

Microsoft Windows Server 2003 vs. Red Hat Enterprise Linux AS 3.0: IT Professionals Running a Production Environment

Test report prepared under contract from Microsoft

Executive summary

Microsoft requested that VeriTest, a division of Lionbridge Technologies, Inc., measure the amount of time a group of IT professionals spent executing various tasks associated with improving the reliability and robustness of back-end infrastructure and end-user services in Windows and Linux production environments within a simulated medium-sized business. VeriTest closely monitored the processes followed and the tools used by the IT professionals to assess the impact on the IT service loss (or business disruption) of end-user services in the simulated business.

Key findings

- ❑ In our tests, the Windows Server 2003 environment had 4:20:19 of average end-user service loss time compared to 4:59:44 of average service loss time for the Red Hat Enterprise Linux AS 3.0 environment on measured service loss events. Lower results are better.
- ❑ In our tests, more work was completed in the Windows Server 2003 environment (280 completed tasks and events) than in the Red Hat Enterprise Linux AS 3.0 environment (248 completed tasks and events) in less average elapsed time (18:44:14 vs. 27:48:05).

VeriTest configured test environments with three Hewlett Packard ProLiant DL380 G3 servers serving as an infrastructure server, email server, and file/print server. In one set of test environments, the servers ran Windows Server 2003 and Exchange Server 2003. Another set of test environments ran Red Hat Enterprise Linux AS 3.0. We specifically configured the test environments in a “failure prone” state. The systems were functional, but lacked basic hardware/software fault tolerance, up-to-date patches, and data access security.

We recruited 36 comparably skilled IT administrators (18 Linux and 18 Windows), who passed a thorough screening process, to administer the test environment. We gave them a series of “proactive” tasks, which involved upgrading and reconfiguring the test systems with the goal of improving the reliability and robustness of the production environment. Proactive tasks ranged from configuring new devices and printers to implementing system backups, system monitoring, and remote access. As they executed these tasks, a VeriTest test proctor initiated “reactive” events (e.g., device or system service failures) that simulated typical system problems and required troubleshooting to resolve. The administrators spent a total of 26 hours spread over four days working on the proactive tasks and reactive events. VeriTest captured timing and task completion results from a variety of sources including administrators’ journal files, instant messaging logs, system service probing script log files, and exit interviews. During exit interviews, over 90% of the IT administrators felt the test environment was realistic and accurately reflected a real world IT environment. Refer to the Testing Methodology section for a description of the test process and a detailed definition of the proactive tasks and reactive events. For each group of test results below, we normalized the data by removing the lowest and highest results for each platform. Refer to the Test Results section for a detailed breakdown and analysis of the test results.

During the test, VeriTest initiated a series of events that broke or disabled various system services in the administrators' test environments. The services remained down until they were fixed by the administrators. We characterized this downtime as "service loss" and used a set of service probing scripts to measure the amount of end-user service loss time caused by the events. Each service loss event targeted a specific system service (e.g., email, printer) and caused that service to become unavailable to the user population. The probing scripts recorded when the service loss was initiated and when it was subsequently fixed by the administrator.

Figure 1 shows the average service loss time encountered in each environment during the test. Lower service loss results are better. The Windows Server 2003 environment had 4:20:19 of average service loss time and the Red Hat Enterprise Linux AS 3.0 environment had 4:59:44 of average service loss time for the measured service loss reactive events. Overall, the Red Hat Enterprise Linux AS 3.0 environment had 15% more average service loss time on the measured service loss reactive events compared to test systems running Windows Server 2003.

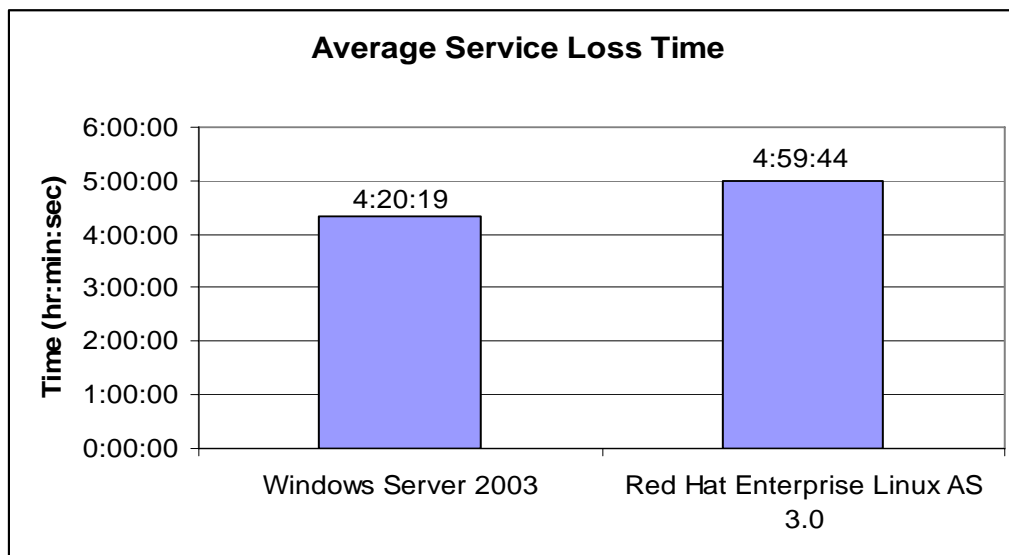


Figure 1: Average service loss time on measured service loss events (lower results are better)

For each proactive task, VeriTest measured the amount of elapsed time each administrator spent researching, designing, implementing, testing, and documenting the implementation. We captured these measurements from the administrator's journal. After the test completed, the VeriTest test proctor conducted interviews with each administrator to validate the number of proactive tasks completed. In addition, the test proctor ran validation scripts on the test systems to verify relevant task functionality. Similarly, VeriTest measured the amount of elapsed time each administrator spent troubleshooting reactive events as well as the number of events successfully resolved by the conclusion of the test.

Figure 2 lists the average amount of elapsed time dedicated to completing proactive and reactive tasks in the Windows Server 2003 and Red Hat Enterprise Linux AS 3.0 environments. These averages only include proactive tasks that were completed by the end of the test. Lower results are better.

On average, the Windows Server 2003 environment required less time to complete proactive tasks and resolve reactive events than the Red Hat Enterprise Linux AS 3.0 environment. The average total time required for Red Hat Enterprise Linux AS 3.0 was 27:48:05 and the average total time required for Windows Server 2003 was 18:44:14, a decrease in average total time of 33% over Red Hat Enterprise Linux AS 3.0. The total times are based on individual average proactive and reactive times, which when added together, may result in a sum higher than 26 hours.

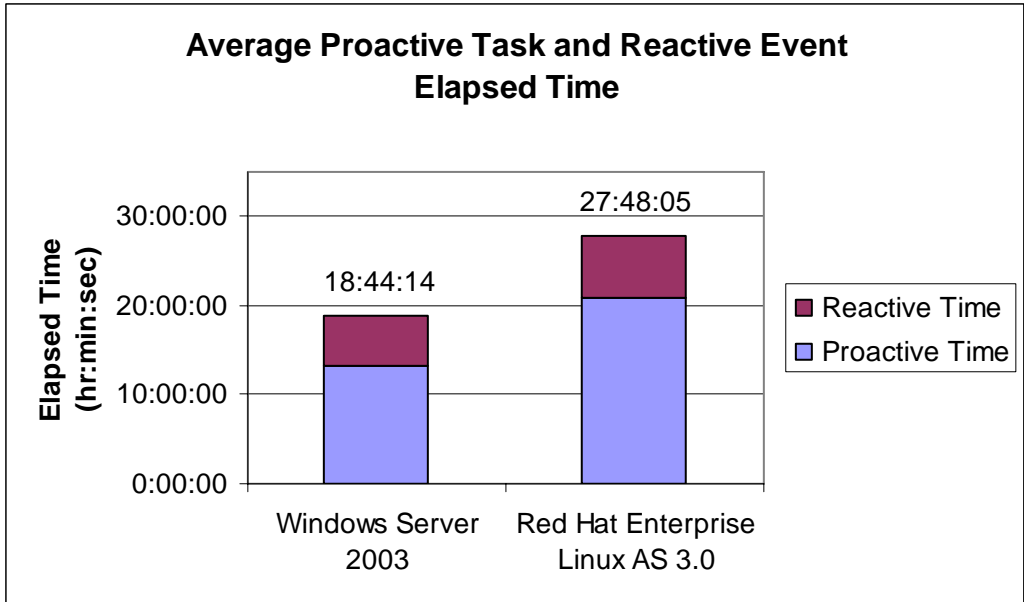


Figure 2: Average elapsed time spent on proactive tasks and reactive events (lower results are better)

Figure 3 lists the total number of proactive tasks and reactive events successfully completed in the two environments. A total of 280 tasks and events were completed in the Windows Server 2003 environment compared to 248 in the Red Hat Enterprise Linux AS 3.0 environment.

Combining the results in Figures 2 and 3, in our tests more work was completed in the Windows Server 2003 environment in less elapsed time than in the Red Hat Enterprise Linux AS 3.0 environment.

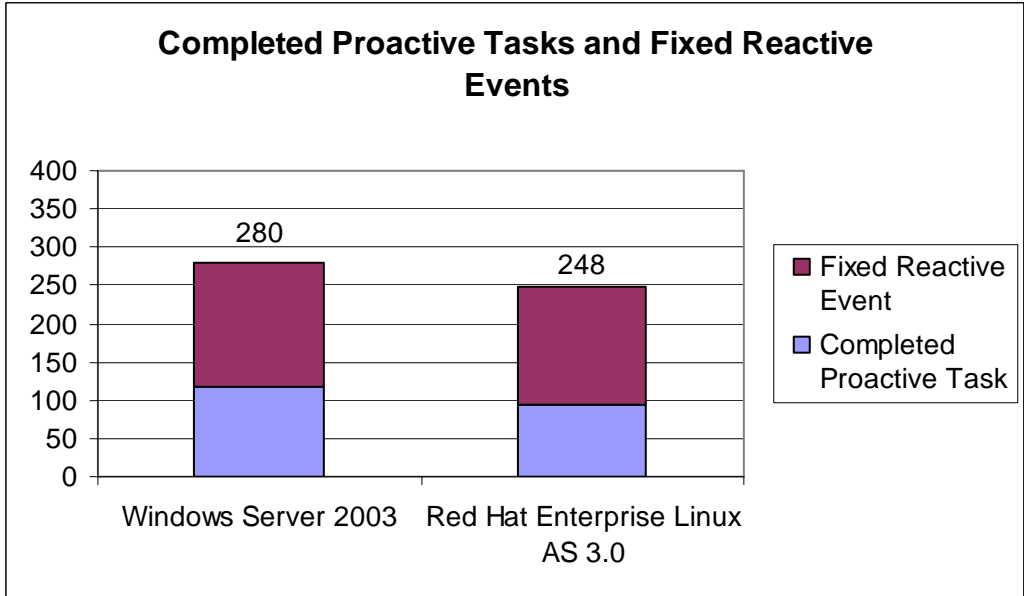


Figure 3: Number of completed proactive tasks and fixed reactive events (higher results are better)

Testing methodology

Microsoft requested that VeriTest, a division of Lionbridge Technologies, Inc., measure the amount of time a group of IT professionals spent executing various tasks associated with improving the reliability and robustness of back-end infrastructure and end-user services in Windows and Linux production environments within a simulated medium-sized business. VeriTest closely monitored the processes followed and the tools used by the IT professionals to assess the impact on the IT service loss (or business disruption) of end-user services in the simulated business.

VeriTest configured test environments with three Hewlett Packard ProLiant DL380 G3 servers serving as an infrastructure server, email server, and file/print server. In one set of test environments, the servers ran Windows Server 2003 and Exchange Server 2003. Another set of test environments ran Red Hat Enterprise Linux AS 3.0. We specifically configured the test environments in a “failure prone” state. The systems were functional, but lacked basic hardware/software fault tolerance, up-to-date patches, and data access security.

We recruited 36 comparably skilled IT administrators (18 Linux and 18 Windows) to administer the test environment. We gave them a series of “proactive” tasks, which involved upgrading and reconfiguring the test systems with the goal of improving the reliability and robustness of the production environment. Proactive tasks ranged from configuring new devices and printers to implementing system backups, system monitoring, and remote access. As they executed these tasks, a VeriTest test proctor initiated “reactive” events (e.g., device or system service failures) that simulated typical system problems and required troubleshooting to resolve. The administrators spent a total of 26 hours spread over four days working on the proactive tasks and reactive events. As they completed the tasks, they documented their time on task and general test experience in a local journal file.

The following paragraphs represent the background narrative given to each test administrator:

“Airdrome.net is a medium-sized business with 200 employees. The company has never had a proactive full-time IT administrator. The company has relied on piecemeal administration from a number of sources for the past few years. The current back-end infrastructure includes an infrastructure, email, and file/print server. The systems have not been proactively managed and are generally in a “failure prone” state where any failure could cause serious disruptions to the company.

New management is moving the company in a different direction which requires a reliable, available IT infrastructure. Airdrome.net has just hired its first full time administrator to assess the state of the network, fix any issues he or she may discover, and implement a series of best practices to improve the reliability of the infrastructure. At the same time, there remain 200 employees who must have day-to-day access to email, network shares, print services, and IT support for fixing/troubleshooting problems as they arise.

You are being brought in to fix the problems with the infrastructure as quickly as possible and, yet, still remain available to respond to trouble tickets as they are submitted to you via instant messages from the user population. The highest priority assignment is to improve the robustness and fault tolerance of the existing infrastructure ASAP. You must not only execute several proactive tasks, similar to the work performed by typical system administrators, but respond to reactive events. A proactive task is defined as a project that an administrator works on in the background. Examples include enhancing security or adding new hardware. The order in which you perform these proactive tasks will be left to your discretion. However, new printer and tape drive hardware has just been purchased, and Airdrome.net management has made this a top priority to install and configure, so this is the first set of proactive tasks that you must execute. These tasks are typically not time critical and are subject to multiple interruptions by reactive events.

A reactive event is defined as a user- or system-initiated event that requires immediate attention. Examples include failed hardware/software or a user data access problem. Reactive events become the highest priority task for the administrator as soon as the

trouble ticket is submitted. For this test we will be using a simple notification system for trouble tickets based on instant messages. We will use an instant message trouble ticket system because it is a faster, more immediate tool than the typical database-based system more commonly used by IT professionals. It also provides us with a time stamped record of when tickets are submitted and fixed. A test proctor will send you an instant message informing you of a problem he is having with the network or a network resource. As soon as the administrator receives the instant message trouble ticket, the proactive task currently in progress will be put aside or paused, and the administrator will switch focus to the reactive task. Please note that this test simulates a real environment with end users and network monitoring needs. As an administrator would do in a real world situation you should not passively wait for trouble tickets. Instead, you should be constantly monitoring the network in an attempt to detect problems as they happen and fix them before they impact the user community.”

The following sections describe specific parts of the test methodology in more detail, including the proactive tasks and reactive events executed by the administrators, test metrics, the general test process, the test environment definition, and the participant recruiting process.

System reconfiguration: proactive task definition

VeriTest provided each administrator with a list of proactive tasks to complete during the test. These tasks reflected typical background IT administrative projects completed when upgrading and reconfiguring a system and primarily involved improving the robustness and reliability of the test environment. Each task included a set of minimum acceptable criteria. The minimum acceptable criteria defined the minimum work necessary to get full credit for completing the proactive task and standardized the work performed by the administrators on each task. All tasks were to be implemented with existing OS tools and utilities (Backup Utility for Windows, dump/restore, etc.) or with freely available downloadable third-party applications (for example, third-party monitoring tools such as Nagios and LogSurfer).

We suggested administrators remain mindful of the time constraints they faced and recommended that they spend their time wisely and not use the entire test cycle designing an overly complex/elegant solution that only addressed one task. Administrators were instructed to move on to the next proactive task after completing the minimum acceptable criteria for the current proactive task. If they had free time at the end of the test cycle, they could implement additional functionality above and beyond that specified in the minimum acceptable criteria. Their goal was to implement as many tasks as possible in the allotted test time.

VeriTest classified two of the nine proactive tasks—configuring a new tape drive and configuring a network printer—as high priority tasks. Administrators were instructed to complete these tasks first. Once the administrators completed the high priority tasks, they were free to execute the remaining proactive tasks in any order.

Below is a list of the nine proactive tasks. Minimum acceptable criteria for each task follow as bullet points.

High priority tasks (complete these tasks first)

- **Task: Configure new tape device and driver**
 - Configure the tape backup device on the file server system and verify that it is operational by copying and restoring data from tape
- **Task: Configure new network printer**
 - Verify that the printer can successfully print

Remaining tasks (prioritize as you see fit)

- **Task: Implement system backups**
 - Develop a full/incremental backup plan including the ability to store tapes off-site
 - Do a full backup of all file shares on the file server
 - Do a full backup of user mailboxes on the email server
 - Do a full backup of the directory database on the infrastructure server

- **Task: Improve system fault tolerance/redundancy**
 - Configure redundant system services such as directory, DNS, WINS, DHCP (where applicable)
 - Move email mailboxes and file share data to RAID 5 partitions
- **Task: Implement basic administrator remote access**
 - Implement remote management access from the client system to any of the server systems (allows remote server management within the local network)
- **Task: Implement routine system/security monitoring process**
 - Design a system monitoring procedure that can be manually followed by a junior IT administrator and includes at a minimum monitoring the logs of critical system services such as directory, email, file, DHCP, DNS, WINS, and print as well as monitoring security events such as logons and logoffs
- **Task: Apply updated system and application patches**
 - Update infrastructure/email/file servers to the latest OS service pack/patch level
 - Update infrastructure/email/file applications to latest patch/service pack level
- **Task: Change user account information**
 - Change the user name for the eng1, eng2, eng3 users to sales61, sales62, sales63, remove access from engineering resources, and add access to sales resources
- **Task: Implement better data access security**
 - Tighten file share security to meet the following needs:
 - public share - read/write access by corporate group
 - home share - read/write access by owner of the individual home directory
 - accounting share - read/write access by accounting group
 - engineering public share - read access by engineering/sales, write access by engineering group
 - engineering private share - read/write access by engineering group
 - hr public share - read access by corporate group, write access by hr group
 - hr private share - read/write access by hr group
 - sales public share - read access by corporate group, write access by sales group
 - sales private share - read access by sales/accounting, write access by sales group
 - Create the following group structure:
 - corporate group - all employees
 - accounting group - accxx users
 - engineering group - engxx users
 - Make the network printer available to all engineering users
 - Verify the printer can only be accessed by engineering users
 - hr group - hrxx users
 - sales group - salesxx users

System troubleshooting events: reactive event definition

As the administrators designed and implemented the proactive tasks, a VeriTest test proctor generated a sequence of thirteen reactive events that required system troubleshooting. After generating the event, the test proctor (acting as a user) issued a trouble ticket to the administrator describing the symptom of the event. These reactive events simulated IT requests from the user population (e.g., restore files, restore deleted mail) as well as hardware/software issues (e.g., printer doesn't work, can't receive email). The administrators were instructed to treat a reactive event as their highest priority activity. As soon as the administrators received the event, they stopped working on their current proactive task and focused all their effort on diagnosing and resolving the reactive event. They recorded the time spent on each reactive task in their journals.

The VeriTest test proctor made every effort to generate reactive events to all of the administrators at the same time. The test proctor notified the administrator of a new reactive event by sending a trouble ticket using the Gaim instant message application. The administrator and the test proctor communicated back and forth regarding the status of the trouble ticket using Gaim. We enabled Gaim logging, which created a time stamped record of all communication, including when the reactive event was initiated and fixed.

The administrators could issue two possible responses to the trouble ticket based on their knowledge of the event:

- I have received your trouble ticket and will investigate the problem. I will send a follow-up email to let you know when I have fixed your problem.
- I have received your trouble ticket and am already aware of the problem. I am working on it and will send a follow-up email to let you know when I have fixed your problem.

The test proctor issued the reactive events according to a fixed schedule. Typically the administrators handled between two and four reactive events per test day. Below is a chronological list of the thirteen reactive events issued during the test. Each event includes a description of the event, the trouble ticket associated with the event, and the event initiation time for the event.

Reactive 1 – Mail performance (CPU hogging application that restarts on reboot)

Time – Day 1 @ 2:30 PM

Delay between executing the event and sending the trouble ticket: 10 minutes

Trouble ticket contents – The performance of the mail system seems sluggish.

Description – Test proctor remotely initiates an application on the email server that uses 100% of the available CPU cycles. The administrator must troubleshoot general performance issues on the email server. This involves identifying the application hogging CPU cycles and removing the application from the boot-up sequence.

Reactive 2 – File deletion (User accidentally deletes simple file)

Time – Day 1 @ 4pm

Delay between event execution and sending the trouble ticket: none

Trouble ticket contents – I accidentally deleted a file that I'm using to prepare next year's budget. I need to get this file restored as soon as possible. The name of the file is 2005_budget_data.doc and it's located on the acc share in the budget directory. Please let me know as soon as I can access the file again.

Description – Test proctor remotely deletes a file from the acc share. The administrator must restore the file from backups (which at this point in the test probably do not exist).

Reactive 3 – Cannot create file (Runaway log file)

Time – Day 2 @ 9:00 AM

Delay between arrival of administrator on the second test day and sending the trouble ticket: 10 minutes

Trouble ticket contents – I'm not able to create any files on the public share.

Description – Test proctor creates a single log file in the public share that occupies all remaining available space in the partition. The administrator must troubleshoot general file sharing issues on the file server. This involves identifying which partition is out of space and deleting the runaway log file.

Reactive 4 – Cannot receive mail (Stop SMTP mail process)

Time – Day 2 @ 11am

Delay between event execution and sending the trouble ticket: 10 minutes

Trouble ticket contents – External users are not able to send me email. They receive a message indicating the mail could not be delivered to my account within the specified time limit. Please take a look and let me know when I should be able to receive external mail.

Description – Test proctor remotely stops the SMTP service. The administrator must troubleshoot the problem and restart the SMTP mail process on the email server

Reactive 5 – Cannot access Internet (DHCP conflict: no leases available)

Time – Day 2 @ 3pm

Delay between event execution and sending the trouble ticket: 10 minutes

Trouble ticket contents – I'm currently logged on as user acc1 on the client computer, and I'm no longer able to browse the Internet or access any files stored on the network.

Description – Test proctor fills up all of the available DHCP leases and releases the lease on the client system. This causes an error when the client system attempts to renew its lease. The

administrator must troubleshoot general lack of network connectivity on the client system. The solution is to add additional addresses to the DHCP address pool and renew the DHCP lease on the client.

Reactive 6 – Cannot print (Printer IP address reverts to default value)

Time – Day 2 @ 5pm

Delay between event execution and sending the trouble ticket: 10 minutes

Trouble ticket contents – I'm no longer able to print. It looks like the printer is broken.

Description – Test proctor resets the IP address on the network printer to its default value (which is a static IP address incompatible with test environment's IP address scheme). The administrator must troubleshoot printer problems and restore the IP configuration to DHCP for the network printer.

Reactive 7 – Cannot access public share (Hardware drive failure occurs)

Time – Day 3 @ 9am

Delay between arrival of administrator on the third test day and sending the trouble ticket: 10 minutes

Trouble ticket contents – I'm no longer able to access the public file share.

Description – Test proctor removes and reinserts the Slot 1 drive containing the file shares on the file/print server. If the administrator has RAID 5 configured on the file/print server, the RAID partition automatically rebuilds and the test proctor does not issue the trouble ticket. If the administrator does not have RAID 5 configured on the file/print server, the test proctor deletes the file shares and issues the trouble ticket. The administrator must restore the contents of the file shares from backups due to the loss of the drive containing the shares.

Reactive 8 – File deletion (User accidentally deletes simple file)

Time – Day 3 @ 12am

Delay between event execution and sending the trouble ticket: none

Trouble ticket contents – I accidentally deleted a file that I'm currently editing. I need to get this file restored as soon as possible. The name of the file is sales_process.doc and it's located on the salespri share in the strategy directory. Please let me know as soon as I can access the file again.

Description – Test proctor remotely deletes a file from the salespri share. The administrator must restore the file from backups.

Reactive 9 – Mail deletion (Mail message deletion)

Time – Day 3 @ 2:30pm

Delay between event execution and sending the trouble ticket - none.

Trouble ticket contents – I've accidentally deleted a message that I need restored ASAP. Can you restore the message to my mailbox from abc@xyz.com with the subject header Re: Hubble Space Telescope 2.0 and let me know when it is available?

Description – Test proctor deletes a message from user acc1's mailbox. The administrator must restore the email through backups or through deleted message recovery in Exchange.

Reactive 10 – Cannot log on (Directory server goes down)

Time – Day 3 @ 4:30pm

Delay between event execution and sending the trouble ticket: 10 minutes

Trouble ticket contents – I'm not able to log on using my account from the computer named client.

Description – Test proctor remotely powers down the infrastructure server. The administrator must power on the server. Note that this event is not performed if the administrator has redundant directory services implemented at the time of the event.

Reactive 11 – File deletion (User accidentally deletes complex file)

Time – Day 4 @ 9:30am

Delay between event execution and sending the trouble ticket: none

Trouble ticket contents – I accidentally deleted a spreadsheet and its linked files that I'm using to prepare this quarter's budget. I need to get these files restored as soon as possible. The names of the files I need are Q3_2004_proj.xls on the acc share in the projections directory along with

\\hrpub\information\hr_data.xls, \\salespub\information\sales_data.xls, and \\public\information\pub_data.xls. Please let me know as soon as I can access the files.

Description – Test proctor remotely deletes all files associated with a linked spreadsheet. The administrator must restore all of the files from backups.

Reactive 12 – File performance (Local denial of service)

Time – Day 4 @ 10:30am

Delay between event execution and sending the trouble ticket: 10 minutes

Trouble ticket contents – It's taking an unusually long time to copy files from the public file share to my local client computer.

Description – Test proctor remotely initiates applications on the file and email servers that saturate the network interface to the file server. The administrator must troubleshoot general performance issues on the file server. This involves identifying the Denial of Service attack, tracking the source, and killing the application on the email and file systems.

Reactive 13 – Incorrect directory permissions (File permission problems)

Time – Day 4 @ 12:00am

Delay between event execution and sending the trouble ticket: none

Trouble ticket contents – I'm no longer able to save the file1.txt file located in the archive directory on the acc share.

Description – Test proctor remotely sets file and directory permissions on the archive directory in the acc share such that the administrator has access to some files but not others. The administrator must troubleshoot general permissions issues associated with the file1.txt file. This involves fixing the local file permissions as well as the directory permissions.

Test metrics

VeriTest measured a series of test metrics for the proactive tasks and reactive events. The proactive task metrics primarily involved measuring how much time the administrators spent on each proactive task along with gauging how much of the minimum acceptable criteria they completed. The reactive event metrics were more complex and involved time-on-task metrics, event detection metrics, event prevention metrics, and service loss metrics. VeriTest recorded test metric data consistently from numerous sources including trouble ticket instant message logs, test proctor and administrator journals, and background service availability probing scripts. The probing scripts ran on the test proctor systems and tested the availability of services on the test environment servers several times a minute. The scripts used pings to test for system availability as well as service specific probes of the directory, email, and DHCP services. The scripts also probed for the availability of the file shares. Note that the last probe depended on the ability of the scripts to map the network shares. The VeriTest test proctor parsed the probing script logs and recorded timestamps reflecting state changes of the probed services.

We enabled the Network Time Protocol (NTP) and configured a common time source (ncnoc.ncrn.net) on all systems in the administrator's test environment (including the test proctor system). This synchronized the system clocks and allowed us to calculate metrics based on timestamps.

Proactive task metrics

For eight of the proactive tasks, VeriTest measured how much elapsed time the administrator spent researching, designing, implementing, testing, and documenting the implementation. We captured these measurements from the administrator's journal. Each time the administrator started a new proactive task, they entered a new time stamp in their journal along with a standardized description of the task. If a reactive event occurred that caused them to switch context, they entered a timestamp in their journal to indicate when they switched from the current proactive task to another event. Subsequently, they entered another timestamp in their journal when they resumed working on the previously interrupted proactive task. VeriTest used the set of timestamps associated with a proactive task to calculate the elapsed time spent implementing the task.

We measured the time required to apply system and application patches differently from the other proactive tasks. We allowed the administrators to download and install system and application patches as a background activity, which reflects the way administrators typically implement this task. For example,

administrators could switch to another proactive task or work on a reactive event while the patches were downloading, or they could download the patches overnight or during lunch. As a result, the time associated with the proactive patching task in the administrators' journals reflects the time spent initiating and monitoring the patch process and not the actual system (or wall clock time) required to download and install the patches. Therefore, we used the information in the administrators' journals primarily to capture the qualitative assessment of the patch process and to track the tools and processes used to apply patches. VeriTest engineers downloaded and installed patches for each platform and measured the system time required to complete the task. We used these results as a best case indication of the quantitative impact of installing patches on each platform.

After the test completed, the VeriTest test proctor conducted interviews with each administrator to further validate how much of the minimum acceptable criteria they completed for each proactive task and to capture additional qualitative information about their experiences. We used a simple scoring system to measure the quantitative amount of work completed by the administrator. We assigned one point to each of the nine proactive tasks (9 points total). We awarded the point for a task if the administrator completed all of the minimum acceptable criteria for that task. For tasks that had multiple requirements, the administrator had to successfully complete all of the requirements to get the point. Administrators who successfully implemented the minimum acceptable criteria for all nine proactive tasks scored 9 points.

Reactive Event Metrics

Microsoft defined a list of metrics and requested we capture those metrics for the reactive events. There are four classes of metrics: All, Detectable, Service loss, and Preventable. The All class defines metrics that are measured for all of the reactive events. The Detectable class defines metrics for events that could be detected by the administrator via ad hoc monitoring or automatic system notification prior to receiving a trouble ticket. The Service loss class defines metrics for events that cause disruption of a system service from the end user's perspective. The Preventable class defines metrics for events that could be prevented by the administrator through proper test environment configuration. Note that several events are in more than one class. Figure 4 lists the relevant reactive events in each class.

Detectable	Service Loss	Preventable
Reactive 1 – Mail performance	Reactive 3 – Cannot create file	Reactive 7 – Cannot access public share
Reactive 3 – Cannot create file	Reactive 4 – Cannot receive mail	Reactive 10 – Cannot log on
Reactive 4 – Cannot receive mail	Reactive 5 – Cannot access Internet	
Reactive 5 – Cannot access Internet	Reactive 6 – Cannot print	
Reactive 6 – Cannot print	Reactive 7 – Cannot access public share	
Reactive 7 – Cannot access public share	Reactive 10 – Cannot log on	
Reactive 10 – Cannot log on		
Reactive 12 – File performance		

Figure 4: Reactive event class mappings

Below is a description of the metrics captured for each of the reactive event classes:

All Reactive Events

Event Initiation Time: Depending on the event, this time is calculated from the wall clock time when the VeriTest test proctor initiates the event, the wall clock time when the administrator starts testing at the beginning of the day (for events that are initiated overnight or before the administrator arrives in the morning), or service failure times recorded by system probing scripts. When possible, we initiated the same event for all administrators at the same time.

Trouble Ticket Time: Wall clock time when the VeriTest test proctor issues a trouble ticket for an event to the administrator. The test proctor sent trouble tickets to all administrators at the same time. By default for non-detectable events, the trouble ticket time is equal to Event Initiation Time. For detectable events, the trouble ticket time is equal to Event Initiation Time + ten minutes. The test proctor records this time from the timestamp of the initial trouble ticket instant message.

Event Resolution Time: Wall clock time when the administrator closes the trouble ticket as resolved and is verified by the test proctor. This time is recorded by the test proctor from the timestamp of the resolution instant message to the trouble ticket.

Event Time: Event Resolution Time - Event Initiation Time. Lower values are better.

Event Resolution Occurred: Binary indication of whether the administrator resolved the event (state=yes) or not (state=no). The test proctor records this state based on the contents of the trouble ticket resolution email sent by the administrator. State=yes is better.

Detectable Reactive Events

Event Detection window: Trouble Ticket Time - Event Initiation Time. Typically this is ten minutes for detectable events and zero minutes for non-detectable events.

Event Detection Time: Wall clock time when a administrator detects a system problem either through manual ad-hoc monitoring or through automatic system notification. The administrator records this time in their journal. The administrator also records their hypothesis of the system problem in their journal. Note that Event Detection Time must be less than or equal to Trouble Ticket Time.

Event Detection Lag Time: Event Detection Time - Event Initiation Time. Lower values are better.

Event Detection Occurred: Binary indication of whether the administrator detected the event (state=yes) or not (state=no) before receiving the trouble ticket. The VeriTest test proctor sets the state=yes if the administrator's journal or instant message log clearly shows event detection before the trouble ticket was received. Otherwise, the test proctor sets state=no. State=yes is better.

Service Loss Reactive Events

Service Outage Time: The Service Outage time for Reactive 3 and Reactive 7 corresponded to the wall clock time when the administrator started the test that day. The Service Outage time for the remaining reactive events was the larger of:

1. The wall clock time when the service probing scripts recorded a service failure for the service targeted by the reactive event. The service probing scripts ran on the test proctor system and continually tested the availability of various system services on the test environment servers.
2. The wall clock time stamp when the reactive event trouble ticket was issued minus ten minutes.

This accounts for the fact that the service outage may not be precisely initiated in each test environment at exactly the same time. This time is only valid for reactive events where a service outage is possible.

Service Restored Time: The Service Restored time for Reactive 7 – cannot access public share was the time stamp when the administrator indicated a confirmed successful event resolution in their instant message logs. The Service Restored time for the remaining reactive events was the time stamp when the service transitioned from the unavailable to the available state. This time stamp is automatically recorded by service probing scripts running on the test proctor system. These scripts determine when the service availability stops and restarts. This time is only valid for reactive events where a service outage is possible.

Service Loss Time: Service Restored Time - Service Outage Time. Lower values are better. The Service Loss time was zero for Reactive 7 – cannot access public share and Reactive 10 – cannot log on if the administrator successfully prevented service loss through the addition of system fault tolerance features such as RAID 5 and redundant directory services. We gave special consideration to the service loss time associated with Reactive 7. In this event, a simulated drive failure destroyed the shared data on the file server. In most cases, the administrators prevented the event through RAID 5 configuration or successfully restored the lost data from tape backups. However, in some situations, the administrator did not have a valid

backup. We treated this case as a catastrophic data failure and assigned the administrator a service loss penalty. The penalty equaled the average service loss time for the Reactive 7 – cannot access public share event incurred by all administrators using the respective platform. For example, the Windows penalty was the average service loss for all Windows administrators for Reactive 7.

Service Loss Occurred: Binary indication of whether the system service targeted by the event became unavailable (state=yes) or not (state=no). If state=no, then Service Loss Time is 0. The VeriTest test proctor sets this metric based on the service probing script logs. This metric only applies to reactive events where it is possible to automatically probe for service availability. State=no is better.

Preventable Reactive Events

Prevention Occurred: Binary indication of whether the administrator modified the test environment such that the preventable event was avoided (state=yes) or not (state=no). Note that this metric only applies to preventable events. Before initiating the event, the test proctor will test to see if the event has been avoided through test environment modification. If it has, the test proctor will record this metric as yes, set the Event Time and Service Loss Time to 0, and skip sending the trouble ticket. State=yes is better.

General test design process

Prior to test execution, VeriTest developed the test methodology including the definition of the proactive tasks and reactive events, the test metrics, and the high-level specification of the hardware/software components for the Windows and Linux test environments.

VeriTest engineers installed and configured the Windows Server 2003 test environment based on the general guidelines illustrated in the Microsoft Medium Business Solution for Core Infrastructure (http://www.microsoft.com/technet/itsolutions/smbiz/mits/intro/mit_intro_1.mspx). Additionally, VeriTest engineers performed internal tests of the proactive tasks and reactive events in the actual Windows Server 2003 test environment. These internal tests validated that the proactive tasks and reactive events could successfully be completed in the Windows Server 2003 test environment within the time allotted.

VeriTest contracted a Linux consultant to install and configure the Red Hat Enterprise Linux AS 3.0 test environment. The Linux consultant specialized in designing computer solutions for business IT environments and had over ten years of hands-on experience with Linux including eight years of experience with Red Hat Linux. The Linux consultant installed Red Hat Enterprise Linux AS 3.0 on the three test servers and configured OpenLDAP, DNS, DHCP, Sendmail, and Samba. VeriTest engineers with five and seven years of Linux experience respectively worked with the Linux consultant and validated that the proactive tasks and reactive events could successfully be completed in the Red Hat Enterprise Linux AS 3.0 test environment within the time allotted.

In keeping with the goals of the test, both the Windows Server 2003 and the Red Hat Enterprise Linux AS 3.0 test environments were intentionally configured in a “failure prone” state. Basic services like directory, DNS, DHCP, email, and file sharing were functional, but the test environments did not have any hardware/software redundancy configured, up-to-date software patches installed, or basic data security configured.

Once the baseline test environments were in place, VeriTest performed a series of “dry run” tests with two Windows administrators and two Linux administrators. We followed the same recruiting process (described below) to recruit participants for the dry runs. We recruited a junior and a senior IT administrator as the two participants for each platform with the expectation that a broad range of skills would provide the most valuable feedback. The dry run participants executed the proactive tasks and reactive events over a 26 hour period. Based on the feedback from the dry run participants, we made only minor adjustments to the test methodology. This report describes the final version of the methodology.

After finalizing the test methodology, VeriTest recruited 18 Windows IT administrators and 18 Linux IT administrators for a total of 36 test participants. Testing took place at VeriTest’s Research Triangle Park, NC, facility from November 2004 through January 2005. Typically four participants (two Windows and two Linux administrators) executed the test each week. A VeriTest engineer proctored the test and monitored the progress of each administrator. Figure 5 shows the schedule for a typical weekly test cycle.

Day 1

9:00: Participants arrive at the lab

9:00—9:30: Process paperwork

9:30—11:30: Orientation process

1. Introductions
2. Time sheets
3. Overview and goals of the test
4. Test journaling process discussion
5. Test packet contents discussion

11:30—1:00: Test Bed assignments, review of materials, sample task execution, and sample trouble ticket test

1:00—2:00: Lunch

2:00—6:00: Begin first task

Day 2

9:00—1:00: Tasks

1:00—2:00: Lunch

2:00—6:00: Tasks

Day 3

9:00—1:00: Tasks

1:00—2:00: Lunch

2:00—6:00: Tasks

Day 4

9:00—1:00: Tasks

1:00—2:00: Lunch

2:00—6:00: Exit Interviews (staggered throughout the afternoon. One hour allotted per administrator).

Figure 5: Typical weekly test schedule

Test environment - hardware

We configured a test environment that simulated the infrastructure of a medium-sized business. Each test environment contained three Hewlett Packard ProLiant DL380 G3 servers, one Dell OptiPlex GX115 client system, one IBM ThinkPad A21m journaling system, one Dell OptiPlex GX115 proctor system, and a Hewlett Packard DeskJet 2300n network printer. Please refer to Appendix A for detailed information on the hardware configuration of the systems in the test environment.

The three ProLiant DL380 G3 systems served as the infrastructure (directory, DNS, DHCP), email, and file servers for our simulated business. The client system served as a typical end user work system. The administrator documented their test experience and performed all research on the IBM ThinkPad system. The VeriTest test proctor monitored test execution and injected reactive events into the test environment from the proctor system. Figure 6 shows a block diagram of the test environment.

Test Environment

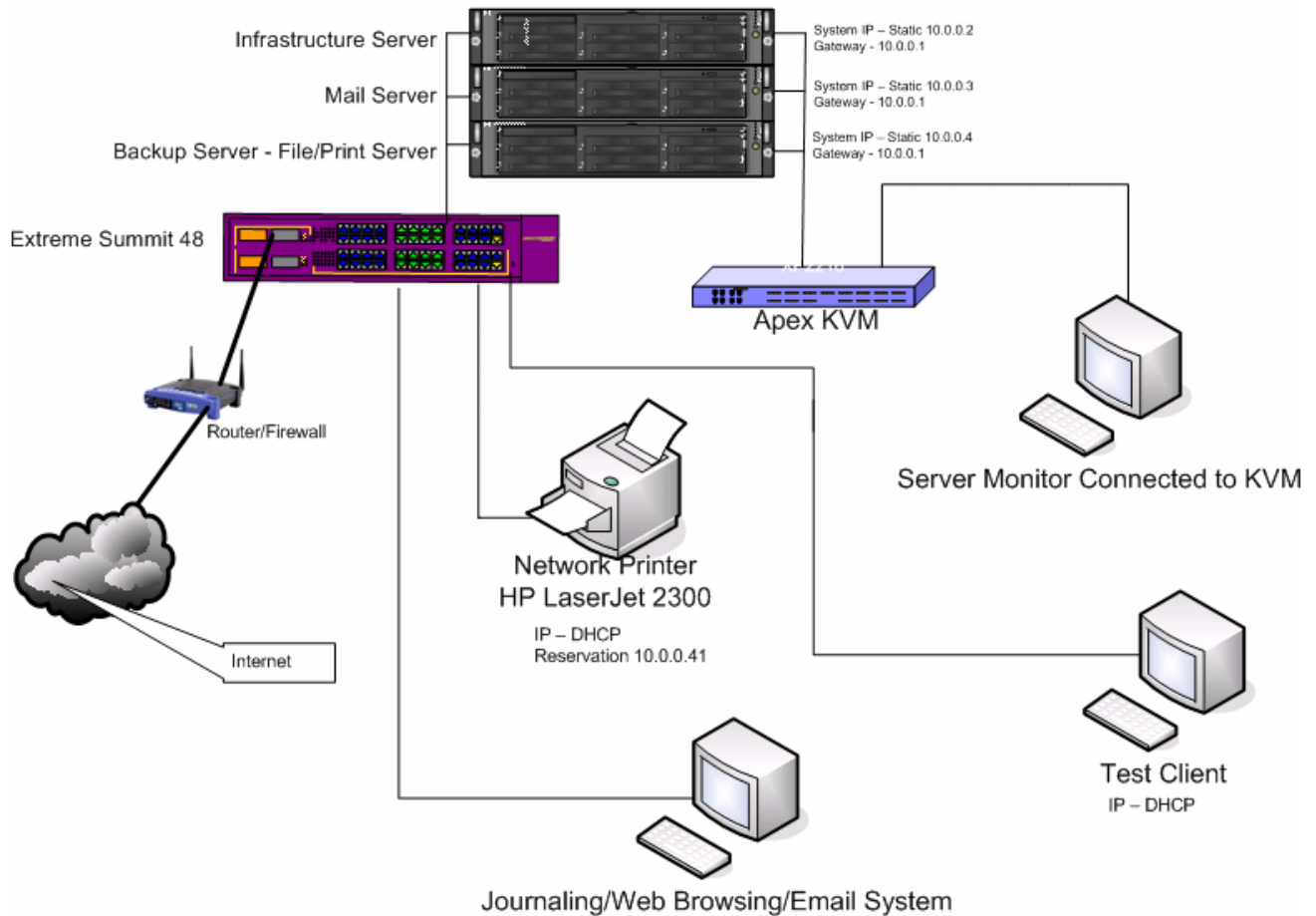


Figure 6: Test environment block diagram

We connected the primary network adapter of each system and the printer to an Extreme Networks Summit48 Ethernet switch. Additionally, we connected the Integrated Lights Out management port of each ProLiant server to the Summit48 switch. We connected the test environment to the Internet with a Linksys WRT54G four-port router. We connected a switch port on the Linksys router to the Summit48 switch with a crossover cable and connected the WAN port on the router to our Internet provider. We configured static IP addresses on the WAN and local side of the router, enabled Network Address Translation (NAT), and disabled DHCP and the integrated wireless radio. We connected the keyboard, mouse, and video connectors for the three servers and the client system to an Apex Outlook 1160ES sixteen port KVM. We set the printer to factory defaults before each test.

Each ProLiant DL380 G3 server contained four 36GB hot-pluggable drives. We installed the OS on a 25GB partition on the Slot 0 drive of each server. The remaining drives were unused on the infrastructure and email servers. We installed approximately 14.8GB of data on a 36GB partition on the Slot 1 drive of the file server. This data was shared to the user population. The file server also contained a Hewlett Packard DAT 72 tape drive. The test administrators used the tape drive to backup user and system data from the three servers. Figure 7 summarizes the drive assignments on the ProLiant DL380 G3 systems.

Drive assignments	
Infrastructure System:	File System:
Slot 0: OS	Slot 0: OS
Slot 1-3: Spare Drives	Slot 1: File Share Drive
Email System	Slot 2-3: Spare Drives
Slot 0: OS	Slot 4-5: DAT 72 Tape Drive
Slot 1-3: Spare Drives	

Figure 7: ProLiant DL380 G3 drive assignments

Microsoft supplied the 12 ProLiant DL380 G3 servers and four DeskJet 2300n printers for the test. VeriTest supplied the remainder of the equipment. We configured a total of four identical test environments defined in Figure 6. Typically, during each week of the test, we assigned two Red Hat Enterprise Linux AS 3.0 administrators and two Windows Server 2003 administrators to the four test environments. We reset the test environments to a known state before each test cycle. The next section, Test environment – software, describes the software state of the test environment at the beginning of each test cycle.

Test environment - software

We partitioned the services required to run our medium business across the three ProLiant DL380 G3 servers in each test environment as follows:

Infrastructure server

- Hosts centralized directory containing user and machine account information
- Primary authentication provider
- Hosts DHCP server
- Hosts DNS server

Email server

- Hosts primary email server application
- Hosts email databases for each user

File/Print server

- Hosts nine shares containing business data exported to user population
- Hosts tape drive for backups
- Hosts print server

In keeping with the goals of the test, both the Windows Server 2003 and the Red Hat Enterprise Linux AS 3.0 test environments were intentionally configured in a “failure prone” state. Basic services like directory, DNS, DHCP, email, and file sharing were functional, but the test environments did not have any hardware/software redundancy configured, up-to-date software patches installed, or basic data security configured. Each test environment did have a unique fully qualified domain name that mapped to valid public DNS records. We also set consistent administrator passwords on each server and the client system to simplify administration. Finally, we configured Network Time Protocol (NTP) with a common time source (ncnoc.ncren.net) on all of the systems in the test environment. This ensured that all systems had consistent clock settings, which allowed us to capture meaningful timestamps during the test.

VeriTest engineers installed and configured the Windows Server 2003 test environment. VeriTest contracted a Linux consultant to install and configure the Red Hat Enterprise Linux AS 3.0 test environment. The Linux consultant installed Red Hat Enterprise Linux AS 3.0 on the three test servers and configured OpenLDAP, DNS, DHCP, Sendmail, and Samba.

During exit interviews, over 90% of the IT administrators felt the test environment was realistic and accurately reflected a real world IT environment. One administrator commented that he thought the test environment was actually “too stable” and in much better working condition than the typical medium-sized IT environment.

Refer to Appendix F for a list of the high-level steps performed to configure the software environment on each of the three servers and the client system. For both the Windows and Linux test environments, we configured the infrastructure server first followed by the email and file servers. After completing the steps listed in Appendix F, we captured images of each system before we started testing. Before each test cycle, we loaded a copy of the saved image on each of the systems. This ensured that each system was in the same software state at the beginning of each test cycle.

Figure 8 lists the nine shares configured on the file server as well as the directory structure beneath each share. We configured identical share names in Windows Server 2003 and Red Hat Enterprise Linux AS 3.0. The Directory location column shows the full path to each share on the respective platform. We populated the shares with approximately 8,406 files totaling 14.8GB.

Share name	Directory location	Description
public	F:\public, /share/public	contains Airdrome.net public files
home	F:\home, /share/home	contains all of the Airdrome.net home directories
acc	F:\acc, /share/acc	contains Accounting group resources
engpub	F:\engpub, /share/engpub	contains Engineering group public files
engpri	F:\engpri, /share/engpri	contains Engineering group private files
hrpub	F:\hrpub, /share/hrpub	contains HR group public files
hrpri	F:\hrpri, /share/hrpri	contains HR group private files
salespub	F:\salespub, /share/salespub	contains Sales group public files
salespri	F:\salespri, /share/salespri	contains Sales group private files

F:\public, /share/public	F:\engpri, /share/engpri
\events	\plans
\manuals	\budget
\information	\research
F:\home, /share/home	F:\hrpub, /share/hrpub
Contains a subdirectory for each user, for example	\forms
\acc1	\procedures
\acc2	\information
F:\acc, /share/acc	F:\hrpri, /share/hrpri
\projections	\employees
\budget	\budget
\information	\corporate
F:\engpub, /share/engpub	F:\salespub, /share/salespub
\projects	\contacts
\information	\information
\documentation	\publications
	F:\salespri, /share/salespri
	\strategy
	\projections
	\budget

Figure 8: File share definition and directory structure on the file server

General test execution process

At the start of each new test cycle, the IT administrators attended an orientation session where VeriTest personnel described the test structure, the proactive tasks and reactive events, the test environment, and the journaling procedure. VeriTest gave administrators a written test packet that documented the information covered in the orientation. After the orientation, each administrator was assigned a test environment and had the remainder of the morning to familiarize themselves with the information in the test packet and the test environment. Also during this time, the VeriTest test proctor gave each administrator a sample proactive task to complete. The administrators documented their execution of the sample task using the journaling instructions described during the orientation. As administrators executed the sample proactive task, they were interrupted by a sample test trouble ticket that tested their ability to switch focus between proactive tasks and

reactive events. The VeriTest proctor examined the administrators' journals after they completed the sample task and event to validate proper journaling procedures.

After completing the morning orientation session, the administrators broke for lunch. After lunch, the administrators started executing the proactive tasks defined in the test methodology. Throughout the test, the VeriTest proctor sent reactive events to the administrators in the form of trouble tickets. Upon receipt of the trouble ticket, the administrators stopped working on their current proactive task and starting working on the solution to the trouble ticket. They documented in their journals their experiences and time spent on each task during the test. The administrators spent a total of 26 hours executing the test. At the completion of the test, the VeriTest proctor conducted an exit interview and a task validation interview with each administrator. The exit interview recorded feedback from the administrators on their test experience including their assessment of the test environment and of their performance on the proactive tasks and reactive events. During the task validation interview, the VeriTest proctor went over the proactive task list with the administrator and recapped the number of proactive tasks that were partially or fully completed by the administrator.

Administrators were allowed to bring in outside resources such as books and magazines during the test. They were allowed to search the Web and interact with online message boards to help troubleshoot and diagnose problems. However, they were not allowed to call, instant message, or otherwise contact colleagues during the test.

IT administrator recruitment process

VeriTest designed and implemented a structured participant recruitment process in order to recruit participants for the test that matched an IT generalist administrator profile. Specifically, we targeted candidates with a broad range of hands on IT administration skills (directory, DNS, DHCP, email, file/print, networking, etc.) rather than candidates who were experts in any one area. We posted job requirements on a number of online job sites as well as performed our own online searches to find qualified candidates. We performed an initial screening of the resumes we received and eliminated any candidates that did not have recent hands on administrative experience with Windows Server 2000/2003 or Red Hat Linux, or did not have experience in at least two of the three following areas: directory, email, and file/print administration.

We performed phone screens of the remaining participants using the questionnaires listed in Appendix C (one questionnaire applied to Windows candidates and the other applied to Linux candidates). The questionnaires contained questions designed to validate the breadth of the candidate's hands on administration experience. The phone screen results also captured the candidate's self-appraised experience level in a range of IT administration areas. We eliminated any candidates whose phone screen responses did not serve to validate the hands on administrative experience reflected on their resumes.

We gave a written test to all candidates that successfully passed the phone screen. Appendix D lists the Windows and Linux versions of the test. The test contained five easy questions, 11 medium-difficulty questions, and six difficult questions covering various aspects of system administration. In general, to receive a passing grade, participants had to provide correct answers to three or more of the five easy questions, five or more of the 11 medium-difficulty questions, and three *or fewer* of the six difficult questions. Candidates who missed more than three of the easy questions were categorized as under qualified and eliminated from consideration. Candidates who correctly answered more than three of the difficult questions were categorized as over qualified and eliminated as well. Candidates who successfully passed the written test were then scheduled to test based on their availability.

We used the self-appraisal results of the phone screen and the written test results to assess the skill levels of the candidates. We recruited similar numbers of novice, intermediate, and advanced Windows and Linux participants based on the results of our screening process. The majority of the actual test participants for both Windows and Linux had intermediate skill levels. We also included participants with novice and advanced skill sets to ensure a complete range of results and recruited the same balance for the Windows and Linux environments. However, we ensured that the average skill level for both the group of 18 Windows administrators and the group of 18 Linux administrators was at an intermediate skill level.

Journaling process

Administrators documented how much time they spent on each proactive task and reactive event in a Word document journal located on an IBM ThinkPad A21m laptop in each test environment. In addition to recording the time spent on each task, the administrators also logged in the journal the general sequence of steps they followed to complete specific tasks and events. The timestamps and logs represented how the administrators allocated time to various tasks during the test. We used the data from the journal as one of the sources for calculating the metrics defined in the Test Metrics section. Other sources included instant messaging logs, system service probing script log files, and exit interviews.

Appendix B lists the journaling process described to the administrators by the VeriTest test proctor during test orientation. As part of orientation, each administrator was given a sample task to document using the journaling process. After each administrator completed the task, the VeriTest proctor reviewed his or her journal to ensure that the administrator followed the journaling process. The VeriTest test proctor identified any deviations from the proper journaling process and recommended steps to correct the errors.

Special instructions

Feedback from the “dry run” tests indicated several test areas that needed better documentation. In response, we created a set of special instructions intended to address these areas. Appendix E lists the special instructions and the following paragraphs provide some additional background.

The dry run participants felt that the interface for the HP Array Configuration Utility installed as part of SmartStart 7.10 (Windows) or the ProLiant Support Pack version 7.11 (Linux) was somewhat confusing. In response, we created a short “how-to” guide for using the utility. We referenced the guide as part of administrator orientation and we included a copy of the guide in each administrator’s test packet.

We found that instructions for configuring the HP DAT 72 tape drive and the HP DeskJet 2300n network printer for Linux were not included in the default documentation set provided with the equipment. To help expedite installation of these devices under Red Hat Enterprise Linux AS 3.0, we supplied a list of online URLs that contained instructions for setting up the hardware. We verified with HP that these online resources were officially supported. We included references to these online resources in the Linux administrator’s test packet, and specifically told the Linux administrators that these resources would help streamline the installation process.

Test results

The following sections list the test results for the Windows Server 2003 and Red Hat Enterprise Linux AS 3.0 environments. We captured the results from the administrators’ journal files, instant messaging log files, system service probing script log files, and exit interviews. Refer to the Testing Methodology section for a more detailed description of the test metrics. For each group of test results below (proactive, reactive, and service loss/event prevention), we normalized the data by removing the lowest and highest results for each platform. The results tables contain data for the remaining 16 Windows Server 2003 administrators and 16 Red Hat Enterprise Linux AS 3.0 administrators.

Through exit interviews, we found that over 90% of the administrators participating in the test felt the test environment was realistic and accurately reflected a real world IT environment. A Windows Server 2003 administrator commented that the test environment was very standard and did reflect an accurate medium sized business. A Red Hat Enterprise Linux AS 3.0 administrator indicated that the setup was great and the equipment was really good. Another Red Hat Enterprise Linux AS 3.0 administrator commented that the environment was fairly close to a real world environment and that it was better set up than most places in terms of consistency—most small businesses with 200 people would be in much worse shape.

Test system reconfiguration: proactive task results

VeriTest provided each administrator with a list of proactive tasks to complete during the test. These tasks reflected typical background IT administrative projects completed when upgrading and reconfiguring a system and primarily involved improving the robustness and reliability of the test environment. For each proactive task, VeriTest measured how much elapsed time the administrator spent researching, designing, implementing, testing, and documenting the implementation. We captured these measurements from the administrator’s journal. Each time administrators started a new proactive task, they entered a new time stamp in their journal along with a standardized description of the task. As administrators switched tasks throughout the day, they added time stamps to the journal, tracking the amount of time spent on each task or event. After the test completed, the VeriTest test proctor conducted interviews with each administrator to assess the number of proactive tasks completed by each administrator. In addition, the test proctor ran validation scripts on the test systems to further verify relevant task functionality. Refer to the Testing Methodology Proactive Tasks Definition and Test Metrics sections for a description of the tasks and how we calculated the proactive time on task.

On average, the Windows Server 2003 environment required less time to complete proactive tasks than the Red Hat Enterprise Linux AS 3.0 environment. Overall, the average total time required for the Red Hat Enterprise Linux AS 3.0 administrators to complete the proactive tasks was 20:55:13, and the average total time required for the Windows Server 2003 administrators to complete the proactive tasks was 13:11:56, a 37% decrease in average total time compared to Red Hat Enterprise Linux AS 3.0 administrators.

Figure 9 lists the average length of time spent completing eight proactive tasks in the Windows Server 2003 and Red Hat Enterprise Linux AS 3.0 environments (refer to the discussion below on the ninth proactive task – Applying updated system and application patches). For individual times, refer to Appendix G. We calculated the average of tasks completed by adding the times of the completed tasks and dividing by that subset of tasks.

Proactive Task	Red Hat Enterprise Linux AS 3.0 Average of Tasks Completed (HH:MM:SS)	Windows Server 2003 Average of Tasks Completed (HH:MM:SS)
Configure new tape device and driver	2:15:58	0:54:54
Configure new network printer	1:29:21	0:31:27
Implement system backups	1:55:17	2:17:49
Implement better data access security	3:35:17	2:58:55
Improve system fault tolerance/redundancy	7:59:35	3:44:00
Implement basic administrator remote access	0:35:18	0:28:45
Implement routine system/security monitoring process	1:48:26	1:31:27
Change user account information	1:16:01	0:44:39
Totals	20:55:13	13:11:56
Windows % decrease in average total time	37%	

Figure 9: Proactive Tasks - Average Time Required for Implementation

Figure 10 lists the total number of proactive tasks completed in the Red Hat Enterprise Linux AS 3.0 and Windows Server 2003 environments. We considered a proactive task complete if the administrator successfully implemented all minimum acceptable criteria for that task. See Proactive Task Definition in the Testing Methodology section for definitions of the minimal acceptable criteria.

Proactive Task	Red Hat Enterprise Linux AS 3.0 Completed Tasks	Windows Server 2003 Completed Tasks
Configure new tape device and driver	16	16
Configure new network printer	16	16
Implement system backups	10	11
Implement better data access security	2	7
Improve system fault tolerance/redundancy	2	9
Implement basic administrator remote access	14	14
Implement routine system/security monitoring process	11	13
Apply updated system and application patches	14	15
Change user account information	10	16
Totals	95	117

Figure 10: Proactive Tasks - Total Tasks Completed

Windows Server 2003 required about half the amount of time to complete directory-related proactive tasks such as group creation, directory redundancy, and user management compared to Red Hat Enterprise Linux AS 3.0. When implementing better data access security, the Red Hat Enterprise Linux AS 3.0 average time to complete was more than 30 minutes longer than the average time to complete required by Windows Server 2003. The Red Hat Enterprise Linux AS 3.0 average time to complete the system fault tolerance and redundancy task was more than 4 hours longer than Windows Server 2003, and the average time to change user account information was more than 30 minutes longer compared to Windows Server 2003.

From our participant screening process, 67% of our Linux administrators rated themselves as having at least intermediate knowledge of LDAP. However, during the test, Red Hat Enterprise Linux AS 3.0 administrators struggled to complete OpenLDAP directory-related proactive tasks. In the Red Hat Enterprise Linux AS 3.0 environment, only two administrators successfully implemented OpenLDAP redundancy. For other directory-related tasks: ten successfully changed three user accounts and two administrators set up group structures and implemented the designated security permissions.

We believe a primary factor for the disparity in these results is the complexity of managing OpenLDAP on Red Hat Enterprise Linux AS 3.0 compared to the relative simplicity of managing Active Directory on Windows Server 2003. Windows Server 2003 includes integrated tools for managing Active Directory and configuring redundant Active Directory services. The Active Directory Users and Computers management tool provides a graphical interface for managing groups, users, and systems. An integrated wizard-based tool, dcpromo, provides step-by-step instructions for setting up redundant Active Directory services on multiple servers. Three Windows Server 2003 administrators applauded the ease of setting up Active Directory redundancy. One specifically mentioned that configuring Active Directory redundancy was much easier than expected.

In contrast, there is no universally accepted OpenLDAP management tool for Red Hat Enterprise Linux AS 3.0. Half of the Red Hat Enterprise Linux AS 3.0 administrators mentioned some type of problem configuring LDAP or finding a tool to successfully manage OpenLDAP. The Red Hat Enterprise Linux AS 3.0 administrators chose several different OpenLDAP management tools. The most widely used tool was a GUI browser-based tool called Webmin. Other tools used included LDAP Account Manager, LDAP Browser/Editor, and the Idealx SMB-LDAP command line tools installed on the systems by VeriTest (information provided to the Linux administrators during orientation indicated the Idealx SMB-LDAP tools were pre-installed on the infrastructure server). According to the Red Hat Enterprise Linux AS 3.0 administrators' journals, the Webmin tool did not properly synchronize the Posix and Samba user account information. In general, Red Hat Enterprise Linux AS 3.0 administrators had the most success managing OpenLDAP with the provided SMB-LDAP tools from Idealx.

Finding documentation for configuring OpenLDAP/Samba redundancy was challenging for Red Hat Enterprise Linux AS 3.0. Administrators commented that the available OpenLDAP/Samba redundancy

documentation focused on redundancy implementations where all of the components were on a single system and did not provide enough examples for administrators to set up redundancy on multiple systems.

The average time spent for Red Hat Enterprise Linux AS 3.0 on the tape device and printer configuration proactive tasks was more than two hours greater than Windows Server 2003 (3:45:19 vs. 1:26:21). Several Red Hat Enterprise Linux AS 3.0 administrators commented that the tape drive configuration process was confusing and frustrating. One mentioned specifically that configuring the tape drive was hard to understand and that he didn't like having to create scripts to enable the drive. In general, the device driver installation process on Red Hat Enterprise Linux AS 3.0 is not as consistent as the binary driver installation packages for Windows Server 2003, resulting in more diversity in the steps required to install and configure devices. Also, hardware manufacturers have their own proprietary hardware naming conventions in Red Hat Enterprise Linux AS 3.0 (e.g., /dev/cciss on the HP ProLiant DL380 G3 systems). In Windows Server 2003, the device hardware naming is universal across manufacturers. Also the low level specifics of the device's architecture are more exposed in Red Hat Enterprise Linux AS 3.0 compared to Windows Server 2003. This can be an advantage in using the device, but it may introduce more complexity during device configuration. Note that the HP tape drive and printer driver CD included with the devices contained Windows Server 2003 drivers, but did not contain Red Hat Enterprise Linux AS 3.0 drivers. VeriTest provided special instructions to the Red Hat Enterprise Linux AS 3.0 administrators containing URL's to Web sites with specific information on how to set up the HP tape drive and printer hardware. However, although part of their orientation, not all administrators read or followed the special instructions. One Red Hat Enterprise Linux AS 3.0 administrator commented that when you go to a client site, you rarely have all the documentation and drivers in one place, and that he forgot to use the provided information to configure the tape drive. Some Red Hat Enterprise Linux AS 3.0 administrators configured the tape drive and printer in less than an hour and all administrators did successfully configure the tape drive and printer. Their completion times did not necessarily correlate with skill level. No Windows Server 2003 administrators had any issues with tape drive or printer configuration.

We measured the time required to apply system and application patches differently from the other proactive tasks. We allowed the administrators to download and install system and application patches as a background activity, which reflects the way administrators typically implement this task. For example, administrators could switch to another proactive task or work on a reactive event while the patches were downloading, or they could download the patches overnight or during lunch. As a result, the time associated with the proactive patching task in the administrators' journals reflects the time spent initiating and monitoring the patch process and not the actual system (or wall clock time) required to download and install the patches (the time spent initiating and monitoring the patch process ranged from approximately 30 minutes to 3 hours for the Windows Server 2003 administrators and approximately 12 minutes to 1 hour and 47 minutes for the Red Hat Enterprise Linux AS 3.0 administrators). Therefore, we used the information in the administrators' journals primarily to capture their qualitative assessment of the patch process and to track the tools and processes used to apply patches. VeriTest engineers downloaded and installed patches for each platform and measured the system time required to complete the task. We used these results as a best case indication of the quantitative impact of installing patches on each platform.

The Red Hat Enterprise Linux AS 3.0 patch update tool, up2date, provided a single interface for downloading kernel, library, and application updates. The tool was simple to use and run. Two Red Hat Enterprise Linux AS 3.0 administrators praised up2date; however, one complained that the unreliability of the progress indicator made it difficult to gauge the completion of the patch process and another complained that the patch process hung several times. The version of up2date included in the default Red Hat Enterprise Linux AS 3.0 installation is outdated. Before the Red Hat Enterprise Linux AS 3.0 administrator can download and install new packages, a new version of up2date must be installed. By default the kernel packages are flagged to be skipped; however, administrators can choose to update the kernel. Fourteen Red Hat Enterprise Linux AS 3.0 administrators chose to select all packages for download. Updating the kernel does not force the administrator to reboot the server. At the end of the up2date process the administrator is prompted to perform a system restart for the kernel to take effect. Of the 14 Red Hat Enterprise Linux AS 3.0 administrators that updated the kernel, ten chose to reboot after applying the new kernel.

The Windows Server 2003 update process required downloading critical updates for the OS from one location followed by a separate process to update Exchange Server 2003. Several Windows Server 2003 administrators complained that they had to download an additional hotfix from a third location in order to

actually install the Exchange Server 2003 updates. However, note that if the Red Hat Enterprise Linux AS 3.0 environment had included a similar integrated messaging solution, such as Novell GroupWise, the Red Hat Enterprise Linux AS 3.0 administrators would have been required to access more than one location for updates as well. Also, while patching the email server, the Windows Update tool presented a warning that one critical update was not installed. To install this critical update, the Windows Server 2003 administrator had to reboot and run Windows Update a second time. At this point the missing critical update was detected and installed. A second reboot was required to apply this update.

The up2date tool required fewer steps than Windows Server 2003, but it introduced system robustness problems. The up2date process downloaded new patches that introduced several system reliability problems. Four of the Red Hat Enterprise Linux AS 3.0 administrators indicated that the patching process caused system reliability problems and spent time troubleshooting and repairing the systems. The patching process updated Samba, resulting in changes to the contents of the Samba secrets.tdb file on the file server for each administrator that completed this task. This caused network shares to become inaccessible. The administrator was then required to troubleshoot and fix Samba on the file server. Documentation on the samba.org Web site indicates that updating Samba may cause changes to the secrets.tdb file. Four Red Hat Enterprise Linux AS 3.0 administrators never successfully diagnosed and fixed the secrets.tdb problem. Starting the week of 12/22/04 to 12/30/04, new updates on the Red Hat update servers caused administrators to experience two problems. The first problem added an Ethernet hardware address line in the ifcfg-eth0 file, causing the network connection on all three servers to fail after reboot. The second problem caused DNS (bind version 9.2.2-21 updated to 9.2.4-5_el3) to become unstable resulting from a replacement of the named.conf file. No Windows Server 2003 administrators cited comparable issues with critical updates.

The up2date process took 2 hours 50 minutes for a complete download and installation of packages. There were approximately 665,337KB of Red Hat rpm update packages available for download; 374 packages for the directory server, 372 packages for the email server and 373 packages for the file server. The Windows Update tool for the directory and file servers detected 33 critical updates and service packs and 34 critical updates for the email server. The administrator does not have to reboot at the completion of the update process, but the updates do not take effect until a reboot has occurred. Every Windows Server 2003 administrator chose to reboot each server. The approximate time to complete the update process for critical updates was 32 minutes on the Windows Server 2003 systems. There are separate sites for downloading Service Pack 1 (101869KB) and a required hotfix (831464) for Exchange Server 2003. The approximate time to download and install the hotfix and Service Pack 1 for Exchange Server 2003 was 32 minutes.

Figure 11 summarizes the qualitative patch results captured from the journals and the quantitative patch results captured through best case patch scenarios performed by VeriTest engineers.

		Windows Server 2003	Red Hat Enterprise Linux AS 3.0
Task Time (Quantitative) Times VeriTest validated in the lab	Download Time	0:26:00 (0:05:00 critical updates) (0:21:00 Exchange SP1)	1:15:00
	Total Patch Time	1:04:00 (0:32:00 critical updates) (0:32:00 Exchange SP1)	2:50:00
Journaling (Qualitative)	Patch Update Tools Used	Windows Update	up2date
	Activities Journalled	Installing Microsoft Baseline Security Analyzer, Installing System Update Services	Installing patches overnight or during lunch, researching yum tool
	System Breakages: # of administrators that never resolved system stability issues caused by patching (percentage of administrators)	0 (0%)	4 (25%) <i>e.g., Samba and network issues</i>

Figure 11: Applying system and application patches proactive task summary

Windows Server 2003 administrators had more difficulty with the email-related proactive tasks (backing up mailboxes and moving mailboxes to a RAID 5 partition) than the Red Hat Enterprise Linux AS 3.0 administrators. Note that this test targeted administrators with general IT skill sets who may not be as familiar with tasks such as moving mailboxes compared to administrators with specialized IT messaging skill sets. Four of the Windows Server 2003 administrators failed to successfully back up the Exchange mailboxes on the email server. Ten Windows Server 2003 administrators wrote in their journals that they weren't sure how to back up Exchange mailboxes. We instructed the administrators to use built-in OS tools for backups, which would be the Backup Utility for Windows for Windows Server 2003. The Backup Utility for Windows includes support for backing up Exchange mailboxes, but most Windows Server 2003 administrators were not familiar with its use. Although the Backup Utility for Windows provides basic backup and restore functionality, Microsoft recommends, and most companies and messaging specialists choose to implement, a 3rd party backup solution geared specifically towards mission critical applications like email. Also, several Windows Server 2003 administrators commented that the Backup Utility for Windows documentation and integrated help did not explain very well how to back up Exchange mailboxes. The process of backing up an Exchange information store is more complicated due to its design as a transaction-oriented database. Most Windows Server 2003 administrators wrote in their journals that they needed to research how to move the Exchange information store (mailboxes) as part of configuring a separate RAID 5 partition for the mailboxes.

System troubleshooting events: reactive event results

As the administrators designed and implemented the proactive tasks, a VeriTest test proctor generated a sequence of 13 reactive events that required system troubleshooting. After generating the event, the test proctor (acting as a user) issued an instant message trouble ticket to the administrator describing the symptom of the event. These reactive events simulated IT requests from the user population (e.g., restore files, restore deleted mail) as well as hardware/software issues (e.g., printer doesn't work, can't receive email). The administrators were instructed to treat a reactive event as their highest priority activity. As soon as the administrators received the event, they stopped working on their current proactive task and focused all their effort on diagnosing and resolving the reactive event. They recorded the time spent on each reactive task in their journals. At the end of the test VeriTest analyzed the journals and instant message logs to determine the amount of time each administrator spent on reactive events. Refer to the Testing Methodology Reactive Event Definition and Test Metrics sections for a description of the events and how we calculated the reactive time on task.

In our group of administrators, we found that Windows Server 2003 administrators required less average time, overall, to fix reactive events. The average total time required for the Red Hat Enterprise Linux AS 3.0 administrators to complete the reactive events was 6:52:52, and the average total time required for the Windows Server 2003 administrators to complete the reactive events was 5:32:18, a 20% decrease in average total time compared to Red Hat Enterprise Linux AS 3.0 administrators. The Windows Server 2003 administrators successfully fixed more reactive events than the Red Hat Enterprise Linux AS 3.0 administrators. They also detected more than twice as many events as the Red Hat Enterprise Linux AS 3.0 administrators.

Figure 12 lists the average length of time the Red Hat Enterprise Linux AS 3.0 and Windows Server 2003 administrators worked on the thirteen reactive events. For individual times, refer to Appendix G. We calculated the total time required for the administrators on each platform by adding the average reactive event times for all administrators.

Reactive Event	Red Hat Enterprise Linux AS 3.0 Average (HH:MM:SS)	Windows Server 2003 Average (HH:MM:SS)
Reactive 1 - Mail performance	0:23:21	0:33:52
Reactive 2 - File deletion	0:25:21	0:15:32
Reactive 3 - Cannot create file	0:25:44	0:21:18
Reactive 4 - Cannot receive mail	0:12:57	0:50:33
Reactive 5 - Cannot access Internet	1:00:27	0:19:20
Reactive 6 - Cannot print	0:44:44	0:37:08
Reactive 7 - Cannot access public share	1:33:32	0:26:31
Reactive 8 - File deletion	0:18:26	0:11:53
Reactive 9 - Mail deletion	0:17:00	0:49:47
Reactive 10 - Cannot log on	0:22:59	0:04:07
Reactive 11 - File deletion	0:28:45	0:15:11
Reactive 12 - File performance	0:32:38	0:37:27
Reactive 13 - Incorrect directory permissions	0:06:58	0:09:40
Totals	6:52:52	5:32:18
Windows % decrease in average total time	20%	

Figure 12: Reactive Events - Average Time Required to fix Reactive Events

Figure 13 lists the total number of reactive events the Red Hat Enterprise Linux AS 3.0 and Windows Server 2003 administrators, as a group, fixed within the three-day test. The Fixed column indicates the number of administrators who successfully resolved the event. The Failed column indicates the number of administrators who failed to fix the event. The N/A column indicates the number of instances that the administrator's system was in a state that prevented VeriTest from executing the reactive event and submitting the trouble ticket for that event at the scheduled time. For example, administrators who received an N/A for Reactive 13 – Incorrect directory permissions did not have groups set up at the time and did not receive a trouble ticket for that event.

Reactive Event	Red Hat Enterprise Linux AS 3.0			Windows Server 2003		
	Fixed	Failed	N/A	Fixed	Failed	N/A
Reactive 1 – Mail performance	16			16		
Reactive 2 – File deletion	1	15		1	15	
Reactive 3 - Cannot create file	16			16		
Reactive 4 - Cannot receive mail	16			16		
Reactive 5 - Cannot access Internet	16			16		
Reactive 6 - Cannot print	15		1	16		
Reactive 7 - Cannot access public share	11	5		14	2	
Reactive 8 – File deletion	9	4	3	11	2	3
Reactive 9 – Mail deletion	11	5		2	14	
Reactive 10 - Cannot log on	16			15		1
Reactive 11 – File deletion	9	2	5	12		2
Reactive 12 – File performance	13	3		15	1	
Reactive 13 - Incorrect Directory Permissions	4		12	11		5
Totals	153	34	21	163	34	11

Figure 13: Reactive Events Completed

Red Hat Enterprise Linux AS 3.0 administrators spent, on average, approximately one hour fixing the DHCP reactive event, Reactive 5 – Cannot access Internet, compared to approximately 19 minutes for their Windows counterparts. Troubleshooting this event in Red Hat Linux Enterprise Linux AS 3.0 requires looking at not only the DHCP configuration files, but also the dhcpd.leases files which are stored in a separate location. However, in Windows Server 2003 all of the configuration and lease information is stored in the Windows DHCP management snap-in. Both operating systems generate log records that should have helped diagnose this problem.

Red Hat Enterprise Linux AS 3.0 administrators also spent more time working on the RAID event, Reactive 7 – Cannot access public share. While Windows Server 2003 administrators only required approximately 26 minutes to fix this problem, Red Hat Enterprise Linux AS 3.0 administrators required one hour 33 minutes to restore access to the public share. In this event, the VeriTest test proctor simulated a drive failure by removing and reinserting the drive containing all of the share data on the file server. If the drive was part of a fault-tolerant RAID 5 stripe, no data loss occurred and the VeriTest test proctor did not issue a trouble ticket. If the drive had no fault tolerance, the VeriTest test proctor deleted all of the file share data and issued a trouble ticket. Fewer Red Hat Enterprise Linux AS 3.0 administrators (three) versus Windows Server 2003 administrators (seven) configured the public share on a RAID 5 fault-tolerant partition prior Reactive 7. As a result, four more Red Hat Enterprise Linux AS 3.0 administrators received the trouble ticket and had to troubleshoot the event. Administrators implemented RAID through the HP Array Configuration utility. We

provided special instructions for both platforms on how to use this utility. We received mixed feedback on this utility. Seven Windows Server 2003 administrators and two Red Hat Enterprise Linux AS 3.0 administrators had problems or complained about the HP Array Configuration utility. However, four Windows Server 2003 administrators and two Red Hat Enterprise Linux AS 3.0 administrators liked the utility and praised its ease of use.

Windows Server 2003 administrators spent more time on events involving the mail server than Red Hat Enterprise Linux AS 3.0 administrators (Reactive 4 – cannot receive mail and Reactive 9 – mail deletion). The majority of the Exchange experience of the Windows Server 2003 administrators in the test was with Exchange 5.5 or Exchange 2000, while only two Windows Server 2003 administrators indicated Exchange Server 2003 experience. The Windows Server 2003 administrators spent an average of approximately 50 minutes to resolve Reactive 4, whereas the Red Hat Enterprise Linux AS 3.0 administrators spent approximately 13 minutes. After we deleted the email message for Reactive 9, two Windows Server 2003 administrators successfully restored the deleted email, while eleven Red Hat Enterprise Linux AS 3.0 administrators successfully restored the deleted email. Lack of familiarity with Exchange Server 2003 may have deterred Windows Server 2003 administrators from utilizing tools, such as the Exchange Deleted Items Recovery feature, which reduces the time and effort required to restore deleted emails (only two Windows Server 2003 administrators took advantage of the Exchange Deleted Item Recovery feature). One of the two Windows Server 2003 administrators familiar with Exchange Server 2003 commented that he liked the improved functionality of Exchange 2003, especially the feature [Exchange Deleted Item Recovery] to recover deleted emails. Another Windows Server 2003 administrator who was not familiar with Exchange Server 2003 commented that there was so much available Exchange documentation, that if you didn't know what you were looking for, it was really time consuming. This disparity could also be attributed to the dependency of Exchange on the Active Directory database store, which required additional steps for Windows Server 2003 administrators, as opposed to Sendmail, which is not tightly coupled with directory services. Also, in Red Hat Enterprise Linux AS 3.0, the flat mailbox files can be readily analyzed with the text-based tools native to the operating system. It is worth noting that Exchange Server 2003 contains many features not found in Sendmail including calendaring and contact management, tight integration with directory services, and integrated mobile access (e.g., Outlook Web Access and ActiveSync for accessing email on mobile devices such as Smartphones and PDAs).

For the detectable events, VeriTest delayed ten minutes after initiating the event before submitting the trouble ticket. The score for detectable events was binary. If administrators detected the event within the ten-minute window they received a score of 1. Administrators who did not detect the event received a score of 0. We used a combination of the instant message log and the administrator journal to determine whether or not event detection occurred. We gave each administrator the option to respond to a trouble ticket with one of two possible responses: 1) I have detected the problem and am currently investigating it or 2) I will investigate the problem. If the administrator returned the first response, we referred to the journal to verify that the administrator had detected the event, had made a note to that fact, and had begun to work on the problem. The administrator received a score of 1 with supporting evidence in the journal. If there was no corroborating data in the journal to support the response, the administrator received a score of 0 for detection. If the administrator responded with the second response, the administrator received a score of 0 for the event.

Figure 14 lists the number of events the Linux and Windows administrators detected before receiving a trouble ticket.

Event	Red Hat Enterprise Linux AS 3.0 Events Detected	Windows Server 2003 Events Detected
Reactive 1 - Mail performance	0	0
Reactive 3 - Cannot create file	0	6
Reactive 4 - Cannot receive mail	0	0
Reactive 5 - Cannot access Internet	1	1
Reactive 6 - Cannot print	0	0
Reactive 7 - Cannot access public share	0	2
Reactive 10 - Cannot log on	4	2
Reactive 12 - File performance	0	0
Totals	5	11

Figure 14: Reactive Events - Event Detection

We saw five total event detections by Red Hat Enterprise Linux AS 3.0 administrators and 11 by Windows Server 2003 administrators. The main difference between the two groups can be seen in Reactive 3 – Cannot create file. Six Windows Server 2003 administrators detected this reactive event. No Red Hat Enterprise Linux AS 3.0 administrators detected this event prior to receiving the trouble ticket. In this event, the test proctor filled up all of the available disk space on the data partition of the file server preventing the creation of additional files. Of special interest is the fact that Windows Server 2003 displays a popup balloon message on the task bar (shown in Figure 15) when a file system becomes low on space. When the Windows Server 2003 administrators arrived in the morning, they likely saw this warning message, which helped them to detect the Reactive 3 event before the trouble ticket was sent. The other major reactive event detected before we sent the trouble ticket was Reactive 10 – Cannot log on. Four Red Hat Enterprise Linux AS 3.0 administrators and two Windows Server 2003 administrators detected this event before we issued the trouble ticket. The directory server actually powered off as part of this event, which may have given an audible indication to administrators of a possible problem.

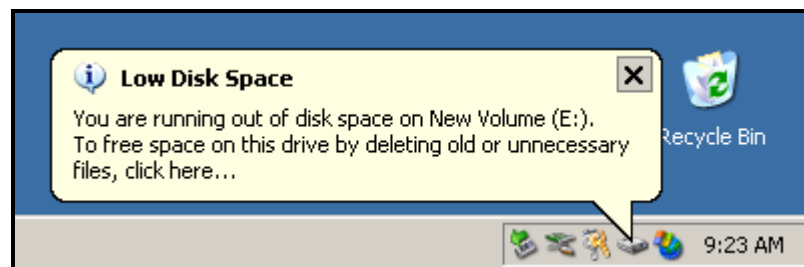


Figure 15: Windows Server 2003 low disk space alert

Service loss and event prevention results

The service loss metrics measured the amount of system service downtime caused by a series of reactive events initiated by the VeriTest test proctor. Each service loss reactive event targeted a specific system service (e.g., email, printer) and caused that service to become unavailable to the user population. Refer to the Test Methodology Reactive Event Definition and Test Metrics sections for a description of the reactive events associated with service loss and the definition of the service loss metrics.

The Windows Server 2003 environment had 4:20:19 of average service loss time and the Red Hat Enterprise Linux AS 3.0 environment had 4:59:44 of average service loss time for the measured service loss reactive events. Overall, the Red Hat Enterprise Linux AS 3.0 environment had an increase of 15% in average service loss time on the measured service loss reactive events compared to test systems running Windows Server 2003. Note that lower service loss numbers are better.

Figure 16 contains the service loss results. The table contains the average service loss time for each administrator for the service loss related events. For individual times, refer to Appendix G.

Event	Red Hat Enterprise Linux AS 3.0 Average (HH:MM:SS)	Windows Server 2003 Average (HH:MM:SS)
Reactive 3 - Cannot create file	0:39:53	0:49:13
Reactive 4 - Cannot receive mail	0:15:52	1:07:10
Reactive 5 - Cannot access Internet	1:07:36	0:25:29
Reactive 6 - Cannot print	1:19:00	0:49:30
Reactive 7 - Cannot access public share	1:27:55	1:04:33
Reactive 10 - Cannot log on	0:09:29	0:04:25
Totals	4:59:44	4:20:19
Red Hat Enterprise Linux AS 3.0 % increase in average service loss time	15%	

Figure 16: Service Loss Results

The average service loss associated with Reactive 5 – cannot access Internet was approximately 40 minutes higher for Red Hat Enterprise Linux AS 3.0 administrators compared to Windows Server 2003 administrators. In this event, the VeriTest test proctor released the DHCP lease on the test client and configured the test server's DHCP settings so there were no available leases. As mentioned earlier, some of this disparity may be due to the split of the Red Hat Enterprise Linux AS 3.0 DHCP management into two files: the dhcpd.conf file containing the DHCP configuration settings and the dhcpd.leases file containing the list of active leases. Also, there was no provided tool to quickly view DHCP lease status in Red Hat Enterprise Linux AS 3.0. The Windows Server 2003 DHCP management utility combined the configuration settings and lease management into a single tool which included a status view of the currently assigned leases. Note that both Windows Server 2003 and Red Hat Enterprise Linux AS 3.0 generated log records indicating that there were no available leases remaining.

The average service loss associated with Reactive 7 – cannot access public share was approximately 20 minutes higher for Red Hat Enterprise Linux AS 3.0 administrators compared to Windows Server 2003 administrators. This difference resulted in an average service loss time for Reactive 7 of one hour and 27 minutes for Red Hat Enterprise Linux AS 3.0 administrators versus one hour and four minutes for Windows Server 2003 administrators. In this event, the VeriTest test proctor simulated a drive failure by removing and reinserting the drive containing all of the share data on the file server. If the drive was part of a fault-tolerant RAID 5 stripe, no service loss occurred. If the drive had no fault tolerance, the VeriTest test proctor deleted all of the file share data resulting in a service loss. Fewer Red Hat Enterprise Linux AS 3.0 administrators (three) versus Windows Server 2003 administrators (seven) configured the public share on a RAID 5 fault tolerant partition prior Reactive 7. As a result, four more Red Hat Enterprise Linux AS 3.0 administrators incurred service loss for that event. Also, more Red Hat Enterprise Linux AS 3.0 administrators (six) versus Windows Server 2003 administrators (two) suffered catastrophic data loss for this event due to lack of valid backups of the public share data. In the case of catastrophic data loss, we assigned a service loss penalty equal to the average service loss time for Reactive 7 incurred by all administrators using the respective platform. For example, the Linux service loss penalty was the average service loss for all Red Hat Enterprise Linux AS 3.0 administrators for Reactive 7.

The average service loss associated with Reactive 4 – cannot receive email was approximately 50 minutes greater for Windows Server 2003 administrators compared to Red Hat Enterprise Linux AS 3.0 administrators. This difference resulted in an average service loss time for Reactive 4 of one hour and seven minutes for the Windows Server 2003 administrators versus approximately 16 minutes for Red Hat Enterprise Linux AS 3.0 administrators. In this event, the administrators had to troubleshoot problems receiving external email. The event resolution involved restarting the SMTP service. We believe a primary factor for the results disparity is that the SMTP service is only one of numerous Exchange services, while it is a primary component of Sendmail. Also, access to the interface for managing the Exchange SMTP service requires

expanding several layers of items in the Exchange System Manager tool. As a result, it is more time consuming to isolate the problem in Windows Server 2003. As mentioned previously, the Windows Server 2003 administrators in general spent more time on Exchange related reactive events than the Red Hat Enterprise Linux AS 3.0 administrators spent on Sendmail related reactive events. This may be related to the Windows Server 2003 administrators' lack of Exchange Server 2003 expertise. We did find that the more experienced Windows Server 2003 administrators tended to resolve this event quicker. Unfamiliarity with the dependence of external mail on the SMTP protocol made this event difficult for the less experienced Windows Server 2003 administrators. Also, the less experienced Windows Server 2003 administrators commented that the Microsoft Exchange SMTP documentation wasn't very helpful resolving this event.

The event prevention metric indicated whether or not the administrator successfully prevented system disruption (and associated service loss) by configuring additional fault tolerance and redundancy in the test environment. The following reactive events were classified as preventable events:

- Reactive 7 – cannot access the public share
- Reactive 10 – cannot log on

If the administrator successfully moved the file share data to a fault tolerant RAID 5 partition on the file server before the VeriTest test proctor issued Reactive 7, we recorded a successful event prevention. We noted the administrator's RAID configuration before issuing the event. Similarly, if the administrator configured redundant directory services before the VeriTest test proctor issued Reactive 10, we recorded a second successful event prevention. The system service probing logs recorded the state of directory redundancy at the time the Reactive 10 was issued.

Overall, Windows Server 2003 administrators had four times the number of prevented events compared to the Red Hat Enterprise Linux AS 3.0 administrators (16 vs. 4). Seven of the Windows Server 2003 administrators prevented Reactive 7 through RAID 5 redundancy compared to three event preventions for Red Hat Enterprise Linux AS 3.0 administrators. One possible factor for this difference is that the Windows Server 2003 administrators spent less time on the device configuration proactive tasks, which allowed more time to configure RAID 5 redundancy on the file server. Nine Windows Server 2003 administrators prevented Reactive 10 through directory service redundancy compared to one event prevention for Red Hat Enterprise Linux AS 3.0 administrators. This disparity is primarily due to the simplicity of configuring redundant Active Directory services through the dcpromo wizard tool in Windows Server 2003 compared to the complexity of configuring OpenLDAP redundancy through the LDAP configuration files in Red Hat Enterprise Linux AS 3.0.

Figure 17 lists the number of events successfully prevented by Linux and Windows administrators.

Reactive Event	Event Prevention	
	Red Hat Enterprise Linux AS 3.0	Windows Server 2003
Reactive 7 - Cannot access public share	3	7
Reactive 10 - Cannot log on	1	9
Totals	4	16

Figure 17: Event Prevention results for Linux and Windows Administrators

Appendix

A. Hardware and software configuration information

Directory, Email server	
Model	HP ProLiant DL380 G3
BIOS	ProLiant System BIOS – P29 (6/23/2004)
Processor(s)	2 – Intel Xeon™ 3.2 GHz with Hyper Threading enabled
L2 Cache	512 KB
L3 Cache	2 MB
Memory	1 GB
Disk controller(s)	HP Smart Array 5i (64MB, V2.58)
Drive(s)	4 – 36.4GB Wide UltraSCSI 15K RPM (HP model BF03685A35) Drives located in Slots 0, 1, 2, 3
CD-ROM	HP CD-ROM SN-124
Network Adapter(s)	2 – integrated HP NC7781 Gigabit Server Adapters
Video	ATI RAGE XL PCI (B41) 8 MB
Other	Integrated Lights-Out 1.51 Mar 05/2004
OS	Windows Server 2003 Red Hat Enterprise Linux AS 3.0
Software	Tight VNC 1.2.9 (Windows) or X11vnc 0.6.2-1.1 (Linux) Trend Micro ServerProtect 5 (Windows) or Trend Micro ServerProtect for Linux 1.3 (Linux)

Figure 18: Directory and email server hardware configuration

File server	
Model	HP ProLiant DL380 G3
BIOS	ProLiant System BIOS – P29 (6/23/2004)
Processor(s)	2 – Intel Xeon™ 3.2 GHz with Hyper Threading enabled
L2 Cache	512 KB
L3 Cache	2 MB
Memory	1 GB
Disk controller(s)	HP Smart Array 5i (64MB, V2.58)
Drive(s)	4 – 36.4GB Wide UltraSCSI 15K RPM (HP model BF03685A35) located in drive slots 0, 1, 2, and 3
CD-ROM	HP CD-ROM SN-124
Network Adapter(s)	2 – integrated HP NC7781 Gigabit Server Adapters
Video	ATI RAGE XL PCI (B41) 8 MB
Other	Integrated Lights-Out 1.51 Mar 05/2004 HP StorageWorks DAT 72 tape drive (model Q1529A Rev: E001) located in drive slots 4 and 5
OS	Windows Server 2003 Red Hat Enterprise Linux AS 3.0
Software	Tight VNC 1.2.9 (Windows) or X11vnc 0.6.2-1.1 (Linux) Trend Micro ServerProtect 5 (Windows) or Trend Micro ServerProtect for Linux 1.3 (Linux) Samba 3.0.7 (Linux)

Figure 19: File server hardware configuration

Client system	
Model	Dell OptiPlex GX115

BIOS	Dell A03
Processor(s)	1 – Intel Pentium™ III 866 MHz
L2 Cache	256 KB
Memory	256 MB
Drive(s)	1 – 20GB Maxtor 5T020H2 IDE
CD-ROM	TEAC CD-224E
Network Adapter(s)	1 – integrated 3Com 3C920 Fast Ethernet Controller (3C905C-TX compatible)
Video	Integrated Intel 82815 (4MB)
OS	Windows XP Professional SP1
Software	Symantec Norton Anti-Virus Corporate Edition 9.0

Figure 20: Client system hardware configuration

Journaling system	
Model	IBM ThinkPad A21m
BIOS	IBM KXET 36WW (1.09), 5/8/2003 or IBM KXET 35WW (1.08), 10/15/2002
Processor(s)	1 – Intel Pentium™ III 700 MHz
L2 Cache	256 KB
Memory	192 MB
Drive(s)	1 – 10GB Hitachi DK23BA-10B
CD-ROM	Hitachi DVD-ROM GD S200 or Matsita DVD-ROM SR-8175
Network Adapter(s)	1 – integrated 3Com 10/100 Mini PC Ethernet Adapter
Video	Integrated ATI RAGE Mobility P/M AGP 2x(A21/2), 4MB
OS	Windows XP Professional SP1 or SP2
Software	Microsoft Office Professional Edition 2003 SP1 Mozilla FireFox 1.0 Gaim 1.0.2 GTK+ Runtime 2.4.10 rev b Symantec Norton Anti-Virus Corporate Edition 9.0 Google Toolbar for Internet Explorer Microsoft .NET Framework 1.1

Figure 21: Journaling system hardware configuration

Test Proctor system	
Model	Dell OptiPlex GX115
BIOS	Dell A03
Processor(s)	1 – Intel Pentium™ III 866 MHz
L2 Cache	256 KB
Memory	256 MB
Drive(s)	1 – 20GB Maxtor 5T020H2 IDE
CD-ROM	TEAC CD-224E
Network Adapter(s)	1 – integrated 3Com 3C920 Fast Ethernet Controller (3C905C-TX compatible) 1 – Intel PRO/100+ PCI Ethernet Controller
Video	Integrated Intel 82815 (4MB)
OS	Windows 2000 Server SP4
Software	Microsoft Office Professional Edition 2003 SP1 Gaim 1.0.2 GTK+ Runtime 2.4.10 rev b Symantec Norton Anti-Virus Corporate Edition 9.0 ActiveState Perl 5.8.4 Build 810 Putty 0.54

	Tight VNC 1.2.9 Microsoft ISA Server 2004
--	--

Figure 22: Test proctor system hardware configuration

Network printer	
Model	HP LaserJet 2300n
Firmware	20031124 04.048.0
Personalities	PCLXL, PCL, PS
Memory	8 MB Flash, 48 MB SDRAM
Interface	HP JetDirect J6057A

Figure 23: Network printer hardware configuration

Network switch	
Model	Extreme Networks Summit48
Firmware	4.1.19b2
Ports	48 10/100, 2 GBIC

Figure 24: Network switch hardware configuration

Network router	
Model	Linksys WRT54G79D
Firmware	2.04.4
Ports	4 10/100 internal, 1 10/100 WAN
Configuration	Wireless Network Mode disabled DHCP server disabled Port 25 port forwarding to email server enabled Static IP address

Figure 25: Network router hardware configuration

B. Administrator journaling instructions

Below are the written instructions administrators were given for journaling. These instructions were reviewed during the orientation and were available for reference throughout the test.

This project depends heavily on how accurately administrators track how long each task, proactive and reactive, takes. We have created a Word document for journaling your work. In this journal we need you to take notes on what you are doing and associate a time/date stamp with each context switch. You will be mimicking a three day slice of life of a network administrator. You will be implementing solutions to your test environment and reacting to problems being reported by “users.” As soon as a task is started, a journal entry must be made. A second entry must be made upon completion. However, if you are in the middle of working on something, you must create a journal entry stating you received a trouble ticket; you are breaking away from the task on which you are working and beginning work on the solution to the trouble ticket. At the completion of work on the reactive task, a journal entry must be made to indicate completion. At that point you have the option to return to the original task or move to another task.

You will also need to create a journal entry to indicate you are going off-task, breaking for lunch, breaking for the day, whatever.

We will have a very specific set of Journal entry “titles” to use for both proactive tasks and reactive tasks. You will be provided with a text file on the Desktop of your journaling system which will have the Description of each task you must use and the minimal criteria for the task. **Copy and paste the description into the “Task” field in the journal. Copy and paste the minimum criteria into the top of the “Journal/Notes”**

field in the journal. We ask you to use these descriptions to maintain consistency between test administrators. With the minimum criteria as the first item in the entry field, we feel you will have a clearer idea of what is expected in the task.

Proactive Tasks

There are nine proactive tasks that need to be completed within the three-day test. For each task, there will be three phases: Research & Design, Implementation & Test, and Document, described below. When you begin each phase, type the description in this form:

Task – Research & Design

Task – Implement & Test

Task – Document

NOTE: Beginning the next phase of a task is an indication of both the conclusion of the previous phase and the beginning of the next phase.

Research & Design Phase. This phase will consist of gathering information, software and drivers from the internet, newsgroups, ftp sites, wherever you can gather information to help you create a solution to a task. **All research should be done on the laptop.** It might also involve reading through the printer manual and other documentation you have received for the hardware in your test bed. There may be no research. You may know from experience how to implement a particular solution. Whatever is done for the Research Phase must be noted in your journal. Design your solution and note the steps in your journal you intend to take in order to implement the solution. The record of what you did in this phase will be the entry you create in your journal. To get credit for this phase you must submit a time/date stamped journal entry.

Implement & Test Phase. Implement your designed solution and make notes in your journal any deviations from your designed approach. Verify that your implementation works. Note the steps you took to verify your working implementation. The record of what you did in this phase will be the entry you create in your journal. To get credit for this phase you must submit a time/date stamped journal entry.

Document Phase. This phase will consist of pulling together the results of your Research and Implementation phases. Write a “how-to” in your journal typical of what you would type up to give to fellow or junior administrators in the company to allow them to know how you did this task and to give them enough information to allow them to perform the task on their own.

Reactive Events:

If you receive a trouble ticket in the middle of one of these tasks, create a new journal entry and copy/paste the subject line into the description field of the new journal entry.

Reactive 1 – Task

The proctor will send an instant message to you. As soon as you receive this trouble ticket, stop what you are doing. Reply to the email with one of these two possible responses.

- I have received your trouble ticket and will investigate the problem. I will send a follow-up email to let you know when I have fixed your problem.
- I have received your trouble ticket and am already aware of the problem. I am working on it and will send a follow-up email to let you know when I have fixed your problem.

We will have both responses as part of the text of the trouble ticket. Delete the response that does not apply. Copy and paste the subject line of the email into the Description field in journal (e.g., Subject: Reactive 1—Deleted File). Begin work on fixing the issue in the trouble ticket.

When you are finished fixing the problem in the trouble ticket, or have determined you are unable to fix the problem, send an email to the proctor indicating the status of the problem: Fixed or Unable to Fix at this time.

There is only one time point to collect; the point at which you begin to work on the reactive. At the completion of the reactive task, create a new journal entry, copy and paste the name of the next Proactive Task you are working on (**NOTE:** This may be a continuation of a task you had started interrupted by a reactive task prior to completing). The time stamp of this next journal entry indicates both the time the reactive event is completed and when the next (or resumed) proactive task begins.

C. Phone screen questionnaire

Windows phone screen questionnaire

Name of Applicant: _____

Availability:

Would you be available to come in for ~30 hours of testing during the week? (Y/N) _____

IT Admin Level (Beginner(1-2)/Intermediate(2-4)/Advanced(5+)): _____

IT Admin Yrs Exp: _____

Certifications: _____

Windows

Windows Admin (yrs exp): _____

Windows Server 2003 (yrs exp): _____

Other Windows Server OS's and their years experience

List the typical number of client workstations you have administered

Ask the following six questions in the context of each of these categories:

Active Directory

1) Rate your level of hands-on AD administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical AD administration tasks you performed

4) List the administration tools you used on AD servers

5) Describe any special AD monitoring tools you used

6) Describe typical troubleshooting you performed

7) Describe the Active Directory topology you have administered

DNS

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of DNS servers you administered

3) Describe typical administration tasks you performed on DNS

4) List the administration tools you used

5) Describe any special DNS monitoring tools you used

6) Describe typical troubleshooting you performed

DHCP

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical administration tasks you performed

4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

WINS

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered that run WINS

3) Describe typical administration tasks you performed on WINS

4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

File

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of File servers you administered

3) Describe typical administration tasks you performed on File Servers

4) List the File administration tools you used

5) Describe any special monitoring tools you used on your File servers

6) Describe typical troubleshooting you performed on your File servers

Print

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of Print servers you administered

3) Describe typical administration tasks you performed on Print Servers

4) List the Print administration tools you used

5) Describe any special monitoring tools you used on your Print servers

6) Describe typical troubleshooting you performed on your Print servers

Remote Access

What kind of remote access configurations have you implemented? (SSH; remote desktop, RAS, terminal services, standalone VPN for win)

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you administered via RA
- 3) What sort of RA tasks have you performed, what have you used it for?
- 4) List the remote access administration tools you used [what have you used to manage your remote access environment? If it was an appliance, what appliance?]
- 5) What monitoring did you do to make sure it was secure
- 6) Describe typical troubleshooting you performed (e.g., tried to log on and couldn't get through, how you set up, managed and monitored is key here)

Security

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you administered the security on
- 3) Describe typical administration tasks you performed
- 4) List the security tools you used
- 5) Describe any special security monitoring tools you used
- 6) Describe typical troubleshooting you performed on security

Backup/Restore

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you backed up
- 3) Describe typical backup tasks you performed
- 4) List the backup tools you used
- 5) Describe any special monitoring tools you used
- 6) Describe typical troubleshooting you performed

Network Management

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you administered
- 3) Describe typical administration tasks you performed
- 4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

Exchange

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of mail servers you administered

3) Describe typical administration tasks you performed on mail servers

4) List the email tools you used

5) Describe any special email monitoring tools you used

6) Describe typical email troubleshooting you performed

Other Email

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical administration tasks you performed

4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

Patch Management

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you managed patches on

3) Describe typical patch management tasks you performed

4) List the patch management tools you used

5) Describe any special patch level monitoring tools you used

6) Describe typical troubleshooting you performed

Linux phone screen questionnaire

Name of Applicant: _____

Availability:

Would you be available to come in for ~30 hours of testing during the week? (Y/N) _____

IT Admin Level (Beginner(1-2)/Intermediate(2-4)/Advanced(5+)): _____

IT Admin Yrs Exp: _____

Certifications: _____

Linux

Linux Admin (yrs exp): _____

Red Hat Advanced Server (yrs exp): _____

Other Linux distributions and their years experience

List the typical number of client workstations you have administered

Ask the following six questions in the context of each of these categories:

LDAP

1) Rate your level of hands-on LDAP administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical LDAP administration tasks you performed

4) List the administration tools you used on LDAP servers.

5) Describe any special LDAP monitoring tools you used

6) Describe typical troubleshooting you performed

7) Describe the OpenLDAP topology you have administered

DNS

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of DNS servers you administered

3) Describe typical administration tasks you performed on DNS

4) List the administration tools you used

5) Describe any special DNS monitoring tools you used

6) Describe typical troubleshooting you performed

DHCP

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical administration tasks you performed

4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

Samba

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

- 2) List the typical number of servers you administered that run Samba
- 3) Describe typical administration tasks you performed on Samba
- 4) List the administration tools you used
- 5) Describe any special monitoring tools you used
- 6) Describe typical troubleshooting you performed

Print

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of Print servers you administered
- 3) Describe typical administration tasks you performed on your Print servers
- 4) List the Print administration tools you used
- 5) Describe any special monitoring tools you used on your Print servers
- 6) Describe typical troubleshooting you performed on your Print servers

Remote Access

What kind of remote access configurations have you implemented? (SSH; remote desktop, RAS, terminal services, standalone VPN for win)

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you administered via RA
- 3) What sort of RA tasks have you performed, what have you used it for?
- 4) List the remote access administration tools you used [what have you used to manage your remote access environment? If it was an appliance, what appliance?]
- 5) What monitoring did you do to make sure it was secure?
- 6) Describe typical troubleshooting you performed (e.g., tried to log on and couldn't get through, how you set up, managed and monitored is key here)

Security

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you administered the security on
- 3) Describe typical security administration tasks you performed
- 4) List the (administration) security tools you used
- 5) Describe any special security monitoring tools you used
- 6) Describe typical troubleshooting you performed on security

Backup/Restore

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you backed up (administered)

3) Describe typical backup (administration) tasks you performed

4) List the (administration) backup tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

Network Management

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical administration tasks you performed

4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

Sendmail

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of mail servers you administered

3) Describe typical administration tasks you performed on mail servers

4) List the email (administration) tools you used

5) Describe any special email monitoring tools you used

6) Describe typical email troubleshooting you performed

Other Email

1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category

2) List the typical number of servers you administered

3) Describe typical administration tasks you performed

4) List the administration tools you used

5) Describe any special monitoring tools you used

6) Describe typical troubleshooting you performed

Patch Management

- 1) Rate your level of hands-on administration experience: 0 – none, 1 – novice, 2 – intermediate, 3 – advanced. If the response is 0 or 1, skip to the next category
- 2) List the typical number of servers you managed patches on (administered)
- 3) Describe typical (administration) patch management tasks you performed
- 4) List the (administration) patch management tools you used
- 5) Describe any special patch level monitoring tools you used
- 6) Describe typical troubleshooting you performed

D. Windows and Linux written tests

Below are the Windows and Linux written tests given to participants as part of the recruiting process. In the samples below, the questions are marked with easy (E), medium (M), and hard (H) labels. These labels were removed and the questions were randomly ordered in the test given to the participants.

Windows Written Test

E.1 – Which of the following is the most secure Windows file system format (select only one)?

- FAT
- NTFS
- EXT3
- FAT32

E.2 – Which of the following service's primary function is to translate names into numerical IP addresses (select all that apply)?

- DNS
- DHCP
- TCP/IP
- WINS

E.3 – Which of the following applications is used to view Windows system log records (select all that apply)?

- Performance Monitor
- Event Viewer
- System Information
- Services

E.4 – List a Windows command line tool that can be used to check for network connectivity between two systems.

E.5 – Which of the following RAID schemes provides the least protection from a single drive failure (select only one)?

- RAID 0
- RAID 1
- RAID 5
- RAID 0+1

M.1 – List a Windows application that can be used to manually renew or release a DHCP lease.

M.2 – List a Windows command line tool that can be used to map and unmap a network share.

M.3 – Which of the following protocols ensures reliable delivery of network packets (select only one)?

- ICMP
- IP
- TCP
- UDP

M.4 – What are Organizational Units (OU) typically used for in Active Directory?

M.5 – What is the standard TCP port number used by the SMTP protocol?

M.6 – Describe the procedure for changing the set of users allowed to access a file.

M.7 – Describe the procedure to view the status of jobs in the print queue for a network printer.

M.8 – Explain the difference between DNS forward lookup zones and reverse lookup zones.

M.9 – List a Windows application that can be used to create new user accounts in an Active Directory based Windows domain.

M.10 – What is the primary responsibility of the system acting as the Master Browser?

M. 11 – Describe the purpose of DCPROMO and what this tool is used for.

H.1 – For each of the following Active Directory operations master roles, indicate whether the role applies forest-wide or domain-wide.

_____	Relative ID (RID) master
_____	Schema master
_____	Infrastructure master
_____	Primary Domain Controller (PDC) emulator master
_____	Domain naming master

H.2 – Explain the difference between recursive and iterative DNS queries and list an example of when each type of query would be used.

H.3 – Explain the advantages of a front-end/back-end Microsoft Exchange topology.

H.4 – List three network protocols commonly used to create Virtual Private Networks (VPNs).

H.5 – Describe how to enable disk quotas on an NTFS directory.

H.6 – What is the TCP port used by Active Directory?

Linux written test

E.1 – Which of the following set of file permissions is the most secure (select only one)?

- rwxrwxrwx
- rw-rw-rw-
- rw-rw----
- rw-----

E.2 – Which of the following service's primary function is to translate names into numerical IP addresses (select all that apply)?

- DNS
- DHCP
- TCP/IP
- SMB

E.3 – Which of the following directories typically contains Linux system log files (select all that apply)?

- /var
- /etc
- /bin
- /usr

E.4 – List a Linux command that can be used to check for network connectivity between two systems.

E.5 – Which of the following RAID schemes provides the least protection from a single drive failure (select only one)?

- RAID 0
- RAID 1
- RAID 5
- RAID 0+1

M.1 – List a Linux command that can be used to manually renew or release a DHCP lease.

M.2 – List the command to restart the Samba processes.

M.3 – Which of the following protocols ensures reliable delivery of network packets (select only one)?

- ICMP
- IP
- TCP
- UDP

M.4 – What are Organizational Units (OU) typically used for in LDAP?

M.5 – What is the standard TCP port number used by the SMTP protocol?

M.6 – Describe the procedure for changing the set of users allowed to access a file.

M.7 – Describe the procedure to view the status of jobs in the print queue for a network printer.

M.8 – Explain the difference between DNS forward lookup zones and reverse lookup zones.

M.9 – List the Linux command used to add new user accounts to an OpenLDAP directory server.

M.10 – What is the primary responsibility of the system acting as the Master Browser?

M.11 – Describe what the purpose of LAM (LDAP Account Manager) is and what the tool is used for.

H.1 – List three different authentication mechanisms supported by OpenLDAP.

H.2 – Explain the difference between recursive and iterative DNS queries and list an example of when each type of query would be used.

H.3 – Explain the function of an application based on the Sendmail milter API.

H.4 – List three network protocols commonly used to create Virtual Private Networks (VPNs).

H.5 – Explain the function of the Samba winbind daemon (winbindd).

H.6 – What is the TCP port used by LDAP?

E. Special instructions

HP Array Configuration Utility on Windows 2003

Starting the HP Array Configuration Utility

- Start->All Programs->HP System Tools->HP Array Configuration Utility->HP Array Configuration Utility
- Choose Local Application mode (Default)
- Click "OK" to accept the security windows
- Once the URL hpapp://ACU-XE/ACU-XE.htm click refresh. This will redirect you to the Array Configuration Utility 7.15.19.0.
- Click "yes" to accept the trusted site.
- Click "ok" to accept the security configuration

HP Array Configuration Utility Web Interface

- To create an RAID array
 - Make sure the Smart Array 5i Controller in Embedded Slot is highlighted by clicking on it.
 - On the right side panel select the **create array**.

- The right side panel will change to present you with a Select Drive Type of Array.
- Select your drives and click “OK.”
- Once you created the Array, highlight the Unused space (new array) on the configuration view panel by clicking on the array.
- On the right side panel click **create logical drive**.
- Configure your logical drive and click “OK.”
- On the right side panel under the Controller State, click **Save** to save your configurations.

For additional information read the readme.txt located at Start->All Programs->HP System Tools->HP Array Configuration Utility->README.TXT

HP Array Configuration Utility on Linux

Starting the HP Array Configuration Utility

- Running the command **cpqacuxe** will start the utility daemon. The utility might be running in the background.
- Connect to <http://127.0.0.1:2301>
 - Once connected you will be presented with security certificate window. Click “OK” to accept. A security warning window will appear. Click “OK” to accept and move on. You will be redirected to a secure System Management Homepage.

HP Array Configuration Utility Web Interface

- Logon with username of **administrator** and password **Rochoom9**
- On the left side panel there. Under **Integrated Agents** click on **Array Configuration Utility**. After clicking security warning windows will show up. Click “OK” to accept and move on. After accepting “OK” you will into the HP Array Configuration Utility 7.15.19.0.
- To create an RAID array
 - Make sure the Smart Array 5i Controller in Embedded Slot is highlighted by clicking on it.
 - On the right side panel select the **create array**.
 - The right side panel will change to present you with a Select Drive Type of Array.
 - Select your drives and click “OK.”
 - Once you created the Array, highlight the Unused space (new array) on the configuration view panel by clicking on the array.
 - On the right side panel click **create logical drive**.
 - Configure your logical drive and click “OK.”
 - On the right side panel under the Controller State, click **Save** to save your configurations.

Troubleshooting

- After clicking on **create array**. You may be presented with a right side panel which contains only an “OK”. The solution to this problem is to click on **exit ACU** on the upper right side. Click on **array configuration utility**. The controller will be locked. To unlock the controller maximize the web browser. Click on the **override** link. This will bring you back to the **array configuration utility**.
- If you are presented with a locked controller. To unlock the controller maximize the web browser. Click on the **override** link. This will bring you back to the **array configuration utility**.

Stopping the HP Array Configuration Utility

- Running the command **cpqacuxe -stop** will stop the utility daemon.

For additional information check the **/opt/compaq/cpqacuxe** directory.

HP StorageWorks DAT 72 Tape Drive and Linux

This document is additional information for the HP StorageWorks DAT 72 Tape drive configuration for the Linux operating system. The HP DAT 72 tape drive is connected to the HP SmartStart 5i RAID controller. The HP SmartStart 5i RAID controller device name on the Linux operating system is **cciss**. Other official sources

of reference can be found on the web at www.cpqlinux.com and locally on the Linux operating system documentation folder.

HP LaserJet 2300 Series Printer and Linux

This document is additional information for the HP LaserJet 2300 series network printer on the Linux operating system. The official web sites where you can find HP LaserJet 2300 series printing information include, www.linuxprinting.org and <http://www.hp.com/go/linux>

F. Test system software configuration setup steps

The following sections list the high-level steps performed to configure the software environment on each of the three test servers and the client system. For both the Windows Server 2003 and Red Hat Enterprise Linux AS 3.0 test environments, we configured the Infrastructure server first followed by the Email and File servers. After completing the steps listed below, we captured images of each system before we started testing. Before each test cycle, we loaded a copy of the saved image on each of the systems. This ensured that each system was in the same software state at the beginning of each test cycle.

Windows Server 2003 Infrastructure server setup steps

1. Create 25GB NTFS partition on the drive in Slot 0
2. Use Hewlett Packard SmartStart 7.10 to perform a default install of Windows Server 2003 Standard Edition into the Slot 0 partition
3. Configure static IP and gateway addresses
4. Install Windows Server 2003 support tools from the Windows Server 2003 CD
5. Run dcpromo to install Active Directory and DNS
6. Raise the Domain Functional Level to Windows Server 2003
7. Configure valid DNS forwarders and create Active Directory-based forward and reverse lookup DNS zones
8. Install DHCP and create a scope with 10 addresses and the gateway, domain, DNS, and WINS options
9. Configure a reservation for the network printer
10. Install WINS
11. Enable WINS lookup in the forward and reverse DNS zones
12. Install the Group Policy Management Console located at <http://www.microsoft.com/windowsserver2003/gpmc/default.mspx>
13. Populate Active Directory with 200 users (acc1 – 50, eng1 – 50, hr1 – 50, sales1 – 50)
14. Create mailboxes for all 200 users
15. Install Trend Micro ServerProtect 5 Anti-Virus software
16. Enable Network Time Protocol via the w32tm command
17. Set administrator password to standard value per Windows Server 2003 requirements

Windows Server 2003 Email server setup steps

1. Create 25GB NTFS partition on the drive in Slot 0
2. Use Hewlett Packard SmartStart 7.10 to perform a default install of Windows Server 2003 Standard Edition into the Slot 0 partition
3. Configure static IP and gateway addresses. Set the address of the primary DNS and WINS server to the infrastructure server
4. Install Windows Server 2003 support tools from the Windows Server 2003 CD
5. Add the server to the domain
6. Install Windows Exchange 2003 Standard Edition
7. Install the Exchange 2003 management tools on the infrastructure server
8. Disable relaying on the Exchange Default SMTP virtual server
9. Add an MX record for the email server to the DNS forward lookup zone on the infrastructure server
10. Populate each of the 200 user mailboxes with 200 messages
11. Install Trend Micro ServerProtect 5 Anti-Virus software
12. Enable Network Time Protocol via the w32tm command

13. Set administrator password to standard value per Windows Server 2003 requirements

Windows Server 2003 File/Print server setup steps

1. Create 25GB NTFS partition on the drive in Slot 0
2. Use Hewlett Packard SmartStart 7.10 to perform a default install of Windows Server 2003 Standard Edition into the Slot 0 partition
3. Configure static IP and gateway addresses. Set the address of the primary DNS and WINS server to the infrastructure server
4. Install Windows Server 2003 support tools from the Windows Server 2003 CD
5. Add the server to the domain
6. Use the HP Array Configuration Utility to create a 36GB NTFS F: partition on the Slot 1 drive.
7. Create nine directories on the F: partition. Populate the directories with 8,406 files totaling approximately 14.8 GB.
8. Enable file sharing on each root level directory on the F: partition and enable full control sharing permissions for the Everyone group.
9. Enable full control security rights for the Everyone and Users groups on the root directory of the F: drive.
10. Install Trend Micro ServerProtect 5 Anti-Virus software
11. Enable Network Time Protocol via the w32tm command
12. Set administrator password to standard value per Windows Server 2003 requirements

Red Hat Enterprise Linux AS 3.0 Infrastructure server setup steps

1. Create 25GB ext3 root partition and 2GB swap partition on the drive in Slot 0
2. Install Red Hat Enterprise Linux 3.0. Disabled the firewall option and made the following adjustments to the default package list:
 - Added KDE Desktop Environment
 - Added Editors
 - Added Office/Productivity
 - Added Graphics
 - Added Mail Server
 - Removed Windows File Server
 - Added DNS Name Server
 - Added MySQL database – add php-mysql
 - Added Network Servers – add freeradius, krb5-server, openldap-servers
 - Added Development Tools
 - Added Kernel Development
 - Added X Software Development
 - Added Gnome Software Development
 - Added KDE Software Development
 - Added Legacy Software Development
 - Added System Tools – add ethereal-gnome
3. Install the Hewlett Packard ProLiant Support Pack version 7.11 for Red Hat Enterprise Linux 3.0
4. Configure static IP and gateway addresses
5. Configure valid DNS forwarders and create forward and reverse lookup DNS zones
6. Install DHCP and create a scope with 10 addresses and the gateway, domain, and DNS, options
7. Configure a reservation for the network printer
8. Install Trend Micro ServerProtect for Linux 1.3 Anti-Virus software
9. Enable Network Time Protocol
10. Create email aliases for the root and administrator accounts to the adminuser account
11. Configure OpenLDAP 2.0.27-11 (this is the default version shipped with Red Hat Enterprise Linux 3.0). See below for a detailed list of configuration steps for Samba and OpenLDAP.
12. Populate OpenLDAP directory with 200 users (acc1 – 50, eng1 – 50, hr1 – 50, sales1 – 50)
13. Set administrator password to standard value

Red Hat Enterprise Linux AS 3.0 Email server setup steps

1. Create 25GB ext3 root partition and 2GB swap partition on the drive in Slot 0

2. Install Red Hat Enterprise Linux 3.0. Disabled the firewall option and made the following adjustments to the default package list:
 - Added KDE Desktop Environment
 - Added Editors
 - Added Office/Productivity
 - Added Graphics
 - Added Mail Server
 - Removed Windows File Server
 - Added MySQL database – add php-mysql
 - Added Network Servers – add freeradius, krb5-server
 - Added Development Tools
 - Added Kernel Development
 - Added X Software Development
 - Added Gnome Software Development
 - Added KDE Software Development
 - Added Legacy Software Development
 - Added System Tools – add ethereal-gnome
3. Install the Hewlett Packard ProLiant Support Pack version 7.11 for Red Hat Enterprise Linux 3.0
4. Configure static IP and gateway addresses
5. Install Trend Micro ServerProtect for Linux 1.3 Anti-Virus software
6. Enable Network Time Protocol
7. Configured and started Sendmail and the IMAP server
8. Create email aliases for the root and administrator accounts to the adminuser account
9. Run authconfig and configure OpenLDAP as the authentication provider
10. Add an MX record for the email server to the DNS forward lookup zone on the infrastructure server
11. Populate each of the 200 user mailboxes with 200 messages
12. Set administrator password to standard value

Red Hat Enterprise Linux AS 3.0 File/Print server setup steps

1. Create 25GB ext3 root partition and 2GB swap partition on the drive in Slot 0
2. Install Red Hat Enterprise Linux 3.0. Disabled the firewall option and made the following adjustments to the default package list:
 - Added KDE Desktop Environment
 - Added Editors
 - Added Office/Productivity
 - Added Graphics
 - Added Mail Server
 - Added MySQL database – add php-mysql
 - Added Network Servers – add freeradius, krb5-server, openldap-servers
 - Added Development Tools
 - Added Kernel Development
 - Added X Software Development
 - Added Gnome Software Development
 - Added KDE Software Development
 - Added Legacy Software Development
 - Added System Tools – add ethereal-gnome
3. Install the Hewlett Packard ProLiant Support Pack version 7.11 for Red Hat Enterprise Linux 3.0
4. Configure static IP and gateway addresses
5. Install Trend Micro ServerProtect for Linux 1.3 Anti-Virus software
6. Enable Network Time Protocol
7. Create email aliases for the root and administrator accounts to the adminuser account
8. Create SSH key pair and installed the public key on the infrastructure server
9. Download, build, and configure Samba 3.0.7 (this was the latest available version at the start of our test. We installed the latest version to work around known problems with Samba/LDAP integration). See below for a detailed list of configuration steps for Samba and OpenLDAP.
10. Use the HP Array Configuration Utility to create a 36GB ext3 partition on the Slot 1 drive. Mount the partition on the /share mount point.

11. Create nine directories under /share that match the shares defined in the Samba smb.conf file. Populate the directories with 8,406 files totaling approximately 14.8GB.
12. Set administrator password to standard value

Windows XP Professional Client system setup steps

1. Create 20GB partition on the system drive
2. Install Windows XP Professional
3. Install Windows XP Professional Service Pack 1
4. Perform Windows Update to download the latest patches (note that this was done before the start of each test cycle)
5. Install Symantec Norton Anti-Virus Corporate Edition 9.0
6. Perform Live Update to download the latest virus definitions (note that this was done before the start of each test cycle)
7. Install Microsoft Office 2003 SP1
8. Configure the primary network adapter to use DHCP
9. Enable Network Time Protocol
10. Set administrator password to standard value
11. Add the client system to the Active Directory or Samba domain

The following steps describe in detail the Samba/OpenLDAP configuration process on the Red Hat Enterprise Linux AS 3.0 infrastructure, email, and file servers. At the end of the configuration steps are copies of the smb.conf and slapd.conf files used on the file and infrastructure servers respectively.

Samba/OpenLDAP setup steps

1. Download Samba 3.0.7 and required tools on the file server
 - a. Mkdir /root/samba-config-programs
 - b. Cd /root/samba-config-programs
 - c. Download Samba-3.0.7.tar.gz from www.samba.org
 - d. Download pam_ldap.tgz from www.padl.com
 - e. Download perl-ldap-0.3202.tar.gz from ldap.perl.org
 - f. Download Convert-ASN1 1-0.18.tar.gz from cpan.org
 - g. Download Crypt-Smbhash-0.02.tar.gz from cpan.org
 - h. Download smbldap-tools-0.8.5.tgz from www.idealx.org
 - i. Scp /root/samba-config-programs/* root@directory:/root/samba-config-programs
2. Configure SSH for file to infrastructure server access
 - a. ssh-keygen -t dsa -f ~/.ssh/id_dsa
 - b. cd ~/.ssh
 - c. scp id_dsa.pub root@directory:~/.ssh (you might have to create /root/.ssh on directory)
 - d. ssh root@directory
 - e. cd ~/.ssh
 - f. cat id_dsa.pub >> authorized_keys2
 - g. chmod 640 authorized_keys2
 - h. rm -f id_dsa.pub
3. Build packages on the file server
 - a. Untar Convert-ASN1-0.18.tar.gz
 - b. cd Convert-ASN1-0.18 and run perl Makefile.pl
 - c. make
 - d. make test
 - e. make install
 - f. Untar perl-ldap-0.3202.tar.gz
 - g. cd to perl-ldap-0.3202 and run perl Makefile.pl (accepted all defaults)
 - h. make
 - i. make test
 - j. make install
 - k. Untar pam_ldap.tgz (version 1.75)
 - l. cd to pam_ldap-175
 - m. ./configure

- n. make
 - o. make install
 - p. Untar Crypt-SmbHash-0.02.tar.gz
 - q. cd to Crypt-SmbHash-0.02 and run perl Makefile.pl
 - r. make
 - s. make test
 - t. make install
 - u. Untar samba-3.0.7.tar.gz
 - v. cd to samba-3.0.7/source
 - w. ./configure --with-ldapsam --bindir=/usr/bin --sbindir=/usr/sbin --sysconfdir=/etc/samba --enable-cups --with-privatedir=/etc/samba/private --with-lockdir=/etc/samba/locks --with-piddir=/etc/samba/pids --with-configdir=/etc/samba --with-logfilebase=/var/log/samba --with-ldap --with-ads --with-smbmount --with-acl-support --with-winbind && make && make install
4. Configure the smb.conf file – refer to the smb.conf example at the end of Appendix F.
 5. Edit the smbusers file
 - a. set root=Administrator admin
 6. Copy the Samba schema from the file server to the infrastructure server
 - a. cd /root/samba-config-programs/samba-3.0.7/examples/LDAP
 - b. scp samba.schema root@directory:/etc/ldap/schema
 7. Build the SMB-LDAP tools on the file server
 - a. cd /root/samba-config-programs
 - b. untar smbldap-tools-0.8.5.tgz
 - c. cd smbldap-tools-0.8.5
 - d. cp * /usr/local/sbin
 - e. mkdir /etc/smbldap-tools
 - f. cp {smbldap.conf, smbldap_bind.conf, smbldap_tools.pm} /etc/smbldap-tools/
 - g. vi /etc/smbldap-tools/smbldap_bind.conf and add valid dc's and password
 - h. cp /etc/smbldap-tools/smbldap_bind.conf to /usr/local/sbin/
 8. Configure /etc/smbldap-tools/smbldap.conf on the file server
 - a. set ldapTLS=0
 - b. set valid suffix
 - c. set hash_encrypt=MD5
 - d. replace PDC-SMB3 in userSmbHome and userProfile with File
 - e. set userHomeDrive=U:
 - f. set mailDomain
 - g. set with_smbpasswd=1
 9. Create Samba directories
 - a. mkdir /etc/samba/profiles
 - b. chmod 1777 /etc/samba/profiles
 - c. mkdir /etc/samba/netlogon
 - d. mkdir /etc/samba/netlogon/scripts
 - e. run testparm -s | more to check for samba configuration is correct
 10. Configure OpenLDAP on the infrastructure server
 - a. Untar Convert-ASN1-0.18
 - b. cd Convert-ASN1-0.18 and run perl Makefile.pl
 - c. make
 - d. make test
 - e. make install
 - f. Untar perl-ldap-0.3202
 - g. cd to perl-ldap-0.3202 and run perl Makefile.pl (accepted all defaults)
 - h. make
 - i. make test
 - j. make install
 - k. Untar pam_ldap (version 1.74)
 - l. cd to pam_ldap-175 and run ./configure
 - m. make
 - n. make install

- o. Untar Crypt-SmbHash-0.02
 - p. cd to Crypt-SmbHash-0.02 and run perl Makefile.pl
 - q. make
 - r. make test
 - s. make install
11. Configure /etc/openldap/ldap.conf on the infrastructure server
 - a. set SIZELIMIT to 120000
 - b. set TIMELIMIT to 15
 - c. set DEREFL to never
 - d. set HOST to infrastructure server IP address
 - e. set BASE to valid dn
 - f. set binddn to valid dn
 - g. set bindpw to valid password
 - h. set pam_password md5
 - i. set ssl no
 12. Configure the /etc/openldap/slapd.conf file on the infrastructure server - refer to the slapd.conf example at the end of Appendix F.
 13. Link /etc/openldap/ldap.conf /etc/ldap.conf on the infrastructure server
 - a. rm /etc/ldap.conf
 - b. ln -s /etc/openldap/ldap.conf /etc/ldap.conf
 14. Configure Samba secrets database on the file server
 - a. smbpasswd -w password
 - b. scp /etc/samba/private/secrets.tdb [root@directory:/etc/samba/](#)
 15. Run authconfig on the infrastructure server
 - a. select Use LDAP
 - b. set Server: = <infrastructure server IP address>
 - c. set Base DN: = valid suffix
 - d. select Use LDAP Authentication
 - e. /etc/init.d/ldap start
 16. Run authconfig on the file server
 - a. select Use LDAP
 - b. set Server: = <infrastructure server IP address>
 - c. set Base DN: = valid suffix
 - d. select Use LDAP Authentication
 17. Record the Samba SID in the smbldap.conf file on the file server
 - a. /etc/init.d/smb start
 - b. net getlocalsid (note you will see a "smbldap_search_suffix:" error which is OKAY, as long as a SID is created)
 - c. /etc/init.d/smb stop
 - d. cd /etc/samba/locks
 - e. rm -rf *
 - f. vi /etc/smbldap-tools/smbldap.conf and paste SID returned by getlocalsid into SID=
 18. Configure Smb-LDAP tools on the infrastructure server
 - a. cd /root/samba-config-programs
 - b. untar smbldap-tools-0.8.5.tgz
 - c. cd smbldap-tools-0.8.5
 - d. cp * to /usr/local/sbin
 - e. mkdir /etc/smbldap-tools
 - f. cd /etc/smbldap-tools
 - g. scp [root@file:/etc/smbldap-tools/](#).
 19. Configure /etc/smbldap-tools/smbldap.conf on the infrastructure server
 - a. set with_smbpasswd=0
 20. Start OpenLDAP and populate it on the infrastructure server
 - a. /etc/init.d/ldap restart
 - b. smbldap-populate
 - c. /etc/init.d/ldap restart
 21. Start Samba on the file server

- a. /etc/init.d./smb start
- 22. Test LDAP on the infrastructure server and configure Administrator and root accounts
 - a. slapcat (checks ldap database)
 - b. ldapsearch -x -b "valid suffix" "(ObjectClass=*)"
 - c. smbldap-passwd Administrator
 - d. smbldap-usermod -s /bin/bash -d /root Administrator
 - e. smbldap-usershow Administrator
 - f. smbldap-useradd -c root root
 - g. smbldap-usermod -a -g 0 -u 0 root
 - h. smbldap-passwd root
 - i. chkconfig --level 2345 ldap on
- 23. Test Samba on the file server
 - a. smbclient -L localhost -U% (should display smb config as anonymous)
 - b. smbclient -L localhost -U root (should display smb config as root)
 - c. chkconfig --level 2345 smb on
 - d. chkconfig --level 2345 winbind on
 - e. ssh [root@directory](#) smbldap-usershow root (should display root user info)
- 24. Run authconfig on the email server
 - a. select Use LDAP
 - b. set Server: = <infrastructure server IP address>
 - c. set Base DN: = valid suffix
 - d. select Use LDAP Authentication
 - e. /etc/init.d/sendmail restart
- 25. Create Windows built-in groups on the infrastructure server
 - a. net groupmap modify ntgroup="Domain Admins" unixgroup=root type=domain
 - b. net groupmap modify ntgroup="Domain Users" unixgroup=users type=domain
 - c. net groupmap modify ntgroup="Domain Guests" unixgroup=nobody type=domain
 - d. net groupmap modify ntgroup="Administrators" unixgroup=sys
 - e. net groupmap modify ntgroup="Users" unixgroup=users
 - f. net groupmap modify ntgroup="Guests" unixgroup=nobody
 - g. net groupmap modify ntgroup="System Operators" unixgroup=daemon
 - h. net groupmap modify ntgroup="Account Operators" unixgroup=wheel
 - i. net groupmap modify ntgroup="Backup Operators" unixgroup=bin
 - j. net groupmap modify ntgroup="Print Operators" unixgroup=lp
 - k. net groupmap modify ntgroup="Replicators" unixgroup=kmem
 - l. net groupmap modify ntgroup="Power Users" unixgroup=sys
- 26. Configure client account on the infrastructure server
 - a. smbldap-useradd -w client\$
 - b. smbldap-usershow client\$
- 27. Add the client computer to the domain
 - a. Right click on My Computer
 - b. Select the Properties tab
 - c. Select the Computer Name tab
 - d. Select Change
 - e. Click on Domain (under Member Of section)
 - f. Enter domainname
 - g. Click OK
 - h. Enter root and root password to join domain

/etc/samba/smb.conf file contents on the file server

```

#===== Global Settings =====
[global]

workgroup = <insert valid workgroup name>
netbios name = File

```

```

server string = Domain Samba Server

printcap name = /etc/printcap
load printers = yes
printing = cups

log file = /var/log/samba/%m.log
max log size = 500000

security = user

encrypt passwords = yes
obey pam restrictions = no

#
# Adding LDAP backend/frontend
#
ldap passwd sync = Yes
passdb backend = ldapsam:ldap://directory.xx.xxx.xx
ldap delete dn = yes
ldap admin dn = cn=Manager,dc=xx,dc=xxx,dc=xxx
ldap suffix = dc=xx,dc=xxx,dc=xxx
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Computers
add user script = ssh root@directory "smbldap-useradd -a -m '%u'"
delete user script = ssh root@directory "smbldap-userdel '%u'"
add group script = ssh root@directory "smbldap-groupadd -p '%g'"
delete group script = ssh root@directory "smbldap-groupdel '%g'"
add user to group script = ssh root@directory "smbldap-groupmod -m '%u' '%g'"
delete user from group script = ssh root@directory "smbldap-groupmod -x '%u' '%g'"
set primary group script = ssh root@directory "smbldap-usermod -g '%g' '%u'"
add machine script = ssh root@directory "smbldap-useradd -w '%u'"
abort shutdown script = /sbin/shutdown -c
idmap backend = ldap:ldap://directory.xx.xxx.xx
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind enum users = yes
winbind enum groups = yes
winbind separator = /
winbind use default domain = Yes
use sendfile = Yes
map acl inherit = Yes
nt acl support = yes
printer admin = Administrator, root

dos charset = 850
Unix charset = ISO8859-1

username map = /etc/samba/smbusers

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

interfaces = eth0, lo
bind interfaces only = yes

```

```

local master = yes
os level = 99
domain master = yes
preferred master = yes
domain logons = yes

logon script = logon.bat
logon drive = U:
logon path = \\%L\profiles\%U

name resolve order = host bcast wins lmhosts

dns proxy = yes

#===== Share Definitions =====
[$IPC]
    path = /tmp
    hosts allow = 10.0.0. 127.

[homes]
    comment = Home Directories
    path = /share/home
    browseable = no
    writable = yes

# Un-comment the following and create the netlogon directory for Domain Logons
[netlogon]
    comment = Network Logon Service
    path = /etc/samba/netlogon/scripts
    guest ok = yes
    writable = no
    share modes = no
    locking = no

# Un-comment the following to provide a specific roving profile share
# the default is to use the user's home directory
[Profiles]
    path = /etc/samba/profiles
    browseable = no
;    guest ok = yes
    writable = yes

# NOTE: If you have a BSD-style print system there is no need to
# specifically define each individual printer
[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no
# Set public = yes to allow user 'guest account' to print
    guest ok = no
    writable = no
    printable = yes

[public]
    comment = Public Stuff
    path = /share/public
    public = yes
    writable = yes

```

```

[acc]
    comment = Accounting share
    path = /share/acc
    public = yes
    writable = yes
    printable = no

[engpub]
    comment = Engineering public share
    path = /share/engpub
    public=yes
    writable = yes
    printable = no

[engpri]
    comment = Engineering Private share
    path = /share/engpri
    public = yes
    writable = yes
    printable = no

[hrpub]
    comment = HR public share
    path = /share/hrpub
    public = yes
    writable = yes
    printable = no

[hrpri]
    comment = HR private share
    path = /share/hrpri
    public = yes
    writable = yes
    printable = no

[salespub]
    comment = Sales public share
    path = /share/salespub
    public = yes
    writable = yes
    printable = no

[salespri]
    comment = Sales private share
    path = /share/salespri
    public = yes
    writable = yes
    printable = no

```

/etc/openldap/slapd.conf file contents on the infrastructure server

```

include          /etc/openldap/schema/core.schema
include          /etc/openldap/schema/cosine.schema
include          /etc/openldap/schema/inetorgperson.schema
include          /etc/openldap/schema/nis.schema

```

```

#include          /etc/openldap/schema/redhat/autofs.schema
#include          /etc/openldap/schema/redhat/kerberosobject.schema
include          /etc/openldap/schema/samba.schema

#referral      ldap://root.openldap.org

pidfile         //var/run/slapd.pid
argsfile        //var/run/slapd.args

access to
attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdLastSet,sambaPwdMustC
hange
    by dn="cn=Manager,dc=xx,dc=xxx,dc=xx" write
    by self write
    by anonymous auth
    by * none
access to *
    by * read

#####
# ldbm database definitions
#####

database        ldbm
suffix          "<replace with valid suffix>"
rootdn          "<replace with valid dn>"
rootpw          <replace with valid password>
directory       /var/lib/ldap
# Indices to maintain
Index objectClass,uidNumber,gidNumber,memberUid,sambaSID,
sambaPrimaryGroupSID,sambaDomainName          eq
index cn,sn,uid,displayName    pres,sub,eq
index default      sub

```

G. Individual test results

The following tables contain the individual proactive, reactive, and service loss elapsed times for the 18 Windows 2003 Server and 18 Red Hat Enterprise Linux AS 3.0 administrators. We captured the results from the administrators' journal files, instant messaging log files, and system service probing script log files. For the results listed in the Test Results section, we normalized the data by removing the lowest and highest results for each platform (the low and high results are displayed with a bold font in the following tables)

Proactive Task	L1	L2	L3	L4	L5	L6
Configure new tape device and driver	1:30:00	1:17:00	4:01:06	0:56:32	2:51:18	1:50:32
Configure new network printer	1:53:00	1:16:00	0:26:11	0:18:51	1:01:24	1:07:11
Implement system backups	N/A	N/A	N/A	1:01:32	4:05:57	N/A
Implement better data access security	N/A	5:58:00	N/A	3:26:30	N/A	N/A
Improve system fault tolerance/redundancy	N/A	N/A	N/A	N/A	N/A	N/A
Implement basic administrator remote access	0:08:00	0:03:00	N/A	0:46:34	0:32:24	N/A
Implement routine system/security monitoring process	2:36:00	N/A	1:06:05	4:02:38	N/A	N/A
Change user account information	1:15:00	0:30:00	N/A	2:02:20	N/A	N/A
Totals	7:22:00	9:04:00	5:33:22	12:34:57	8:31:03	2:57:43

Proactive Task	L7	L8	L9	L10	L11	L12
Configure new tape device and driver	0:31:38	8:27:15	4:32:06	1:10:14	0:43:35	4:02:25
Configure new network printer	1:38:49	4:39:59	3:12:49	0:52:01	0:33:14	1:51:01
Implement system backups	1:21:32	0:55:09	N/A	N/A	1:22:02	N/A
Implement better data access security	1:57:19	N/A	N/A	5:05:27	2:59:44	1:52:07
Improve system fault tolerance/redundancy	9:08:46	N/A	N/A	N/A	N/A	N/A
Implement basic administrator remote access	0:15:12	0:18:06	N/A	0:27:23	1:12:02	0:03:43
Implement routine system/security monitoring process	0:27:58	N/A	0:39:56	0:03:30	0:45:50	N/A
Change user account information	1:43:47	N/A	N/A	2:02:31	0:03:17	2:04:59
Totals	17:05:01	14:20:29	8:24:51	9:41:06	7:39:44	9:54:15

Proactive Task	L13	L14	L15	L16	L17	L18
Configure new tape device and driver	0:46:41	1:10:17	0:17:56	2:15:50	1:41:27	0:33:28
Configure new network printer	0:52:55	1:21:00	2:46:31	0:40:22	0:25:32	0:24:54
Implement system backups	2:17:37	1:30:15	2:22:10	1:04:05	3:12:27	5:33:12
Implement better data access security	N/A	N/A	3:47:55	N/A	N/A	2:41:22
Improve system fault tolerance/redundancy	6:50:25	N/A	N/A	N/A	N/A	2:20:54
Implement basic administrator remote access	0:59:11	1:25:37	1:25:22	0:24:59	0:12:33	0:53:56
Implement routine system/security monitoring process	3:06:40	N/A	0:56:04	1:20:43	4:47:23	1:17:32
Change user account information	0:52:19	N/A	0:47:42	1:18:15	N/A	1:02:53
Totals	15:45:48	5:27:09	12:23:40	7:04:14	10:19:22	14:48:11

Proactive Task	W1	W2	W3	W4	W5	W6
Configure new tape device and driver	0:46:00	0:51:00	0:46:42	0:41:32	1:22:44	1:13:45
Configure new network printer	0:29:00	0:40:00	0:21:08	0:41:29	0:59:37	2:18:35
Implement system backups	1:21:00	N/A	1:45:38	3:28:28	1:40:30	N/A
Implement better data access security	N/A	N/A	4:55:31	4:16:30	1:30:31	N/A
Improve system fault tolerance/redundancy	0:34:00	6:52:00	N/A	2:36:04	N/A	N/A
Implement basic administrator remote access	0:29:00	0:20:00	0:41:55	0:29:37	0:34:24	N/A
Implement routine system/security monitoring process	4:06:00	0:33:00	1:57:02	N/A	N/A	N/A
Change user account information	0:25:00	0:18:00	0:06:40	1:36:17	1:31:15	N/A
Totals	8:10:00	9:34:00	10:34:36	13:49:57	7:39:01	3:32:20

Proactive Task	W7	W8	W9	W10	W11	W12
Configure new tape device and driver	0:37:30	0:46:05	0:30:59	0:30:04	1:38:29	0:35:12
Configure new network printer	0:57:34	0:17:49	0:32:52	0:27:49	0:42:03	0:17:42
Implement system backups	1:51:20	0:42:56	0:46:54	N/A	N/A	2:23:13
Implement better data access security	2:05:49	2:06:51	1:53:01	4:08:00	2:54:26	1:17:26
Improve system fault tolerance/redundancy	4:33:50	N/A	4:05:36	4:56:36	N/A	5:09:39
Implement basic administrator remote access	N/A	0:10:30	0:14:20	0:02:03	0:23:08	1:01:49
Implement routine system/security monitoring process	0:40:01	0:40:16	0:23:54	0:32:24	1:53:40	0:35:05
Change user account information	0:31:25	1:04:40	0:08:49	2:29:48	0:27:15	0:08:04

Totals	11:17:29	5:49:07	8:36:25	13:06:44	7:59:01	11:28:10
---------------	----------	---------	----------------	----------	---------	----------

Proactive Task	W13	W14	W15	W16	W17	W18
Configure new tape device and driver	0:23:43	1:19:22	0:28:23	0:52:26	1:04:46	1:54:33
Configure new network printer	0:29:28	0:19:34	0:13:15	0:33:10	0:29:07	0:24:33
Implement system backups	3:49:39	2:31:42	5:04:28	1:24:01	1:30:50	N/A
Implement better data access security	2:12:20	8:55:54	0:30:19	2:19:10	1:33:13	N/A
Improve system fault tolerance/redundancy	6:12:59	2:40:19	2:03:27	2:48:13	2:36:52	N/A
Implement basic administrator remote access	0:37:28	0:48:29	0:19:34	0:20:46	0:23:43	N/A
Implement routine system/security monitoring process	2:02:26	1:46:04	0:43:53	1:00:00	3:18:54	N/A
Change user account information	0:45:19	0:05:58	0:33:08	0:38:54	0:28:07	N/A
Totals	16:33:22	18:27:22	9:56:27	9:56:40	11:25:32	2:19:06

Reactive Event	L1	L2	L3	L4	L5	L6
Reactive 1 - Mail performance	0:06:00	0:09:00	0:02:36	0:12:14	0:53:53	0:15:07
Reactive 2 - File deletion	0:07:00	0:24:00	0:02:20	0:13:06	0:21:55	0:03:06
Reactive 3 - Cannot create file	0:15:00	0:06:00	0:04:01	0:10:59	0:48:41	0:08:54
Reactive 4 - Cannot receive mail	0:03:00	0:03:00	0:11:05	0:05:12	0:19:59	0:05:30
Reactive 5 - Cannot access Internet	0:13:00	0:18:00	1:55:39	0:03:53	1:07:55	2:02:10
Reactive 6 - Cannot print	0:36:00	0:15:00	1:13:47	0:23:40	1:35:37	1:39:04
Reactive 7 - Cannot access public share	0:41:00	0:23:00	4:10:26	0:00:00	0:21:23	1:58:12
Reactive 8 - File deletion	0:20:00	0:08:00	0:02:05	0:08:47	0:18:11	0:16:18
Reactive 9 - Mail deletion	0:09:00	0:07:00	0:00:40	1:28:53	0:04:00	0:02:37
Reactive 10 - Cannot log on	0:01:00	0:22:00	0:16:08	0:25:05	0:14:10	0:04:05
Reactive 11 - File deletion	0:29:00	n/a	0:01:32	0:08:27	n/a	0:15:48
Reactive 12 - File performance	0:35:00	0:23:00	0:25:01	0:12:43	0:49:34	1:43:10
Reactive 13 - Incorrect directory permissions	n/a	n/a	n/a	0:05:45	n/a	n/a
Totals	3:35:00	2:38:00	8:25:20	3:38:44	6:55:18	8:34:01

Reactive Event	L7	L8	L9	L10	L11	L12
Reactive 1 - Mail performance	0:03:01	0:24:08	0:47:31	0:27:30	0:03:55	0:49:55
Reactive 2 - File deletion	1:51:13	0:14:42	0:16:57	0:10:10	0:44:22	0:41:08
Reactive 3 - Cannot create file	0:18:50	0:10:00	0:49:33	0:24:29	1:04:54	1:29:06
Reactive 4 - Cannot receive mail	0:02:31	1:05:05	0:35:40	0:06:51	0:00:34	0:11:08
Reactive 5 - Cannot access Internet	0:29:45	2:22:02	1:01:42	1:54:45	1:39:13	0:53:47
Reactive 6 - Cannot print	0:43:44	0:28:02	n/a	1:02:34	0:09:12	1:01:34
Reactive 7 - Cannot access public share	0:00:00	1:25:24	5:00:48	0:07:31	2:35:07	2:47:32
Reactive 8 - File deletion	0:12:28	0:12:37	n/a	0:03:11	1:40:49	0:10:45
Reactive 9 - Mail deletion	0:09:37	0:40:45	0:02:58	0:14:44	0:06:40	0:12:01
Reactive 10 - Cannot log on	0:09:14	0:05:31	1:15:16	0:02:35	0:08:43	2:46:43
Reactive 11 - File deletion	n/a	0:12:07	n/a	2:43:56	n/a	0:20:57
Reactive 12 - File performance	0:30:39	0:05:47	0:32:30	0:02:16	2:10:36	0:10:44
Reactive 13 - Incorrect directory permissions	0:02:03	n/a	n/a	n/a	0:13:07	n/a
Totals	4:33:05	7:26:10	10:22:55	7:20:32	10:37:12	11:35:20

Reactive Event	L13	L14	L15	L16	L17	L18
Reactive 1 - Mail performance	0:20:24	0:12:24	0:08:23	1:25:17	0:04:46	0:05:12
Reactive 2 - File deletion	0:08:38	0:53:27	0:09:36	1:11:15	0:06:03	0:08:59
Reactive 3 - Cannot create file	0:08:17	0:18:03	0:06:24	0:17:16	0:29:27	0:04:48

Reactive 4 - Cannot receive mail	0:02:38	0:07:20	0:00:22	0:29:18	0:05:17	0:01:57
Reactive 5 - Cannot access Internet	0:09:24	1:06:50	0:11:04	0:41:51	1:02:55	0:05:43
Reactive 6 - Cannot print	0:10:13	2:11:59	0:07:50	1:32:39	0:12:09	0:11:01
Reactive 7 - Cannot access public share	0:51:18	8:11:13	0:00:00	1:17:18	3:17:35	0:00:00
Reactive 8 - File deletion	n/a	n/a	0:07:48	0:18:35	n/a	0:00:40
Reactive 9 - Mail deletion	0:03:25	0:42:44	0:09:36	0:37:10	0:22:58	n/a
Reactive 10 - Cannot log on	0:00:00	0:05:30	0:01:45	0:05:37	0:09:57	0:00:00
Reactive 11 - File deletion	0:06:42	n/a	0:07:33	0:28:08	0:22:05	0:20:14
Reactive 12 - File performance	0:04:09	0:34:41	0:05:52	0:42:48	0:08:12	0:04:14
Reactive 13 - Incorrect directory permissions	n/a	n/a	n/a	n/a	n/a	0:04:35
Totals	2:05:08	14:24:11	1:16:13	9:07:12	6:21:24	1:07:23

Reactive Event	W1	W2	W3	W4	W5	W6
Reactive 1 - Mail performance	1:28:00	0:18:00	0:29:53	0:20:51	0:27:09	2:13:15
Reactive 2 - File deletion	1:05:00	0:07:00	0:05:47	0:08:05	0:06:03	0:42:27
Reactive 3 - Cannot create file	0:10:00	0:20:00	0:04:01	0:14:38	0:24:21	0:18:43
Reactive 4 - Cannot receive mail	1:34:00	0:21:00	0:08:46	1:17:23	2:03:30	0:49:29
Reactive 5 - Cannot access Internet	0:13:00	0:42:00	0:16:21	0:31:39	0:25:30	0:17:20
Reactive 6 - Cannot print	0:45:00	0:37:00	0:11:55	0:29:27	1:04:46	0:50:01
Reactive 7 - Cannot access public share	0:00:00	0:17:00	0:04:32	1:01:48	2:52:03	0:49:39
Reactive 8 - File deletion	0:15:00	n/a	0:21:03	0:22:34	0:06:32	0:04:16
Reactive 9 - Mail deletion	0:32:00	0:49:00	0:03:39	0:54:58	0:02:14	0:54:14
Reactive 10 - Cannot log on	0:00:00	0:00:00	0:07:15	0:13:10	0:02:51	0:23:10
Reactive 11 - File deletion	n/a	0:12:00	0:03:51	0:09:15	0:08:57	0:10:37
Reactive 12 - File performance	0:34:00	0:45:00	0:35:25	1:24:43	0:31:47	0:56:40
Reactive 13 - Incorrect directory permissions	n/a	n/a	0:07:38	0:18:52	0:09:26	n/a
Totals	6:36:00	4:28:00	2:40:06	7:27:23	8:25:09	8:29:51

Reactive Event	W7	W8	W9	W10	W11	W12
Reactive 1 - Mail performance	0:15:22	0:07:49	0:00:52	0:10:34	0:21:51	1:14:25
Reactive 2 - File deletion	0:05:30	0:13:44	0:13:32	0:10:18	0:09:21	0:47:26
Reactive 3 - Cannot create file	1:55:33	0:12:12	0:06:28	0:09:00	0:36:34	0:16:14
Reactive 4 - Cannot receive mail	0:05:40	1:34:21	0:06:52	0:12:25	0:23:26	0:15:54
Reactive 5 - Cannot access Internet	0:25:04	0:29:47	0:14:21	0:22:36	0:20:19	0:17:06
Reactive 6 - Cannot print	1:50:07	0:10:11	0:12:50	0:08:55	1:18:40	0:03:47
Reactive 7 - Cannot access public share	0:00:00	0:11:09	0:00:00	0:06:27	0:00:00	0:14:48
Reactive 8 - File deletion	0:06:26	0:11:26	0:02:52	n/a	0:05:35	0:02:57
Reactive 9 - Mail deletion	2:34:17	1:05:57	0:29:12	0:47:25	0:39:41	0:53:37
Reactive 10 - Cannot log on	0:00:00	0:13:16	0:00:00	0:00:00	0:00:00	0:00:00
Reactive 11 - File deletion	0:03:43	0:13:21	0:04:06	0:27:15	0:14:56	0:08:11
Reactive 12 - File performance	0:48:26	0:25:11	0:09:00	0:07:07	0:41:01	0:15:02
Reactive 13 - Incorrect directory permissions	0:14:34	0:25:33	0:02:10	0:03:52	0:04:38	0:05:08
Totals	8:24:42	5:33:57	1:42:15	2:45:54	4:56:02	4:34:35

Reactive Event	W13	W14	W15	W16	W17	W18
Reactive 1 - Mail performance	0:14:02	0:10:12	0:28:32	0:35:45	0:06:10	1:11:15
Reactive 2 - File deletion	0:10:46	0:03:46	0:06:47	0:01:52	0:04:42	0:21:21
Reactive 3 - Cannot create file	0:06:03	0:05:24	0:13:28	0:00:00	0:34:33	1:01:46
Reactive 4 - Cannot receive mail	0:22:10	1:43:56	2:10:16	0:09:39	0:17:00	3:13:20
Reactive 5 - Cannot access Internet	0:07:50	0:05:57	0:27:06	0:05:11	0:02:27	0:48:40
Reactive 6 - Cannot print	0:41:37	0:21:36	0:46:03	0:15:04	0:19:57	2:47:01

Reactive 7 - Cannot access public share	0:00:00	0:00:00	1:26:52	0:00:00	0:00:00	0:42:34
Reactive 8 - File deletion	0:05:23	n/a	0:35:48	0:07:15	0:10:09	0:12:11
Reactive 9 - Mail deletion	0:17:59	2:07:44	0:55:31	0:29:18	0:08:51	3:04:30
Reactive 10 - Cannot log on	n/a	0:02:07	0:00:00	0:00:00	0:00:00	0:08:50
Reactive 11 - File deletion	0:06:29	n/a	1:12:31	0:16:45	0:04:47	0:09:55
Reactive 12 - File performance	0:21:06	0:25:12	1:10:47	0:12:32	0:45:14	2:15:59
Reactive 13 - Incorrect directory permissions	n/a	n/a	0:04:56	0:05:39	0:06:02	n/a
Totals	2:33:25	5:05:54	9:38:37	2:19:00	2:39:52	15:57:22

Service Loss Event	L1	L2	L3	L4	L5	L6
Reactive 3 - Cannot create file	0:46:28	0:18:02	0:19:48	0:17:59	0:37:30	0:20:34
Reactive 4 - Cannot receive mail	0:12:17	0:06:36	0:12:12	0:13:25	0:24:59	0:11:21
Reactive 5 - Cannot access Internet	0:21:58	1:18:57	2:16:06	0:04:17	3:11:35	2:39:12
Reactive 6 - Cannot print	0:44:54	0:22:20	0:16:30	0:33:08	3:46:01	3:34:02
Reactive 7 - Cannot access public share	0:52:42	0:25:37	1:34:50	0:00:00	1:34:50	5:00:29
Reactive 10 - Cannot log on	0:07:04	0:13:47	0:19:26	0:00:08	0:16:31	0:09:40
Totals	3:05:23	2:45:19	4:58:52	1:08:57	9:51:26	11:55:18

Service Loss Event	L7	L8	L9	L10	L11	L12
Reactive 3 - Cannot create file	1:39:22	0:21:28	1:00:36	0:32:22	1:05:34	1:33:44
Reactive 4 - Cannot receive mail	0:11:50	0:14:43	0:25:53	0:11:28	0:12:55	0:18:38
Reactive 5 - Cannot access Internet	0:37:47	1:13:04	1:52:14	0:58:49	1:42:28	1:01:31
Reactive 6 - Cannot print	0:52:35	1:04:04	n/a	1:08:22	0:16:36	2:23:20
Reactive 7 - Cannot access public share	0:00:00	1:46:37	1:34:50	0:14:32	2:45:24	2:59:06
Reactive 10 - Cannot log on	0:03:33	0:12:46	0:17:42	0:11:04	0:00:19	0:02:05
Totals	3:25:07	4:52:42	5:11:15	3:16:37	6:03:16	8:18:24

Service Loss Event	L13	L14	L15	L16	L17	L18
Reactive 3 - Cannot create file	0:19:44	0:21:36	0:20:41	0:23:46	0:39:29	0:15:58
Reactive 4 - Cannot receive mail	0:11:58	0:15:13	0:11:08	0:37:16	0:13:18	0:12:01
Reactive 5 - Cannot access Internet	0:18:19	1:15:01	0:18:37	0:36:55	0:53:53	0:18:30
Reactive 6 - Cannot print	0:19:45	4:24:34	0:16:02	2:56:45	0:20:05	0:17:21
Reactive 7 - Cannot access public share	1:34:50	1:34:50	0:00:00	1:34:50	4:53:35	0:00:00
Reactive 10 - Cannot log on	0:00:00	0:11:43	0:07:22	0:13:55	0:14:21	0:00:00
Totals	2:44:36	8:02:57	1:13:50	6:23:27	7:14:41	1:03:50

Service Loss Event	W1	W2	W3	W4	W5	W6
Reactive 3 - Cannot create file	0:17:16	0:31:29	0:10:14	0:16:21	0:38:45	0:55:05
Reactive 4 - Cannot receive mail	1:05:10	0:19:33	0:13:30	1:26:17	3:16:54	1:00:07
Reactive 5 - Cannot access Internet	0:18:51	0:37:27	0:30:01	0:39:09	0:22:57	0:22:44
Reactive 6 - Cannot print	0:13:40	0:41:22	0:21:48	0:38:19	1:07:01	0:21:59
Reactive 7 - Cannot access public share	0:00:00	1:04:26	0:22:06	3:20:14	1:04:26	1:31:13
Reactive 10 - Cannot log on	0:00:00	0:00:00	0:17:19	0:13:54	0:16:48	0:03:35
Totals	1:54:57	3:14:17	1:54:58	6:34:14	6:46:51	4:14:43

Service Loss Event	W7	W8	W9	W10	W11	W12
Reactive 3 - Cannot create file	7:25:32	0:01:16	0:12:28	0:15:57	0:41:43	0:10:30
Reactive 4 - Cannot receive mail	0:13:15	3:04:33	0:17:39	0:17:30	0:30:21	0:24:10
Reactive 5 - Cannot access Internet	0:32:15	0:26:16	0:21:42	0:29:07	0:28:07	0:25:34
Reactive 6 - Cannot print	1:57:31	2:53:43	0:17:43	0:19:05	1:45:30	0:13:21
Reactive 7 - Cannot access public share	0:00:00	2:23:45	0:00:00	5:01:45	0:00:00	1:15:41
Reactive 10 - Cannot log on	0:00:00	0:13:50	0:00:00	0:00:00	0:00:00	0:00:00
Totals	10:08:33	9:03:23	1:09:32	6:23:24	3:25:41	2:29:16

Service Loss Event	W13	W14	W15	W16	W17	W18
Reactive 3 - Cannot create file	0:11:09	0:13:53	0:18:29	0:07:56	0:47:28	1:11:09
Reactive 4 - Cannot receive mail	0:24:38	1:48:35	3:09:46	0:19:34	0:22:40	5:09:48
Reactive 5 - Cannot access Internet	0:16:58	0:14:38	0:33:35	0:12:06	0:08:18	0:57:55
Reactive 6 - Cannot print	1:03:28	0:30:30	0:24:55	0:20:48	0:21:57	3:04:56
Reactive 7 - Cannot access public share	0:00:00	0:00:00	1:09:11	0:00:00	0:00:00	2:07:04
Reactive 10 - Cannot log on	n/a	0:00:49	0:00:00	0:00:00	0:00:00	0:18:49
Totals	1:56:13	2:48:25	5:35:56	1:00:24	1:40:23	12:49:41

VeriTest (www.veritest.com), the testing division of Lionbridge Technologies, Inc., provides outsourced testing solutions that maximize revenue and reduce costs for our clients. For companies who use high-tech products as well as those who produce them, smoothly functioning technology is essential to business success. VeriTest helps our clients identify and correct technology problems in their products and in their line of business applications by providing the widest range of testing services available.

VeriTest created the suite of industry-standard benchmark software that includes WebBench, NetBench, Winstone, and WinBench. We've distributed over 20 million copies of these tools, which are in use at every one of the 2001 Fortune 100 companies. Our Internet BenchMark service provides the definitive ratings for Internet Service Providers in the US, Canada, and the UK.

Under our former names of ZD Labs and eTesting Labs, and as part of VeriTest since July of 2002, we have delivered rigorous, objective, independent testing and analysis for over a decade. With the most knowledgeable staff in the business, testing facilities around the world, and almost 1,600 dedicated network PCs, VeriTest offers our clients the expertise and equipment necessary to meet all their testing needs.

For more information email us at info@veritest.com or call us at 919-380-2800.

Disclaimer of Warranties; Limitation of Liability:

VERITEST HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING, HOWEVER, VERITEST SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ALL PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY TESTING DO SO AT THEIR OWN RISK, AND AGREE THAT VERITEST, ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN ANY TESTING PROCEDURE OR RESULT.

IN NO EVENT SHALL VERITEST BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS TESTING, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL VERITEST'S LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH VERITEST'S TESTING. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.