

Top 10 Items Found by Citrix Consulting on Assessments

Overview

This whitepaper highlights the most common risk areas found in customer environments during assessments. Citrix Consulting has several service offerings within the Analysis Phase of the [Citrix Methodology](#), but the first, and still the most popular service offering today, is the *Application Virtualization Assessment* (formerly called the *Infrastructure Assessment*). Citrix Consulting conducts AVAs or IAs to obtain the business and technical drivers of a project, examine a customer's current or proposed infrastructure, determine requirements for a Citrix implementation and identify potential risk areas. Typically, the findings of the assessment are used as input in the Design Phase. While each assessment is unique, Citrix Consulting has found that certain issues persist from customer to customer. The goal of this document is to identify these common issues, describe why they pose a potential risk to the implementation and provide Citrix best practices and recommendations to overcome them.

Target Audience

This document is intended for system administrators, architects and engineers that are responsible for designing, implementing, managing or maintaining a Citrix environment. This analysis may also be beneficial to Citrix partners who conduct similar assessments.

Table of Contents

- Overview 1
 - Target Audience..... 1
- Top 10 3
 - 10. Policy Management 3
 - 9. Citrix Knowledge and Training 3
 - 8. XML Traffic..... 4
 - 7. Single Farm vs. Multiple Farm Design..... 4
 - 6. Test Environment..... 4
 - 5. Systems Management and Monitoring 5
 - 4. Server Tuning and Optimizations 5
 - 3. Terminal Server Profile Design 6
 - 2. Load Management 6
 - 1. Printer Drivers 7
- Conclusion..... 8
 - About Citrix Consulting 8



Top 10

This section contains a summary of the most prevalent risk areas found in customer environments over the last five years (2004-2008). The sample set was approximately 100 different customer environments ranging from small implementations (less than 10 servers) to enterprise deployments (more than 100 servers or 5,000 concurrent users).

It is important to note that the items listed below are in descending order based on **popularity** (10 to 1 with 1 being the most common issue). The rankings are not based on **criticality** or **importance**.

10. **Policy Management**
9. **Citrix Knowledge and Training**
8. **XML Traffic**
7. **Single Farm vs. Multiple Farm Design**
6. **Test Environment**
5. **Systems Management and Monitoring**
4. **Server Tuning and Optimizations**
3. **Terminal Server Profile Design**
2. **Load Management**
1. **Printer Drivers**

10. Policy Management

Both Microsoft Group Policy Objects (GPOs) and Citrix policies play an important role in Citrix environments. Citrix Consulting has found that many customers do not create a “baseline” Citrix policy. This is typically a policy that applies to all servers or users that has many common settings and optimizations. Unused virtual channels, such as audio or COM port mapping, should be disabled whenever possible to optimize the ICA protocol and improve overall session performance. Bandwidth restrictions and common printing configurations are also ideal candidates for inclusion in a baseline Citrix policy. A sample baseline Citrix policy can be found in [Appendix A of this whitepaper](#).

Citrix Consulting has also found that many customers are not fully aware of the GPOs that are being applied to their Citrix servers. Due to the hierarchical structure of Active Directory, GPOs can be implemented at multiple levels. This complexity can make it very difficult to determine the impact on the Citrix environment. Many times, changes to GPOs are implemented without proper change control procedures. Citrix has been involved in several troubleshooting incidents where GPOs were applied unknowingly and misconfigured GPOs were the root cause of the issue. Both Citrix and Microsoft recommend using tools such as the [Resultant Set of Policy snap-in](#) to understand the cumulative effects of multiple GPOs applied at various levels within Active Directory.

Citrix policies and GPOs are powerful tools that help maintain standardization and consistency. Citrix Consulting recommends customers continue to use them in their implementations, but be mindful of the impact these policies can have on Citrix servers. In addition, proper change control procedures should be followed at all times.

9. Citrix Knowledge and Training

Citrix Consulting has found that many customers do not have the proper knowledge or training to design or implement a Citrix environment in accordance with best practices. In addition to on-the-job experience, Citrix recommends customers receive formal Microsoft and Citrix training. Citrix has also found that several customers do not have current Citrix or Microsoft certifications. With every new release of Citrix XenApp and the Windows Server Operating System, there are

several underlying changes and new features that are critical to understand. Citrix highly recommends customers stay current on their Microsoft and Citrix certifications. For those enterprise customers, Citrix recommends administrators obtain MCSE/MCITP and CCIA certifications. The CCIA certification is important for those individuals that develop architecture designs or plan future migrations.

A list of all available training classes and certification programs offered by Citrix can be found [here](#). In addition, [Citrix Education can be contacted directly](#) for custom training that can be delivered at a customer site – many enterprise customers find this approach the most efficient and cost-effective.

8. XML Traffic

Citrix Consulting has found that many customers do not secure the XML traffic from Web Interface to the XML Brokers (typically the Zone Data Collectors). As a result, usernames and domain names are sent in clear-text across the network. Passwords are also not encrypted, but they are scrambled using simple XOR encoding. Although this traffic is typically isolated to the internal network, Citrix recommends encapsulating this traffic via SSL. Customers can use Citrix SSL Relay, IPSec policies or other means to secure the XML traffic so that passwords are encrypted when sent across the network.

7. Single Farm vs. Multiple Farm Design

Citrix is continually improving the scalability of a single XenApp farm and most customers can implement one production farm and be successful. However, due to a variety of technical and business reasons which are discussed below, large and enterprise customers should consider a multiple farm design as opposed to a single farm design.

- **Technical Reasons.** The current architecture of a Citrix farm and zones, specifically components such as the Local Host Cache and IMA Service, present scalability challenges when a single farm supports a large number of users and servers. Large farms also typically have over 1,000 published resources. As a result, application enumeration time and performance degradation of the Data Store can become problematic. These types of issues and many more only occur in large farms.
- **Business Reasons.** Due to operational procedures or a customer's support structure, many customers may want to consider multiple farms to ease administration and day-to-day management. Some customers isolate mission-critical applications from other line of business applications to provide added flexibility when performing upgrades to newer versions of the mission-critical applications, for example. Other customers choose to implement multiple farms if there are different teams or resources managing distinct sets of Citrix servers.

Unexpected issues and scalability obstacles will undoubtedly continue to surface as extremely large loads are placed on components such as the IMA Service and Zone Data Collectors. While Citrix is committed to resolving these issues as quickly as possible once they are identified, many of these issues would never be encountered if the size of a farm were reduced. Customers should understand the business impact these issues could potentially cause and weigh that against the additional overhead of managing multiple farms. Given the robust processes and tools that many customers develop to automate many management tasks, the additional overhead associated with managing multiple farms is usually minimal.

There are many approaches that can be taken when determining how to segment users and applications into separate farms, and these are typically driven by a customer's unique business requirements. It is also important to note that care should be taken so as not to create too many farms – a final number of production farms can only be determined after a proper design and thorough testing.

6. Test Environment

Citrix has found that many customers lack an isolated test environment for Citrix infrastructure. Some customers place test servers in a separate application silo within the production farm. Other customers create a separate zone within the production farm in an attempt to isolate the non-production servers from the production environment. Citrix highly

recommends creating an isolated test or development farm so the production farm's Data Store is not affected by any components in the test farm. All printer drivers, applications and hotfixes should be tested rigorously in the isolated test farm before attempting to install them on any production servers.

In addition to an isolated test farm, many customers should consider an isolated Active Directory environment for testing. Many Citrix products such as XenApp, Password Manager and Provisioning Server tightly integrate with Active Directory and can require significant changes in some cases. For large to enterprise environments, it is considered a Citrix best practice to create an isolated Active Directory environment to test all changes to Group Policy, schema updates, DNS, etc. As always, the test farm and test AD infrastructure should resemble the production environment as closely as possible. Virtualization products such as [Citrix XenServer](#) are excellent options for implementing the test infrastructure described above.

5. Systems Management and Monitoring

Many customers have a sufficient number of systems management tools to effectively monitor Citrix deployments, but Citrix has found that most customers do not customize alert thresholds properly or administrators perform troubleshooting in a reactive manner as opposed to a proactive manner. Citrix recommends leveraging the vendor-supplied systems management software in combination with [Citrix EdgeSight](#) for a complete monitoring solution. Other tools such as [Microsoft System Center Operations Manager](#) (formerly called MOM) are also widely used to complement a monitoring solution. The latest versions of XenApp also come with a Health Monitoring and Recovery (HMR) agent – Citrix recommends leveraging the default health check tests and the additional HMR tests that can be downloaded for free on Citrix's website [here](#). This suite of monitoring tools and agents allow administrators to find and resolve issues before they become problematic.

In addition to utilizing the proper tools, it is important that customers configure alerts and customize thresholds appropriately for their environment. Citrix recommends conducting performance and scalability testing to gather baseline data. Using this baseline data, administrators can then properly configure alert thresholds based on their unique hardware configurations, application sets and use cases.

Citrix has also found that the majority of customers that implement Resource Manager only use the default metrics. Citrix recommends adding additional metrics, such as Data Store Connection Failures and Zone Data Collector Elections, in order to properly monitor a XenApp environment. As mentioned previously, each metric's thresholds should also be customized after ample testing. Tools such as [EdgeSight for Load Testing](#) are excellent options for conducting performance and scalability testing.

4. Server Tuning and Optimizations

Citrix has found that almost all customers are not properly tuning or optimizing their XenApp servers in some way. Simple items, such as tuning kernel memory or applying optimizations documented in the Advanced Concepts Guide, are often overlooked. Since the majority of Citrix customers are still running XenApp on the Windows Server 2003 32-bit platform, it is critical to use a kernel debugger to understand memory bottlenecks and properly tune items such as Paged Pool Memory and System Page Table Entries (PTEs). Tuning these areas of kernel memory can greatly increase user density on 32-bit systems and is considered a Citrix best practice.

Customers should also be implementing the many server optimizations that are documented in the freely available Citrix [Advanced Concepts Guide](#). In addition to Terminal Server and XenApp-specific optimizations that can be incorporated as part of an automated server build or implemented via Group Policy, customers should also be optimizing the Windows Operating System by disabling any unused services and features.

By tuning kernel memory and implementing server optimizations, customers can increase user density and ultimately reduce hardware costs by consolidating member servers. These optimizations allow Terminal Services and XenApp to run in the most efficient manner possible.

3. Terminal Server Profile Design

Terminal Server profile design is one of the most critical areas in any Citrix deployment – it can be the difference between poor performance and strong user adoption. Citrix Consulting has found that many customers have logon times greater than 20 seconds, and in most cases, this can be attributed to poor profile and policy design. Although Terminal Server profile design is outside the scope of this whitepaper, many customers can improve their profile solution by understanding [the Citrix best practices in this area](#) (ironically, this KB article is also the most read KB article in Citrix’s history).

Since many customers implement roaming profiles, folder redirection is of primary importance. Citrix best practices dictate that the ‘My Documents’ and ‘Application Data’ folders be redirected in most cases. Folder redirection reduces logon times, minimizes profile corruption and reduces the size of the “core” profile. Enterprise customers may require other folders to be redirected based on business requirements and this can be accomplished by implementing a Group Policy Object to redirect the appropriate shell folders using the registry. Citrix Consulting often utilizes custom ADM templates to accomplish this task.

Another common mistake that some customers make is using a single roaming profile across multiple application silos or load managed groups. When a user utilizes applications from multiple silos, the roaming profile is subject to “Last Writer Wins” (LWW) conflicts as described in [page 13 of this whitepaper](#). This can result in the loss of personalized settings and an inconsistent user experience. Hybrid, flex, multiple roaming profiles or a combination of roaming and mandatory profiles are typically implemented in complex enterprise environments with multiple load managed groups. Other customers utilize third-party solutions, such as [Citrix User Profile Manager](#), to mitigate the risks associated with LWW conflicts. However, with proper design and the addition of [Group Policy Preferences](#), which gives administrators the flexibility to manage most items that had to historically be done using logon scripts, most of the third-party solutions are only required in the most complex and demanding environments. Citrix recommends each organization understand their unique business and technical requirements before designing and implementing a Terminal Server profile solution.

2. Load Management

Citrix has consistently found that many customers’ load evaluators are not configured according to Citrix best practices. Some customers implement the ‘Advanced’ load evaluator and others try to create a ‘Custom’ load evaluator. Citrix also finds that a large number of customers are still using the ‘Default’ load evaluator, which does not give a true indication of load since it is exclusively based on the number of users logged onto a given server. Customers should be aware that when new servers are built and added to the farm, the ‘Default’ load evaluator is applied to the server. As part of the server build process, Citrix recommends using an MFCOM script to assign the proper ‘Custom’ load evaluator after the server joins the farm. An example script that Citrix Consulting has used in the past to accomplish this task can be found [here](#).

Citrix recommends implementing ‘Custom’ load evaluators after proper performance and scalability testing. In complex environments with multiple application silos, Citrix often recommends creating unique ‘Custom’ load evaluators for each application silo, effectively resulting in “load managed groups”. These load evaluators may have different rules and thresholds depending on the different resource bottlenecks identified during testing. If proper testing cannot be performed prior to production, Citrix Consulting recommends implementing the following ‘Custom’ load evaluator which can be applied to all servers as a baseline:

<u>Rule</u>	<u>Setting</u>
CPU Utilization	Full Load: 80%, No Load: 10%
Memory Usage	Full Load: 80%, No Load: 10%
Load Throttling	High
Server User Load	X

Since the logon process is one of the most intensive actions a XenApp server undertakes, it is important to add the new ‘Load Throttling’ rule that was introduced in XenApp version 4.5. This effectively limits the number of simultaneous logons that can occur at any given time. It also prevents the “black hole” effect when a new server is brought online. The ‘Server User Load’ rule is also included for capping purposes – this is considered a best practice for resiliency. Customers can choose an initial value of 100 (denoted by ‘X’ above), but it is highly recommended that this value be customized after

scalability testing. It is also important to note that the CPU and Memory “full” thresholds have been reduced from the default 90% - Citrix Consulting has found that performance degradation typically occurs when the CPU Utilization or Memory Usage is approximately 80-85%. The combination of these rules and settings typically provide the most effective load management scheme.

1. Printer Drivers

On almost every assessment that Citrix has conducted over the last five years, an inconsistent set of printer drivers are found across the servers within the farm. This can be verified by accessing the drop-down list within the management console to determine which drivers are installed on each particular XenApp server. More than likely, there will be a different number of drivers installed on each server in the farm. These inconsistencies can make it extremely difficult to troubleshoot printing issues in the environment. Citrix recommends customers limit the number of native drivers installed on each server in the farm. Additionally, the number of drivers should be consistent across each server and each printer driver should be tested for Terminal Services compatibility. Utilities such as [StressPrinters](#) can assist administrators with this task.

By default, users have the ability to install printer drivers on Terminal Servers, so it is important to lock this capability down. Most customers implement a Citrix policy that effectively disables users from installing drivers via *ICA* sessions. But many customers forget to lock down users’ ability to install printer drivers via *Remote Desktop Protocol (RDP)* sessions. If an organization has an inconsistent set of drivers across their XenApp servers and has implemented the Citrix policy that prevents automatic driver installation, it is typically the administrators that are unknowingly installing printer drivers when they connect using RDP. In order to proactively circumvent this issue, Citrix recommends implementing the appropriate Group Policy to disable all users from redirecting printers when connecting using the Remote Desktop Protocol. Some organizations choose to disable “Windows Printer Mapping” on the RDP listener using the Terminal Services Configuration tool or even rename the `ntprint.inf` file on each Terminal Server, but Citrix recommends using Group Policy to ease administration and reduce management overhead.

Conclusion

This whitepaper documented the most common risk areas or issues found during assessments conducted by Citrix Consulting over the past five years. Many of the items discussed, such as load management and printer drivers, can be implemented or corrected in a matter of hours or days. Other items, such as Terminal Server profile design and XenApp farm design, may take organizations weeks or months to correctly implement or rectify. Citrix recommends customers prioritize each of the risk areas in their particular environment and address them in the order of criticality as determined by the business.

In addition to documenting the top issues found in customer environments, Citrix also provided best practices and recommendations to mitigate each risk. If additional information or technical guidance is needed on a particular issue, organizations can [contact Citrix Consulting](#).

About Citrix Consulting

Citrix Consulting has been formally conducting IAs, Health Checks and AVAs since 1999. Citrix Consulting is a world-class provider of professional services specializing in the analysis, design, and implementation of Citrix technologies. Through the use of proven methodologies, tools and best practices, Citrix Consulting helps ensure the successful implementation of Citrix technologies. Citrix Consulting focuses on engagements with enterprise customers who have complex, mission-critical or large-scale deployments of Citrix technologies. These engagements are typically the most challenging in scope and complexity, and require Consultants who are uniquely qualified with Citrix product expertise. Citrix Consulting has regional offices on every continent except Antarctica.

Notice

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. CITRIX SYSTEMS, INC. ("CITRIX"), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

This publication contains information protected by copyright. Except for internal distribution, no part of this publication may be photocopied or reproduced in any form without prior written consent from Citrix.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2009 Citrix Systems, Inc., 851 West Cypress Creek Road, Ft. Lauderdale, Florida 33309-2009 U.S.A. All rights reserved.

Version History			
Author	Version	Change Log	Date
Hector Lima	0.9	Original Content from IAs Conducted in 2000 and 2001	8/31/2001
Scott Thompson	1.0	Original Document QA	9/17/2001
Nick Rintalan	1.9	Updated Content Based on Assessments Conducted from 2004-2008	12/17/2008
Mike Schaeffer	2.0	Document QA	12/24/2008
Nick Rintalan	2.01	Clarified XML Traffic Password Encoding	2/4/2009



851 West Cypress Creek Road Fort Lauderdale, FL 33309 954-267-3000 <http://www.citrix.com>

Copyright © 2009 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix ICA, Citrix MetaFrame, and other Citrix product names are trademarks of Citrix Systems, Inc. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.