

ServerProtect 5

on MS Windows 2000
with Terminal Services

- Functionality and Performance Test -



Group Technologies AG

Business Unit **asp4you**

Copyright by WTS-Center

Ottostrasse 4

D-76227 Karlsruhe

Phone. +49/ 07 21-49 01-0

Fax +49/ 07 21-49 01-199

E-Mail: skinzel@wts-center.de

<http://www.wts-center.de>

ServerProtect 5 Functionality and Performance Test



1	Introduction	3
2	Test Environment.....	4
2.1	Network Infrastructure	4
2.2	Hardware Specification.....	4
2.2.1	Windows 2000 Terminal Server.....	4
2.2.2	PC Clients.....	5
2.3	Software Specifications	5
2.3.1	MS Windows 2000 Terminal Services.....	5
2.3.2	CITRIX MetaFrame Server	5
2.3.3	ServerProtect 5.....	5
3	Functionality Test	6
3.1	Introduction	6
3.2	Installation all components on Terminal Server.....	6
3.3	ServerProtect Remote installation of the Normal Server.....	6
3.4	De-installation	7
3.5	Real-Time Scan.....	7
3.6	Scan Now.....	7
3.7	Task Scan.....	7
3.8	Alert Methods.....	7
3.9	ServerProtectServerProtectUpdate and Roll Back.....	7
4	Performance Tests.....	9
4.1	Real-Time Scan.....	9
4.1.1	CPU and Memory Resources for SPNTSVC.EXE	9
4.1.2	Behaviour of the Terminal Server with 20 connected users.....	10
4.2	Scan Now and Task Scan	11
4.2.1	CPU and Memory Resources for SPNTSVC.EXE	11
4.2.2	Behaviour of the Terminal Server with 20 and 40 connected users.....	12
4.3	Information Server and Management Console.....	14
5	Summary.....	17
5.1	Real-Time Scan.....	17
5.2	Scan now and Task Scan.....	17

1 Introduction

The following documentation describes the functionality and performance characteristics of the system resources of ServerProtect 5 from Trend Micro Inc. running on a Windows 2000 server with Terminal Services.

The goal of the test was to get information about the principal functionality of the ServerProtect modules and their specific functions to show usability in a thin client- and server based environment and to show the influence of the software to the server performance and to the server sizing.

2 Test Environment

The tests were run in the WTS-Center in Karlsruhe in the following environment.

2.1 Network Infrastructure

For the test a switched 100 Mbit/s Fast Ethernet network was used.

2.2 Hardware Specification

2.2.1 Windows 2000 Terminal Server

A HP NetServer LPr with hardware resources typically used in customer environments as Terminal Server was used.

This hardware is sufficient for about 50 concurrent user sessions running Microsoft Office in a Terminal Server environment (this number is application specific).

2.2.1.1 Processors

2 x INTEL Pentium III, 550 MHz

2.2.1.2 Graphic

CIRRUS LOGIC graphic adapter, on Board

(This component had no influence on the test results, and is therefore mentioned for over-all documentation only).

2.2.1.3 Hard Drives

2 x HDs HP 9,1 GByte, U2W-SCSI, configured as RAID-1 system (hardware mirroring) with a net capacity of 9 GB (18 GB gross), connected to a RAID Controller HP NetRAID 3si, on channel 1.

This configuration is according to recommendations of Microsoft and Citrix for such installations. For performance reasons it is not recommended to use a RAID 5 system.

The following partitions have been configured:

- C:\ (WTS-System drive - NTFS) Total: 9 GB
- D:\ (CDROM – CDFS)

Server drive re-mapping was used for the tests with MetaFrame, which maps the drives as following:

- M:\ (WTS system drive - NTFS) Total: 9 GB
- N:\ (CDROM – CDFS)

2.2.1.4 Memory

1 GByte, SDRAM PC100

2.2.2 PC Clients

2.2.2.1 Standard Office PC

Different standard office PCs with INTEL Pentium/Pentium II CPU ranging from 133-400 MHz with 64 MB RAM and different standard SVGA graphic adapters were used as clients.

2.3 Software Specifications

2.3.1 MS Windows 2000 Terminal Services

Operating system: Microsoft (R) Windows 2000 English + Service Pack 1 with Windows 2000 Terminal Services™.

The same installations were done with the German versions of the used software. Differences in the performance tests are not expected.

2.3.2 CITRIX MetaFrame Server

The Windows Terminal Services have been extended by Citrix MetaFrame-Server from CITRIX version 1.8 for Windows 2000 Service Pack 2 and Feature Release 1.

2.3.3 ServerProtect 5

ServerProtect 5 consist of 3 applications:

- Management Console: admin.exe version 5.20.0.1635
- Information Server: EarthAgent.exe version 5.20.0.1635
- Normal Server: spntsvc.exe version 5.20.0.1635

The tests have been run with:

engine version 5.210-1011

pattern version 795

3 Functionality Test

3.1 Introduction

The functionality of the software was tested on a Windows 2000 Terminal Server. Therefore most function calls have been tested according to Trend Micro specifications. No adjustments are necessary.

3.2 Installation all components on Terminal Server

ServerProtect consists of three components:

- Management Console
- Information Server
- Normal Server

All three components were installed on the Windows Terminal Server. The installation was done according to Microsoft methodology over settings – add/remove software.

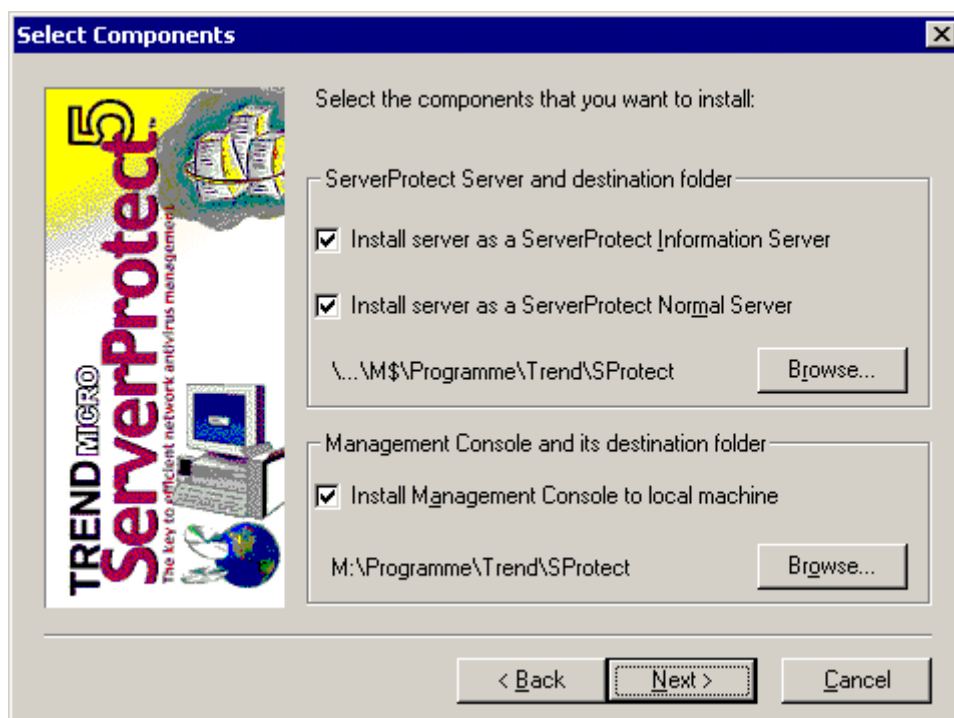


Figure 3-1 : Select Components when installing ServerProtect 5

3.3 ServerProtect Remote installation of the Normal Server

ServerProtect has been designed as a three tier application. This enables you to install all three components on one computer or individually on different machines. Especially in big server farms ServerProtect provides the capability to administrate all servers from one management console including installation/uninstallation/update on servers without any reboot.

For this test, the Information Server and Management Console was installed on an NT4 Server. The target of the remote installation of the Normal Server was a Windows 2000 Terminal Server.

Moving the Normal Server to another Information Server has also been successfully tested.

3.4 De-installation

The following scenarios have been successfully tested:

- De-installation of all three local components
- Remote de-installation of the remote installed Normal Server

3.5 Real-Time Scan

The following scenarios have been successfully tested:

- Enabled Real-Time Scan with incoming and outgoing and separate incoming and outgoing file transfers.
- Scan levels for compressed files:
Without compressed files, scan level 1 and scan level 5
- Actions:
Bypass, Delete, Rename, Move, Clean for file and macro viruses

3.6 Scan Now

The following scenarios have been successfully tested:

- All local drives as well as selected mapped network drives.
- Scan levels for compressed files:
Without compressed files, scan level 1 and scan level 5
- Actions:
Bypass, Delete, Move, Clean for file and macro viruses

3.7 Task Scan

The following scenarios have been successfully tested:

- All local drives as well as selected mapped network drives.
- Scan levels for compressed files:
Without compressed files, scan level 1 and scan level 5
- Actions:
Bypass, Delete, Move, Clean for file and macro viruses

3.8 Alert Methods

The following scenarios had been tested with success:

- Windows NT event log:
- Message box to a specific computer:

3.9 ServerProtectServerProtectUpdate and Roll Back

The update from the internet as well as the roll back was tested successfully. The deploy on the local Terminal Server machine, as well as the remote deploy from the NT4 Server to the Terminal Server passed the test.

ServerProtect 5 Functionality and Performance Test

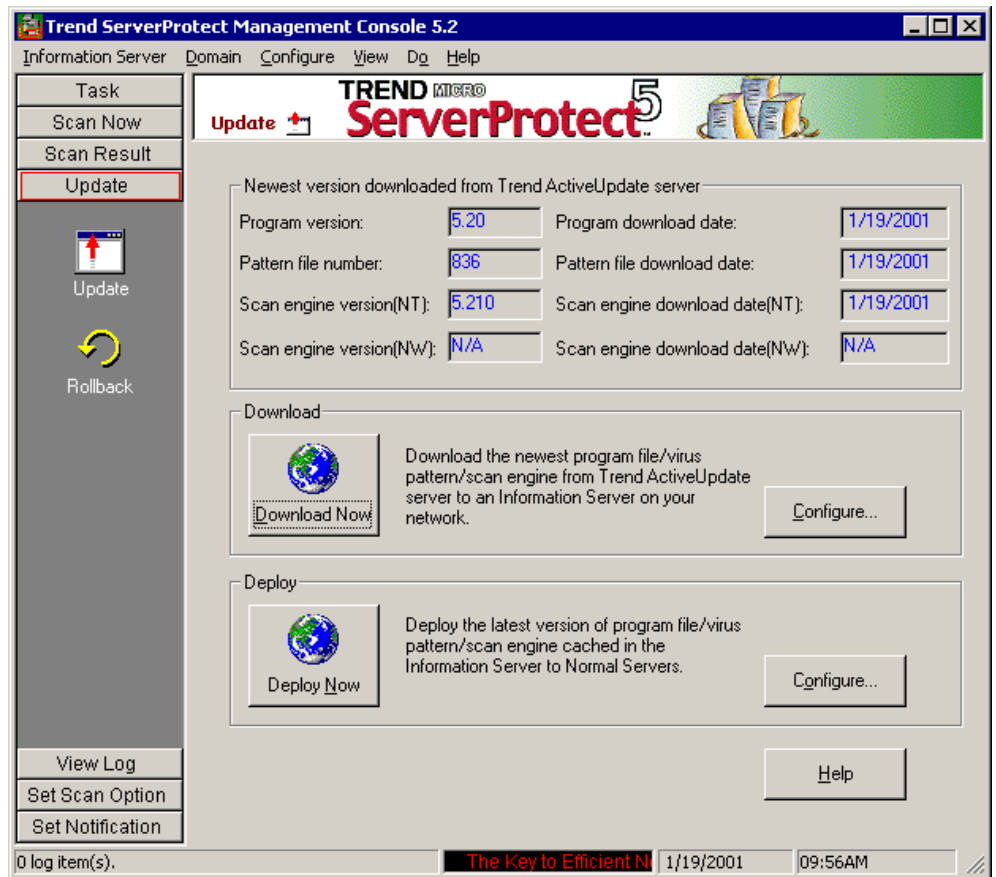


Figure 3-2 : Update and Deploy of new patterns, scan engine and program version

4 Performance Tests

4.1 Real-Time Scan

During the tests the loads of the available processors were measured. These loads can basically be divided into two categories:

Kernel mode

The Kernel mode has operating system specific functions, e.g. I/O of calls, write operations on hard disk, etc. Processes running in the Kernel mode have higher internal permissions and priorities.

User mode

In the user mode the entire application-specific logic is executed, e.g. special calculations within the application.

For a virus scan application, it is expected that nearly the complete CPU load will occur in the kernel mode.

Storage utilization

On a multi-user operating system such as Windows Terminal Server or Windows 2000 Server, all users log into so-called virtual sessions. Each virtual session receives his own virtual address space and therefore his own memory storage. Since applications do not run on the computer system of the clients, but on the Terminal Server, special attention has to be directed toward the available memory storage.

The scan application running as a service will be loaded only once during system start-up for the whole system, not in each client session.

4.1.1 CPU and Memory Resources for SPNTSVC.EXE

The SPNTSVC.EXE is the scanning application running as a service on each Normal Server.

The following scenarios have been tested successfully:

- Without appearing viruses:
20 users running the "Power User Word/Excel Scenario" from the Citrix Server Test Kit . No viruses were copied to the hard disk.
- Real-Time Scan with scan level x ...:
One user runs a batch file which copies the sample viruses to the hard disk and deletes it in a loop.
- An additional test has been run with nested compressed files
- The last test was run with an additional load from 20 users

Notes to the column CPU utilization:

The add-on "while active" means the values were written to the database only when the CPU had a load of more than 1%. This occurred only in the case that a virus had been detected. In the first row, the over-all CPU utilization was used instead of the "while active" value.

ServerProtect 5 Functionality and Performance Test



	CPU utilization while active (%)			Memory Working Set while active (MB)	Memory Peak Working set (MB)	Peak page file usage (MB)
		kernel mode	user mode			
Without appearing viruses (over-all CPU utilization)	0,3	0,3	0	n/a	6,1	3,3
Real-Time Scan with scan level 0 for compressed files, outgoing	5,9	3,9	1,1	5,6	5,7	2,9
Real-Time Scan with scan level 0 for compressed files, incoming	7,0	5,0	2,0	5,6	5,7	2,9
Real-Time Scan with scan level 0 for compressed files, incoming and outgoing	4,7	3,5	1,2	5,6	5,7	2,9
Real-Time Scan with scan level 5 for compressed files, incoming and outgoing	4,9	3,5	1,4	5,6	5,7	2,9
Real-Time Scan with scan level 5 for compressed files, incoming	7,2	5,1	2,1	5,6	5,7	2,9
Real-Time Scan with scan level 5 for compressed files, outgoing	5,3	3,9	1,4	5,6	5,7	2,9
Real-Time Scan with scan level 5 for compressed files, incoming and outgoing with nested zip files	4,1	3,2	0,9	3,8	6,4	2,9
Real-Time Scan with scan level 5 for compressed files, incoming and outgoing with zip files and 20 users load	5,7	4,3	1,4	5,6	5,7	2,9

Table 4-1 : CPU utilization Scan now with different parameters (SPNTSVC.EXE)

For all scenarios the overall CPU utilization was at 0.5 %, and the active / load ratio for all scenarios was below 0.5 %. Considering that in the test scenarios a user copied all the sample viruses in a loop to the hard disk, which caused some hundreds of virus alerts per minute, the Real-Time Scan does not influence a real productive system.

Since the SPNTSVC.EXE runs as a separate service once on each server and is not executed in each session, all values are in a really uncritical area.

4.1.2 Behaviour of the Terminal Server with 20 connected users

To test the behaviour of the Windows Terminal Server with and without Virus Scan with 20 logged-on users, we used the Citrix Server Test KIT to place the load on the Terminal Server. The connected users run the "Power user Word/Excel scenario" from the Citrix Server Test Kit. The users:

- Create a table in an Excel worksheet
- Write a letter in Word
- Format the letter as series-letter

Within this scenario each user creates some files and saves them to the disk in different versions from time to time.

The following diagram shows an over-all impression of the CPU time for both tests:

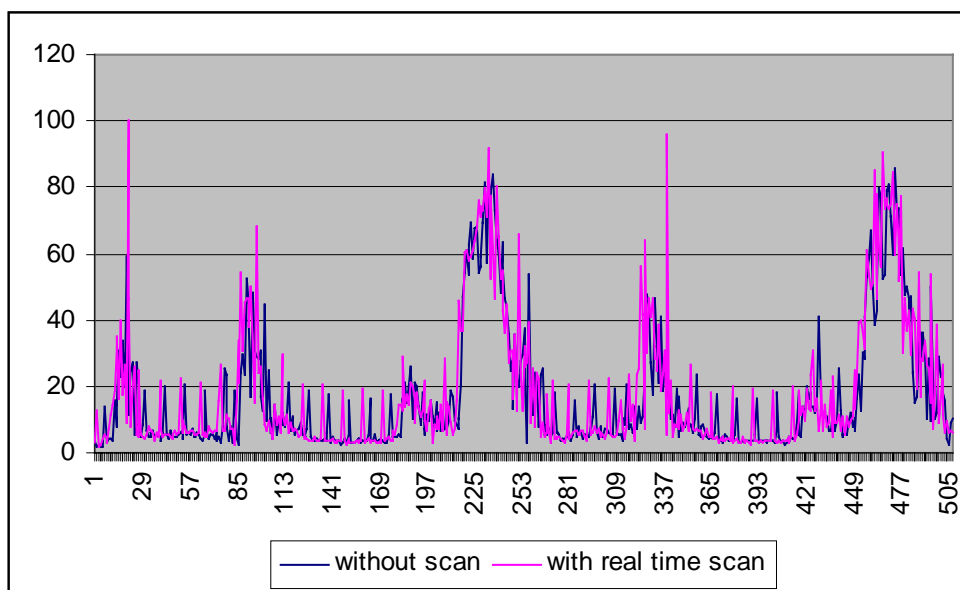


Figure 4-1 : CPU Utilization with 20 connected users

The most important information in the above diagram is that the peak values are of a very short duration. The values on the x-axis are in seconds. There is no detectable influence of the Real-Time Scan on the timeline of running processes.

The following table compares the CPU and memory parameters of the measured scenario.

CPU Time (%)	Without Scan	Real-Time Scan
Min.	1,7	1,6
Max.	85,5	100
Average	16,7	18,1
Memory Committed Bytes (MB)		
Min.	482,75	480,95
Max.	655,37	652,56
Average	585,69	584,06

Table 4-2 : CPU and Memory utilization running 20 power user Word/Excel scripts with Real-Time Scan

These results also show that the “Real-Time Scan” does not influence a real productive Terminal Server.

4.2 Scan Now and Task Scan

“Task Scan” works like the “Scan Now” function with the difference that they can be scheduled. The results for both are the same.

4.2.1 CPU and Memory Resources for SPNTSVC.EXE

Also for the Scan Now module, SPNTSVC.EXE is the scanning application, running as service one time for each Normal Server.

ServerProtect 5 Functionality and Performance Test



The following scenarios have been tested:

- Without user load:
Scanning the hard disc when no user is connected to the Terminal Server. There are three priorities to choose: Low, Middle, High.
- With 20 connected users running the power user Word/Excel scenario from the Citrix Server Test Kit.

During this test about 15,000 files were scanned. About 100 files were infected and detected by ServerProtect.

	CPU utilization while active (%)			Memory Working Set while active (MB)	Memory Peak Working set (MB)	Peak Pagefile usage (MB)	Scan time (h:min)
		kernel mode	user mode				
Scan Now without connected users priority Low	86,8	86,5	0,3	5,6	5,8	2,9	5:00
Scan Now without connected users priority Middle	81,9	81,6	0,3	5,6	5,8	2,9	5:19
Scan Now without connected users priority High	78,8	78,6	0,2	5,6	5,8	2,9	5:34
Scan Now with 20 connected users priority Low	39,1	38,5	0,6	5,5	5,6	2,8	5:43
Scan Now with 20 connected users priority Middle	37,7	37,3	0,4	5,5	5,6	2,8	6:01
Scan Now with 20 connected users priority High	37,4	37,0	0,4	5,5	5,7	2,9	5:52
Scan Now with 40 connected users priority Low	29,2	28,8	0,4	5,8	6,1	3,3	10:52
Scan Now with 40 connected users priority Middle	30,1	29,7	0,4	5,8	6,1	3,3	10:25
Scan Now with 40 connected users priority High	21,8	21,6	0,2	5,9	6,1	3,3	15:22

Table 4-3 : CPU utilization Scan now with different parameters (SPNTSVC.EXE)

4.2.2 Behaviour of the Terminal Server with 20 and 40 connected users

The following diagrams show the CPU utilization with 20 and 40 connected users running the "Power User Word/Excel scenario".

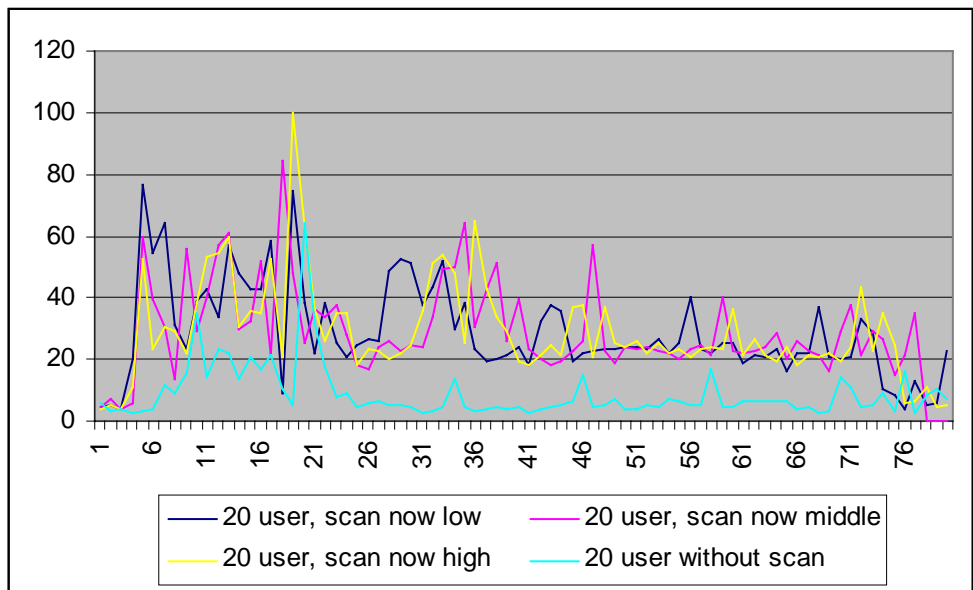


Figure 4-2 : CPU Utilization with 20 connected users

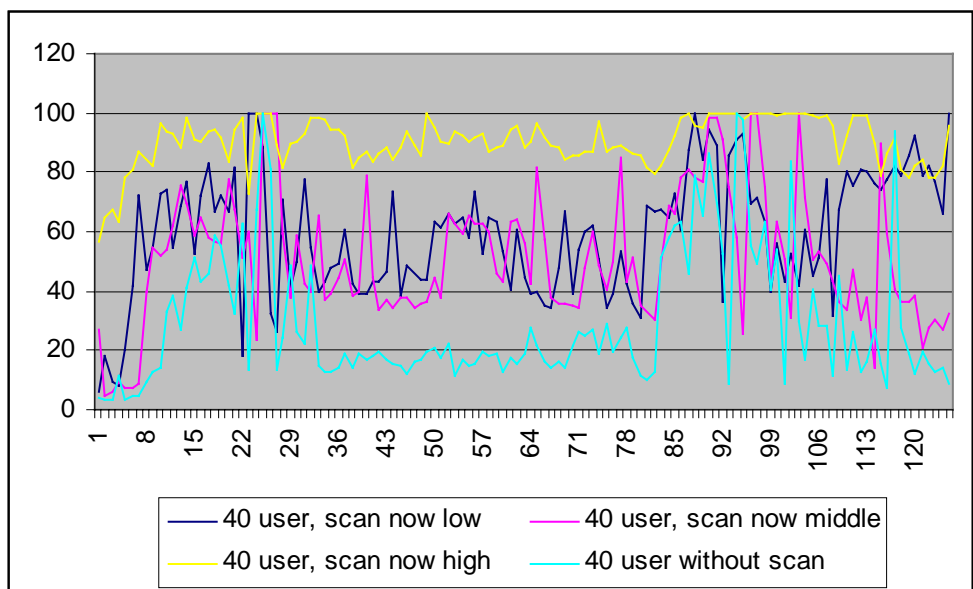


Figure 4-3 : CPU Utilization with 40 connected users

The diagram shows that ServerProtect 5 takes the overall load on the server into consideration. Only when the load is very high (40 users) and the scan priority is set to High will the Windows Terminal Server work on a critical load level (see Figure 5-3). The over-all CPU is higher than 70% for the majority of the test time.

The influence on the user sessions is very small. There are only very small delays in the characteristic of the diagrams.

CPU Time (%)	20 users Low	20 users Middle	20 users High	40 users Low	40 users Middle	40 users High
Min.	2,34	4,21	3,58	6,07	4,69	56,39
Max.	76,72	84,17	100	100	100	100
Average	28,59	29,83	29,66	55,27	52,17	86,74

Table 4-4 : CPU Time running power user script Word/Excel

ServerProtect 5 Functionality and Performance Test



4.3 Information Server and Management Console

The following results show the resources that the Information Server and Management Console need when running on a Windows Terminal Server.

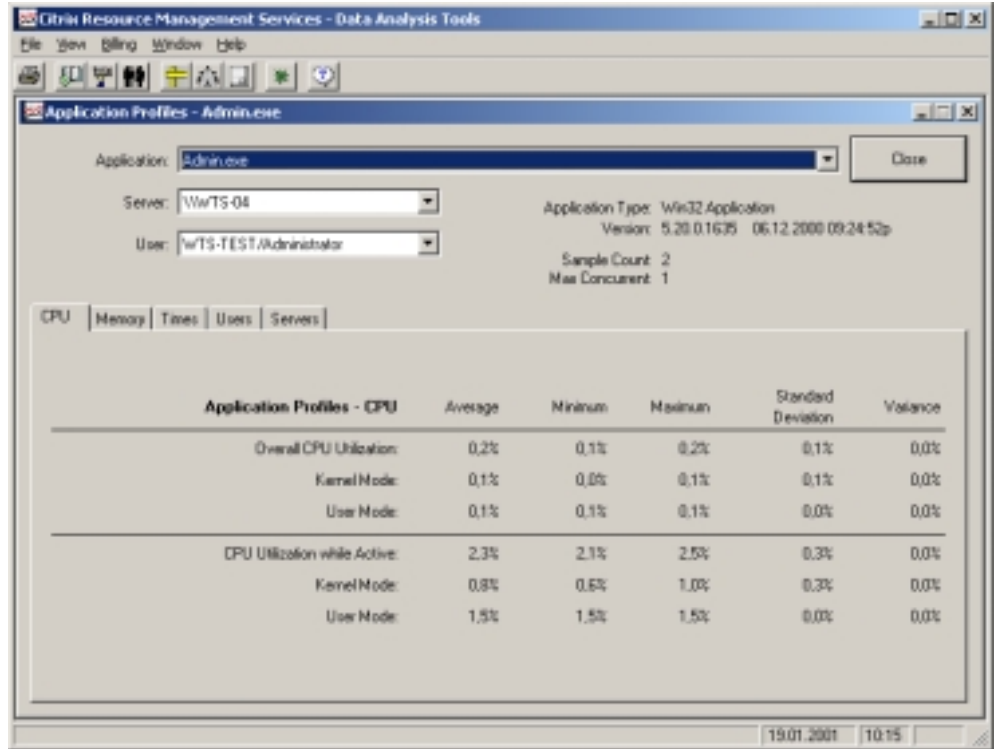


Figure 4-4 : CPU Utilization for the Management Console (ADMIN.EXE)

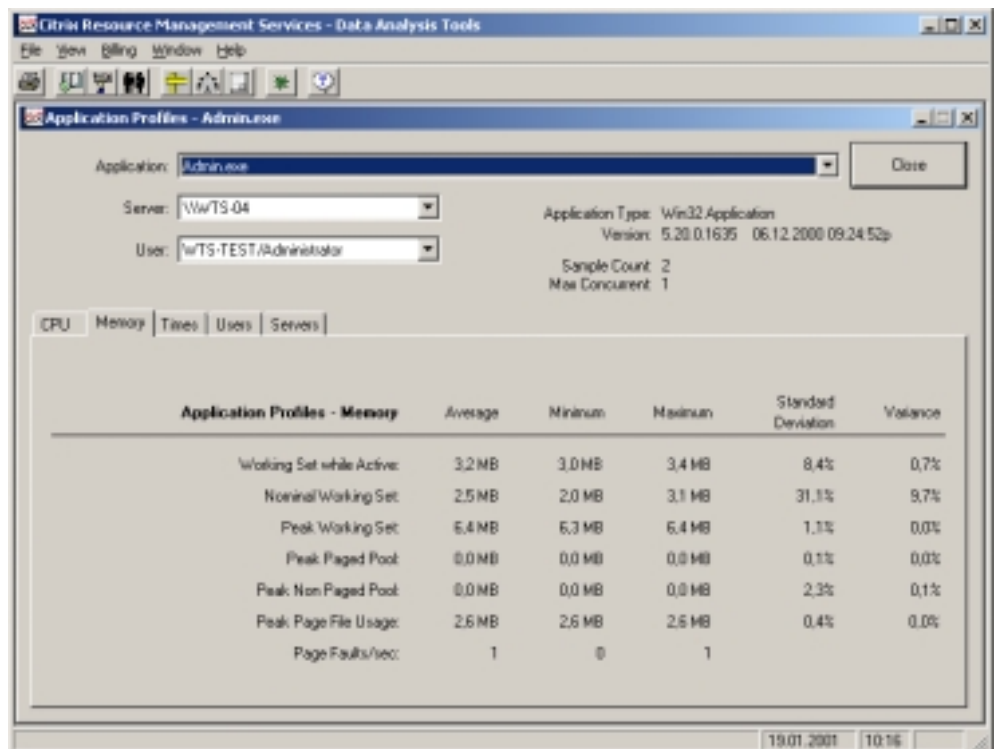


Figure 4-5 : Memory Load for the Management Console (ADMIN.EXE)

ServerProtect 5 Functionality and Performance Test

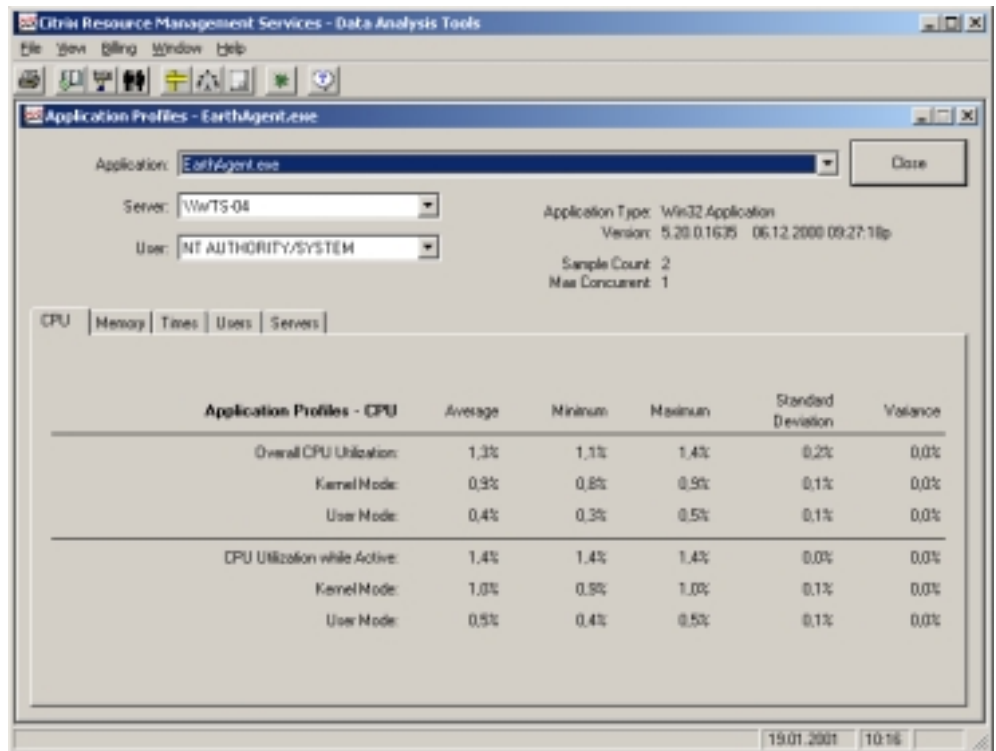


Figure 4-6 : CPU Utilization for the Information Server (EARTHAGENT.EXE)

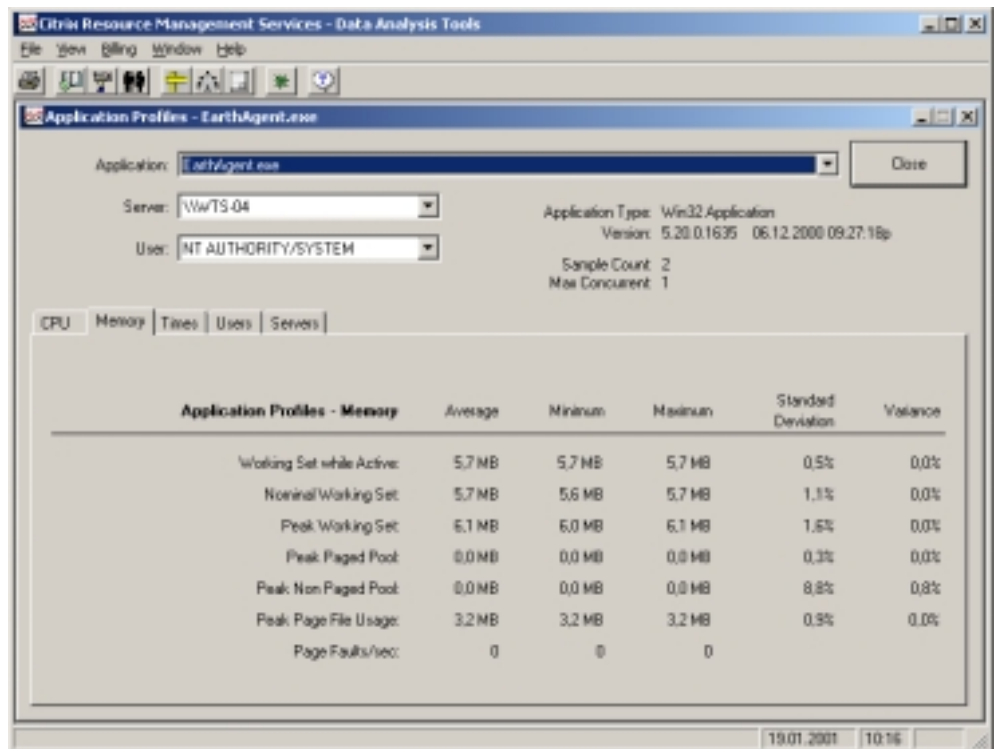


Figure 4-7 : Memory Load for the Information Server (EARTHAGENT.EXE)

During the entire measuring period the values were cumulated, i.e. the tested modules of the application were started and terminated properly. During these tests no unexpected program termination occurred, e.g. a so-called "Blue Screen Of Death".

These data records were written into a database using the "CITRIX Resources Management Kit".

ServerProtect 5

Functionality and Performance Test



Since in a productive environments only one Information Server runs, the Management Console normally runs on the Administrators desktop PC. Considering the very low load that both the Information Server and Management Console produce, they do not influence a real production Windows Terminal Server.

5 Summary

All in all, ServerProtect 5 is well suited for use on a Terminal Server. When using “Scan Now” or “Task Scan” special care needs to be taken concerning the parameters.

5.1 Real-Time Scan

Comparing the results of the test, we recommend using Real-Time Scan for incoming and outgoing files with a scan level of 5 for compressed files. The differences were too marginal (for some reasons there were worse results for only incoming files) compared to the restriction of scanning at a lesser priority.

5.2 Scan now and Task Scan

We recommend that you use Scan Now or Task Scan at a time when no users are connected to the Terminal Server (e.g., at night before running backup tools).

If this is not possible scan priority Low is recommended.