DATA SHEET

CA Unified Infrastructure Management for Windows Servers

At a Glance

CA Unified Infrastructure Management (CA UIM, formerly CA Nimsoft Monitor) for Windows servers provides a comprehensive solution that monitors, collects and analyzes performance of core Windows server components to ensure that your business critical servers are performing optimally all the time. The solution monitors core server resources (CPU, memory, disk, event logs and more) and enables management of remote processes and services (automated and manual start/restart/stop). Server status and performance information is presented in real-time alarm dashboards, performance trend reports and/or SLA compliance reports.

Key Benefits/Results

- Short time to value
- Increase the productivity of your IT resources
- Adaptable to monitor any Windows environment
- Helps consolidate system resources and distribute load evenly
- Increase end-user productivity and response

Key Features

- Customizable thresholds
- Simple drag-and-drop configuration
- Highly customizable performance, trend and service level reports
- Combine several data sources in a single graph
- Over 960 performance monitor counters
- Automated and manual corrective action (start/restart/stop services)
- Real-time service and technology dashboards

Business Challenges

Whether your organization is a small business or a large enterprise, managing a Microsoft Windows based environment is a daunting task. Undoubtedly, your end users require peak performance and high availability of your Windows infrastructure—any day, any time.

Solution Overview

CA UIM for Windows servers provides a comprehensive solution for improving the end-user experience. From monitoring the application response time at the desktop to monitoring the performance and availability of the entire IT infrastructure, CA UIM can give you a complete, 360 degree view of business critical services. All CA UIM information is correlated to business service dashboards and measured against pre-defi ned service level agreements (SLAs) to warn you against SLA threatening conditions.

Critical differentiators

CA UIM uses a Message Bus Architecture as a core element that is streamlined, comprehensive and efficient. It enables all monitoring components to communicate with each other, without direct program-to-program connections and acts as an abstraction layer between the core system and the monitoring probes. This leads to significant improvements in reliability, scalability and development agility.

CA Unified Infrastructure Management includes the following probes:

CPU, disk and memory: The CDM probe provides advanced monitoring of CPU, disk and memory attributes including:

- Computer uptime (hourly)
- CPU percent broken down by user/system/wait idle
- Single and multi-CPUs supported, including threshold alerts when the difference between CPUs breaches a threshold
- Disk usage in total (MB), free (MB), used percent.
- Threshold alerts can be set for free space in MB or percent and multiple disks are supported
- Memory usage and memory paging
- Processor queue length

Processes: This probe monitors processes and windows to detect error situations such as process state, memory usage, CPU usage, number of instances and threads.

Logmon: The log file monitoring probe will scan Windows and ASCII based log files and automatically look for essential information in system and application log files.

Reboot: This probe checks its confi guration to determine if a reboot is needed and performs the reboot automatically.

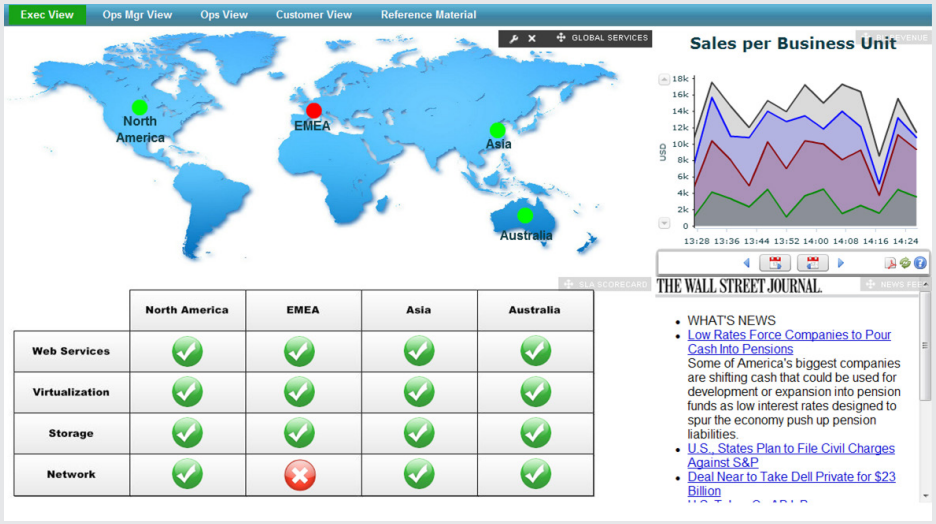
Services: The services probe allows for remote management of services, and monitors the expected running state (i.e. running, stopped) and can automatically take action (i.e. start, stop, restart).

Perfmon: The perfmon probe monitors performance counters on Windows servers. Alarms can be sent on unexpected values, and quality of service messages can be assessed and saved for historical performance reporting and SLA reports.

Windows event log: The Windows event log probe generates alerts based on messages from the Windows event logs.

Printers: The printer monitoring probe monitors printers defi ned on the computer. Remote printers are included when a user name/password is supplied.

Sample "Executive View" containing monitoring content, a 3rd party news widget and custom business data.



Active Directory: The Active Directory probe extracts values of the directory services, DNS server and file replication service event logs.

File and directory monitoring: The file and directory probe monitors files in specific directories. Alarms can be sent on number of files, age of files and space used by files. Related Products/Solutions

Supported Environments

In addition to CA UIM for Windows servers, modules exist for other server platforms such as UNIX, Linux, IBM Power Systems (formerly AS/400 and iSeries) and Novell Open Enterprise Server (formerly NetWare). These are complemented by database monitoring modules for all common databases, application modules for Exchange, Lotus Notes and other widely deployed applications; and solutions for managing your network infrastructure, including routers, switches, firewalls and more.

CA UIM is a rapidly deployed solution that requires minimal customization and administration.

For more information, please visit **ca.com/uim**

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**.