Gaining a Holistic View of the Citrix End-User Computing Environment—and Beyond

Optimizing Service Levels with CA Unified Infrastructure Management

Allan Andersen
Principal Enterprise Solutions Architect
In the battle to optimize service levels in their Citrix end-user environments, too many administrators are being forced to rely on guesswork, trial and error, and finger pointing. The challenge is that Citrix environments, with their complex interdependencies, pose a number of monitoring challenges. Further, these environments don’t operate in a vacuum: They rely on a broad IT ecosystem that has to be functioning optimally if end users are to experience the performance and availability required. To effectively manage service levels in these environments, IT organizations need a solution that offers collaborative, multi-faceted capabilities—and that’s exactly what customers get from CA Unified Infrastructure Management.
Executive Summary

Challenge

All too often in Citrix environments, as soon as an end user experiences a performance issue, it is the Citrix administrator that is guilty until proven otherwise. Exacerbating matters is that these administrators rely on isolated, domain-specific point solutions to monitor Citrix performance. Operating in a reactive mode, they look to verify that they’re not responsible—and then start the process of working with other teams to find out where the issue actually is. Meanwhile, the duration of outages and issues continues to mount.

Opportunity

With CA Unified Infrastructure Management (CA UIM, formerly CA Nimsoft Monitor), IT teams can more efficiently and effectively optimize service levels in Citrix environments. CA UIM equips administrators with a unified monitoring view of Citrix environments and the rest of the organization’s infrastructure and applications. As a result, organizations can rely on monitoring experts that can leverage a true end-to-end view of service levels. Featuring such sophisticated capabilities as correlation and dynamic alert management, the solution can assist with troubleshooting and root-cause analysis. Finally, CA UIM equips administrators with broad insight into the performance of the Citrix environment over time, so they can more effectively manage planning and impact assessments.

Benefits

CA UIM offers sophisticated capabilities that enable IT teams to monitor and manage their Citrix environments within the context of the entire IT ecosystem. Instead of relying on Citrix application managers to also handle monitoring, IT teams can enable their monitoring experts to focus on tracking the performance and availability of the Citrix environment along with the rest of the organization’s infrastructure and applications. As a result, IT teams can get past the guesswork and finger pointing that come from relying on disparate, disjointed tools—and start more quickly, efficiently and effectively managing service levels. With these capabilities, organizations can reduce monitoring cost and effort. At the same time, they can speed issue detection and resolution, so end users enjoy higher performance and better reliability.
Why is Citrix Monitoring So Difficult?

Through its application and desktop virtualization solutions, Citrix centralizes and streamlines the delivery and management of end-user computing services. By leveraging Citrix XenApp and Citrix XenDesktop, customers can realize a range of significant benefits, including increased flexibility and reduced cost and risk. Further, through their support for mobile application delivery and outsourcing scenarios, these solutions even enable organizations to pursue new business models.

However, in spite of all these benefits, these solutions can also pose significant challenges for IT organizations. Most critically, while the centralization of desktop and application management enables a range of benefits, it can also introduce a single point of failure. Further, any time performance issues arise, it has a direct impact on end users, potentially a large number of users. As a result, tracking and optimizing performance and availability of these services is critical. For IT staff, monitoring performance and troubleshooting issues in these environments presents several key challenges.

Dissecting the interdependencies in a Citrix environment

When users can’t login to Citrix or are having issues once they’ve logged in, they usually open a ticket related to Citrix. While the issue may have to do with Citrix, it may not. To deliver the overall service, a lot of interdependent components need to function optimally, any of which can present bottlenecks that affect performance and up time. In this regard, it is critical to underscore that Citrix service levels rely on more than Citrix software.

Generally, we can dissect the areas that have to be monitored into three categories: Business applications, Citrix components and infrastructure components. Following is some additional information on each area:

Business applications

At any given time, employees aren’t using a Citrix application per se, they’re using email, office applications and a broad array of other business applications. These applications, and their associated systems, need to be functioning optimally. Being able to track the performance and availability of these applications separately from the Citrix delivery infrastructure is usually the first step in troubleshooting potential problems.
Citrix components
A Citrix environment is typically comprised of the following elements:

• Citrix XenApp servers, which are comprised of such elements as Zone Data Collectors (ZDCs) and worker groups.
• Citrix XenDesktop Controllers (DDCs)
• Citrix Provisioning Services (PVS)
• Web Interface or StoreFront
• Profile and licensing servers

In addition, NetScaler and CloudBridge are often used for connecting users to the Citrix service. For each of these components, there are many important metrics that can be monitored. For Citrix XenApp, this would include processor queue length, application resolution time, XML queues and Windows and Citrix services and processes.

Infrastructure components
Citrix service levels are reliant upon an array of infrastructure components:

• **Network.** The network is the life-blood of any Citrix deployment. The network is responsible for delivering services to end users. Further, the network connects many disparate components. Fundamentally, network performance and reliability is critical; if connectivity issues arise between users and the data center, the user experience will be adversely affected—no matter how the rest of the environment is performing. Even relatively minor performance bottlenecks that arise in the network can have significant implications for end users and operations.

• **Storage.** The storage infrastructure is critical for Citrix XenDesktop deployments. To ensure optimal configurations, it is vital to understand read/write patterns, both during boot-storms and normal operations. These metrics are also important when evaluating the use of RAM-caches, SSDs and other technologies in an effort to reduce cost versus optimizing performance.

• **Hypervisors.** The performance of the underlying hypervisor that is used for hosting virtual desktops is a critical factor for XenDesktop. In addition, the hypervisor is increasingly critical for XenApp as well, given that it has become common to deploy XenApp worker groups in virtualized environments via PVS.

• **Servers.** Microsoft Active Directory, Microsoft SQL Server and Web servers (including those hosting Web Interface or Storefront), can all be a single point of failure, so monitoring their availability is vital.

• **Converged infrastructure platforms.** Cisco UCS, VCE Vblock and NetApp FlexPod have emerged as optimal platforms for hosting Citrix application and desktop virtualization. Consequently, the internal functioning of these platforms, such as fabric interconnects, have to be monitored.

“The network is the life-blood of any Citrix deployment. The network is responsible for delivering services to end users. Further, the network connects many disparate components.”
The need for unified monitoring

Each of the element types outlined above has unique monitoring requirements according to the specific role they play in supporting end-user services. Sometimes Citrix users may be affected by poor performance of a Citrix worker group. In other cases, user experience may be compromised by an application issue. To quickly triage issues, it is vital that IT organizations gain monitoring coverage that fosters collaborative information sharing and unified visibility among different IT teams. In addition, it is important to establish pre-defined troubleshooting workflows, which can help improve the efficiency and efficacy of individual team members.

End-user experience monitoring

In the end, what matters most in Citrix environments is the quality of service end users are actually experiencing. User experience can be divided into two key aspects:

• **The login experience.** Login experience can be affected by many different components. Most are related to performance of the Citrix components and connectivity between the components. Potential issues can range from lagging responsiveness that irritates users to unresponsive servers that completely disable login functionality.

• **Session experience.** Once the user is logged into the session, there are many potential sources of issues that users can encounter. The main contributor to a poor user experience is often session latency between the end user and the system and the application. In the case of XenDesktop, the overall performance of the virtual desktop can also cause degradation of the experience. Compounding matters is the fact that the so-called “last mile” to the end user is delivered via an optimized remote protocol, either using the Independent Computing Architecture (ICA) protocol or HDX, which runs on ICA. ICA and HDX obfuscate the network traffic, which makes it extremely difficult to analyze what the actual performance is for the end user. However, it is vital to monitor and track the key metrics that can affect the user’s session experience, and to do so with minimal impact to the actual sessions.

“Measurement is the first step that leads to control and eventually to improvement. If you can’t measure something, you can’t understand it. If you can’t understand it, you can’t control it. If you can’t control it, you can’t improve it.”

—H. James Harrington

1. CIO, September 1999, page 19
Leveraging a Unified Monitoring Solution

CA Unified Infrastructure Management (CA UIM) is a full featured, truly unified monitoring solution that enables IT teams to work collaboratively, more effectively minimize outages and maximize service levels—not only in Citrix environments, but across the IT landscape. With CA UIM, organizations can leverage visibility into all their Citrix components, and they can effectively track all the critical infrastructure elements that can affect the end-user experience—including the network, servers, converged infrastructure platforms and more.

Get actionable monitoring insights—not noise

Gaining extensive monitoring coverage and capturing massive volumes of monitoring data won’t be a benefit if it ultimately just generates noise, and ultimately leads administrators to miss the alerts that really matter. CA UIM offers a unique distributed message-bus architecture that enables administrators to do efficient monitoring and collection of data. This architecture offers maximum efficiency, which can significantly improve performance and scalability, especially in large-scale XenApp and XenDesktop environments.

Further, CA UIM gives administrators the flexibility to tailor their monitoring approaches to their specific environments. For example, on a metric-by-metric basis, administrators can select which data to publish automatically to the central monitoring system and those on which alerts should solely be issued when thresholds are exceeded. In addition, there are also several configuration options that enable administrators to minimize the performance impact on monitored systems by de-selecting groups of metrics that may not be needed for their environment.

Figure A.

CA UIM offers customizable dashboards that provide administrators with a quick overview of the overall health of a Citrix XenApp environment.
Leverage automation to align with best practices from Citrix

Citrix provides best-practice guidelines for monitoring XenApp and XenDesktop environments. For example, the Citrix Operation Guide for Monitoring provides specific guidance into thresholds to set for specific metrics, steps for troubleshooting and more. With CA UIM, IT teams can tailor configurations to these guidelines and even automate responses. For example, if a critical issue arises, CA UIM can automatically spot that a threshold has been breached, take a snapshot of processes and services that are running, and attach those pertinent details to the alert. This helps system administrators quickly identify if any processes or services are consuming too much of a system's resources.

Gain detailed monitoring of Citrix servers

CA UIM offers comprehensive monitoring coverage of servers within Citrix environments, including XenApp, XenDesktop, PVS, Web servers and more. The solution can track CPU, disk and memory performance for all relevant servers. This monitoring coverage is essential for understanding your environment baselines and thresholds and also for gaining insights into resource planning. CA UIM can monitor all critical Citrix and Windows processes and services and automate the restarting or stopping of these processes as needed. Further, the solution can monitor server logs and events for pertinent information.

Track Citrix activities

CA UIM offers comprehensive monitoring coverage of activities within Citrix environments. The solution offers the option to monitor logs and events from Windows event logs, which include Citrix-specific log entries, including errors and warnings. Several Citrix components, including PVS, Machine Creation Services (MCS), Web-interface and XenApp, have additional documentation around errors and events that can be easily captured. However, administrators need to be judicious about capturing these types of events so alarm systems don’t get inundated.

CA UIM can also provide in-depth visibility into Citrix session activities, which offers critical context for assessing and correlating many other metrics. Administrators can simply choose to track active and connected XenApp sessions per server or per server farm over time, or they can monitor more sophisticated queues and registration events. The solution enables administrators to distinguish between active sessions versus connected sessions, which is key to capacity planning and optimizing configurations in the Citrix system.

With CA UIM, you can also monitor individual session performance. In Citrix XenApp environments, this primarily focuses on latency experienced by the end user. In Citrix XenDesktop environments, this often pertains to the tracking of individual CPU and memory performance metrics. This information can be used to see if individual users, locations or specific servers are having latency-related issues, which is a key indicator of a poor end-user experience. Depending on your organization’s specific needs, you can use CA UIM to capture hundreds of additional metrics regarding performance or activities in your Citrix environment.
Leverage flexible network monitoring

As mentioned previously, the network represents a critical aspect to the end user experience, supporting both inter-component communications and communications between the end user and the Citrix service. CA UIM offers the robust network monitoring coverage your administrators need to understand and manage how the network is performing.

In addition to offering basic SNMP monitoring, CA UIM helps administrators track and baseline response time between key components, such as between Active Directory and the Citrix infrastructure. This visibility is vital in setting appropriate thresholds, which is a fundamental aspect to effective network monitoring.

To get additional insight into your network, you can also use CA UIM to incorporate NetFlow monitoring and analysis into your Citrix environment. This enables you to perform deep analysis of the traffic coming into the Citrix environment, so for example you can distinguish between someone working with the business’ SaaS application and someone streaming music to their virtual desktop.

Automate testing of application response time

One of the simplest yet most powerful features of CA UIM is its ability to do synthetic response-time monitoring. With this capability, you can automatically replicate an end user logging in to various applications and desktops from multiple locations. This gives you an easy, ongoing way to ensure the applications and desktops running in your Citrix environments are functioning as needed—or that you find out immediately if not. For example, CA UIM enables you to get early visibility if a XenApp server has been unresponsive for any reason. This application response time monitoring also enables your team to establish effective baselines in terms of what typical latency is expected from specific locations, and to ensure alerts get generated if any abnormal conditions arise.

Figure B.
Synthetic response-time testing for Citrix XenApp and Citrix XenDesktop enables administrators to get early notification of any degradation in the end-user experience.
Best Practices for Optimizing Your CA UIM Implementation

The following sections feature some high-level guidelines for maximizing the advantages of the advanced functionality that CA UIM delivers.

Actively tracking performance versus alerting

For many performance counters or metrics, it is not very valuable to collect historical metrics but rather to establish alerting so that administrators find out if specific thresholds have been exceeded or specific events have been occurring for a specified duration. Following are a few examples:

- **Disk monitoring.** Monitoring disk performance is both simple and important, so you might want to actively monitor, alert and collect disk-queue-length metrics. On the other hand, since disk space is usually not changing that fast, disk space metrics should be monitored and alerts should be generated when thresholds are broken, but the system should not actively collect the metrics and publish them to the central system for reporting and trending.

- **Memory and CPU monitoring.** When monitoring memory and CPU, administrators will often establish thresholds in which 80% utilization represents a warning level, while 90% represents a critical level. However, traffic spikes can quickly flood your event management system. This is a case where organizations can leverage the time-over-threshold analytics capabilities of CA UIM. These analytics capabilities help automate the process of distinguishing between intermittent spikes that don’t affect service levels and real, significant performance issues. While you can still collect the memory and CPU information for trending and capacity planning, you can do so in a more streamlined way that can significantly reduce the volume of metrics collected.

- **Change initiatives.** During significant change initiatives, such as major hardware or software upgrades, more extensive metrics should be collected. Having additional metrics can help you better evaluate before-and-after pictures and validate assumptions. When you have answered your questions and validated your assumptions, you can switch back to regular operational monitoring. CA UIM offers configuration templates that make it easy to do this swapping of monitoring configurations.

Choosing between remote and agent-based monitoring

CA UIM is an “agent optional” solution when it comes to server and application monitoring, which means it can monitor many environments remotely as well as through the installation of agents on the system being monitored. The optimal approach will vary depending on the Citrix components being monitored:

- **XenApp.** If you have less than 20-25 XenApp servers in each farm, and CA UIM is primarily monitoring for sessions and basic XenApp performance, you can use remote collection of metrics. However, if you want to monitor log files, you have more than 25 servers in the farm or you wish to have metrics generated at less than five-minute intervals, you should install locally.

- **XenDesktop.** In these environments, there’s no significant difference between remote and local collection. However, if you want to capture logs you should employ local monitoring.
• **PVS servers.** For PVS, you should use remote monitoring, unless you want to monitor logs.

• **Web servers.** It is advisable to do remote monitoring of Web Interface and StoreFront, unless you want to monitor logs.

• **Virtualization.** In virtualized environments, remote monitoring should be employed.

**Determining how extensively to monitor individual session activity**

There is a fine balance between the need to do deep monitoring and the need to manage the performance of the monitored environment and the monitoring system itself. For instance, there are a lot of metrics that can be collected around individual sessions. If you have 10,000 active sessions and want to collect 10 metrics for each session every five minutes, that would generate 1.2 million data points per hour or about 200 million data points per week—that is a big haystack and there will be a lot of needles. On the other hand, you could monitor locally and generate alerts without collecting the metrics, but you would have to design your alert management system to avoid a lot of noise.

However, deep session monitoring can be useful as a forensic tool for analyzing persistent issues with applications, locations or even individual users, but not for operational monitoring. Your monitoring strategy should focus on eliminating or reducing issues that have a large impact, for example, affecting 100s or 1,000s of users, and on addressing repeatable problems that can automatically be remediated and resolved via pre-defined workflows.

“**When the Citrix environment goes beyond supporting niche applications and use cases and becomes a standard corporate deployment method, it is imperative to formalize and refine the processes and roles surrounding troubleshooting and root-cause analysis.”**

**Organizational Recommendations**

When the Citrix environment goes beyond supporting niche applications and use cases and becomes a standard corporate deployment method, it is imperative to formalize and refine the processes and roles surrounding troubleshooting and root-cause analysis. This is fundamentally a matter of aligning responsibilities with domain expertise and establishing effective communications between teams.
Aligning roles with domain expertise

The help desk team should always handle the initial end-user incident request. These staff members may use such tools as Citrix Desktop Director to determine if the issue is localized to the end user’s configuration or environment, and whether simple pre-defined actions can fix the problem. The Citrix team—the staff with Citrix domain expertise—should work closely with the help desk team to define the top five to ten simple remediation actions that can usually be done in an automated fashion or by checking key settings and thresholds.

The monitoring team should be responsible for doing initial triage of problems and managing troubleshooting workflows. They have all the processes and tools to quickly determine if an issue is related to infrastructure components (such as network connectivity), Citrix components, the application environment or mobile end-point connectivity. Again, the Citrix team should work closely in transferring some of their domain expertise around monitoring to the central monitoring team, so that appropriate triage can be done quickly and efficiently. Together, the teams should establish effective pre-defined workflows that will determine whether, based on the insights gathered, the issue should be directed to the Infrastructure monitoring team, the Citrix team, the application team or another group.

The Citrix team members need to remain the domain experts in Citrix, given the many intricacies that affect service levels in Citrix end-user computing environments, such as PVS streaming, logon experience, HDX configuration, image management and so on. However, with CA UIM, Citrix administrators can get the same insight as other teams, so they can do the root-cause analysis in context of the other domains. Having this unified visibility is critical because many problems that arise in Citrix environments do not have a single root cause, but are rather due to a combination of technologies and events. Having unified, correlated intelligence is therefore critical to establishing what factors are causing the issue and how to address it.

Service levels should be tracked and the Citrix team should own the process for improving the overall service. While it may delegate key aspects of the service to the central infrastructure monitoring and help desk teams, the Citrix team still retains the ultimate responsibility for the Citrix service.

The Citrix team should own the overall lifecycle and retain operational responsibility for delivering a superior end-user experience at a reasonable cost. Moving operational monitoring responsibilities to the infrastructure monitoring team will not only add more domain expertise around the monitoring discipline, but also free up the Citrix team to focus on delivering new services for the business.

Communication and process flow

Communication and established process flows between teams are critical. Here are some questions to consider in evaluating these areas:

- Are the different teams meeting on a regular basis?
- Is the change management process integrated so that the help desk, infrastructure and application teams are aware when new software is being deployed or when infrastructure upgrades are being done?
- Are the hand-offs and roles clearly defined among the different teams?
Further, there needs to be a common platform for analyzing and sharing monitoring information. Without all these aspects, teams work in isolation, simply focusing on whether their domain is the source of an issue.

The CA Technologies Advantage

With CA UIM, your organization can leverage a unified, comprehensive and easy-to-use monitoring solution that provides critical insights and significant value to the entire IT organization. CA UIM enables administrators to gain the insights required to improve service levels of Citrix, and virtually all the organization’s vital business services.

Instead of having to procure, deploy and support many point monitoring tools, your organization can leverage a single, unified platform that provides all the monitoring coverage required. The solution offers the insights and automation that enable faster triage, troubleshooting and remediation. As a result, the solution enables your organization to enhance service levels and optimize the end-user experience.

Using a unique message-bus architecture, CA UIM offers many advantages, including extensibility, scalability, flexibility and simplicity. CA UIM delivers a number of advantages to Citrix environments:

- CA UIM comes with sophisticated monitoring capabilities, such as advanced event and alert management, root-cause analysis, performance baselining and analytics, which are critical for reducing noise and enabling administrators to quickly identify the core issues effecting the end-user experience.

- CA UIM offers the multi-tenancy support and sophisticated service level management that address key requirements of a range of large enterprise IT teams and service providers.

- By enabling you to incorporate Citrix monitoring into the larger infrastructure monitoring landscape, CA UIM helps reduce the chaos, fire drills and lost time spent chasing answers among disparate monitoring silos and teams.

CA also provides additional solutions for doing deep application transaction analysis and network performance management. This includes capabilities for analyzing the performance and availability of backend applications and services that are being accessed via the Citrix delivery infrastructure. These capabilities are critical for analyzing the end-user experience. Combining these solutions allows for even faster triage when users encounter issues.
Conclusion

A Citrix end-user computing environment is like a living organism. It is dynamic, sometimes unpredictable and it needs a lot of constant care and attention. With so many interdependent elements, Citrix environments can be challenging to manage, but given the direct impact these services have on end users, effective monitoring and management of these environments is critical. With CA UIM, organizations can establish unified monitoring views of all the elements that affect the performance of Citrix services. As a result, CA UIM enables IT organizations to work more efficiently, collaborate more effectively and ultimately gain the insights they need to ensure users enjoy consistently optimized service levels.

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.