Cooperation - a better form of university networking ? Implementing remote administration for widespread Windows networks

Claus Peter Buszello, Matthias Fay and Wolfgang Schmid

Albert-Ludwigs- Universität Freiburg

fay@forst.uni-freiburg.de
Werderring 6, 79085 Freiburg im Breisgau
www.forst.uni-freiburg.de/adminice

Keywords: *remote-administration, software-distribution, windows, cooperation*

Abstract: *We would like to demonstrate how the need for a better administration of computing resources and the required manpower - based on the desire for a more effective use of the existing modern network infrastructure - led to a cooperation between different branches of the Faculty of Forest Sciences at Freiburg University.*

The growing demands of computer network administration require a considerable number of highly qualified administrators, who are difficult to find and extremely expensive. On the other hand, universities tend to develop their own solutions and capabilities. Therefore a small group of 5-6 students was formed, which together could administrate a number of workgroups spread all over the campus. One task was to develop a system of remote administration for all the clients, a problem solved by script-based tools developed as part of the project. Another important concern is security. The tightening of the security in the Windows NT domain first caused some worries among the users about their freedom to install software for testing purposes; yet ultimately it was the development of a sophisticated structure that changed these worries into a perception of improved data security and high availability.

On the one hand, our concept is based on a reliable network, central backup and DNS provided by the University Computing Center, but on the other hand we are providing central storage and software distribution, web, mail and news servers using a heterogeneous network consisting of a Windows NT Enterprise cluster, three Sun Solaris servers and about 100 Windows NT clients. The major instance of communication between users and administrators is a web-based troubleticket system implemented for this network.

Finally, in the last two years we have managed to reduce the costs of administration and of the acquisition of new devices by implementing a centralized system.

Preface

In strong correlation with the still growing importance of computers in all areas of universities the demands on the machines themselves have risen to a maximum level. This development has been taken care of by the manufacturers of hardware and the developers of software. On the other hand the amount of information that has to be handled is still growing. The process of globalisation has reached universities, too. So external developments call for a cooperation, which can be supported by a sophisticated network structure. In addition, in Germany a better cooperation between the areas of research and teaching has also been discussed, focussing especially on the financial aspect.

These issues have been discussed in the department of forestry at Freiburg University. The result was the desire to reduce computational costs. At the same time Matthias Fay was able to offer a solution based on a concept just developed by himself and Claus Peter Buszello at the university computing centre for the students' computer pools. The advantages of a cooperation lay at hand. Many research projects are supported by different branches in the department. In order to facilitate the data exchange the new network concept offered promising solutions, which in return could reduce computational costs and hence improve research capabilities. The concept did also fit very well for a phenomenon typical for universities, the fact that purchasing new hardware is better accepted by university administration than employment of new administrators. There is a tendency to cut jobs rather than to cut money for the purchase of new hardware.

In the next chapters we will demonstrate how the Adminice system works, why it is easy to implement and maintain, why it is reducing administration costs and how it is providing a structure that eases the data exchange between members of the faculty. Great emphasis has to be put on the fact that each computer on the world running under MS Windows NT or 2000 that is a member of the Windows domain can profit from the advantages of the concept without any special features.

Current status and possible ways out of it

In this chapter we would like to describe our observations of the computer usage before the implementation of the Fnet and how we developed solutions for existing problems.

Status

At the time being most of the computers in the faculties are using different operating systems. In most cases each branch of a department has a student employed for administrating the computers. In this case the administrator has to perform many complete reinstallations of the systems in order to provide a sufficient availability of the computers, a time consuming process. Therefore not much time is left for system development. In most cases keeping the standard, in most cases an antiquated standard, is the only thing going on. Another great disadvantage of this situation is that knowledge is acquired and kept in one branch of the department. The rapidly

increasing knowledge required for administrating these computers has to be provided by one person. The administrator has to pass all that knowledge and information over to his successor, which is also taking a lot of time. Finally this has lead to the situation that very often assistant lecturers are administrating their systems by themselves as far they can in order to get the required availability of their computers. So they are spending time required to research for maintaining their computers.

Another important issue heavily neglected is data security and backup. In most cases a severe breakdown of the machine results in the worst case, the irretrievable loss of data.

In most cases the users do not have the necessary feeling for security issues. Very often they use standard installations of operating systems which do not provide an acceptable security level. On quite a lot of computers not even a virus scanner can be found. In addition to that the fact should be mentioned that these computers, running under Windows 95, have fixed IP addresses and data stored on a local hard disk, which is quite often shared. This scenario can only be described as an undesired open door publishing of sensitive data.

There are also different versions of software and operating systems installed within the same department causing serious problems in data exchange.

Possible ways out of it

In order to eliminate all these problems the idea to put the administration of the computers in different departments in one hand appeared to be the ideal solution. The centrepiece of our concept is the bundling of know how in one institution, resulting in the provision of a continuously lasting and highly available system. In order to make it possible for the administrator to keep up with the knowledge and even improve it, but also to provide a better security a system had to be developed that could possibly save the administrators a lot of time. As mentioned above, form our point of view the greatest obstacles to an effective administration are the time consuming installations of operating systems, software and hotfixes. So our most important concern was to find a way how to perform these jobs automatically. The great amount of time saved by this could then directly be used for acquiring new knowledge and improving the system. The improved efficiency at the time being makes it also possible to administrate the two clustered servers and about 100 workstations with costs of the administrators of about 933? per month, which means 111? per computer per year including backup, installation of new hardware and making plans for further developments. Also included in this price is the installation of all new software including updates and of new hardware devices.

But anyway our best argument in the discussion is that the solution is absolutely free. We have made Adminice open source, it is available for everyone.

Possible Obstacles

The situation before the change to the Fnet described above was also marked by a greater freedom of the users. If a user wanted to install a trial version of software that might be required, he just installed it. He also had the freedom to write files everywhere on the local hard disk. In the beginning of the Fnet there were several people heavily complaining that they had to pass over computer sovereignity to the network administrators. The reduction of the users' rights first seemed to be an essential disadvantage of greater relevance than the reduction of the downtime of the machine and the reduced time for a reinstallation of the computer.

In order to provide the safest and most reliable configuration the users' files had to be stored on a central fileserver. This again basically means that the users have to give their data to another institution, where the data is basically accessible for the administrators. In this case again users feared a possible manipulation of their data, data, which before had been stored on a Windows 95 client with a fixed IP address, without any restriction in file permission. It has taken great effort to convince these users that their data was finally safer in the new system than it had been before. So the greatest problem was to eliminate the users' reservation by providing a maximum data security combined with a relationship of mutual trust.

First observations

Since the introduction of the Fnet in August 1999 the users' reservations have remarkably declined. The users' attitude towards the system has become better and better. Even the strongest opponents make statements like "One can realise easily how the availability of computers have improved". Unfortunately we have no means by which we can measure the improved effectiveness. By what we have been told so far we can state that it has improved. Projects like the SFB 433, in which several branches of the department participated, would have been faced with serious problems in data exchange and not to forget the redundancies that would inevitably have occurred without a central file and backup server. All of this would definitely not have been possible without the desire for a cooperation. The basic desire for cooperation can be supported by a sophisticated network, which in return encourages for further cooperation because it is the basis for a better cooperation.

Another great advantage of the cooperation is that the bundling of interests improved the position of the participating institutes within the department.

Implementation of the system

The cooperation would not have worked without finding a way to centralise administration tasks and the distribution of software. The implementation and maintenance of the system with only three people employed for 38 hours per month can only be achieved if these do not have to install each computer completely by themselves. The time necessary for administrating the computers could not have been planned if each user had full control over his or her PC.

In essence the implementation of the system is based on Windows NT clients, but several tests have also proven that the system can be used on Windows 2000 clients without any modifications or limitations. As servers we are using a Windows NT High Availability Cluster and a Sun Solaris Server, which is mainly used for GIS-applications and for service purposes, like web-serving, email etc.

For the system had to fit into the network structure provided by the university computing centre, we are using the following services: TCP/IP network with fixed addresses, DNS and central backup (ADSM). On the one hand these services are important but on the other hand they are not required for running our system. So we will leave these aside.

Server Hard- and Software

Centralisation requires several investments in hardware for the server and network infrastructure. We think, a High Availability Cluster is inevitable for projects of a certain size. So our hardware consists of two IBM Netfinity Servers connected by two Serve Raid adapters

to an IBM Expansion Bay providing about 100GB RAID5 disk space. We use Windows NT Enterprise Edition as operating system. In case of a hardware failure of one machine this software performs the action of handing resources over to the other server. Above all this provides a use of the system without any interruption for the users and administrators as well.

Client Hard- and Software

There is only a few requirements to the hardware of the clients. The only have to fulfil the minimum requirements for Windows NT or Windows 2000. The operating system is installed the same way on all workstations (out of the box). The user only realises that he or she can perform the same work on each workstation. This is finally achieved by using just one domain for the whole network and roaming profiles.

Hotfixes and Patches

The most critical point in maintaining workstations is the provision of security hotfixes and bugfixes of the operating system. In most cases this field is almost completely neglected because as a result of the numerous fixes provided and required, the installation of the operating system becomes a very time consuming procedure. And continuous checking is also necessary in order not to leave out a client. For an automatic installation of all the patches and fixes on each workstation in the domain we developed our own solution.

Once the standard installation of the operating system on the workstation has been completed, a service is installed which is primarily doing one thing. After booting the system and hence the starting of the service a script called c:dmdo.cmd is started, which is performing several tasks, e.g. the synchronisation of the clock. But most important, a batch-file on a defined server share is executed, which then installs all required MS service packs, self-made patches and hotfixes on the workstation. Each patch installed creates an entry in a log file called patch.log, where all patches installed are registered. The system then has to reboot and the next patch that is not in the patch.log gets installed by the service. This procedure continues until all patches are installed.

The most important patch is a collection settings improving the security of the client. File permissions and registry permissions are set, registry settings are updated. This “sealing“ of the client is providing an excellent protection from Trojan horses like Netbus or password sniffers but also from viruses. Another advantage of the automatic installation of patches is that none of them can be forgotten.

Software installation

The probably most time consuming process, the installation of software, has been automated in quite a similar way. An identical installation of software on clients with identical installation of the operating system should not be a great problem. Again the major problem is the spatial distribution of the clients and the provision of consistency. So we developed a service that does not necessarily have to run on an NT Server, like in our case, a service that according to a list of clients automatically distributes the desired software to these clients.

Basically software is making the following changes to the system:

a. modifying the registry under
   - HKEY_LOCAL_MACHINE
   - HKEY_CURRENT_USER
b. copying new files to the hard disk
c. replacing existing files, especially .dlls
d. adding entries to existing files, e.g. .inis

In accordance to these modifications instances were developed that can find out these changes. We also wanted to exclude the use of any commercial products. Everything also had to appear in clear text so that all changes could be comprehensible.

Creating a package starts out on a recently installed machine by creating an image of the machine. MD5 checksums of all files are created so that all changes made to the directories can be found out. For this purpose we also tried to use sysdiff.exe and several other commercial solutions but it turned out that none of them was capable of finding out all changes made to the system, resulting in corrupt packages. A complete image of the registry is also created. After the installation process another image of the machine is created. The two images are compared with each other resulting in a package consisting of the following elements:

1. Clear text files consisting of all changes made to the registry in
   a) HKEY_LOCAL_MACHINE: .hlm-file
   b) HKEY_CURRENT_USER: .hcu-file
2. All new files copied to the hard disk during the installation process are reflected in the same structure on the server, e.g. a newly installed c:þrogramsþrogram.exe is mirrored in a directory on the server by¸þrogramsþrogram.exe
3. changed .dlls and .ocxs
4. updated .ini files

Once the package is created it is ready to be distributed on the target machine. The changes made to the LOCAL_MACHINE part of the registry are directly copied to the machine. The CURRENT_USER modifications are copied to the user’s registry at his or her next logon. The new files are directly copied to the target machine, while the .dll and .ocx files perform a version check on the files already installed, existing files are only replaced by newer ones. The .ini files are modified only by the new entries created during the installation routine.

In addition, file permissions can be set automatically during the distribution, dependencies between certain packages can bet set.

So far we have created about 80 different software packages, including MS Office, MS Internet Explorer 5.5, Adobe Photoshop, SAS, SPSS. We have also installed several device drivers for printers, scanners etc. All of them are working just fine without any limitations in usage. The average time for creating a new package is about one hour. We then developed a service, called iserver, running on the server that automatically distributes the software packages to the desired workstations in the domain. So if e.g. new computers have to be installed, a standard installation of the operating system is performed and the admdo-service is installed, the rest is taken care of automatically once the iserver is started. There is only one condition for the automatic distribution of the software, the computer has to be a member of the domain. The machine can be set up everywhere. Once it is a member of the domain on which the iserver is installed, it can use all the features described above. At the moment the workstations in our domain are distributed all over Freiburg, they are in five different subnets, but all of them are equal members of the domain profiting from the services provided.

Another important issue only briefly mentioned above is security. We tried to enhance data security to the maximum level possible in order not to be dependent on the ADSM backup of the university computing centre. So far we have not been. We are currently planning to perform our own backup on a new DLT stacker. We also keep on searching for security holes and bugs and try to eliminate them.

User support

For the network is distributed all over the city and the administrators are not continuously present, a communication system had to be at the users' service through which the users can report problems to the administrators. This was solved by the development of a web-based trouble ticket system.

The solution is based upon an Apache web server connected to a MySQL database. The user addresses to the information page of the Fnet, where a sheet can be found asking for information about the problem and occurring error messages. After the form has been filled properly the administrator in charge receives an email containing the required information from the page the user has just filled out. The administrator in charge can then give the problem a priority, suggest a possible solution and pass the problem to another administrator. The administrator responsible for the problem can then read the hints given by the other administrators. He can also update the entries for solution and register the time spent on solving the problem. Once the problem is solved, it disappears from a page showing all unsolved problems. That way a problem is prevented from remaining unsolved. Another advantage is that all the time spent on administrating is registered. For all problems solved are stored in the database we are producing a knowledge base for the solution of all problems that have appeared so far.

Conclusion

The experiences made so far have shown that our software distribution system is running very well. Most of the everyday problems appear because of the tight security settings in our systems. In some cases software needs write permission in the system directory in order to save user settings, which in this case have to be redirected to the home directory of the user. Once these problems are realised creating new packages working with our tight security settings hardly cause any problems. We expect that this problem will soon disappear because Windows 2000 does not grant the user the write right in the \winnt-directory, one of the mainly affected directories.

It has turned out that this software distribution system has paved the way for an automated software distribution in bigger organisations. A possible scenario is a share, from which all Windows NT workstations of the whole university can automatically install the latest patches. The only condition is an installed AdmDo service and a local administrator trusting the share. Only few modifications would have to be made; e.g. installing a service pack would require just one more step, which is copying executable on the local hard disk before installing the service pack, in order to avoid possible blue screens caused by non-continuous flow of data.

A software distribution system for the whole university would also be possible. Central servers could provide and distribute packages.

This system is perfectly made for keeping security standards and keeping up the provision of software. Using this system the administrator does not always have to be up to date in security issues. He does not have his time on software installations either, and still his security is up to date. In university many Windows NT workstations and servers can be found with only Service Pack 1 installed. This is mainly caused by the fact that in addition to their actual job many researchers have to do administrative jobs and therefore do not have time to spend on such allegedly unimportant issues. This again calls for cooperation. In our opinion cooperation is the basis for a satisfying (university) networking. The sometimes exaggerated individualism of university departments appears to be one of the greatest obstacles for establishing an effective network structure. This is why the title of this abstract is “Cooperation, a better form of university networking?“