WHITE PAPER | JANUARY 2015

CA Unified Infrastructure Management for Networks

Table of Contents

Solution Overview	3
Key Features	4
Specialized Probes	6
SNMP Poller and Trap Listener Probes	7
Specialized Gateways	8
Performance Trend Reporting	9
SLA Creation, Monitoring and Reporting	9
Advanced Network Analysis Features	9
Conclusion	10

Executive Summary

CA Unified Infrastructure Management (CA UIM, formerly CA Nimsoft Monitor) delivers availability, performance and service level management for heterogeneous IT networks. The solution automatically discovers network devices and interfaces and monitors device health and performance. CA UIM also provides bandwidth performance and analysis reporting for critical network circuits (WAN/LAN). CA UIM delivers network availability and performance information in rich graphical dashboards and reports. These dashboards and reports can be offered via a secure, multi-tenant Web portal, enabling both enterprises and service providers to efficiently deliver this information to internal or external audiences.

Solution Overview

In the application economy, organizations' fortunes will increasingly rest on the innovation and availability of applications. This means the networks that support critical business services have to be highly available and optimized. To meet these objectives, administrators need to have 360-degree visibility of their networks. With CA UIM, administrators can gain the complete visibility they need to track, manage and optimize their networks, so they consistently deliver the highest levels of business service quality.

CA UIM offers the following features:

- Enables automatic discovery and bulk network monitoring configuration
- Monitors availability and response times to all network devices
- Monitors interface bandwidth and error rates
- Monitors SNMP-enabled devices via polling and trap reception
- Monitors device Syslogs
- Offers powerful pre-packaged and customizable dashboards
- Delivers intelligent alarms and SLA reporting

In addition, CA UIM detects, isolates and accelerates resolution of the following issues:

- Broken network connectivity links
- Excessive network latency
- Network device degradation and failure
- Network interface degradation and failure
- Excessive bandwidth utilization

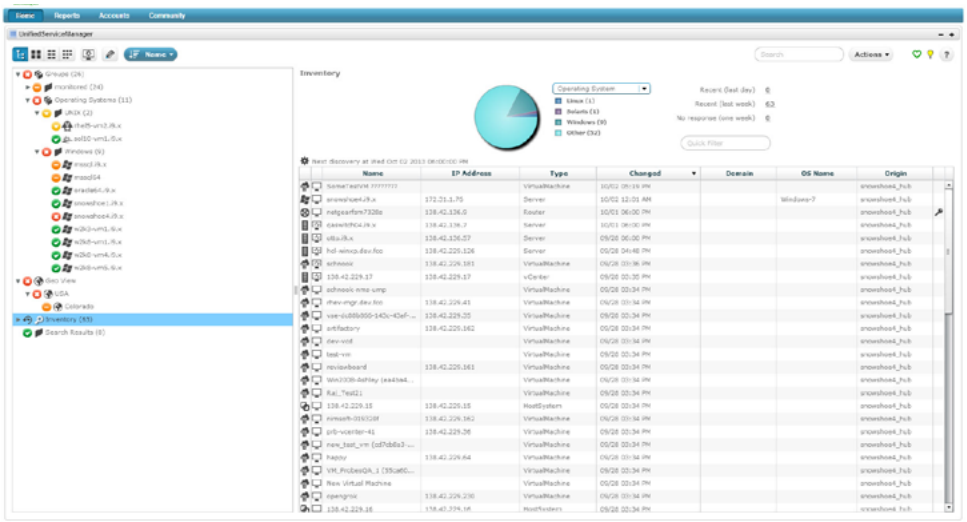
Key Features

Automatic discovery and bulk network monitoring configuration

CA UIM significantly reduces the time it takes to configure monitoring. By leveraging the solution's automatic discovery and monitoring templates, administrators can set up monitoring of thousands of network devices and interfaces—and do so in minutes rather than hours. The product's automated discovery wizard finds and lists all addressable network devices. Users can then apply filters to select devices and then either create new templates or edit existing ones to do bulk configuration of the monitoring of their network environments.

Figure A.

CA UIM automatically discovers and displays addressable devices.



Real-time dashboards and alarms

CA UIM enables you to create and customize user-specific network monitoring dashboards. Alarm dashboards can show up-to-the-minute status of critical network links, bandwidth utilization, network latency, response times and other important network metrics.

Figure B.

CA UIM delivers intuitive, real-time views of network status.

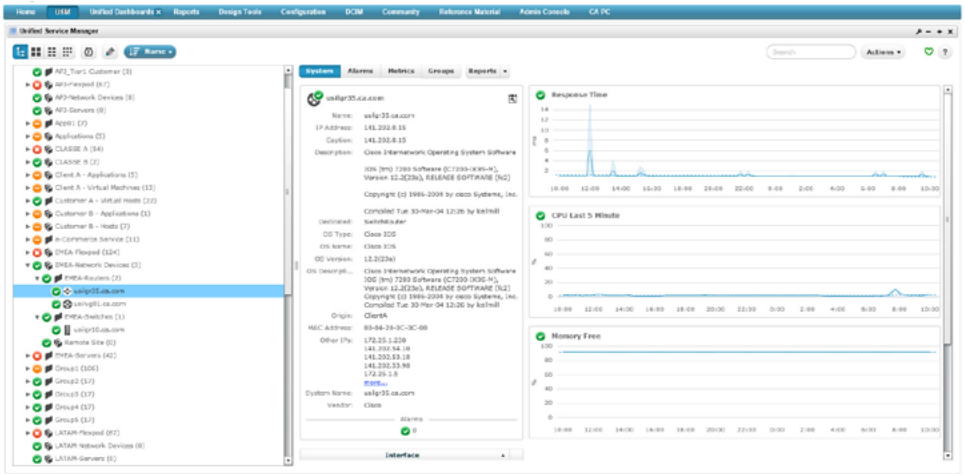
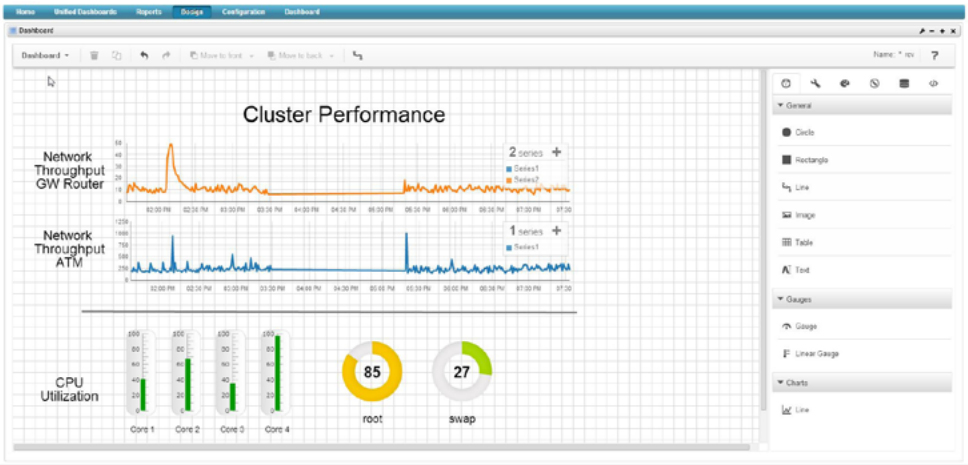


Figure C.

CA UIM custom dashboards enable users to gain anytime, anywhere access to monitoring data.



Custom HTML 5 dashboards

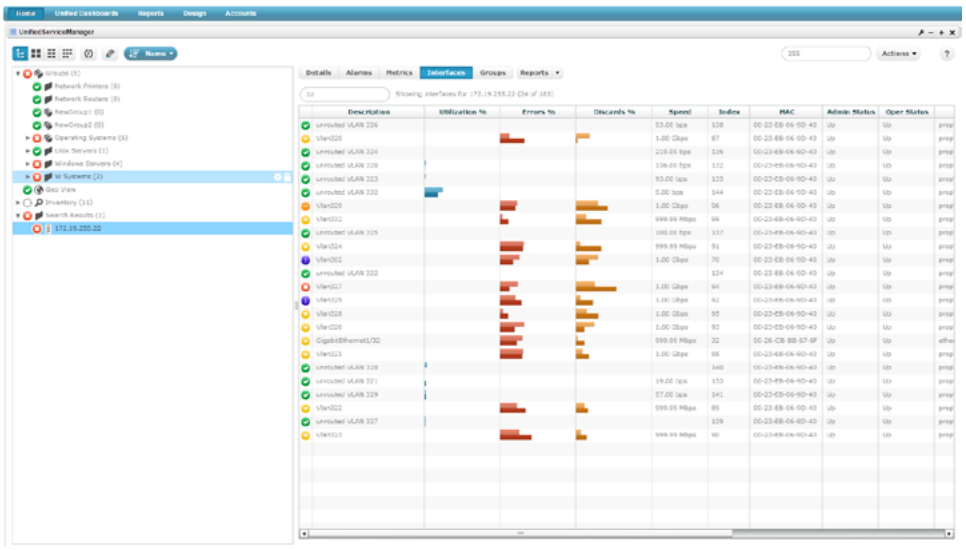
CA UIM provides streamlined, intuitive custom dashboards that you can access on PCs and mobile devices, so you can get real-time, convenient access to the monitoring data that matters to you.

Pre-packaged network interface views

CA UIM offers pre-packaged network interface views that can enhance your staff's visibility and productivity. Through these views, administrators can quickly determine the status of critical network components, and get the detailed information they need to find and fix performance issues.

Figure D.

CA UIM network interface views offer administrators detailed information for finding and fixing issues.



Analytics and dynamic thresholds

CA UIM allows you to set alarm thresholds for each of your key network performance indicators. If a given metric exceeds the established threshold, an alarm of user-defined severity is generated. You can also leverage dynamic thresholds to limit alarms to those that matter most, so you can improve staff productivity and minimize false alarms. In addition, you can use these advanced analytics features:

- **Time-to-threshold analytics**. Through this capability, the product identifies threats of potential performance degradation and issues an early warning—before internal and external customers are affected. Through these analytics, CA UIM can predict when an infrastructure element might experience difficulty. The product uses the data from the baseline period to construct a trend line that establishes expected performance over time and then spots behavior that represents a departure from this trend line.
- **Time-over-threshold analytics**. Through these analytics, CA UIM helps you identify real, persistent performance issues and eliminate false alarms associated with occasional spikes. The product compares the value of each key performance indicator (KPI) to a predefined threshold and reports if the value has been "too wrong for too long." Instead of generating a trap each time the threshold is crossed, the algorithm determines the aggregate duration of violations within a monitoring window to filter out spikes and determine real, persistent problems.

High scalability and multi-tenancy support

With CA UIM, you don't have to worry about outgrowing your monitoring solution. CA UIM can scale from supporting 100 to more than 100,000 devices, and it has been proven in some of the largest and most complex network environments. In addition, the product's multi-tenant architecture enables you to efficiently scale and personalize service offerings to any number of internal groups or external customers.

Specialized Probes

CA UIM is comprised of a set of specialized probes and gateways that provide automated and GUI-driven access to device status information. All solution probes have their own interface to facilitate administrative and operational activities.

Network connectivity probe

To ensure business continuity, CA UIM provides a robust network and application connectivity monitoring function. This ensures that end users and business consumers have access to business-critical network devices, services and applications.

Connectivity monitoring—broad device and services support

The solution includes connectivity monitoring for any IP-enabled device, including routers, switches, servers, printers and more. A specialized probe uses ICMP or "ping" tests (ICMP ECHO) to verify network connectivity between the host on which the probe resides and the targeted remote system. The probe will also test connectivity to TCP-based services, such as Telnet and HTTP, as well as any other application with a designated service port.

Connectivity response time measurement—network latency monitoring

Through the process of connectivity monitoring, the network connectivity probe will record response times to and from network devices, services and applications to aid in pinpointing areas of excessive network latency. Network connectivity status reports and round trip performance trend reports are available. Report data can be leveraged for SLA creation, monitoring and reporting.

Connectivity probe—flexible deployment

CA UIM offers extremely flexible deployment options to ensure connectivity testing is being performed between the applications and network devices that warrant close scrutiny. Unlike other market offerings, which only support centralized polling from a management server, the lightweight network connectivity probe can be deployed strategically throughout the business infrastructure. For example, in a distributed application environment, the network connectivity probe can be deployed directly on application servers and configured to test connectivity to the end users who need access to those business-critical servers. Conversely, it is possible to deploy the network connectivity probe directly on end-user workstations to monitor for connectivity to the applications' servers that the user community needs access to. Businesses with branch offices may consider deploying the network connectivity probe on edge devices to monitor link connectivity between the IT data center and remote offices.

Connectivity probe—flexible, reliable notification

CA UIM provides flexible and reliable alert notification and data transport options. In cases where the network link between the probe and CA UIM management console is disabled, the probe will buffer alert and performance data locally until a failed network connection has been resolved. In addition, the connectivity probe supports cellular communications for off-network alert notification and performance data transmission. This feature eliminates the need to rely upon a potentially broken network for data transport.

SNMP Poller and Trap Listener Probes

SNMP collector probe

SNMP is a standard protocol for managing devices on IP networks. SNMP consists of an application layer protocol, a database schema and a set of data objects. Typical devices that support SNMP are routers, switches, servers, workstations and printers. The SNMP data monitoring probe allows you to track the performance of these network devices. The probe supports more than 4,100 models from over 120 vendors. Within the product, users can get a direct link to a website that lists supported SNMP devices and their associated MIB object identifiers (OID), vendors, vendor certifications, metric families and metrics.

SNMP MIB poller and browser

CA UIM provides a specialized probe that can poll standard or proprietary MIB objects from SNMP-compliant devices. MIB objects can be monitored for threshold violations and alerts can be generated where necessary. Additionally the polled MIB data can be archived for trend reporting and also leveraged for SLA creation, monitoring and reporting. The probe offers a flexible interface for configuring unique MIB object poll requirements and also comes equipped with a MIB browser.

SNMP trap receiver

SNMP-enabled network devices, including routers, switches, servers and printers, can be configured to report a variety of error conditions in the form of SNMP "traps." Traps are automatically forwarded to a designated server—typically a network management server.

CA UIM comes equipped with a specialized SNMP trap receiver probe. By default, the product will listen to port 162, however the port number can be reconfigured. Any incoming SNMP traps will then be converted to events formatted for CA UIM. The formatted events will then be analyzed for alert generation or archived for trend reporting. The trap receiver probe offers an intuitive GUI to convert the SNMP traps to user-friendly alert messages. Out-of-the-box support is available for Compaq Insight Manager and Dell Open Manage traps.

SNMP trap sniffer

The SNMP trap receiver probe (described above) also provides a real-time trap "sniffer" function. The probe watches the network in promiscuous mode to see all SNMP traps on the network wire. The probe's graphic user interface displays all traps in an active scrolling list as they are detected. Pressing the start button in the probe's interface easily activates the sniffer function. A green diode indicates that sniffing is in progress. Individual traps that are sniffed can be selected and quickly added into the CA UIM event monitoring system. Each trap that is selected through the probe's graphic interface will have its own monitoring profile automatically defined. The monitoring profile dictates how SNMP traps should be processed when they arrive in the CA UIM system. SNMP event messages can be restructured and event counts, alert thresholds and alert severity can also be defined.

Specialized Gateways

Third-party network management system SNMP gateway

CA UIM provides an SNMP gateway that will transform CA UIM alarm messages to SNMP trap messages that are readable by any SNMP-based event manager. Predefined SNMP gateway solutions are available for HP OpenView Network Node Manager, CA Unicenter-TNG and BMC Patrol Enterprise Manager (PEM).

Syslog gateway

Device Syslogs are a critical source of network status information. This is especially true for non-SNMP enabled devices. The CA UIM Syslog gateway acts as a gateway to the Syslog "world." Most network devices, such as routers, switches, firewalls and UNIX servers, report events using SNMP as well as using the well known Syslog format. The Syslog gateway will listen to port 514/udp when running in a receive mode. All incoming Syslog messages will be acted upon using the defined receive mode:

- Generate CA UIM alarms
- Generate SYSLOG-IN (for post-processing) messages
- Log to file

The Syslog gateway also includes a graphical Syslog viewer to view messages as they occur.

Performance Trend Reporting

CA UIM offers a robust performance reporting solution that will allow administrators to track and spot trends in network availability and performance. The solution can track a range of parameters from a service level perspective, including network interface utilization, error rates, connectivity failures, latency and any other technical items. All network availability and performance data collected by CA UIM probes can be utilized for quality of service and performance report generation.

SLA Creation, Monitoring and Reporting

CA UIM offers a robust SLA creation, monitoring and reporting solution. Quality of service and performance data collected by the CA UIM probes can be leveraged to calculate and report on service level compliance and breaches. All SLA and performance reports are viewable in HTML format via Web browser.

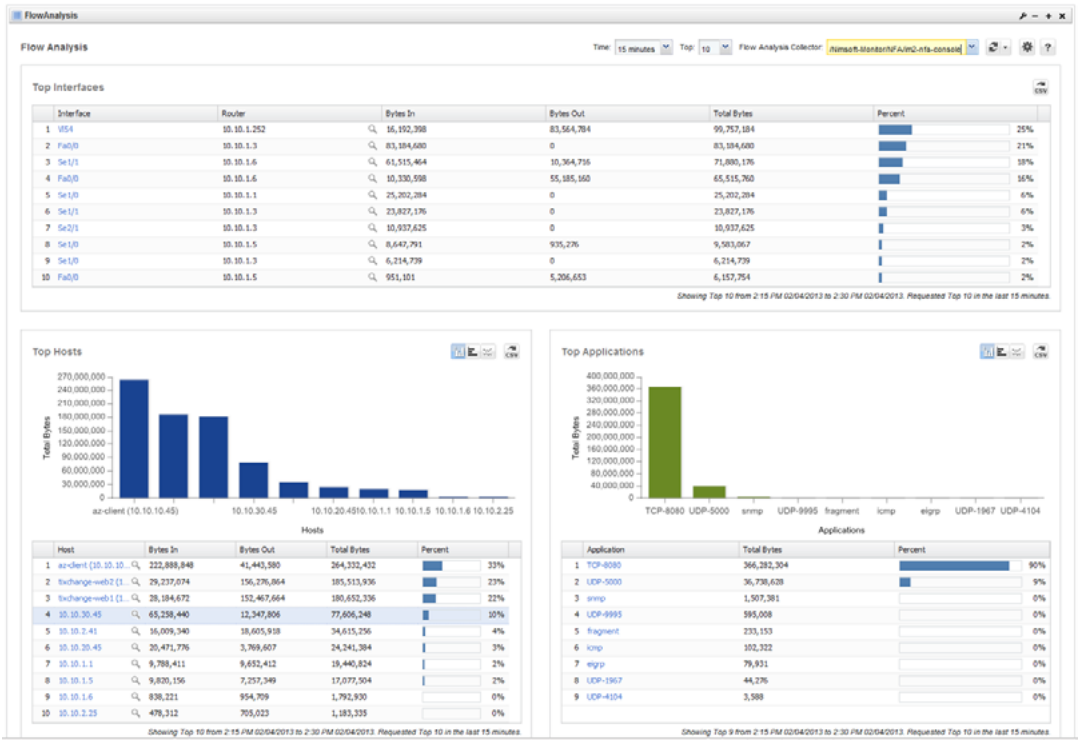
Advanced Network Analysis Features

Network traffic flow

CA UIM helps you leverage IP traffic information in your organization, so you can better understand usage patterns, manage workloads and resources and improve service levels. The product makes it easy to visualize where the main network traffic flows are, assess performance data from different angles and drill down to get the specific data you need to make the most informed decisions.

Figure E.

CA UIM delivers powerful insights into network traffic flows.



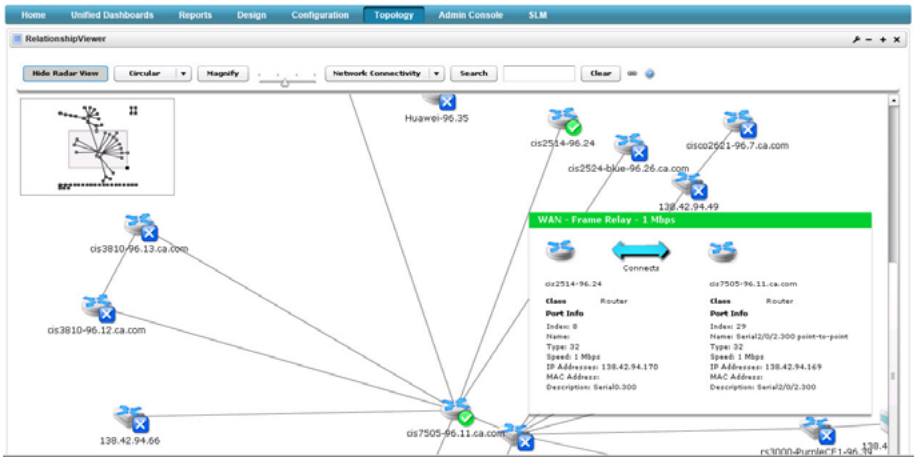


Figure F.

CA UIM features at-a-glance views of network topologies.

Root-cause analysis and topology

CA UIM offers a visual topology and relationship viewer that enables you to select from different layout formats, including orthogonal, hierarchal, circuit, circular, natural and organic. To support the administration of large-scale networks, CA UIM offers an automatic micromap that enables you to view the entire network topology. You can traverse the micromap and zoom in on different network segments as required. Plus, you can mouse over individual IP devices and see specific details of that device. The topology view is automatically overlaid with availability and status data of all monitored IP devices. Connection properties are displayed when you click on a line or connection between two devices. The connection properties show the connection status (SNMP operational and administrative status) and connection speed as well as each device and each interface on either end of the connection.

Conclusion

In the application economy, ensuring network availability becomes an increasingly high-stakes endeavor. CA UIM monitors network connectivity to devices and application services, measuring accessibility and network latency. With CA UIM, administrators can gain the comprehensive and detailed insights they need to effectively track, manage and optimize network performance.

For more information, visit **ca.com/network-monitoring**.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

CS200-113657_0115