Centralized Approach to Large User and Computer Infrastructure management

Pavel Babinec[1], Lukáš Rychnovský[2], Pavel Tuček[3]

Institute of Computer Science, Masaryk University, Botanická 68a, Brno, Czech Republic
{babinec[1], rychnovsky[2], tucek[3]}@ics.muni.cz

Keywords
Network Infrastructure Management, Centralized Approach, Active Directory Forest, Centrally managed User Accounts, Profiles, and Software

1. EXECUTIVE SUMMARY

Masaryk University has approximately 65,000 user accounts (students and employees) distributed into nine faculties. Not long ago, each faculty had to solve the problem of keeping the information about users actual by itself. They did this by maintaining their own user database, and regularly importing new information about users into their infrastructure, because these information are used to allow access to computers, study rooms, turnstiles, etc. To avoid the need of doing this for each faculty separately, centralized solution of these actions was necessary to develop.

1.1. Background

Microsoft Active Directory technology was chosen for storing all necessary data and one central forest root domain was created. This forest root domain is managed by a small group of enterprise administrators and contains user data (accounts, passwords, policies, etc.) similar for every faculty participating in this infrastructure. This removes the need of keeping a copy of user database at each faculty. Centralized approach was also chosen for user profile storing, which is provided by a central fault-secure server solution, regularly backed-up onto tapes. Thanks to this centralization user data travel from one computer to another across the infrastructure along with users, allowing them to access their own documents, desktop and profile on any student computer at Masaryk University. Each faculty involved is represented by a child domain in the infrastructure, which is used to maintain student computers. Local faculty administrators are only responsible for reinstalling computers and assigning software to them. Installation of computers is fast and unattended, needing only restart and entering the password. Follow-up computer configuration and software installation as well as deploying security updates and anti-virus software updates are also managed centrally.

1.2. Conclusions

This approach is a well-balanced combination of the centralized infrastructure management, and the distributed user support. Local administrators are meant to be solving less serious issues allowing the enterprise administrators to focus on the functionality.

2. MANAGEMENT OF USER ACCOUNTS

Nowadays, Masaryk University has about 65,000 active users stored in an infrastructure based on Microsoft Active Directory technology. It consists of one forest root domain used for storing data, which are common for the whole forest (e.g. user accounts, passwords, and forest-wide used group policies) and several child domains, each representing one participating faculty. Each domain contains three Microsoft Windows 2003 R2 Servers – two domain controllers and one member server used for management.

2.1. User Accounts

The forest root domain is connected to both personal and student agenda. The user database is synchronized every day – new users are created, old users disabled or deleted. Users are also put into appropriate groups to distinguish their pertinence. The granularity is such that students can be assorted up to level of studying subjects and employees up to level of workplaces.

2.2. Guest Accounts

Guest user management of accounts for external co-workers (e.g. conference visitors) as well as for external library visitors is available through a simple website. Here, appropriate user rights are assigned and a guest account in Active Directory is created. At this moment the user account becomes full-featured component of the infrastructure, allowing non-university contributors to use some or all of the resources available.

3. STORAGE OF USER DATA

Every user created in Active Directory user database has also a roaming user profile created at the first logon. This profile is downloaded from the central storage every time user logs onto a computer, which is why user's desktop, documents, and application settings are always available. When the user finishes working and logs off this newer updated profile is uploaded back to the central storage, keeping it actual. The central storage consists of Hewlett-Packard MSA-1000 disk array of total capacity of 1 TB mirrored, serviced by two servers using Microsoft Cluster Service technology, which allow switching the servers when one of them failures or restarts without disconnecting users. At present time, the file system holds approximately 12 million files which take up approximately 750 GB and users have a 100 MB quota. We are currently looking for a new solution due to increasing capacity demands. All data from the disk array are regularly backed-up onto tapes located in a geographically separated location.

4. MANAGEMENT OF COMPUTERS

Computers belonging to this infrastructure (about 800 computers at present) are spread into child domains according to belonging to faculty. Local faculty administrators are responsible for their functionality, which means limited hardware support, reinstalling computers if needed, and assigning software to them. Installations are solved using unattended technology and use PXE network boot – after restarting the computer and entering a password, the computer downloads installation files and finishes the operating system installation. After rebooting a follow-up configuration of the computer comes on. This means setting up a common environment for users and installing assigned software. Both these tasks are managed centrally on the domain controller using group policies to set up the environment and Microsoft Installer technology to deploy software to computers. Enterprise administrators usually prepare the package - rarely using packages created by snapshots, more often using administration install and installation templates. Local administrators of specified faculty then assign the software to whichever computers they want.

The storage of operating system installation files is once again centralized. All of the workstations are currently using Microsoft Windows XP SP2. It is needed to update the prepared installation every month when new critical and security updates emerge. Thanks to the centralization this is only needed to be done once. The storage itself consists of two clustered servers, both operational to raise performance.

The storage of MSI packages is using Distributed File System technology, replicating data to each faculty's servers, so they can deploy the packages using LAN network (DFS node in the forest root domain is only used in case of faculty DFS node not functional). The DFS replication is configured as Hub-and-Spoke with the forest root domain as the central node. This means that each faculty only needs to communicate and replicate with DFS node in forest root domain and not the other child domains, making managing the network easier and the network itself more secure, speaking of firewalls.

5. GROUP POLICIES

Group policies are used for two purposes – to set-up the environment for users, disabling the part of Microsoft Windows functionality that could cause harm to the infrastructure, and to deploy software to workstations. Substantial percentage of the Group Policy Objects is stored in the forest root domain as they are used forest-wide anyway (e.g. common startup and login scripts, certificates, default user policy, most of the software packages, etc.). Only local faculty settings are created and stored in child domains (e.g. local workstation firewall settings, network printer configuration, specialized software used only within one faculty, etc.). Local faculty administrators have rights necessary to create and apply their own Group Policy Objects, use any of the forest root policies and link the policies to workstations of their faculty.

6. SECURITY

One of the problems, which probably every administrator has to solve, is keeping the infrastructure secure. There are several arrangements which are used at Masaryk University to prevent damage to the environment. There are only a few possibilities of approaching the infrastructure from outside of the university as it is protected by firewalls from most of the outside traffic. In addition, you have to be logged onto university VPN network and assigned a VPN IP address otherwise you will not be granted access. Strict firewall rules are also applied inside the infrastructure, allowing only necessary traffic, especially between servers and workstations. Child domains are also strictly separated. There is no need for them to communicate as they have all the common data they need accessible in the forest root domain. There is also a set of scripts which regularly parse domain controller's logs. They warn about bad logins (bad username or password log entries) via email in terms of minutes and about possible functional issues every night also via email. Another security issue is keeping the computers "up-to-date". This means watching and applying at least critical and security updates and keeping anti-virus software databases actual.

6.1. Microsoft Updates

Two Windows System Update Services servers clustered via Network Load Balancing technology are used for distribution of Microsoft Updates to computers. Servers are set-up to synchronize with Microsoft servers every night, downloading and storing all product updates in six languages. Every computer in the infrastructure is set to be updating against this cluster on which critical and security updates are approved for installation. Other types of updates (such as rollups or service packs) are only approved for detection or installation to certain group of computers if desired. Big advantage of having all of the computers update against self-administered WSUS server is that you can easily check for any update issues centrally. At Masaryk University a script which regularly checks the WSUS database for computers not updating for more than two weeks, was put into operation. It exports information about all computers (IP, computer name, latest update) from both WSUS servers, saves it into a text file and merges them. Then it downloads a file containing information about IP ranges and emails of people responsible for them. Since there are two WSUS databases and many computers can therefore be mentioned more times, the script parses merged document and looks for the latest record for each computer, deleting all other records. In case the date of the latest updating process is more than two weeks old the computer is considered "not updated" and this information is saved into a text file specified by IP range, into which the IP address belong. These files are sent to certain email addresses daily, informing appropriate person about the non-updating computers.

6.2. The Anti-virus software

Masaryk University currently uses the ESET NOD32 anti-virus software, or more precisely its network license. Once again, all computers in all domains are set to regularly check for any updates of this product and install them, if there are any. The ESET server also has a database with information about computers and updates deployed to them.

7. TERMINAL SERVERS

To increase the "user-friendliness" of the environment even more a set of terminal servers was put into operation. The set itself consists of five Hewlett-Packard servers clustered via Network Load Balancing technology. These allow users to work with their data stored at Masaryk University from any place with network connectivity. Users simply log on using the Remote Desktop application and get the same user profile and documents as if they were logged on a computer at university study room. A common set of software is installed and available making the environment as similar to a study room as possible. There are also several products, which are too specialized and too big to be installed on all workstations. These are only deployed using terminal servers, solving the problem of licensing and installing them on every workstation at Masaryk University.

8. CONCLUSION

At Masaryk University a small group of enterprise administrators is taking care of the centrally managed core parts of the infrastructure and its functionality, while numerous administrators spread on faculties take care of accordant workstations and provide user support. In other way than this well-balanced combination of centralized infrastructure management and distributed workstation and user support, it would be virtually impossible to successfully manage several hundreds of computers spread into eight geographically separated locations, all of which are in service for employees and students to use.

9. REFERENCES

Microsoft WSUS website (2008). *Windows Server Update Services (WSUS) Home*. Retrieved May 7, 2008, from: http://technet.microsoft.com/en-us/wsus/default.aspx.

Microsoft NLB website (2008). *Network Load Balancing: Frequently Asked Questions*. Retrieved May 10, 2008, from: http://technet2.microsoft.com/windowsserver/en/library/884c727d-6083-4265-ac1d-b5e66b68281a1033.mspx?mfr=true

Microsoft DFS website (2008). *Distributed File System overview*. Retrieved May 10, 2008, from: http://technet2.microsoft.com/windowsserver/en/library/b3754814-f865-4200-9ae9-66785e5e87c81033.mspx?mfr=true

Heppler, M., Rychnovský, L., Šeděnka, J. (2007). *VPN Based Approach to Centralized Management of Notebook Access to Masaryk University Network*. Retrieved May 10, 2008, from: http://www.eunis.org/events/congresses/eunis2007/CD/pdf/papers/p122.pdf