Citrix Troubleshooting Guide: How to Stop the Blame Game

Abstract

When applications and desktops are delivered over Citrix, the Citrix administration team becomes the front-line for responding to complaints about slow performance. But more than 60 percent of the time, the root cause of the problem lies outside of the Citrix environment. This white paper explains how wire data analytics can enable Citrix administrators to not only see end-user experience for ICA sessions, but also dig into application and infrastructure performance to uncover the real reason for slowdowns.
Rescue Your Day From Troubleshooting Purgatory

Citrix administrators have a problem: getting blamed. If you’ve been supporting a Citrix XenApp or XenDesktop deployment for any amount of time, you have likely been called in to troubleshoot a performance issue that turned out, after hours of investigation, to originate outside of Citrix.

In a 2014 survey on Citrix performance management, 65 percent of respondents reported that over half the performance issues they encounter end up not being caused by Citrix itself. Sixty percent of respondents said that they spend over one-third of their time troubleshooting performance issues rather than working on proactive initiatives.¹

What if Citrix administrators could take that time back?

The key to taking back your time is visibility. What if you could analyze every transaction between every tier of your environment—from the Citrix environment to the applications and infrastructure behind Citrix? If you could see per-user transaction details for ICA sessions, authentication requests, database queries, and storage file access, you would be able to quickly determine whether there was a problem and where it originated. Then you could alert the responsible team and get on with your day.

Keep reading for real-world examples of how actual companies transformed their operations and took back the Citrix team’s time by using ExtraHop wire data analytics. In this paper, you’ll learn:

- What is wire data analytics and how it works
- How one Citrix team used wire data to troubleshoot slow login times
- How wire data can provide insight into areas outside of the Citrix team’s control, such as VPN access

¹ “Citrix Performance Management Report” DABCC, 2014
Wire Data Is Your Missing Piece

The difficult thing about troubleshooting Citrix issues is that Citrix is not a technology; it’s an ecosystem. When Citrix administrators are called on to fix a slowdown, they must be able to investigate not only the Citrix environment, but also the applications that are delivered over Citrix and other ancillary services, such as DNS and authentication.

This is where wire data comes in. Because all the elements involved in applications and Citrix delivery communicate over the wire, the network is an excellent source of objective data. With this approach, there are no agents to deploy and manage, and there is never a question about whether you can trust the information—you know that an error occurred because you saw it pass over the wire!

Getting wire data is no trivial task. First, it requires the reassembly of unstructured packets into complete transactions, flows, and sessions. This is what the ExtraHop platform does in real time at speeds of up to 40 Gbps throughput. The platform then extracts more than 3,000 critical metrics such as server processing time, network transfer time, and Layer 7 application metrics such as files accessed, database stored procedures, authentication requests, and more. These metrics are indexed in a streaming datastore for trending and alerting, and also so that they are available to the user immediately.

The ExtraHop platform is built from the ground up to transform unstructured network packets into structured wire data in real time.
The ExtraHop platform analyzes ICA sessions to measure Citrix launch, load, login, latency, and channel activity metrics, in addition to a number of other application protocols. You can build customizable dashboards to present these metrics along with a runbook so that your support personnel know how to respond to user complaints. For example, you can add instructions for who to contact if logins rise above a threshold right alongside a chart that shows login times.

It is important to note that the ExtraHop platform provides detailed information about the performance of applications and infrastructure outside of Citrix. This capability enables Citrix administrators to have productive conversations with other teams when the cause of a slowdown is not due to the Citrix environment. The ExtraHop platform acts as a single source of operational intelligence for the entire IT organization, helping to open lines of communication and bridge what were previously siloes of technology.

<table>
<thead>
<tr>
<th>Traditional Citrix Monitoring</th>
<th>Citrix Monitoring with ExtraHop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent-based – Many monitoring tools for Citrix require agents to be installed on select servers, which must be managed and can perturb the systems they are supposed to be monitoring.</td>
<td>Passive – ExtraHop requires only a copy of network traffic from a SPAN or network tap. ExtraHop automatically discovers and classifies all devices communicating on the wire.</td>
</tr>
<tr>
<td>Self-reporting – Traditional approaches rely on data that is reported by the server and will not work if the server is unresponsive. Also, this information is limited to what is logged or instrumented.</td>
<td>Observed behavior – Wire data reveals actual behavior observed on the network including login times, bandwidth per application, and bandwidth per virtual channel.</td>
</tr>
<tr>
<td>Resource utilization – CPU, disk, and network resources is sometimes linked to end-user experience, but sometimes not.</td>
<td>Transaction-focused – Analyzing communications between systems is a more reliable means of determining actual causes and proactively monitoring end-user experience.</td>
</tr>
</tbody>
</table>

“While most monitoring solutions appear to be relatively similar, within about 30 seconds it seemed that ExtraHop’s solution was quite a bit different than most of the other solutions out there.”

Gabe Knuth, BriansMadden.com
Real-World Use Cases

ExtraHop has helped a number of IT organizations—including McKesson Managed Services, Steward Health Care System, and Morgan Stanley—solve especially complicated Citrix delivery issues. These organizations have been able to empower their support desks to reduce escalations, reduce login times for users, and equip Citrix administrators and architects with the insights needed to optimize delivery.

Performance for Citrix Over VPN

The first real-world example highlights how the ExtraHop platform equips teams to triage and troubleshoot slow performance issues more quickly, even when the cause lies outside of the Citrix environment.

A Root Cause Outside of Their Control

An Operations team supporting Citrix at a large professional services firm frequently received complaints about slow response times from the field. Even though the team knew that the root cause of poor performance for remote users was frequently outside of their control, they still needed to investigate the Citrix environment and the applications delivered over Citrix. This process was time-consuming but necessary as users in the field relied on these Citrix-published applications to get their jobs done.

Desired Outcome

- Ability to quickly determine whether slow response times reported by end users were due to poor Citrix performance, application issues, network congestion, or other problems.
- Reduce the number of unnecessary support tickets.
- Improve productivity for the Operations team.

To streamline the triage process, the Operations team needed to empower Tier-1 support staff to triage issues so that they only escalated the problems that the Operations team really needed to know about.
The Solution

Using the ExtraHop platform, the Operations team built a dashboard that revealed at a glance which users were experiencing network issues as opposed to Citrix or application issues. The dashboard also functions as a runbook so that Tier-1 support personnel know when to escalate an issue to the Operations team, such as when round-trip time for a particular user IP exceeds 1,000 milliseconds.

The metrics on the dashboard enable the Operations team to track common network metrics that can indicate network congestion or connectivity issues, including: high retransmission counts when users access Citrix applications; client connections with high network error rates; packet drops by the client; and latency by IP and user.

Equipped with this visibility, the Operations team could see that a user with the IP 192.168.252.98 was experiencing slow Citrix response times due to their network connection. They could easily verify that ICA load times exceed SLAs for this client IP, but
also that network failures (send window throttles, in particular) were causing this slowness. Investigating further, the team found that their VPN concentrator was functioning normally and were able to conclude that the poor performance was due to external connectivity factors.

**User Impact**

With the ability to triage performance issues reported by remote users, the Operations team was able to eliminate time spent unnecessarily investigating Citrix and application performance. By equipping the Tier-1 support staff to understand when an issue needed to be escalated, the organization also reduced the number of support tickets for the Operations team by 40%.

**Infrastructure Visibility for Citrix Environments**

This second real-world example showcases how Citrix teams can tie specific front-end behaviors back to activity in the back-end infrastructure. This correlation helps them to quickly pinpoint issues that they might have spent months trying to track down otherwise.

**The “Ghost in the Machine”**

A large research hospital underwent a major virtual desktop infrastructure (VDI) expansion to support 4,000 users and more than 100 applications. Early on, boot-up and application launch times took about 10 to 12 seconds. Over the next several weeks, however, users began to complain about increasingly slow login times. Logins could take as long as 45 seconds, which was completely unacceptable. The slowdowns threatened to derail the VDI initiative.

Internal teams set up to investigate the issue were unsuccessful, even after several months. The tools they used would only confirm that Citrix was indeed experiencing a slowdown. The mystery issue became known as the “ghost in the machine.” The team realized that Citrix is a complex environment with many interdependencies in the background, but they were unable to see the entire delivery chain.
The Solution
The IT team decided to deploy the ExtraHop platform to try and troubleshoot the issue. The next time users reported slow logins, the team investigated the Citrix servers. The IT team identified the particular server associated with the slow login times, then drilled down to see that one user experienced consistently slow load times while most of the other users had load times ranging from five seconds to 30 seconds.

To investigate what was causing this behavior, the team next looked at which other L7 protocols that specific Citrix server used. A gigantic spike in CIFS traffic coincided with the long load time. Focusing on the actual files being transferred, they noticed a significant number of JPEG files in the user’s roaming profile. This user stored photos in his Citrix profile folder. When this particular user logged in, the XenDesktop server would load his profile including the JPEG files, causing storage I/O contention and slowing all concurrent user logins. The IT team fixed this problem by removing the My Pictures folder from user’s profiles.

To proactively monitor this and prevent performance issues in the future, the team built a dashboard to track all of the components of the Citrix XenDesktop delivery chain, including the network, authentication, applications, and storage. This dashboard displayed correlated information on users, files, and client IPs, allowing for quick identification of undesirable user behavior.

Desired Outcome
- Reduce Citrix login times to 10 to 12 seconds.
- Gain visibility into Citrix delivery chain from remote access to XenDesktop servers to authentication and storage.
- Restore user confidence in the VDI rollout.
User Impact

After reconfiguring the user's roaming profile and reducing its size, load times returned to the acceptable launch time of 10 to 12 seconds. The elusive "ghost in the machine" had been found, and user concerns about VDI performance mollified.

With ExtraHop's ability to mine the wire for information, the customer saved over $400,000 on specialist consulting and many hours of troubleshooting. The Citrix administrators now had a way to look across the Citrix environment and the supporting infrastructure.
Conclusion

The ExtraHop platform provides Citrix administrators with the insight they need to stop the blame game. Instead of constantly having to prove that a slowdown is not due to Citrix (proving a negative), they can dig into their wire data to show what is causing the issue whether that be a user’s poor network connection, a DNS misconfiguration, or network storage contention. As a result, you will be able bolster your VDI initiative, open lines of communication with other teams, reduce mean-time-to-resolution, and spend less time in unnecessary troubleshooting exercises.

To learn more about the ExtraHop wire data analytics platform, visit www.extrahop.com/extrahop-in-action/citrix-administrator/