Imaging, Security, Configuration, and Maintenance For the Masses

Brandon Koeller
University of Washington
Box 352820
Seattle, WA 98195
206-616-7219
koeller@u.washington.edu

Karalee Woody
University of Washington
Box 352820
Seattle, WA 98195
206-543-0682
karalee@u.washington.edu

ABSTRACT
Educational Partnerships and Learning Technologies (EPLT) [1] at the University of Washington maintains and supports a fleet of approximately 1,000 general-access student computing workstations across campus. Our services include a broad range of software offerings, multimedia creation capabilities, research support, teaching support, and full featured in-person consulting. The distributed placement of the workstations in a variety of environments, and the high numbers of clients that use them presents some unique technical problems and support issues that EPLT has solved and worked into a robust environment. We have a firm commitment to keeping the workstations as unrestricted as possible, to presenting a consistent, sensible interface to clients, to a fast turnaround between clients and to minimizing downtime of workstations. Using Windows Active Directory [2], Windows Software Update Services [3], Faronics Deep Freeze [4], Symantec Ghost [5], and a small set of custom backend configurations and scripts, we have managed to provide a consistent, robust, full featured computing experience that presently serves up to 60,000 clients per week.

Categories and Subject Descriptors
C.5.3 [**Computer System Implementation**]: Microcomputers – *Personal computers, workstations.*

General Terms
Management, Documentation, Performance, Design, Reliability, Security, Human Factors, Standardization.

Keywords
Imaging, workstation configuration, systems maintenance, Symantec Ghost, Faronics Deep Freeze, general-access computing, Windows Active Directory, Group Policy, scripting, software update services.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
ACM SIGUCCS'05, November 6-9, 2005, Monterey, CA, USA.
Copyright 2005 ACM 1-58113-000-0/00/0004…$5.00.

1. INTRODUCTION
The modern college campus has transformed in the last decade into a typically rich computing environment. Technology has become imbedded into the fabric of academic classes, research, social activities, and everyday communication for faculty, staff, and students alike. That pervasiveness of technology has spawned a density of computers on the average college campus that has brought about a host of management problems. Organizations need to have the right technology service in the right place at the right time for that technology to be really useful to the higher education community and to contribute to the mission of good teaching and learning. This paper seeks to describe one set of management practices, processes, and solutions implemented at a large public research university to effectively maintain a sizeable fleet of distributed general-access computing resources.

The University of Washington is a large, public research university with approximately 43,000 graduate and undergraduate students, 23,500 faculty and staff, and 3,400 instructional faculty.

Our department, Educational Partnerships and Learning Technologies consists of several smaller subgroups that handle a wide variety of technology and outreach programs on campus and in larger communities. The group in charge of the general-access computing resources in question for the purposes of this paper is called Catalyst Client Services [6]. We consist of a Director, a Technology Manager, five full time managers, three of which manage general-access facilities, 10 student employees with system administration duties, and approximately 50 student consultants who staff the lab help desks.

This paper will deal specifically with the Windows PCs in our spaces. While we have a very similar set of management practices in place for our Macintosh systems, we have limited the scope of this paper to just the Windows PC workstations.

2. FACILITIES
2.1 Spaces
We run three basic general-access spaces, two of which are conventional computer labs and one that is a distributed general-access space across 10 of the campus' largest libraries.

Odegaard Undergraduate Library Computing Commons (OUGL Computing Commons) is our largest facility located in the campus' undergraduate library where we take up the entire second floor of the library. We have a mix of Apple Macintosh and Dell PC computers with about 15% of our workstations being Macs.

There are approximately 350 workstations available. The facility is open 24 hours a day, five days a week.

Mary Gates Hall Computing Resource Center (MGH CRC) is located in one of the newer buildings on campus and is near many undergraduate facilities and services. It also contains a mix of Macs and PCs. There are 186 workstations available. The lab layout is much more focused on longer-term activities such as writing and research and provides a large desk for each workstation.

Access+ is a service we operate in collaboration with the Libraries where we provide lab-like workstations throughout the libraries. All workstations have comparable hardware and software specifications to the general-access labs we also operate. There are 260 workstations available in both high traffic areas or in quiet research areas. The project currently is located in nine libraries total, including the four largest libraries on campus.

It is our commitment to keep 95% of the lab equipment operational at all times. On average, we have about 98% operability. The occasional trouble machine is quickly attended to and put back in service. If we need to wait for a replacement part, a workstation may be out of service for a couple of days.

Additionally, we maintain and operate five large computer classrooms that largely employ the exact same management solutions described herein. Our total count of nearly 1,000 workstations includes these workstations, but our usage numbers of clients does not include them.

Equipment and software in all of our general-access facilities is funded by a student governed body known as the Student Technology Fee Committee (STFC). Each quarter, $40 is collected from every student and placed in this fund. Units on campus then submit proposals to the student committee who reviews and either rejects or approves proposals based on a specific set of criteria. STFC guidelines are set forth such that they fund generally accessible technology for students only. They do not fund operational costs, furniture, building renovation, or educational technology for classrooms.

2.2 Clients

Each of our workstations requires the client to authenticate prior to use. Authentication is achieved with the UW Network Identification, UW NetID. UW NetIDs are provided to all UW faculty, staff, and students. In addition to lab access, the UW NetID provides the clients with access to email, web space, and file storage. Currently we grant nearly 60,000 logins per week in all facilities combined, with approximately 15,000 unique clients per week. Over the course of an average quarter, our facilities are visited by 30,000 unique clients and get over half a million individual logins.

3. SERVICES

3.1 Hardware

Thanks to the Student Technology Fee Committee we solve a great many management problems by simply having great, up-to-date, warranteed equipment. Each facility usually has no more than two generations of Dell PCs. Standardization of hardware is a cornerstone of our management systems and the availability of funding via the STFC has allowed us to maintain high quality equipment through yearly upgrades to out of warranty equipment. Our highest end systems at the time of this paper's publishing are P4 3.6 GHz processors, 2GB of RAM, 256MB video cards, 20" LCDs, DVD burners, and gigabit Ethernet. Each facility does have slightly different specs based on the year that equipment was installed, but new equipment is always at the higher end of the technology curve.

All of our client workstations are purchased with a four-year warranty. These workstations are replaced at the end of their warranty. When items leave our lab, they are generally relocated into smaller departmental labs that have a smaller, less intense client base.

3.2 Software

One of the main draws to our facilities is the amount and quality of software that we are able to provide and support. Any kind of standard professional computing functionality is addressed including multimedia applications, programming, office productivity, statistics, and math software. We do limit the amount of software we install to campus standards or to very popular software requested by students. Our average software rollout is approximately 5 GB in size. Each facility strives to keep their software suite looking as much like the others as possible. We have a firm commitment to making each user experience as easy and comfortable as possible for our clients, and we believe consistency of configuration contributes greatly to that.

Licensing is managed concurrently for particularly expensive software such as Adobe products with KeyServer software from Sassafrass.

3.3 Consulting

The core of all our services is our student consultants who staff our lab consultant desks. They answer any questions about software, hardware, or use policies that clients might have. We provide them with a substantial amount of training, access to a large knowledge base, and the ability to capture and track client questions beyond the help desk. These student consultants are the pool from which we typically recruit our 2nd tier systems administrators, which we call Student Leads. Those student leads are responsible for all image building, configuration, deployment, and maintenance.

In addition to our student consultants, we provide a variety of other services to the campus in general with our full time staff including consulting about system management.

4. IMAGING

4.1 Overview

By way of introduction to the following sections, it may be constructive to provide an overview of the entire system. The process starts with a student lead creating a software image on a model system. This image is setup and configured to look exactly like how we want all the systems to look. He or she uploads the image to a server using Ghost. The image is then distributed to all the workstations via Ghost, and is configured to have unique names, IP addresses, and Windows SIDs with Sysprep. Once the machines are imaged, they are then remotely frozen with Deep Freeze. Machines are refreshed between users with a restart, which Deep Freeze restores to its original condition. Updates to

the image are made either with Software Update Services, or with Active Directory scripts. Configuration of workstations via Group Policy is done via Active Directory.

4.2 Creation

The creation of our images is probably the most crucial element of our entire management system. All image creation is handled by our student leads. The average platform lead is responsible for imaging and maintaining approximately 200 workstations. We maintain a large procedural document that contains all the steps involved in creating an image for our labs. The student leads are also responsible for keeping that document up to date.

Some highlights of the imaging document include how to install and setup Windows XP, install and configure every piece of software in the labs, configure printers, setup autologout, security settings, appearance settings, as well as a set of quality assurance steps they perform to verify they have configured everything properly. Particular attention is paid to how things will appear to the client. Each application is launched, sized, and configured to be as ready for client use as possible. Additionally, the windows profile used to configure the software is saved as the default profile. This way, what the Student Lead sees when they create the image is exactly what the client will see. Concurrent licensing controlled applications are keyed to the KeyServer at time of imaging. Custom backgrounds are set, and local configuration scripts and files are staged.

It is useful to note here that our systems are configured such that every user is an Administrator of the workstation they are using. All users are permitted to install any software or delete anything they like. Our users enjoy this kind of freedom to explore and configure the workstation to their preferences. Since Deep Freeze disallows any kind of permanent changes to the software, it is feasible for us to allow this level of access. Further discussion of how this works is in Section 7.1.

Among the last things our Student Leads do is to configure the workstations for deployment with Symantec's Ghost, and software maintenance with Faronics' Deep Freeze. Since we have so many workstations, it becomes difficult to do any kind of manual configuration at time of deployment of the image. As such, we use Microsoft's sysprep product to do post deployment configuration in conjunction with Ghost. Sysprep will join each machine to our Windows Active Directory domain, set the computer name, and set all networking information automatically.

At the time of image creation, we will create a Deep Freeze workstation seed with the correct operational parameters for the workstations in that facility. This seed will be used to push the full Deep Freeze client to the computer after the cast is complete. The machine will then be frozen remotely from a central server administration console and any reboot or update configurations set.

Once the image is installed and configured on one machine it is then rebooted to a ghost client and gathered with a Ghost Server.

4.3 Deployment

With a ghost image on a central server, a ghost server session is started with a known session name and opened up to attach clients. We then boot each machine off of a custom CD that contains a batch file that calls a Perl script and launches the ghost client. The Perl script is how we can have only one imaging CD, but have each client get differentiated settings. As mentioned before, each machine has Sysprep installed on it before it is shutdown for gathering by ghost. The next time that image is booted, sysprep will look for a file called sysprep.ini, which should contain all the particular information for that machine such as machine name and ip information. On the ghost CD, we have a text file that contains every machine's MAC address, as well as the sysprep information that it requires. The Perl script calls a text reader that reads the networking information from the screen dump on boot, then does a lookup in the machine data text file and creates a custom sysprep.ini file on the fly. That sysprep.ini file is copied to the local hard drive so that sysprep can use it on the next boot. The last step in the imaging CD boot up is to launch ghost with preset server parameters so that it connects to the correct server automatically.

After booting all the machines off of the master ghost imaging CD, all that is left to do is to press the start button on the ghost server and wait for the image to cast to all the machines. We use the multicast mode of ghost because any other mode is too network intensive for the number of workstations we maintain. Once the image is done loading, the machines reboot, run sysprep, reboot again and are ready for users to login.

The machines are not quite ready for use at this point, however. Any client that logs in would be able to make any permanent changes to the image, which would make the user experience inconsistent and potentially dangerous for other clients. The last step in our deployment is to install Deep Freeze on all the workstations. From a central Deep Freeze Console, all workstations can be accessed and a Deep Freeze client installed and configured remotely by way of the previously installed seed.

With Deep Freeze installed and the software frozen, the workstations are all ready for use. Note that the only time we actually had to go to each machine was to boot it off of the ghost imaging CD. All other configuration is done remotely. One person can image hundreds of machines at a time with very little effort.

4.4 Updating

Updating an image usually starts with a series of decisions about the urgency of the update. Simple updates that can be made with scripts are tested, and then deployed within hours. If an update is determined to be large enough or unable to be deployed with a script, it is generally noted in a tool such as BugTracker and deployed with the next image deployment. If it is a serious problem or a time sensitive update, a new updated image can be created within hours, and deployed as soon as possible. Non-serious updates are completed at our convenience. Typically, we do image updates approximately every five weeks which is approximately twice per quarter. Windows updates are accomplished via a Software Update Server on a nightly basis.

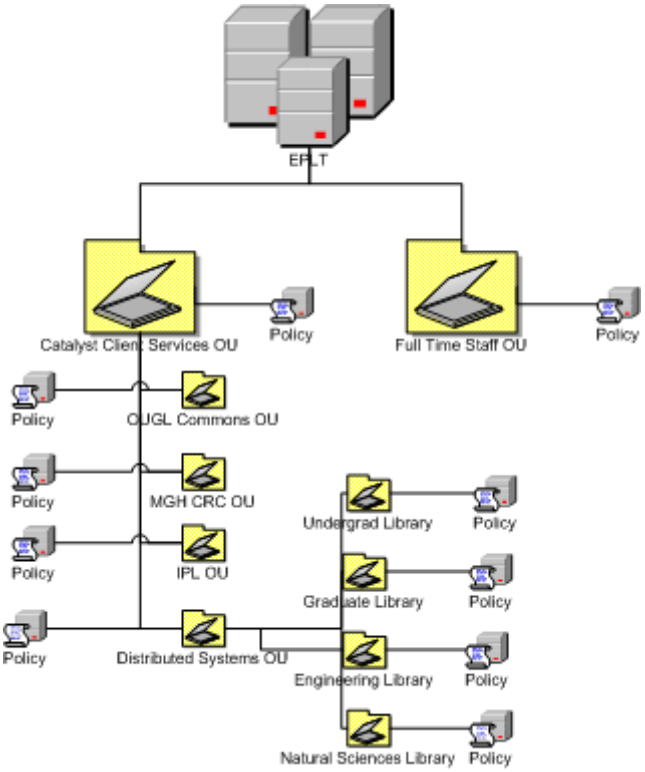
5. CONFIGURATION

5.1 Active Directory

One key tenet of our entire management system is the concept of centralization. The more we can consolidate and reduce the steps it takes to create or deploy an image, the more reliable the system becomes. Microsoft Windows Active Directory technology has

provided us with several opportunities to centralize configuration and to increase the security of our entire fleet. All computers in our fleet are members of a domain, which is in turn, a member domain of a larger campus forest. Each computer has an account in our domain, while users authenticate with credentials in another domain. In this way, we are able to manage machines without having to manage user accounts as well.

Since our domain also serves our larger department, all lab resources are separated into their own set of Organization Units (OUs), including machine accounts, group policies, and user accounts. This OU is delegated to student network administrators who are responsible for maintaining that portion of our domain. Under the main lab OU, there are separate facility OUs as well. This separation of general-access resources into a distinct OU provides a security barrier from the rest of our domain resources and allows us to control resources with a very fine level of granularity.



5.2 Group Policy

One way that we reduce image creation steps is to implement group policy at the domain level rather than at the local machine level. Group policy is, broadly speaking, a set of configuration parameters that control or restrict anything in the Windows environment including appearance, settings, or security. We are able to nest group policies within the labs OU and down into the separate facility OUs to provide for specialized scripts to be run and for facility differences. Any time a decision is made to make a change to group policy such as restricting access to a control panel or updating the windows firewall settings, it need only be changed at the domain level, and the changes will be implemented across the entire fleet within minutes. At present we have group policy settings for the top-level domain, the labs OU, and for each separate facility OU.

5.3 Scripts

Group policy is a very powerful tool, but it does not permit us to make changes to several parts of the Windows environment. Extending our ability to make changes is accomplished through the use of startup, shutdown, login, and logout scripts. Group policy allows system administrators to specify locations of scripts that we want called at each of those four system events.

Each facility maintains its own separate file share to host scripts, but most of them are identical. This setup allows us to first provide some measure of redundancy so if one file server goes down, not all facilities will be without access to their scripts. It also allows us to customize those scripts for each facility.

Before talking about startup and login scripts, it would be constructive to mention that we keep records of every login and logout event that occurs. Client privacy is considered and maintained. Each event is recorded in a central PostgreSQL database that drives a home-grown set of web tools and applications we refer to as LabTracker. Events are inserted into the database via a Perl script called at login or logout that posts an SSL encrypted URL to a central web server.

The startup script contains code to set the login window default domain and view settings and to launch a special application to run in the background that provides several services for users as they work. This service, called launchapp, runs certain other scripts and programs with elevated privileges such as our autologout program and our user file backup service. Occasionally, repair scripts are called in the startup script to fix registry entries or to copy files to the local hard drive. On the OUGL and CRC machines, where the machine is rebooted between every user to refresh the system, the startup script is also where a Perl script is called to report that the system is ready for another user to login to LabTracker.

Our login script calls a Perl script that reports a login event to Labtracker. We also do session specific configuration such as for mail clients. The login script is where many of our fixes get deployed such as printer queue name changes, application registry entries fixes, and file replacement. These fixes in the login script are temporary, and persist only as long as the fix is not incorporated into the final image.

6. SECURITY

6.1 Authentication

Controlling access to our resources has been very helpful in maintaining the machines in a high state of readiness. It also facilitates our usage tracking. Our central computing department on campus (Computing & Communications) provides us with access to a Windows domain that contains a user account and authentication privileges for every owner of a UW NetID, divided into OUs such as Faculty and Staff, Alumni, and Students. We configure all of our workstations to allow logins from the LABS domain, while the machines exist in the EPLT domain. LABS domain account OUs are added to the local machine account groups in order to provide access and access privileges.

6.2 Account Privileges

In the spirit of as much access and openness as possible, we make every user of our machines an Administrator on that particular machine. This allows users to install any software they might want, and to make any interface changes they want during the course of their session. We do limit privileges in some cases where there exists a danger that a user's identity or files could be comprised with other users. One case where client privileges have been restricted to User level is on the Access+ workstations. Since one of the primary design principles for the project was to provide a very short turnaround time between clients to accommodate as many clients as possible during peak times, it became clear that a full system reboot to engage Deep Freeze refreshing functions would be very time consuming. At the same time, client privacy and image stability and consistency needed to be maintained. Clients get User level privileges so that they cannot make too many changes and do not have full file system access, thereby making a simple logout event a basic Windows logout a much safer proposition. However, Access+ workstations are rebooted nightly. As for the rest of the general-access spaces, we can permit Administrator access because any changes a user makes essentially goes away once they logout. Deep Freeze restores the system partition to its default settings upon reboot.

6.3 Virus Protection

Virus protection for users and, to a lesser extent the campus network at large, is accomplished through the use of McAfee's Anti-Virus software [7]. The campus owns a site license and provides the software free of charge to any campus users. Central Computing Services also provides a campus cache of virus descriptor updates which each machine will update against nightly. Deep Freeze protects us from viruses between users by resetting the system back to a known default, and McAfee Anti-virus protects us from infection during any given users' session.

6.4 Network Security

While we do not maintain any of the localized network resources such as routers and switches, we rely on a set of security protocols setup by central computing services that detect certain kinds of bad network traffic streams that indicate an infected or compromised computer and block the computer's MAC address, or the network port in some cases, from accessing off campus network resources. Once the machine has been cleaned of any viruses, Trojans, or other wise restored to a safe state of operations, there is an automated way to get network connectivity to the outside world restored. We rarely get compromised lab workstations, but users who hijack network ports for their laptops often get caught by this network security measure.

6.5 Critical Updates

In the recent past, the largest issue we have had with image maintenance has come with the increasing criticality of deploying Windows Critical Updates. The time frame required from the time a Windows system exploit is released to the time we need to have patches in place on all workstations is often on the scale of hours. Deep Freeze makes scripted incremental changes for system updates like critical updates not viable, however Deep Freeze provides a maintenance mode which un-freezes, then reboots the computer to a mode that allows certain maintenance actions such as updating from a local Windows Software Update Server or refreshing virus definitions to occur without any potential for interruption by clients. We run this maintenance mode nightly in the spaces that close every night, and weekly in the spaces that are open 24 hours a day. Generally, we have the ability to run this maintenance mode and deploy critical updates at will.

6.6 User Data

As mentioned earlier in the scripting section, our login scripts call a homegrown application that backs up user files to a local unthawed drive space so that any files a user creates is saved there until a discreet logout event is initiated. In the case of a catastrophic machine failure or a logout initiated by autologout, all user files will be retained. To retain user privacy, all user files created during a session will be deleted when they initiate a full logout event by double clicking the logout icon on the desktop. Default save locations in all applications has been set to either the Desktop or to My Documents, which are both located in thawed drive space.

6.7 Account Protection

Since user sessions require and retain user credentials, protecting users from other users is important. If a client logs in and walks away without logging out, another client can sit down and potentially determine the UW NetID of the previous client and possibly send email via their account, as well as potentially being able to access UW NetID protected web resources. We provide a significant amount of signage reminding users to protect their UW NetID with a logout, and also provide an autologout service that will logout a machine after a certain amount of idle time which varies from space to space. There has been no significant account theft events reported to us yet.

7. MAINTENANCE

7.1 Between Users

Deep Freeze has been mentioned several times in this paper, as it serves as the core of our user-to-user maintenance. The software essentially prevents a user from making any permanent changes to the hard drive of the computer. Any changes made appear to be real and the system will operate for that user session as if the changes are permanent, but a simple reboot will reset the hard drive back to its original condition. Drives are frozen where no changes persist, or thawed where any changes are permanent and all freezing and thawing operations are controlled by a local system binary that is inaccessible to clients unless they know the correct key combination to bring it up and the password to the client.

8. CONCLUSION

The world of higher education information technology management is, like with many other areas, an increasingly delicate balance between money, time, and resources. Robust, reliable, and well-maintained general-access computing facilities can be a powerful campus resource that can do a great deal to facilitate great teaching and learning.

9. ACKNOWLEDGMENTS

Our thanks to David Cox for his patience and technical brilliance over the years in developing this system.

10. REFERENCES

[1] *Educational Partnerships and Learning Technologies*: http://www.washington.edu/eplt/

[2] *Windows Active Directory*: http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

[3] *Windows Software Update Services*: http://www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.mspx

[4] *Faronics Deep Freeze*: http://www.faronics.com/html/deepfreeze.asp

[5] *Symantec Ghost*: http://www.symantec.com/sabu/ghost/

[6] *Catalyst Client Services*: http://depts.washington.edu/sacg/

[7] *McAfee Anti-Virus*: http://us.mcafee.com/root/package.asp?pkgid=100