Monitoring of a Citrix Infrastructure

Overview

This document describes the monitoring of a Citrix Delivery Center Infrastructure, its components and possibilities. Furthermore, it addresses recommendations regarding the monitoring of performance counters and services.

Acknowledgement:

This document has been created during an engagement of Citrix Consulting for the DSV-Gruppe Deutscher Sparkassenverlag (www.dsv-gruppe.de). All involved people would like to thank DSV for providing the infrastructure and the scenarios in a data center.
# Table of Contents

1. Monitoring of Citrix Components ........................................................................................................ 1  
   1.1 Overview ............................................................................................................................................ 1  
   1.2 Types of Monitoring .......................................................................................................................... 1  
      1.2.1 Hardware Monitoring .................................................................................................................. 1  
      1.2.2 System Monitoring ...................................................................................................................... 1  
      1.2.3 SNMP Monitoring ..................................................................................................................... 2  
      1.2.4 End-to-End-Monitoring ............................................................................................................ 2  
   1.3 Entire Monitoring .............................................................................................................................. 2  
2. Monitoring of Citrix components ......................................................................................................... 4  
   2.1 Monitoring of a XenApp environment ............................................................................................... 4  
      2.1.1 Health Check & Recovery .......................................................................................................... 4  
      2.1.2 SNMP and Performance Counter .............................................................................................. 4  
      2.1.3 Third-Party software-based Agents .......................................................................................... 5  
      2.1.4 Resource Manager ..................................................................................................................... 5  
      2.1.5 Important Components in a Monitoring Architecture ................................................................. 5  
   2.2 Monitoring an Access Gateway Standard ......................................................................................... 5  
   2.3 Monitoring an Access Gateway Enterprise / a NetScaler ................................................................. 6  
      2.3.1 SNMP Monitoring ..................................................................................................................... 6  
      2.3.2 Additional considerations ......................................................................................................... 6  
   2.4 Indirect / Aggregated Monitoring with Citrix NetScaler ................................................................. 7  
   2.5 Monitoring Advanced Access Control and Web Interface ............................................................... 7  
      2.5.1 Types of Monitoring .................................................................................................................. 7  
      2.5.2 Monitoring with a Hardware Load Balancer ............................................................................. 8  
      2.5.3 Critical components ................................................................................................................... 8  
   2.6 Monitoring XenServer ....................................................................................................................... 8  
      2.6.1 XenCenter Alerts ....................................................................................................................... 8  
      2.6.2 Syslog ......................................................................................................................................... 9  
      2.6.3 Additional Monitoring options ................................................................................................. 9  
   2.7 Monitoring XenDesktop .................................................................................................................... 9  
      2.7.1 Desktop Delivery Controller (DDC) .......................................................................................... 10  
      2.7.2 Virtual Desktop Agent (VDA) .................................................................................................. 10  
      2.7.3 Outlook ...................................................................................................................................... 10
2.8 Monitoring Citrix Provisioning Server .................................................................. 10
    2.8.1 Monitoring possibilities ............................................................................. 10
    2.8.2 Additional considerations ......................................................................... 10
2.9 Monitoring Citrix License Server ...................................................................... 11
    2.9.1 Types of monitoring .................................................................................. 11
3. EdgeSight Monitoring ......................................................................................... 12
    3.1 Overview ...................................................................................................... 12
    3.2 Suggestions for data analyzing ..................................................................... 13
    3.3 Active Monitoring of applications ................................................................ 14
    3.4 EdgeSight for NetScaler .............................................................................. 14
4. Integration of Different Types of Monitoring ....................................................... 15
1. Monitoring of Citrix Components

1.1 Overview

“Monitoring” is a generic term for direct systematic data collection, observation, or control of a task or process with technical tools or other monitoring possibilities.

The reason for monitoring is to interact if a controlled process or task is not behaving as expected, or if any threshold of a counter has reached or exceeded a pre-defined value. In other words, monitoring is a special type of logging.

The following figure gives an exemplarily overview of all possibilities of monitoring in a Citrix Infrastructure.

At this point it could already clearly be marked that an End-to-End-Monitoring is not a replacement for all other kinds of monitoring. It can deliver circumstantial evidence at which stage in a process flow issues are occurring. On further analyzing and probably solving the problem all other monitoring possibilities are necessary.

1.2 Types of Monitoring

1.2.1. Hardware Monitoring

In terms of Hardware Monitoring the developers of such solutions intend to use their own proprietary software agent on the system itself. These agents could normally send their events to a SNMP based monitoring environment. This monitoring ensures that administrators are informed if any hardware component is going to fail or failed. The alert itself need to be combined with an email alert so that administrators receive this information. The monitoring itself could not only include failures of hardware it could also be used to see the state of a RAID array or if any cooler is running in a normal manner.

1.2.2. System Monitoring

System Monitoring is based on tracking services and processes on target systems. Usually this monitoring is also based on software agents who are installed on the target systems. These agents allow the monitoring of services and processes as well as monitoring the event viewer. Based on configured thresholds or errors this monitoring can also be configured to report this...
information within an email. Furthermore in case of a stopped service the first taken action could be to restart the service. If the service cannot be restarted an email will be send out.

1.2.3. SNMP Monitoring

With SNMP monitoring also devices which are not capable of running any client software can be monitored. For this reason the IETF ([http://www.ietf.org](http://www.ietf.org)) defined a standard for communication between devices and a central station. Microsoft offers for all server operating systems also the possibility to install a SNMP agent. The central station need to have the corresponding MIB installed to analyze incoming traps.

1.2.4. End-to-End-Monitoring

The entire technical process of each type of monitoring is only looking for each single component but not as a user would. Only single components are monitored and the administrator can assume that all pieces in the entire working flow for a user are working fine. At this point of monitoring an End-to-End Monitoring could be implemented. This type of monitoring allows the administrator a value which is correlating with the satisfaction of users in the environment. End-to-End Monitoring is tracking the entire workflow from a user’s perspective. The result of an End-to-End Monitoring can be used to generate the level at which users are absolutely satisfied and this satisfaction level can be tied to the measured runtime at each component in the entire work flow. This allows an administrator measure a value at which the system is performing well in terms of a user’s perspective. This default value also reflects the default value at which the entire infrastructure is working well based on measured values.

1.3 Entire Monitoring

In a heterogeneous environment all types of monitoring systems are in use. Goal of a holistic monitoring is to centralize each of the used monitoring type and the corresponding alerts or information. Only centralizing within one overview is only half way of implementing a holistic monitoring solution. It is essential to define and create actions based on measured performance counters. Such actions could for example be to send out an email or restarting a service. Each monitored component should receive an action based on its importance. In a regular circumstance an administrator already knows that there is a problem in the environment and is not informed by the user which suffers on trying to work with an offered service. The entire monitoring should be based on pro-active monitoring of the environment. This allows an administrator to see problems at an early stage or already prior the problem is really affecting users. In some environments the user is performing the monitoring as the administrator only knows about the problem after a user is reporting it.
A monitoring solution is also implemented to assure that agreed Service Levels are reached and therefore the availability of systems should reflect Service Level Agreements. The monitoring itself is only providing the framework to observe an environment. The entire monitoring might become useless if administrators or persons are not informed in case of a failover. The outage of a resource should also be send via email to the respective people as in terms of a failover the primary is no longer available and at this point the system is no longer redundant. The architecture of monitoring an environment must take care of defined levels of availability of systems. Based on this architecture an alert can be assigned to different communication levels. For example if a service goes down an email will be send to the administrators, whereas a NetScaler was performing a failover a SMS will be send to an administrator.
2. Monitoring of Citrix components

2.1 Monitoring of a XenApp environment

Citrix included in XenApp 5.0 Platinum Edition also EdgeSight as an End-to-End Monitoring solution. Further information about this type of monitoring will be discussed at a later chapter.

2.1.1 Health Check & Recovery

The Health Check & Recovery functionality provides the ability to monitor specific features of a XenApp Server. This type of monitoring is based on test scripts and can be enhanced for other components. During a default setup of a XenApp the following tests are installed and assigned by default. The default action on reaching the threshold is to send an alert into the Citrix Access Management Console.

Based on scripts further tests can be assigned. These scripts must not only be based on Citrix specific features. As already mentioned the default action is to send an alert to the Citrix Access Management Console. The type of action can be customized such as to restart a service.

Further information about the Health Monitoring & Recovery tests can be found in the following Knowledge Center Article CTX112116 „Creating, Configuring, and Testing Health Monitoring & Recovery Tests“.

2.1.2 SNMP and Performance Counter

On every Windows-based system a monitoring with SNMP could be implemented. Microsoft implemented a SNMP Client within all server operating systems.

During the installation of XenApp several Citrix specific Performance Counters are installed. These counters can be monitored with the Microsoft Performance Monitor. The Microsoft Performance Monitor unlikely intends to create a huge amount of data. This may have a negative impact on analyzing this captured data at a later stage.
2.1.3 Third-Party software-based Agents

Nearly all monitoring software vendors are offering their software-based agent for Windows systems. This agent will be installed on the system and is allowing the monitoring of resources on the target system. Most agents also allow the monitoring of the Microsoft Eventlog or create an alert if a defined Eventlog entry is occurring. This alert can be sent out to the global and centralized system monitoring GUI. These agents are also used to monitor services on the target system. An action can not only be to send out an alert, it could also be used to restart a service.

2.1.4 Resource Manager

Citrix XenApp 5.0 for Microsoft Windows Server 2003 and previous XenApp versions contain Citrix Resource Manager for monitoring purposes. Resource Manager can monitor configured Citrix Performance Counters and on reaching a defined threshold an action can be assigned. All measured metrics are written on a regular base into a Microsoft SQL Database and can be analyzed at a later stage with predefined reports of the Citrix Access Management Console.

2.1.5 Important Components in a Monitoring Architecture

On monitoring a Citrix XenApp environment at least the following services should be considered:

- Citrix Client network
- Citrix Independent Management Architecture
- Citrix MFCOM Service
- Citrix Print Manager
- Citrix XML Service
- Citrix XTE Service
- Terminal Services

This list should be adjusted to the conditions of each installation and probably enhanced to meet all monitoring requirements. Additionally in a Citrix infrastructure the Data Store and the Citrix License Server should be considered in designing the monitoring architecture.

Regarding the Performance Monitor Counters the following Knowledge Center articles can give orientation:

- “Monitoring Server Performance with Citrix Presentation Server”CTX112421
- “XenApp Infrastructure Monitoring and Alerting”CTX118742

Last but not least one special infrastructure service should face a special monitoring. It can be beneficial to monitor the following Performance Counters on the Data Collector.

- ResolutionWorkItemQueueReadyCount (value should be >1)
- WorkItemQueueReadyCount (value should be <1)

2.2 Monitoring an Access Gateway Standard

The Access Gateway Standard is providing active monitoring through an administrative desktop on the Access Gateway itself. This desktop is providing information about active session, resource consumption and network traffic.
Furthermore the Access Gateway Standard is capable of sending events to a Syslog Server for further analysis. The Access Gateway Standard also offers the possibility to send SNMP Traps into a community.

2.3 Monitoring an Access Gateway Enterprise / a NetScaler

2.3.1 SNMP Monitoring

Access Gateway Enterprise / NetScaler can be monitored based on SNMP. An overview of all possibilities to create an SNMP Trap can be found in the Knowledge Center Article CTX117377 „Installation and Configuration Guide – Volume 1“ for NetScaler 8.1. These SNMP Traps can be sent to a central instance for further analysis. Monitoring a NetScaler requires installation of the corresponding MIB on the central instance. The MIBs for HP OpenView and WhatsUpGold are provided on the NetScaler CD.

NetScaler can differentiate two types of generic SNMP Traps and 57 Enterprise specific Traps.

Access Gateway Enterprise / NetScaler can also report events to a Syslog Server for further analysis.

2.3.2 Additional considerations

Most installations of NetScaler hardware are done for a High Availability Pair. In this high redundant configuration it is becoming crucial to get informed as soon as failover occurs. The passive device takes over from the active device and at this moment the environment is not redundant any more. Users are not affected by this failover and have no notice that the provided service is currently no longer available in redundant form. In an environment in which services and resources are provided high available the foundation of high availability is also to get informed as soon as one component of this bond is no longer available. Administrator should react to reestablish high availability as soon as possible. To do so it is crucial that administrators already get noticed if a failover occurs.
## 2.4 Indirect / Aggregated Monitoring with Citrix NetScaler

In addition to monitoring services and functionality of servers it could be beneficial to monitor the availability and functionality through the network. It is best practice to test this service from the point from which it will be used later on. This ensures that also components in between are configured correctly such as a firewall and its corresponding rule set. An example for the Web Interface would look as follows:

The NetScaler is requesting a page from the Web Interface and is testing if this request is replied and the reply is also delivering the expected result. If this test is successfully the Web Interface is reachable and delivering the correct page. If this is not the case a SNMP Trap can be sent out. In case the NetScaler is also acting as a Load Balancer it will remove this failing service out of the Load Balancing alliance.

Depending on the architecture it can become useful to monitor different services. For an Access Gateway Enterprise it can be as follows:

<table>
<thead>
<tr>
<th>Service</th>
<th>System</th>
<th>Test Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Interface</td>
<td>All Web Interface Instances</td>
<td>Web Interface Monitor (NetScaler)</td>
</tr>
<tr>
<td></td>
<td>TCP 80 (or WI InstancePort)</td>
<td></td>
</tr>
<tr>
<td>XMLService / Secure Ticket Authority</td>
<td>All XenApp which are assigned in the architecture for that role</td>
<td>XML Service Monitor (NetScaler)</td>
</tr>
<tr>
<td></td>
<td>TCP 80 (or XML Service Port)</td>
<td></td>
</tr>
<tr>
<td>AD Authentication</td>
<td>Relevant AD Controller</td>
<td>LDAP Monitor (NetScaler)</td>
</tr>
<tr>
<td></td>
<td>TCP 389 (or LDAP Port)</td>
<td></td>
</tr>
</tbody>
</table>

The upside of this method is that all monitors create load. Compared to that load the outcome of these tests is better as functionality and accessibility are tested from the point the services will be used. If the setup is correct the administrator is possible to have a quick overview in the NetScaler GUI which services are up and which are down.

## 2.5 Monitoring Advanced Access Control and Web Interface

### 2.5.1 Types of Monitoring

Both software components are based on Microsoft Server technology and can be monitored with the already mentioned monitoring types. These two types of components should be enhanced with performance counters of the Internet Information Service as both software components are using the Internet Information Services.
2.5.2 Monitoring with a Hardware Load Balancer

Monitoring of Advanced Access Control and Web Interface can also be enhanced through a Hardware Load Balancer. This will ensue that the load management and high availability are effectively performed. Doing so requires the corresponding monitor to be assigned to the services.

2.5.3 Critical components

On a server running the IIS the monitoring should include the following services:

- WWW Publishing Services
- IIS Administrator
- Citrix MFCOM Services
- IIS Worker Process (w3wp.exe)

Enhancing the default performance counters like CPU, Memory and Disk size with this type of counters allow monitoring the health of the server and its services. These counters and thresholds must be customized to reflect the used system at a customer site.

2.6 Monitoring XenServer

XenServer as a hosting infrastructure of a Delivery Center is at a very important place it should be monitored like such. Details about the possibilities of monitoring a XenServer are found in chapter 5 of the XenServers Administrators Guide.

2.6.1 XenCenter Alerts

XenServer has the possibility to create alerts based on defined performance thresholds in a defined time period. These alerts can be created with the current XenServer version for CPU, network and local hard disk of virtual machines and disks of the XenServer. These alerts are created in XenCenter and can send these alerts via SMTP to administrators.

The XenCenter configuration looks as follows:
2.6.2 Syslog

Another or an additional option of monitoring a XenServer is the possibility to log events on a Syslog server. Establishing such a monitoring solution requires a Syslog server in the infrastructure of the customer. The Syslog server receives all system messages of a XenServer or the Resource Pool and is archiving the events. These events can be analyzed on the Syslog server and depending on the Syslog implementation it can be possible to define actions on receiving critical events. The following screenshot is showing an extract of a typical Syslog system:

2.6.3 Additional Monitoring options

In addition to the already discussed monitoring types for XenServer options the following options are available:

- **SNMP**: [CTX116187](#) - How To Add SNMP Support to a XenServer Host
- **Monitoring Agents (OEM)**: Vendors running XenServer as an OEM Version already have implemented their own options to monitor a XenServer. These agents can report to centralized systems and integrate into existing monitoring solutions.
- **Monitoring Agents (3rd Party)**: Companies like Tevron, Hyperic or Splunk are enhancing the management and monitoring possibilities with their own software in a XenServer environment.

2.7 Monitoring XenDesktop

Monitoring the three main components of XenDesktop (Web Interface, Desktop Delivery Controller and Virtual Desktop Agent) different technologies need to be combined. This section
2.7.1 Desktop Delivery Controller (DDC)

Critical component of monitoring the DDC is the pro-active monitoring of the Citrix system services and the Eventlog on the DDC. The following screenshot is showing the system services on a DDC:

Furthermore on enhancing the capabilities of monitoring a DDC, scripts based on PowerShell can be implemented and the output can be analyzed. An overview of the options with PowerShell in a XenDesktop environment can be found at http://community.citrix.com/x/jwCvAg.

2.7.2 Virtual Desktop Agent (VDA)

Monitoring the VDAs can be realized by utilizing Citrix EdgeSight. More information can be found in chapter 3 of this document.

Additionally to that the XenServer monitoring can be used to create alerts based on CPU, memory and hard disk usage.

2.7.3 Outlook

These limited options of monitoring XenDesktop will be enhanced in near future and will reach the level of possibilities such as a XenApp environment.

2.8 Monitoring Citrix Provisioning Server

2.8.1 Monitoring possibilities

Citrix Provisioning Server is based on Microsoft Server architecture and can therefore be monitored with all monitoring options as all other windows-based systems.

2.8.2 Additional considerations

Depending on the location of placing the Write Cache for the vDisk clients it can become necessary to monitor the disk or partition on which the Write Cache resides. The amount of provisioned systems and the Write Cache can load and possibly overload a partition or disk.
2.9 Monitoring Citrix License Server

The Citrix License server is serving as the licensing repository for the entire Citrix infrastructure. Some products such as XenApp can work for some time without a functioning licensing server. In this example the XenApp server itself will act as license server for 30 days. Other products like for example Advanced Access Control is not able to provide this service without a Citrix license server.

Citrix components which are working without a license server (limited to time):

- Citrix XenApp (30 days)
- Citrix XenDesktop (30 days)

Citrix components which are not able to work without a license server or license:

- NetScaler / Access Gateway Enterprise
- Access Gateway Standard und Advanced
- XenServer (not using Citrix license server at current version)
- Provisioning Server (5 Minute Shutdown)

2.9.1 Types of monitoring

The logon workflow in a Citrix infrastructure can be affected by the Citrix license server. If the license server is not capable of providing licenses in the required time it can negatively affect the logon process. The license server should have enough resources available to perform reasonable even during rush hours of logon.

The monitoring of a Citrix license server should additionally to CPU, memory and disk include the value of time it takes to check out a Citrix license. This value can be measured with the performance counter “LastRecordedLicenseCheck-OutResponseTime”. This performance counter should be customized and gets a threshold depending on the used hardware for the Citrix license server.
3. EdgeSight Monitoring

3.1 Overview

Citrix EdgeSight is an End-to-End Monitoring which is recording processes, resources, network utilization on desktop system as well as on Citrix Presentation Servers / XenApp Servers. This data will be monitored during a user is working with the respective device. The captured data will be sent to the EdgeSight Server for central archiving and data analysis. Within the EdgeSight Console administrators or permitted staff are able to analyze the recorded data with mechanisms like Realtime Dashboard, Realtime alerts, Remote Reports and historical reports.

Citrix EdgeSight support assistance in the following sections:

- **Application support** – Monitoring and controlling if an application starts properly, is hanging, creates errors or crashes. Furthermore application utilization and trends can be monitored. It can also create application crash dump files for further analysis.

- **Problem solving** – Condition of monitored systems at the time an error is occurring. It is also capable of monitoring if resources are not released properly after closing an application. It can also deliver information if hardware changes may lead to application issues.

- **Capacity planning and System state** – Testing if the existing hardware would support Operating System upgrades or application upgrades. Comparison of performance data in real-time or using historically data.

- **XenApp Farm Health Monitoring** – Collecting of logon data and login times as well as session information of ICA Sessions.

The architecture of EdgeSight integration could look like the following drawing:

The client component of EdgeSight can also be installed in a virtual desktop environment like XenDesktop. To do so the client component can already be integrated in the image of a XenServer and Provisioning Server environment.

EdgeSight Server can be configured to create alerts which can be forwarded to a central monitoring system or sending an email with the alert to the administrational team.
The EdgeSight Console on analyzing an environment can be as follows:

3.2 Suggestions for data analyzing

It is recommended in a Citrix infrastructure to monitor the CPU utilization, Memory consumption and free disk space in general. In addition to these counters depending on the monitored system the counter set needs to be extended.

On a XenApp Server for example additional performance counter such as Disk Queue Length can offer information about a possible shortage on the disk. In a XenApp environment it is also crucial to monitor services. Recommended services to be monitored are:

- Print Spooler
- Independent Management Architecture Service
- XML Service
- License Server Communication
- Zone Data Collector election
- Load Balancing for XenApp Servers
- Citrix Hotfix Level
- Network Traffic (considering Backend Traffic, ICA, etc.)
This list may only be used as a base foundation for analyzing data and should be extended reflecting the customer’s environment and its requirements.

Analyzing the Eventlog via the EdgeSight Console should be done, as applications sometimes log errors in the Eventlog. Additionally user profile problems are logged in the Eventlog. EdgeSight sometimes delivers more information on application crashes than the Eventlog depending on the architecture of the software.

### 3.3 Active Monitoring of applications

The addition of active monitoring enables IT administrators to schedule scripted tests of live production applications to check that the application is available to users and also that it is responsive. A single user can be scheduled to log into an application from any site and at any time. This test is monitored against performance thresholds set by the administrator producing real time alerts if the thresholds are breached. In the event of an alert, EdgeSight presents the administrator with all of the contextual performance information for the alert to enable fast resolution to the performance issue.

The architecture of Active Monitoring of applications is looking like the following drawing:

![Diagram of Active Monitoring](image)

### 3.4 EdgeSight for NetScaler

EdgeSight for NetScaler transparently instruments client HTML pages, monitoring Web application response time as experienced by end users. This integrated approach to Web application monitoring provides detailed statistics on the trip duration of requests and responses across the web and provides IT managers with granular visibility to the components of application performance.

EdgeSight for NetScaler application monitoring console provides both real-time and historical views to Web application performance. IT administrators are able to monitor the responsiveness of all web applications in real-time to proactively identify potential problems before users are affected. By intelligently aggregating and presenting this data on a historical basis, application managers can better understand how the application performance of individual web pages has changed over time.
4. Integration of Different Types of Monitoring

By mixing the types of monitoring it should always be considered that monitoring itself needs resources. The monitoring architecture should only monitor as much as needed to be able to maintain a system and to see the system state of a server and the services provided on that system. It is necessary to avoid overlapping of monitoring solutions as this overlapping is not creating new information. The overlapping only creates an overhead on the monitored system. The mix itself needs to be adjusted depending on which system it will be implemented. It also needs to be customized in every customer environment to reflect the used infrastructure.

Designing the monitoring components is key to avoid overlapping and to allow reporting into a centralized system. It is not recommended to use too many graphical interfaces to display the measured values and/or the system state of systems. It is desirable that all used types of monitoring are capable of forwarding their alerts, counters, etc. to one central instance. This allows the people of monitoring the system to have an overview of the entire environment within one GUI. Changes in the environment need to be incorporate quickly into the monitoring as otherwise inconsistencies may occur and alerts are sent out useless as the system may be down for maintaining reasons.
An overview of the entire possibilities of monitoring can be summarized in the following graphic on base of the Citrix infrastructure the DSV – Deutscher Sparkassenverlag was providing:
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.

<p>| Version History |
|-----------------|-----------------|-----------------|-----------------|</p>
<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Version</th>
<th>Change Log</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael Palesch Principal Consultant Consulting Services Central Europe</td>
<td>1.0</td>
<td>Initial documentation</td>
<td>March, 6th, 2009</td>
</tr>
<tr>
<td>Thomas Berger Principal Consultant Consulting Services Central Europe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Holger Füßler Senior Network Consultant Consulting Services Central Europe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tarkan Koçoğlu Senior Architect Worldwide Field Readiness &amp; Productivity</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version History

Author(s) | Version | Change Log | Date
--- | --- | --- | ---
Michael Palesch Principal Consultant Consulting Services Central Europe | 1.0 | Initial documentation | March, 6th, 2009
Thomas Berger Principal Consultant Consulting Services Central Europe | | | |
Holger Füßler Senior Network Consultant Consulting Services Central Europe | | | |
Tarkan Koçoğlu Senior Architect Worldwide Field Readiness & Productivity | | | |

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.