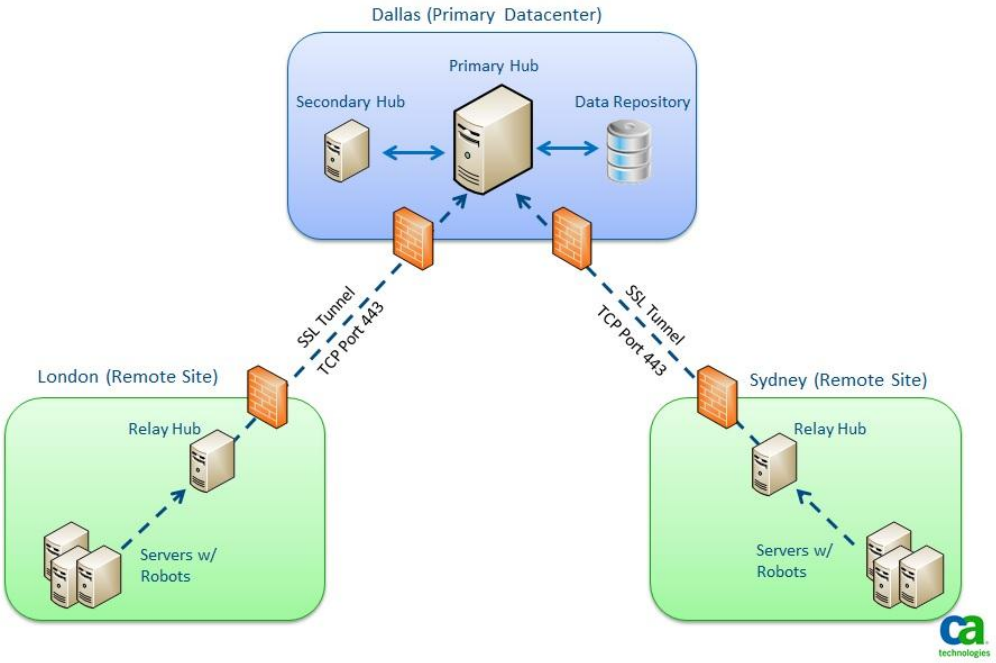
This MSP, prior to adopting CA UIM used a custom solution which had many associated costs of further development and maintenance, so moving to a commercial solution released resources and the burden of upgrading the solution. Furthermore, the move to a subscription model proved preferable to a traditional license.

The next step is to move from detection and response to prevention, and use the knowledge gathered in CA UIM to analyze and understand where and how issues are emerging and dealing with them before they

© Ovum. This White Paper is a licensed product and is not to be photocopied

escalate. There will also be business intelligence opportunities, using data mining tools on the knowledge database. In addition automating root cause analysis is a high priority, driven by customer demand.

Figure 1: CA UIM multi-site deployment



Source: CA Technologies

THE BUSINESS USER PERSPECTIVE

In an exercise to understand its customers, CA Technologies ran a TechValidate survey and found that 65% implemented CA UIM to unify disparate, point monitoring tools. In large enterprises different IT teams (network, operations, development, line of business etc.) will typically have different tools in their separate silos. With the introduction of CA UIM they are able to consolidate these tools and have one team to manage it. This leads to increased productivity with less time spent administering monitoring, only one data repository to manage, and also makes reporting easier as there is consolidation of data into one tool. Customers can expect staff productivity to improve by up to 25%, with staff able to spend more time on other work.

CA Technologies finds that IT operations people immediately understand the benefits of CA UIM. However, conversations with business units are increasing, reflecting the shift to mobile apps taking place and there is a need to ensure the back end servers are problem free. Availability, with downtime measured to a second, becomes an issue, as is performance, such as the time it takes for an app to start. In addition, in the managed services side of the customer base, where customers need to manage remote networks over the Internet, these are strategic business level decisions that CA Technologies is having with these customers, typically at VP level for large service providers to CEO at the tier three / medium size level. The flexible subscription based licensing that CA UIM offers is a key attraction to businesses.

Businesses have the flexibility of adding probes as and when needed and the configuration is seamless, so when adding a new application, say a Salesforce.com application, the CA UIM administrators download the appropriate probe and they are up and running, without needing to write new monitoring scripts. By

© Ovum. This White Paper is a licensed product and is not to be photocopied

integrating monitoring from all probes CA UIM is also able to provide complete views across applications to servers.

Today marketing and sales run e-commerce promotions and flash sales that put pressure on web servers and other back end infrastructure, with massive spikes within a 48 hour period, and the need to ensure smooth operations is a business level concern.

Finally, CA UIM's display of performance and monitoring data can be joined with KPIs from other sources, such as log files or databases. If the application is off-the-shelf there will be a probe for it, otherwise with custom or proprietary applications there is a generic probe with an API that can be used to hook-in information. Monitoring governance will typically be available for 80% of metrics out-of-the-box but there will be 20% which will be vertical specific or customer specific, giving the customer differentiation with its approach. This business-centric monitoring solution relates performance and monitoring back to the business context.

CA UIM has a core SLA management module that allows customers to combine metrics together for correlation purposes and provide rules for when SLAs are to be met. There is also integration with CA Service Operations Insight.

THE END USER PERSPECTIVE

CA UIM collects information from the IT environment via polling or by receiving content directly from devices, by system logs and traps. This information is converted into alerts, events, or fault warnings. Strong alerting mechanisms with de-duplication and correlations are provided that customers can take, drill into and expand the detail. With polled data CA UIM will create performance and availability information. CA UIM is an SLA, monitoring and performance management solution; many customers are misled into thinking CA UIM is just concerned with availability: CA UIM probes will perform performance and/or availability tests.

CA UIM end user response time monitoring tests apps just like a user would, so it is not just testing the servers, and provides proactive notifications and can detect outages. Monitoring information is presented through dashboards and reports as well. The product is multi-tenant so a service product or enterprise can roll out one CA UIM domain and provide role based access into the product to each team or individual to give them a slice of the monitoring world.

Case Study: Austria Technologie & Systemtechnik (AT&S)

AT&S is an electronics industry company first founded in 1987 with operational premises principally in Austria, China, and India. All its data center infrastructure monitoring is carried out centrally from the Austrian location. The infrastructure performance monitoring group comprises seven people and it started its activity some nine years ago with a solution from another major vendor. The key requirement at that time was for monitoring availability of processes and services, and of hard disk space on the servers. Requirements grew over the years for additional monitoring services, for KPIs, reporting, including on historical information, mining system logs, and most crucially for remote access monitoring. The existing tools were prohibitive in accessing this type of data. The switch to CA UIM had the benefit of making the analytics information readily available and by 2013 all AT&S systems were being monitored by CA UIM.

AT&S found additional benefits in making this switch, which could monitor applications and services more deeply than just provide availability information, as well as add monitoring of the storage application and devices. The reporting and historical data is now easily available out-of-the-box with a small amount of configuration. CA UIM also allows the remote monitoring, software delivery, and system management that is

© Ovum. This White Paper is a licensed product and is not to be photocopied

required by the team in Austria to monitor the offshore sites. AT&S also uses CA Client Automation for software delivery, and this is used to deliver the CA UIM agents to all servers in all locations. The monitoring configuration is then applied within the CA UIM console.

Today AT&S monitors over 250 servers and has transparency into historical data, server availability, services, file space data, and application availability. The switch to CA UIM was not a matter of cost – the company needed the right solution to deliver the desired functionality.

One of the challenges for AT&S is the diversity of server configurations, and notifying the right people responsible for maintaining the infrastructure at the remote locations. With CA UIM it is possible to manage these tasks through one configuration. So for example, if a disk is full in India a CA UIM agent picks up the event, sends it to Austria, it is processed and an email is sent out to the responsible engineer in India. Adding a new server is also easy with CA UIM, with minimal effort required.

For the future AT&S expects to need monitoring of mobile devices, but the key activity is ensuring high availability and deep monitoring as the company rolls out new products into the market.

A TECHNICAL PERSPECTIVE

CA UIM is used to monitor: power sources, networks (LAN, WAN, routers, switches, Internet Protocol devices etc.), servers (physical and virtual, with a range of OSs: Windows, Linux, AS400, Novell Netware), databases, commercial application monitoring (e.g. Microsoft Exchange and SharePoint), middleware monitoring (WebLogic etc.), and for custom applications there are generic capabilities to watch error log files, process management logs, and cloud infrastructure (private, public, with specific probes for Amazon, Microsoft Azure, Rackspace, and also SaaS such as Salesforce.com, Google Gmail). In addition there are probes for private cloud monitoring of Vblock technology.

CA UIM uses synthetic transactions with no byte code instrumentation so it is not used for performing deep dive diagnostics and would need to be complemented with say an application performance management tool for code level diagnostics. The sweet spot for CA UIM is server monitoring and in addition its strength in packaged applications is increasingly being realized. It can offer basic database monitoring, and its private cloud monitoring is a core strength.

Looking ahead, CA UIM will be enhancing its network performance monitoring capabilities. For example device certifications and monitor configurations, known as metric families, which are combinations of SNMP objects, and when combined together provide advanced metrics on performance. This will enhance the basic SNMP collection capabilities and some analysis, such as bandwidth usage, currently available in the product.

A key strength of CA UIM is its capability to scale to large network management operations. The current version 7.5 manages 50,000 elements from a single polling engine, and the next version 8.0 will extend to 100,000 elements per single CA UIM polling station.

CA UIM calls its monitoring plug-ins ‘probes’. The different probes run to over a hundred and split into 12 groups: adapter, application, database, gateway, infrastructure, installation, network, SDK, service, service level management (SLM), storage, and system. Some probes are built with partners, for example Agentil developed a robust SAP probe that snaps straight into CA UIM and monitors application specific metrics to help SAP perform at an optimal level. There are probes for monitoring power and cooling, CPU and memory, and these probes have granular monitoring technology to measure specific metrics and/or elements.

For example, in order to monitor a packaged application such as Oracle Financials, a number of probes in combination will be deployed, including a server side perspective, database perspectives, middleware

© Ovum. This White Paper is a licensed product and is not to be photocopied

perspectives, and then add synthetic transactions to exercise the application from the outside in. This probing performs end user response time monitoring but does not go further into APM, for which CA APM offers additional visibility if so required.

The middleware probes are mostly JMX based and /or API based and use polling and threshold verification methodology similar to SNMP polling, where various classes are queried within the middleware management systems and by return provide alarms or performance metrics to administrators. The probes will grab the key metrics customers want and display and threshold them. The analytics capabilities provide trending and base lining on data collected, as well as service level agreement calculations. Multiple metrics for any environment can be correlated for SLA compliance reasons, such as identifying a SLA breach against past performance. The dynamic thresholding looks at normal usage over time and raises alarms at abnormal conditions versus static thresholds. To support these calculations CA UIM has a performance management database, a massive data warehouse of metric time series history.

CA UIM also has network flow analysis capabilities. It uses a harvester collection engine (or server) on the backend and does analytics and displays results on the flow data.

CONCLUSIONS

IT operations today are looking to make their tool investments truly justify the expense, and so are expecting their monitoring solutions to be responsive and wide ranging in coverage as their organizations' demands increase. They need a solution that will realize the ROI, and also reduce costs by rationalizing the buildup of tools that accrue over time, whether through mergers and acquisitions, or previously autonomous departments or business units that are brought under a centralized control.

CA UIM is designed to bring under its wing a diverse, heterogeneous environment, through its unified, single monitoring console, and multiple plug-and-play probes that span legacy to the latest applications, packages, and infrastructure. It is designed to be highly scalable and is ideal for the very largest operations, whether an enterprise user or managed service provider. Its core architecture, exploiting multi-tenant virtualization allows ease of use at reduced operating costs. CA UIM also integrates with the CA Technologies family of IT services solutions, such as CA Service Operations Insight, for gaining a higher level of service management. Overall CA UIM offers a flexible and cost effective IT monitoring solution, with excellent ease of use and the benefits of unified monitoring.

© Ovum. This White Paper is a licensed product and is not to be photocopied

APPENDIX

FURTHER READING

CA Service Operations Insight, Ovum Technology Audit, Jan 2013, IT017-004076.

METHODOLOGY

This white paper is based on Ovum's extensive research experience and briefings with CA Technologies and its customers.

AUTHORS

Michael Azoff, Principal Analyst, Infrastructure Solutions Team

michael.azoff@ovum.com

OVUM CONSULTING

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

DISCLAIMER

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the publisher, Ovum (an Informa business).

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.

© Ovum. This White Paper is a licensed product and is not to be photocopied