Operations Guide: Monitoring

Table of Contents

Introduction

After a new XenDesktop, XenApp or Provisioning Services environment has been designed and rolled out to production, ongoing monitoring is required. Monitoring the new environment enables administrators to address issues proactively. By having an in-depth understanding of current and expected behavior of the various components, administrators are better equipped to discover an issue before it impacts the user community. Furthermore the data tracked during normal operations can be used for trending and capacity planning.

Citrix recommends implementing a monitoring solution, which covers all aspects of an IT environment and allows aggregating all captured data within a single tool or console. This simplifies correlating events or counters of multiple components and enables administrators to easily get an end to end overview. This can decrease the time required to determine the root cause of an issue significantly.

The remaining sections of this document identify the components, performance counters and events which should be monitored during normal operations. Furthermore basic remediation strategies will be provided.

This document is organized as follows:

- **Infrastructure Monitoring:** Within this section details about monitoring key infrastructure components are shared.

- **Performance Monitoring:** This section outlines the key performance counters, which should be tracked within every environment. Furthermore troubleshooting and remediation strategies as well as growth tracking will be discussed.

- **Event Monitoring:** Within this section monitoring of the Windows event log is discussed and links to event log reference documentations are provided.

- **Windows Services:** This section outlines the Citrix and Windows services which play a critical role within XenDesktop, XenApp or Provisioning Services environments. In addition information about the criticality of every service is provided.

- **Availability Monitoring:** Options for monitoring the functionality of services leveraging additional Citrix products or features is discussed within this section. In addition information about the impact of an outage of specific Citrix components is provided.

Infrastructure Monitoring

There are several key aspects which make up the infrastructure supporting the Citrix environment. Among these server hardware as well as the Ethernet networks play a prominent role. It is critical that each area is being monitored effectively since a problem in either could impact the overall performance and availability of the Citrix environment.

Network Monitoring

Most Citrix components and services (such as XenDesktop, XenApp or Provisioning Services) rely on a fast and stable network connection. Therefore it is vital to monitor the availability as well as the performance (such as available bandwidth and latency) for all WAN and significant LAN connections continuously.

Citrix recommends monitoring the following aspects of a network closely:

- **Availability.** An enterprise network consists of a variety of components, which function together to provide the network services. Each individual component such as a firewall, a router or an individual port plays a critical role and its availability needs to be monitored continuously. In addition, an End-to-End monitoring solution, which verifies the network functionality from a client perspective, is highly recommended.

- **Performance.** The effective performance of a network connection is comprised of the following variables:
  Note: *This section will focus on ICA/HDX connections and Provisioning Services vDisk streaming, since these types of network traffic have the largest footprint within typical Citrix environments.*
  - **Available Bandwidth.** Within an ideal world scenario without latency, available bandwidth is maximum physical bandwidth minus currently used bandwidth. In real world scenarios the maximum available bandwidth depends on the latency of a network connection. This is caused by the congestion control protocols, which are built into TCP (please refer to http://en.wikipedia.org/wiki/Transmission_Control_Protocol for more information). Therefore bandwidth monitoring should factor in the latency characteristic of a network connection. The ICA/HDX protocol will automatically adjust to low bandwidth scenarios to ensure a good user experience. However, Provisioning Services (PVS) cannot and active target devices will experience performance problems in a congested network.

  - **Latency.** The latency of a network connection impacts the effective performance perceived by ICA/HDX users and users of PVS target devices. Latency causes slow screen updates and mouse/keyboard input lag for ICA/HDX users and cause slow system and application performance as well as cause system instabilities in PVS. The maximum recommended latency for ICA/HDX connections depend on the use case and cannot be named exactly. For PVS connections the latency should be as low as possible. Therefore PVS servers and target devices should be located within the same data center leveraging a direct network connection.

Citrix recommends monitoring both counters at short intervals (i.e. 30 seconds or less), because even short periods of bandwidth congestion or high latency will impact users (ICA/HDX connections) or PVS targets.

- **Quality.** If network packets are lost in transit and need to be retransmitted overall performance of the network service suffers. Therefore packet loss and packet retransmission should be monitored for all WAN and critical LAN connections. In case any of these counters report unusual high values a detailed analysis of the root cause needs to be performed.

Hardware Monitoring

Because physical servers provide the foundation for all Citrix infrastructure it is important to monitor the availability of the servers as well as the individual server components (i.e. fan speed, power supplies voltages, hard disk faults, CPU temperature, etc.). This monitoring ensures administrators are kept abreast of any hardware component that is about to fail or is entering a failed state.

Most hardware vendors have their own proprietary tools for monitoring their hardware. These tools usually involve software agents that reside on the hardware that capture and forward events to an SNMP-based monitoring solution. Most solutions will alert administrators through email or text messages when thresholds are crossed or errors are detected. Some solutions even allow administrators to define automatic actions to take in the form of scripts or commands when an alert is triggered. Therefore Citrix strongly recommends leveraging the monitoring agents provided by the hardware vendors, whenever possible.

Performance Monitoring

This section describes the objects, counters and thresholds that are recommended to monitor for environments running XenDesktop, XenApp and Provisioning Services. The thresholds presented are based on real world experience but may not apply to all environments. Organizations will need to perform their own baselining, validity testing and validation before implementing within a production environment.
Please note that some hypervisors, such as VMware vSphere, provide specific performance counters for tracking CPU and Memory utilization within virtual machines (i.e. "VM Processor \ % Processor Time"). These performance counters should be used instead of the counters listed below.

The following table describes the performance counters recommended by Citrix Consulting for monitoring Citrix environments. These counters are considered to be a baseline that applies to XenApp, XenDesktop, and Provisioning Services implementations as well as Web Interface and SQL servers. The threshold values shown also apply to all kinds of systems.

System Performance Counters

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting / Remediation
Processor - % Processor Time	% Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the duration of the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.	80% for 15 minutes	90% for 15 minutes	Identify the processes/services consuming processor time using Task Manager or Resource Monitor. • If all processes/services work within normal parameters and the level of CPU consumption is an expected behavior it should be considered to add additional CPU resources to this system in the future. • If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting / Remediation
System - Processor Queue Length	Processor Queue Length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than 10 threads per processor is normally acceptable, dependent of the workload.	5 (per Core) for 5 minutes	10 (per Core) for 10 minutes	A long CPU queue is a clear symptom of a CPU bottleneck. Please follow the steps outlined for counter "**Processor** - % Processor Time"
Memory – Available Bytes	Available memory indicates the amount of memory that is left after nonpaged pool allocations, paged pool allocations, process' working sets, and the file system cache have all taken their piece.	<30% of total RAM	<15% of total RAM	Identify the processes/services consuming memory using Task Manager or Resource Monitor. • If all processes/services work within normal parameters and the level of memory consumption is an expected behavior it should be considered to add additional memory to this system in the future. • If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
Memory – Pages/sec	Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults.	>10	>20	A high value reported for this counter typically indicates a memory bottleneck, except if "**Memory** – Available Bytes" reports a **high** value at the same time. In this case most likely an application is sequentially reading a file from memory. Please refer to KB139609 for further information.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting / Remediation
Paging File - %Usage	This is the percentage amount of the Page File instance in use.	>40%	>70%	Review this value in conjunction with "**Memory** - Available Bytes" and "**Memory** - Pages/sec" to understand paging activity on the affected system.
LogicalDisk/ PhysicalDisk - % Free Space	% Free Space is the percentage of total usable space on the selected logical disk drive that is free.	<10% of physical disk	<5% of physical disk	Identify which files or folders consume disk space and delete obsolete files if possible. In case no files can be deleted, consider increasing the size of the affected partition or add additional disks.
LogicalDisk/ PhysicalDisk - % Disk Time	% Disk Time marks how busy the disk is.	>70% consistently	>90% consistently	Identify the processes / services consuming disk time using Task Manager or Resource Monitor. • If all processes/services work within normal parameters and the level of disk consumption is an expected behavior it should be considered to move the affected partition to a more capable disk subsystem in the future. • If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
LogicalDisk/ PhysicalDisk – Current Disk Queue Length	Current Disk Queue Length provides a primary measure of disk congestion. It is an indication of the number of transactions that are waiting to be processed.	>=1 (per spindle) consistently	>=2 (per spindle) consistently	A long disk queue length typically indicated a disk performance bottleneck. This can be caused by either processes/services causing a high number of I/Os or a shortage of physical memory. Please follow the steps outlined for counter "**LogicalDisk/PhysicalDisk** - % Disk Time" and counter "**Memory** – Available Bytes"

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting / Remediation
LogicalDisk/ PhysicalDisk – Avg. Disk Sec/Read – Avg. Disk Sec/Write – Avg. Disk Sec/Transfer	The Average Disk Second counters show the average time in seconds of a read/write/transfer from or to a disk.	>=15ms consistently	>=20ms consistently	High disk read or write latency indicates a disk performance bottleneck. Systems affected will become slow, unresponsive and application or services may fail. Please follow the steps outlined for counter "**LogicalDisk/PhysicalDisk** - % Disk Time"
Network Interface – Bytes Total/sec	Bytes Total/sec shows the rate at which the network adaptor is processing data bytes. This counter includes all application and file data, in addition to protocol information, such as packet headers.	< 8 MB/s for 100 Mbit/s adaptor <80 MB/s for 1000 Mbit/s adaptor	None	Identify the processes / services consuming network using Task Manager or Resource Monitor. • If all processes/services work within normal parameters and the level of bandwidth consumption is an expected behavior it should be considered to move the respective process/service to a dedicated NIC (or team of NICs). • If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.

Table 1: Generic performance counters which apply to Citrix environments

XenApp Performance Counters

The following represent performance counters specific to a XenApp environment that should be monitored in addition to ensure any issues involving XenApp performance are detected early and addressed appropriately. Please note these counters are listed under the **Citrix MetaFrame Presentation Server object**.

Metric	Description	Warning (Yellow)	Critical (Red)	Applies to
Citrix MetaFrame Presentation Server				
Application Resolution Time (ms)	The time in milliseconds that a resolution took to complete. This is also the time required to determine the "least-loaded" server during an application launch. A baseline would need to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values	• All XML Brokers
DataStore Connection Failure	The number of minutes that the XenApp server has been disconnected from the data store. Threshold should take into account events such as reboots and scheduled maintenance.	>=1	None	• All XenApp Servers
Number of busy XML threads	The number of XML threads currently being processed. There are 16 worker threads in the Citrix XML Service. A count of 16 or more shows that XML requests are not being processed in a timely manner.	>=10 consistently	>=16 consistently	• All XML Brokers
Resolution WorkItem Queue Ready Count	The number of resolution work items (related to application launches) that are ready to be executed. A value above 0 indicates that requests are being queued while IMA handles other requests.	None	>=1	• All XML Brokers • All XenApp Controllers
WorkItem Queue Ready Count	The number of work items that are ready to be executed. A value above 0 indicates that requests are being queued while IMA handles other requests. This counter should not be over 1 for an extended period of time.	None	>=1	• All XML Brokers • All XenApp Controllers

Citrix Licensing				
Citrix Licensing – License Server Connection Failure	Displays the number of minutes that XenApp has been disconnected from the License Server.	>1 minute	>1440 minutes	• All XenApp Servers
Citrix Licensing – Last Recorded License Check-Out Response Time	Displays the last recorded license check-out response time in milliseconds. A value of more than 5000 milliseconds indicates a performance issue at the license server.	>2000ms	>5000 ms	• All XenApp Servers

Table 2: XenApp Performance Counters

Tracking XenApp Growth

The following metrics should be used to track the growth of the infrastructure. Therefore thresholds will not be discussed.

Metric	Description
System Counters	
Process – Private Bytes – ImaSrv	The current size, in bytes of memory that this process (IMA) has allocated and cannot be shared with other processes.
XenApp Counters	
Application Resolutions/sec	The number of resolutions (applicable launch requests) per second.
Application Enumerations/sec	The number of non-XML-based enumerations (requests for application lists) per second.
Filtered Application Enumerations/sec	The number of XML-based enumerations (requests for application lists) per second.
Terminal Services – Total Sessions	Total number of Terminal services sessions.
Citrix Licensing – Average License Check-Out Response Time (ms)	Displays the average license check-out response time in milliseconds. Please note that network congestion can influence the values reported.

Table 3: Performance Counters to track growth of XenApp environment

Web Interface Performance Counters

The following represent performance counters applicable to Web Interface servers that should be monitored, in addition to the general Windows performance counters outlined earlier within this section.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting / Remediation
ASP.NET – Request Queued	The number of requests waiting to be processed by ASP. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values	In case the queue length exceeds the critical limit requests may be rejected. In this case it should be considered to add additional Web Interface servers to the load balancing team in order to distribute the load across more nodes.
ASP.NET – Requests Rejected	The number of requests rejected because the request queue was full.	None	>=1	When this limit is exceeded, requests will be rejected with a 503 status code and the message "Server is too busy." Please follow the steps outlined for counter "**ASP.NET** – Request Queued"

Table 4: Performance Counters to monitor for Web Interface

Tracking Web Interface Growth

The following metrics should be used to track the growth of the infrastructure, therefore threshold alerting do not apply.

Metric	Description
Web Interface Counters	
ASP.NET – Requests Current	The current number of requests, both executing and queued.
ASP.NET – Request Execution Time	The amount of time (in milliseconds) that it took to execute the most recent request.
Web Service – Concurrent Connections	Current Connections is the current number of connections established with the Web service.

Table 4: Performance Counters to track growth of Web Interface environment

XenDesktop Performance Counters

The following represent important performance counters specific to a XenDesktop 5.x environment. The performance counters should be monitored, in addition to the general Windows performance counters outlined earlier within this section, as a best practice so that any issues are detected early and addressed appropriately.

XenDesktop Counters				Troubleshooting / Remediation
Metric	**Description**	**Warning (Yellow)**	**Critical (Red)**	
Database Avg. Transaction Time	The time on average, in seconds, taken to execute a database transaction. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values	In case the reported values exceed the baseline response time constantly, a potential performance issue needs to be investigated at the SQL server level.
Database Connected	Indicates whether this service is in contact with its database. (1 is connected; 0 is not connected)	None	None	Both values report connectivity issues of the XenDesktop Broker service with the XenDesktop database. In case issues are reported, SQL server and network availability needs to be verified.
Database Transaction Errors/sec	The rate at which database transactions are failing.	None	>0	

Table 6: XenDesktop Performance Counters to monitor

Tracking XenDesktop Growth

The following metrics should be used to track the growth of the infrastructure, therefore threshold alerting do not apply.

Metric	Description
Citrix Broker Service – Brokered Sessions	The number of virtual desktop sessions brokered by the Citrix Broker Service.
Citrix XML Service – Avg. Transaction Time (Instances: "Enumerated Resources", and "Launch *"	The time on average, in seconds, taken to process an XML transaction in Citrix Broker Service.

Table 7: Performance Counters to track growth of XenDesktop environment

XenServer Monitoring

When implementing a Citrix virtualization solution such as XenApp or XenDesktop monitoring is a key factor in ensuring high availability and optimal performance. It is just as important to monitor the hosting infrastructure supporting the XenApp or XenDesktop environments. Through XenCenter, XenServer is capable of alerting administrators when certain events of importance occur in the environment.

In XenCenter, alerts can be defined on each VM when:

- CPU usage exceeds a percentage level
- Network usage exceeds specified KB/sec
- Disk usage exceeds specified KB/sec

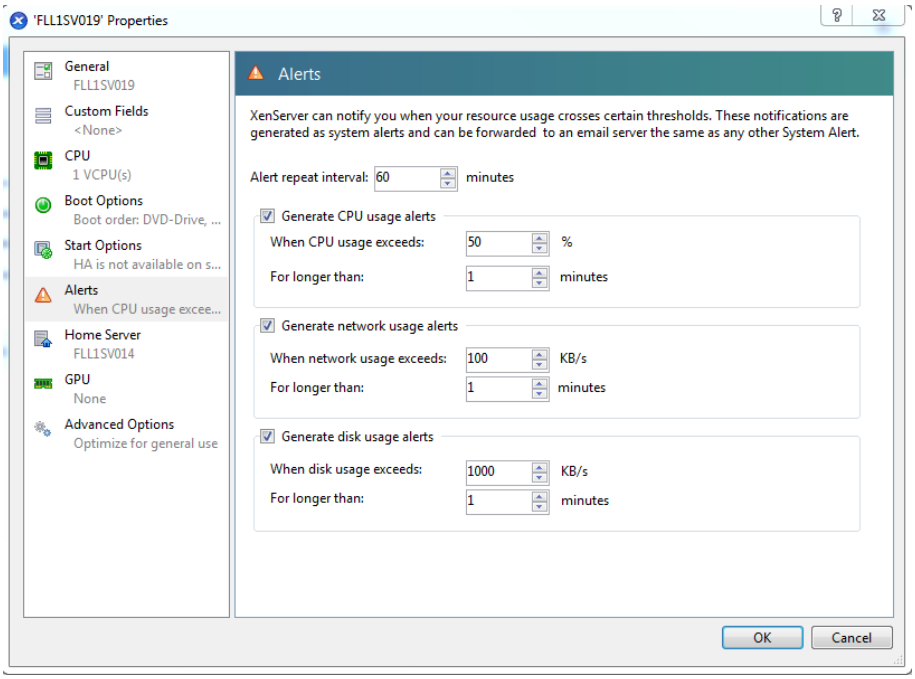

Figure 1: XenServer Alerts Property Page

The XenServer host or the entire pool can be configured to send email alert notifications via SMTP to system administrators.

Workload Balancing

Workload Balancing is a XenServer component, packaged as a virtual appliance that allows creating reports about VM performance in a XenServer environment. Furthermore it evaluates resource utilization and locates virtual machines on the best possible hosts in the pool for their workload's needs. Even if an automatic load balancing of the workloads is not required within an environment Workload Balancing should be implemented for reporting reasons.
Because Workload Balancing captures performance data, it is possible to use this component to generate reports, known as Workload Reports, about a virtualized environment. Workload Reports provide data for a pool or host's health, for auditing, optimizations, and placement (or motion) history. Also, an organization can run a chargeback report that shows virtual machine usage and can help measure and assign costs.
As mentioned earlier, it is not necessary to configure Workload Balancing to make VM placement recommendations or move virtual machines for monitoring and chargeback functionality. However, it is required to configure the Workload Balancing component and the XenServer Resource Pool and, ideally, set critical thresholds to values that reflect the point at which the performance of the hosts in the pool degrades.

For more information, please refer to the XenServer Workload Balancing User Guide.

XenServer Virtual Machine Performance Utility

Although the XenServer Virtual Machine Performance Utility is not a monitoring tool, it can help troubleshooting performance related issues, which is why it will be highlighted within this document.
The XenServer Virtual Performance Utility is a XenServer virtual machine that helps troubleshoot performance related issues, such as poor performance caused by storage I/O and network I/O. The virtual machine, built on Debian Linux, equips with following test utilities and is accessible using a Web based user interface:

- **Disk I/O performance utility** - It can be used to conduct the following disk I/O operations to measure: sequential read/writes and random read/writes with various specified block sizes. This performance testing utility assesses the performance of a given Storage Repository by reading and writing data to a test virtual disk, created by the user specifically for this test.
- **Network I/O performance utility** - It is essentially a modified version of Netperf. Additional information about Netperf can be found at http://www.netperf.org. Netperf runs on the backend and provides end-to-end request/response round trip latency and TCP/UDP throughput tests.

Further information can be found in CTX127065 – XenServer Virtual Machine Performance Utility.

Event Monitoring

Monitoring the Windows Event Log for unknown or critical events can help discover issues proactively and allows administrators to understand event pattern. Citrix recommends monitoring the Windows event logs of all Windows servers closely and investigate for errors pertaining to:

- **Licensing**. Errors in the event log dealing with Terminal Services licensing should be investigated. This might be a result of the installed Citrix product not being able to contact the Terminal Services Licensing Server or the Citrix Licensing Server. If errors in the event log are not reviewed, users might eventually be denied access because they cannot acquire a valid license.

- **Hardware Failure**. Any event notification that relates to a hardware failure should be looked at immediately. Any device that has failed will have an impact on the performance of the system. At a minimum, a hardware failure will remove the redundancy of the component.

- **Security Warnings**. Customers should investigate security warnings or audit failure events regarding failed logons in the security log. This could be an indication that someone is attempting to compromise the servers.

- **Disk Capacity**. As the drives of a Windows system reach 90% of capacity, an event error message will be generated. To ensure continuous service, customers should poll these event errors. As the system runs out of hard disk space, the system is put at severe risk. The server might not have enough space left to service the requests of users for temporary file storage. As the space becomes used, customers should analyze and determine where space is being used and clean up the drives.

- **Application / Service errors.** Any event notification that relates to application or services errors should be investigated. All Citrix software components will leverage the Windows Event Log for error logging. A list of the known Event Log warnings and errors issued by Citrix components can be found at the following links:

    - Event Codes Generated by PVS
    - XenDesktop Broker Event Log Messages
    - XenDesktop VDA Event Log Messages
    - XenDesktop MCS Event Log Messages
    - XenApp Critical Event Viewer Messages
    - Web Interface - Logged Messages and Event IDs

It is important to periodically check the Event Viewer for Citrix related warnings or errors. Warnings or errors that repeatedly appear in the logs should be investigated immediately, because it may indicate a problem that could severely impact the Citrix environment if not properly resolved.

In multi-server environments it becomes easier to administer the servers when logs can be collected and reviewed from a central location. Most enterprise grade monitoring solutions provide this functionality. More sophisticated monitoring solutions enable an administrator to correlate event information with other data points such as performance metrics or availability statistics. In case the selected monitoring solution does not provide this functionality the Windows 2008 R2 EventLog subscription feature can be used. This feature allows administrators to receive events from multiple servers and view them from a designated collector computer. Please see Microsoft TechNet article on how to set this up.

XenServer is also capable of sending its logs to a central syslog server. The administrator sets the IP address of the syslog daemon server in the properties of each XenServer in the pool. This configuration allows administrators to capture real-time activity across multiple XenServer hosts. Further information can be found within the XenServer Admin Guide.

Windows Services

Windows Services that are critical to basic server functionality should be automatically monitored to ensure that they are running properly. The following section provides a list of the common Windows services that should be monitored. The recommended recovery actions for the services listed below are as follows:

- First failure: Restart the Service
- Second Failure: Restart the Service
- Subsequent Failures: Put the server in maintenance mode and investigate the root cause

XenApp Servers

The following services are considered core to a XenApp infrastructure and should be monitored on all XenApp servers as a best practice.

Service Name	Functionality	Risk
Citrix Independent Management Architecture	Provides management services and server-to-server communication for Citrix products. *Dependencies:* • IPSEC Services • RPC Service • Server • WMI Driver Extensions • Workstation	Failure of this service results in the server not allowing any additional users. The server will also not respond to IMA communications from the management console or from any other Citrix component.
Citrix XML Service	Provides an HTTP interface to the ICA browser. It uses TCP packets instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80. Frequently, the Citrix XML Service is plugged into IIS. Therefore the Citrix XML Service may not appear. This does not present a problem. *Dependencies:* • Independent Management Architecture Service • WMI Driver Extensions	The failure of the Citrix XML Service is critical on the zone data collectors. These servers are utilized when the Web Interface tries to determine the least loaded server. If this server fails, the Web Interface will look at the backup server. This can slow down the application enumeration and launching process.
	The Secure Ticket Authority (STA) service is embedded into the Citrix XML service.	Is used by the Access Gateway and Web Interface to create and validate secure tickets. Generally more than one STA is specified for fault tolerance however it should be monitored.

Service Name	Functionality	Risk
Citrix XTE Server Service	Provides necessary Session Reliability. *Dependencies:* None	This service needs to be monitored if the Session Reliability is enabled.
Citrix CPU Utilization Management/Resource Management	Manages resource consumption to enforce entitlement policies *Dependencies:* • RPC Service	These services need to be monitored if CPU optimization is enabled. (Automatically started if CPU Optimization is enabled in the XenApp Console.)
Citrix CPU Utilization Management/User Session sync	Synchronizes the CPU Utilization Management user ID of a process with the user ID of the session owner of the process *Dependencies:* • Citrix CPU Utilization Management/Resource Management	
Citrix CPU Utilization Management/CPU Rebalancer	Installed on Windows Server 2003 multi-processor systems; it is not installed on Windows 2000 Server or servers with only one processor. The CPU Rebalancer service is used to alleviate a Microsoft issue that appears in environments where a lot of short-lived processes are started and stopped. Due to the performance impact the CPU Rebalancer service can have, by default it is set to "Manual." If your environment is running many short-lived applications that all appear to be running on the same CPU, setting the service to "Automatic" is recommended. The CPU Rebalancer service corrects this by balancing the load equally across processors.	Monitored if service is set to 'automatic'. (Set to 'manual' by default and must be manually configured to start automatically on Windows Server 2003 with multiple processors.)
Citrix Print Manager Service	Supports the Citrix Advanced Universal printing architecture *Dependencies:* • Print Spooler • RPC Service	This service needs to be monitored if the Citrix Advanced Universal Printer Driver is used
Citrix Virtual Memory Optimization	Dynamically optimizes applications running on the Citrix XenApp *Dependencies:* None	This service needs to be monitored if memory optimization is used (Automatically started if Memory Optimization is enabled in the XenApp Console.)

Service Name	Functionality	Risk
Citrix MFCOM Service	Provides access to necessary XenApp objects. This service will be present if the license server exists on a server running Citrix XenApp. *Dependencies:* • RPC Service • WMI Driver Extensions	
Remote Desktop Services/Terminal Services	Allows multiple users to be connected interactively to a machine as well as the display of desktops and applications to remote computers. *Dependencies:* • RPC Service	If the Remote Desktop Services service fails, the server will become inoperable requiring a reboot.
Citrix WMI Service	Citrix WMI Service is responsible for sending alerts to the WMI aware monitoring tools.	This service only runs when needed. The failure of the Citrix WMI Service will only result in not receiving updates to WMI aware monitoring tools from the WMI Provider. It will not put the server at severe risk, but it will hinder the ability to monitor the system.
Citrix Client Network	Maps client drives and peripherals for access in sessions. Applicable to XenApp 5 and older. *Dependencies:* • Client Drive Mapping (CDM) • WMI Driver Extensions • Workstation	On failure client drives and peripherals are not accessible.
Citrix Streaming Service/ Citrix Streaming Helper Service	Manages the Citrix Offline Plug-In when streaming applications. *Dependencies:* • RPC Service	On failure streamed applications cannot be accessed.
Server Service	Provides file, print and named-pipe sharing over the network for the server.	On failure the server will not accept new user sessions
Net Logon Service	Provides pass-through authentication of account logon events for systems in a domain.	On failure users of new sessions are unable to authenticate and users of existing sessions may not be able to access network resources.
Remote Procedure Call Service (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	On failure certain network services cannot be accessed.
Workstation Service	Creates and maintains client network connections to remote servers.	On failure certain network services cannot be accessed.

Service Name	Functionality	Risk
Print Spooler	Manages all local and network print queues and controls all print jobs.	On failure printing is not possible for users connected to this server.

Table 5: Services to monitor on XenApp Servers

XenDesktop Services

The following services are considered important for the operations of a XenDesktop environment and should be monitored on all XenDesktop Controllers as a best practice.

Service	Functionality	Risk
Citrix AD Identity Service	Manages Active Directory computer accounts. *Dependencies:* • WMI Service	Machine Creation Service relies on this service to create virtual machines. The machine account becomes tainted at the time of creation if this service is not able to sync with Active Directory.
Citrix Broker Service	Manages connections to virtual machines and applications.	If this service is stopped existing connections are not affected. No new connections can be established.
Citrix Configuration Service	Stores configuration information on the Citrix Services. *Dependencies:* • WMI Service	If this service is stopped, it will not be able to collect information from the Broker Services.
Citrix Diagnostic Facility COM Server Service	Manages and controls Citrix diagnostic trace sessions. *Dependencies:* • RPC Service	This service has no impact on the production environment. It is used to generate CDF trace files which aid in troubleshooting issues.
Citrix Host Services	Manages host and hypervisor connections. *Dependencies:* • WMI Service	It is not possible to connect to the virtual machines when this service is not available.
Citrix Machine Creation Service	Creates new virtual machines. *Dependencies:* • WMI Service	The ability to create virtual machines using Machine Creation Service will not be available if this service is stopped. Provisioning Services is not affected.
Citrix Machine Identity Service	Manages storage of virtual machines. *Dependencies:* • WMI Service	If this service is stopped XenDesktop is not able to manage the storage of the virtual desktops.

Table 6: XenDesktop Services to monitor

Provisioning Server Services

The following services are important to the operations of Provisioning Services for both XenApp and XenDesktop environments. These services should be monitored as part of the monitoring solution on all PVS servers.

Service	Functionality	Risk
Citrix PVS PXE Service	Provides the PVS PXE Boot Server functionality	On failure of this service target devices may not be able to boot successfully if PXE booting is leveraged.
Citrix PVS Stream Service	Streams contents of the vDisk to the target device on demand.	If this service stopped it will not be possible to stream vDisk images.
Citrix PVS SOAP Service	Provides framework for external or existing solutions to interface with Provisioning services.	If this service fails PVS Server to PVS Server communication as well as PVS Console to PVS Server communication is not possible.
Citrix PVS TFTP Service	Provides the TFTP Server functionality	On failure of this service target devices may not be able to boot if this server is used as TFTP server for the bootstrap.
Citrix PVS Two-Stage Boot Service	Provides the bootstrap functionality for devices booting by means of a BDM ISO file	On failure of this service target devices may not be able to boot if a BDM ISO file is used.

Table 7: Provisioning Services to monitor

Citrix Licensing Services

The following Licensing services should be monitored as part of the monitoring solution on the Citrix License Server.

Service	Functionality	Risk
Citrix License Service	Provides licensing service for Citrix products.	Licensing mode changes to grace period when service is stopped or License Server can't be contacted. If not monitored, functionality of Citrix products will cease after grace period expires.
Citrix Licensing WMI	The Citrix License Management Console collects license data information using the WMI service.	

Table 8: Citrix Licensing Services to monitor

Web Interface Services

The following services should be monitored on the server hosting Web Interface.

Service	Functionality	Risk
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. *Dependencies:* • HTTP • RPC Service	Access to XenApp published applications or published desktops will not be available through Web Interface if WWW services is not available.

Table 12: Web Interface Services to monitor

Availability Monitoring

Citrix provides multiple tools to allow an end-to-end monitoring of the functionality of a XenApp / XenDesktop infrastructure. This section will outline the most important monitoring tool sets, their functionality and how they can be integrated into existing monitoring solutions.

NetScaler Monitors

In addition to monitoring the availability of Citrix services running on servers, it is also important to monitor the availability of services through the network. This type of testing simulates how end users will access the Citrix environment in production, so components in between, such as firewalls can be validated that settings are properly configured.

The NetScaler appliance contains a number of built-in monitors that can be used to monitor services for XenApp/XenDesktop environments. The NetScaler also allows administrators to build custom monitors. To learn how to build custom monitors, see Configuring Monitors in a Load Balancing Setup.

The following table lists the built-in monitors available on NetScaler appliances, and which Citrix services they can be used to monitor. Citrix recommends configuring NetScaler to send SNMP traps to the central monitoring infrastructure in case any of the monitors reports an issue. The SNMP MIB can be downloaded at the download tab of the NetScaler GUI or directly from http://<nsip>/support/docs/snmp/HP-Openview/NS-MIB-smiv2.mib.

Monitor	Functionality	Recommended For
TCP-based applications	NetScaler appliance establishes a 3-way handshake with the monitor destination. It can be used to observe TCP or HTTP traffic, or send ping requests.	• Web Interface • License Server
SSL Services	Built-in secure monitors for TCPS and HTTPS. You can use the secure monitors to monitor HTTP as well as non-HTTP traffic. The NetScaler establishes a TCP connection. After the connection is established, the appliance performs an SSL handshake with the server.	• Web Interface • License Server
LDAP Services	The NetScaler periodically checks the LDAP service to which it is bound by authenticating and sending a search query to it. If the search is successful, the service is marked UP. If the LDAP server does not locate the entry, a failure message is sent to the LDAP monitor, and the service is marked DOWN.	• AD Authentication
XML Broker Service	The monitor opens a connection to the service and periodically probes the XML services to which it is bound. If the	• XML Service (XenApp & XenDesktop)

Monitor	Functionality	Recommended For
	server responds as expected within the configured time period, the monitor marks the service UP. If the service does not respond, or responds incorrectly, the monitor marks the service DOWN.	• Secure Ticket Authority
Dynamic Desktop Controller (DDC) Services	The monitor sends a probe to the DDC server in the form of an XML message. If the DDC responds to the probe with the identity of the server farm, the probe is considered to be successful, and the server status is marked UP. If the HTTP response does not have a success code or the identity of the server farm is not present in the response, the probe is considered to be a failure and the server's status is marked as DOWN.	• XenDesktop
Web Interface Services	The NetScaler appliance has two built-in monitor types for monitoring Web Interface servers. The CITRIX-WEB-INTERFACE monitors a dynamic page at the location specified by the site path. The monitor checks for critical failures in resource availability. The CITRIX-WI-EXTENDED monitor verifies the logging process with the Web Interface service. It verifies the validity of the login credentials, correct configuration of the monitor, and the connection to the IIS server.	• Web Interface

Table 13: Built-in NetScaler monitors for Citrix services

XenApp Health Check & Recovery

The XenApp Health Check and Recovery functionality provides the ability to monitor the state of the server farm and discover any health risks. This type of monitoring is based on a standard set of test scripts, which monitors several XenApp services. Aside from the standard set of tests that come with XenApp, additional tests may be imported, or custom tests may be developed.

When a test fails, a recovery action can be defined for the server to take. Administrators can also be alerted and take appropriate steps to remediate the issue. This can be achieved by configuring XenApp Health Check & Recovery to "Alert only" and constantly monitor the eventlog of the XenApp servers for ID 2005 with source "CitrixHealthMon" leveraging the central monitoring solution of an organization. The following are the list of standard Health Check and Recovery tests provided by default (for servers running XenApp 5.0 and older it is required to follow the steps outlined in CTX127154 in order to have access all tests discussed below).

Test	Functionality	Recommended For
Citrix IMA Service Test	This test queries the service to ensure that it is running by enumerating the applications available on the server.	• Data Collectors • XML Brokers • Member Servers
Logon monitor test	This test monitors session logon/logoff cycles to determine whether or not there is a problem with session initialization, or possibly an application failure. If there are numerous logon/logoff cycles within a short time period, the threshold for the session is exceeded and a failure occurs.	• Member Servers
Remote Desktop Services Test	This test enumerates the list of sessions running on the server and the session user information, such as user name.	• Member Servers
XML Service Test	This test requests a ticket from the XML service running on the server and prints the ticket.	• XML Brokers
Check DNS Test	The test performs a forward DNS lookup using the local host name to query the local DNS server for the computer's IP address. A failure occurs if the returned IP address does not match the IP address that is registered locally.	• Data Collectors • XML Brokers • Member Servers
Check Local Host Cache Test	This test ensures the data stored in the XenApp server's local host cache is not corrupted and that there are no duplicate entries. Citrix does not recommend running this test unless the environment is experiencing issues with local host cache corruption. This test can be CPU-intensive, so Citrix recommends using a 24-hour test interval, and keep the default test threshold and time-out values.	• Member Servers

Test	Functionality	Recommended For
Check XML Threads Test	This test inspects the threshold of the current number of worker threads running in the Citrix XML Service. When running this test, use a single integer parameter to set the maximum allowable threshold value. The test compares the current value on the XenApp server with the input value. A failure occurs if the current value is greater than the input value.	• XML Brokers • Member Servers
Citrix Print Manager Service Test	This test enumerates session printers to determine the health of the Citrix Print Manager service. A failure occurs if the test cannot enumerate session printers.	• Member Servers
Microsoft Print Spooler Test	This test enumerates printer drivers, printer processors, and printers to determine whether or not the Print Spooler Service in Windows 2008 is healthy and ready for use.	• Member Servers
ICA Listener Test	This test determines whether or not the XenApp server is able to accept ICA connections. The test detects the default ICA port of the server, connects to the port, and sends test data in anticipation of a response. The test is successful when the server responds to the test with the correct data.	• Member Servers

Table 14: XenApp Health Monitoring & Recovery tests

Impact of Failure of Citrix Components

The following table outlines the impact of failure of central Citrix components and how the risk of failure can be mitigated:

Component	Impact	Risk Mitigation
Shared: Citrix License Server	User logon will take up to 5 seconds longer until cold standby is online	**Backup Requirements:** Full weekly backups are recommended. Also full backups should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** Keep a snapshot of the license server stored in a location where rapid recovery can be assured. Because license files reference the name of the License Server, the backup License Server must have the same name as the primary License Server in order to use the same license files. **Restoration Procedures:** Use the snapshots of the License Server as a cold standby. These servers will have the same name as the primary License Server and will remain in a powered off state.
Shared: Citrix Web Interface Servers	Users will not be able to access virtual applications or desktops until Web Interface servers are back online.	**Backup Requirements:** Full weekly backups are recommended. Also full backups should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** The IIS service on the Web Interface servers should be monitored. Should a single Web Interface server fail, users will be automatically directed to the second Web Interface server. If all Web Interface Servers in a data center fail, users should be directed to Web Interface Servers in another data center. All Web Interface Servers query all Data Collectors and all XenDesktop Controllers. Any users with existing connections will be unaffected. **Restoration Procedures:** Recovery from backup media.

Component	Impact	Risk Mitigation
Shared: Citrix Provisioning Servers	Momentary pause as automated failover occurs. No additional impact when secondary server available. Frozen environment when there is no Provisioning Server available.	**Backup Requirements:** Full weekly backups are recommended and should include the primary vDisk store, backup vDisk store and Provisioning Server database. Also full backups should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** Automated failover between Servers in a Provisioning Services Site. vDisks must be distributed between servers for failover to work. **Restoration Procedures:** Recovery from backup media.
Provisioning Servers: PVS Database	No impact from single SQL Server node failure when a SQL Cluster or Mirror has been configured. Minimal impact when Offline DB Support has been enabled.	**Backup Requirements:** Full weekly backups are recommended. Also full backup should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** The database server should be mirrored or clustered and the PVS databases backed up. **Restoration Procedures:** Fail-over to the functional mirror / cluster node while performing restoration on the failed node. If necessary, the PVS database will be recovered from backup.
XenApp: Citrix ZDC/XML Servers	No impact from single Zone Data Collector failure. Additional time required to enumerate and launch applications/ desktops if both Zone Data Collectors fail	**Backup Requirements:** Full weekly backups of the XenApp vDisks are recommended. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** Two ZDC/XML servers should be implemented for each farm. If the Zone Data Collector fails, Citrix XenApp will automatically transfer this role over to the backup Zone Data Collector. Citrix XenApp Member Servers should be configured to automatically take over the Data Collector role if both dedicated Data Collectors fail. **Restoration Procedures**: Temporarily configure additional servers to be backup ZDC/XML server by adjusting election preference and at Web Interface. Build new operating system and install XenApp in parallel. When build is completed, return ZDC and XML configurations to the standard design.

Component	Impact	Risk Mitigation
XenApp: Citrix XenApp Member Servers	None when sufficient servers are available.	**Backup Requirements:** The Provisioning Services vDisks should be backed up separately. **Redundancy Design:** Install servers with sufficient overhead to host the expected number of users plus the amount of redundancy required. **Restoration Procedures**: Reboot XenApp Server to refresh operating system build. Restore vDisk from backup vDisk store/backup media if necessary.
XenApp: Citrix XenApp Data Store	No impact from single SQL Server failure No impact to users if database is unavailable although administrators will be unable to manage the farm	**Backup Requirements:** Full weekly backups are recommended. Also full backups should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** The database server should be clustered and the XenApp database should be backed up. **Restoration Procedures:** Fail-over to the functional cluster node while performing restoration on the failed node. If necessary, the XenApp database will be recovered from backup.
XenDesktop: Citrix XenDesktop Controllers	No impact from single XenDesktop Controller failure If all XenDesktop Collectors in a specific site are unavailable, new connections to virtual desktops hosted in that site will be unavailable	**Backup Requirements:** Full weekly backups are recommended. Also full backups should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** Multiple XenDesktop Controllers per site with hardware load balancers configured to load balance communications between the virtual desktops and the XenDesktop Controllers. The load balancers should also be configured to monitor the XML service on the XenDesktop Controllers. Should a single XenDesktop Controller fail, virtual desktop and Web Interface connections will be automatically directed to other Controllers. **Restoration Procedures:** Recovery from backup media.

Component	Impact	Risk Mitigation
XenDesktop: Citrix XenDesktop Database	No impact from single SQL Server failure New users will be unable to connect to a virtual desktop if database is unavailable. Any Users with existing connections will be unaffected	**Backup Requirements:** Full weekly backups are recommended. Also full backup should be taken prior to major changes or patching initiatives. Daily incremental backups will also help in mitigating the loss of daily changes to the environment. **Redundancy Design:** The database server should be mirrored or clustered and the XenDesktop databases backed up. **Restoration Procedures:** Fail-over to the functional mirror / cluster node while performing restoration on the failed node. If necessary, the XenDesktop database will be recovered from backup.

Table 15: Impact of failure of Citrix components

Product Versions

Product	Version
XenDesktop	5.0 / 5.5 / 5.6
XenApp	5.0 / 6.0 / 6.5
Provisioning Services	6.x

Revision History

Revision	Change Description	Updated By	Date
1.0	Finalized Document	Thomas Berger, Ed Duncan With feedback from: - Lisa Green – Principal Product Manager - Brendan Lin – Architect - Daniel Feller – Lead Architect - Scott Campbell – Service Delivery Manager - Michael Palesch – Architect - Norman Wright – Director - Ivan Lorente – Architect - Steven Lee – Manager - Desi Molina – Consultant	May 30, 2012
1.1	Added reference to XenServer Performance VM	Thomas Berger	August 24, 2012

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is a leading provider of virtual computing solutions that help companies deliver IT as an on-demand service. Founded in 1989, Citrix combines virtualization, networking, and cloud computing technologies into a full portfolio of products that enable virtual workstyles for users and virtual datacenters for IT. More than 230,000 organizations worldwide rely on Citrix to help them build simpler and more cost-effective IT environments. Citrix partners with over 10,000 companies in more than 100 countries. Annual revenue in 2011 was $2.20 billion.