Non-Restrictive Technology in Education
The reboot-to-restore concept

Last modified: February 2012

Simplifying Computer Management

www.faronics.com

Introduction

Computers have formed part of educational institutions for decades. Computer Aided Instruction was widely accepted in schools in the 1980s. Today, computers have become the sole medium of instruction and multiple Classroom Management Solutions are used by schools to educate students.

In addition to being a medium of instruction, computers are used for collaboration as well. Large computer labs have been set up in schools to broadcast instructions from the teacher as well as for student-teacher and student-student collaboration. Since the computer is the sole medium of instruction, it is critical to have 100% computer uptime.

The increase in the number of computers have increased the workload of IT administrators who are already facing the pressure of huge budget cuts from the government.

This white paper talks about the various challenges faced by the IT administrators in education and recommendations to overcome them.

Educational Environment Computing Situation

There are several problems that educational institutions must deal with in their day-to-day management of computer labs.

Security Threats

Malware, in the form of spyware, viruses, rootkits, Trojans, and keyloggers have become a pervasive and increasingly unmanageable problem. IT staff often have a suite of products to combat the different forms of malware — anti-spyware, antivirus, and adware programs are installed and run frequently on lab machines. These products require management and maintenance; IT staff spend time ensuring that definition files are updated and that patches are applied when they are released.

The high volume of multiple users on the lab machines in an educational environment means users are accessing Web sites or using removable media that could potentially invite malware into a system. The constant management of malware can result in IT administrators locking down certain sites and programs that have been deemed problematic. While this can mean a decrease in malware, it can also mean that the learning environment becomes more restricted for students.

Malicious Users and Innocent Clickers

Students are growing more computer savvy every day. They are capable of downloading programs that can damage a computer — file sharing and p2p programs, keyloggers, and several other programs that can take up bandwidth and affect the efficiency of the lab and of the system. Conversely, “innocent clickers,” who are unaware of the consequences of their actions, can cause serious damage to an operating system. Facebook, Twitter, photo sharing websites and online gaming sites might be used to propagate malware.

Between these two types of users, IT administrators are continually fighting user “sabotage” of software and managing changes made to operating systems that cause computer configurations to be inconsistent across an enterprise. This makes things difficult for instructors who need a uniform environment to teach their classes. The amount of time and resources used to manage this problem can be staggering and financially draining.

IT Resources

In education, a typical ratio of IT support staff to computers is 1:500. Not surprisingly, IT staff are frequently stretched to the limit, and often spend the majority of their time re-imaging and rebuilding machines to keep them up and running. The rebuilding or re-imaging can happen on a weekly or even daily basis, leaving little or no time to make other improvements to labs, or work on troubleshooting more minor issues. This can result in technological demand outpacing technological support, and helpdesk calls can escalate beyond control.

As a result, IT staff would prefer to lock down the machines to prevent users from damaging the machines so they don't have to spend all their time rebuilding them. This means the IT staff can have more control over classroom policy than teachers do, because the IT staff don't want or don't have time to be constantly rebuilding workstations.

Approaches to Security

Lock Down Approach

The most common response to the technological issues facing education, have been restrictive. IT staff lock down computers to prevent any mischief on the part of the students, or as a defense against malware. This response means less rebuilding of machines, but can place severe restrictions on the part of the students' learning environment by not allowing the use of the full functionality of the computers. Technically, this approach still results in a temporary (`TEMP`) file build-up, deterioration, slowness, and issues related to computer degeneration. IT administrators have to eventually rebuild a system that is locked down.

Reactionary Approach

If labs are not locked down, the IT staff is most likely using a reactionary approach to maintain security. The reactionary approach means dealing with computers on an individual basis and using re-imaging or rebuilding as a method of keeping computers uniform and protected.

However, the problems with this approach are many, given the amount of time it takes for the rebuilding process, and the correlating downtime of the machine. This approach is also only a temporary one, and does not deal with the cause of the problems faced by the labs.

The Non-Restrictive Reboot-to-Restore Concept

What if there was a better way? What if IT staff could be assured of not having to re-build damaged workstations but students could still have unrestricted access to computers and be allowed to do whatever they want?

The non-restrictive, reboot-to-restore concept makes this possible. This approach allows students to learn in an unrestricted environment without damage to the computer. Students can freely learn about operating systems and experiment with different programs. They can customize their desktops, delete or create shortcuts, and do virtually anything they want to the computer; the computer's desired configuration is always restored upon reboot. Teachers are assured of a uniform environment in which to instruct; students are guaranteed an unrestricted, available, and perfectly functioning machine; and IT staff does not need to spend valuable time rebuilding or re-imaging machines.

Non-Restrictive Technology Benefits

The benefits of non-restrictive technology are many:

- offers an unrestricted learning environment for students with improved efficiency levels
- eliminates obstacles to initiate technology in learning
- gives students the freedom to experiment and learn without penalty or consequence
- enhances system performance due to improved resource utilization efficiencies
- enhances computer performance by eliminating the need for most routine hard drive maintenance
- ensures consistent configurations
- reduces unnecessary anxiety related to allowing users access
- improves the classroom technology experience
- allows user full access to computer without time-consuming management restrictions

- significantly lowers Total Cost of Ownership for technology assets because of a vast reduction in time and cost spent maintaining and rebuilding machines
- eliminates the hidden costs present in the time teachers and other less qualified people spend troubleshooting computer issues

Faronics Deep Freeze

Deep Freeze preserves your computer configuration. Any changes - either malicious or intentional- are reversed on reboot. This concept is called Reboot-to-Restore, where each reboot restores the computer to its desired configuration. The desired configuration is controlled by an IT administrator and the IT administrator has the ability to change the desired configuration. Faronics Deep Freeze offers a non-restricted learning environment for students, uniform labs for teachers, and leaves IT staff free for more valuable and proactive activities. Faronics has been a pioneer of reboot-to-restore technology since 1999.

The benefits offered by Deep Freeze are many:

- offers the ability to standardize workstation configuration, from the programs installed to the placement of icons on the desktop
- allows for permanent, scheduled, or ad hoc updates to the operating system and software
- downtime is reduced dramatically, in correlation with a vast reduction in maintenance costs
- computers no longer have to be rebuilt or re-imaged; eliminates all software-related issues
- computers are returned to their desired configuration with a quick reboot
- has a small footprint; little disk space is required
- integrates seamlessly with all third-party management applications
- can be easily controlled and configured via the GUI Enterprise Console
- requires no maintenance; no definition files to update and no patches are needed
- supports Windows Updates and Anti-Virus Updates

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% machine availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a market-centric focus, Faronics' technology innovations benefit educational institutions, health care facilities, libraries, government organizations, and corporations.