

# Central Network Management in the University Environment alias Ballad on One University Network Administration

Milan Šorm, Petr Dadák, Hana Netrefová\*

\*Institute of Informatics, Faculty of Business and Economics, Mendel University Brno, Czech Republic  
sorm@uikt.mendelu.cz, dadak@uikt.mendelu.cz, hanac@uikt.mendelu.cz

## Abstract

The speedy development of the information and communication technology in the past few years has caused the physical tools of this technology to at least double in quantity. Since the role of the technology is only to support other university staff and not to yield profit which could be used to finance the development of these offices, it is impossible to staff the central offices for information technology administration at the same speed. The necessary measure to be taken was to work out a methodology which would allow for a minimum number of network administrators to operate and administer all the tools.

The paper describes the process of gradual introduction of new technologies into the University Information System, which minimizes the administrators' tasks (account administration, reconfiguration of network set-up and services, security and system watch, upgrade) by transforming them into fully automatic software.

**Keywords:** Central network management, LDAP, remote configuration Cisco switches, university information system.

## 1 Introduction

The speedy development of the information and communication technology in the past few years has caused the physical tools of this technology – desktops, printers, laptops, PDAs, mobile phones, active elements, access points, cabling, servers, etc. – to at least double in quantity. Since the role of the technology is only to support other university staff and not to yield profit which could be used to finance the development of these offices, it is impossible to staff the central offices for information technology administration at the same speed.

## 2 Problem definition

The necessary measure to be taken was to work out a methodology which would allow for a minimum number of network administrators to operate and administer all the tools. Moreover, the aim was to administer the tools remotely since the university buildings are located in geographically varied regions. There were three intuitive theses which formed the foundation of the new central computer network management at our university: 1) unified system of logging in and working

conditions for all users, 2) minimization of change in the network topology without previous notice and 3) construction of standard tools for self-monitoring of all installed technologies.

## 3 Use only one login per user

To effectuate the unified system of logging in and working conditions for all users, we designed a central LDAP system, which distributed the users' accounts in the computer network according to the rules set in the University Information System. We discuss about our LDAP system at EUNIS conference last year.

The screenshot shows a Mozilla Firefox browser window with the title 'Správa účtu - Mozilla'. The address bar shows the URL <https://is.mendelu.cz/auth/ca/ucet.php?design=mzlu>. The main content area is titled 'Správa účtu' and displays user information: Vaše uživatelské jméno (login): sorm, Identifikaciční číslo v UTS: 1, Univerzitní ID (UNIXové systémy): 10000, Domovský adresář na unikových serverech: /home/sorm, Shell na unikových serverech: /bin/bash, Univerzitní GID: 10000 (Zaměstnanci univerzity), Členství ve skupinách: Studenti ekonomické informatiky, Studenti univerzity, Zaměstnanci univerzity. Below this is a note: V následující tabulce jsou zobrazeny servery, na kterých existuje vaš účet. Heslo do informačního systému se přenáší i na něj uvedené servery (pokud není uvedeno jinak). A table titled 'Informace spořečné pro všechny servery:' lists quota settings for various servers:

Server	Povolené hodnoty kB	Maximální hodnoty kb	Doba tolerance	Kvótu změnil Kdy	Kdo	Platnost účtu do	Stav	Zdůvodnění nároku
akela	10 000 000	90 000	20 000 000	100 000	7 dnů	21. 09. 2004	M. Šorm	aktivní ➔
alf	8 000 000	100 000	10 000 000	200 000	7 dnů			aktivní ➔
anete								aktivní ➔
arsik	8 000 000	10 000	10 000 000	15 000	7 dnů			aktivní ➔
dahla	10 000	2 000	35 000	3 000	7 dnů			aktivní ➔
dist-pf								aktivní ➔
dimal								aktivní ➔
faro								aktivní ➔
kejchal								aktivní ➔
koleje								aktivní ➔
profra								aktivní ➔
q01								aktivní ➔
q16								aktivní ➔
nejpal								aktivní ➔
relay								aktivní ➔
sap-hd								aktivní ➔
smudla								aktivní ➔

The LDAP tree contains information about all users of the network (authentication data) as well as authorization of individual users to enter certain systems or servers (authorization data). One by one, standard files and application servers of the university were connected to the LDAP tree, together with information systems, tools for wireless computer networks, VPN and modem switchboard.

The pictures on this and the previous pages show two applications managing the principle of one login per all users – users accounts overview in LDAP tree and the modification of the standard conditions for assigning accounts at individual servers of our university. Both applications are intended for Czech speaking net administrators and have not been translated into English.

Ozn.	Název	DNS Jméno	Správa uživatelů	Implicitní nároky	Kvóty	Počet účtů	Počet zeblok, číslo	Počet deb. účtů	Upravit	Svervy CPS	Změněno	Změnil
akela	akela.mendelu.cz				2482	0	10				21.11.2003	M. Šorm
alf	alf.mendelu.cz				3220	0	33				14.12.2003	M. Šorm
aneta	webankredit.mendelu.cz				8390	0	0				21.11.2003	M. Šorm
arsik	arsik.mendelu.cz				28	0	1				21.09.2004	M. Šorm
astra	astra.mendelu.cz				73	0	0				11.10.2004	P. Dádák
daniela	daniela.mendelu.cz				8692	1	21				21.11.2003	M. Šorm
dist.pef	dist.pef.mendelu.cz				7667	0	35				07.02.2004	M. Šorm
drimal	drimal.mendelu.cz				2333	0	2				06.08.2004	M. Šorm
faro	faro.mendelu.cz				8193	0	4				30.11.2003	M. Šorm
indica	indica.mendelu.cz				2	1	0				13.10.2004	P. Dádák

Standard working conditions for all users have been provided by central file server (or more servers at individual faculties) whose home volumes are connected at the place of the users' registration. Home volumes assist in distributing the user's profile so the working environment and the set-up of all applications is the same for offices as well as for classrooms. It is teachers in particular who profusely profit by this option to prepare and employ the tools of information technology.

## 4 Disallow changing of network topology

The second principle was to guarantee minimum of changes in the network topology without previous notice from the administrators. The problem was eventually solved by progressive transition of the computer network to Cisco switches (they are easy to configure by IOS commands) technology.

The newly developed module of the University Information System registers all components of the computer network and, according to predefined connections of active elements and computers, remotely configures access authorizations at individual Cisco switches. The following picture shows the sample of the basic application of the module.

Ozn.	Název	Pracoviště	Odpojený uživatel	Typ	Autom. konf.	Sledovat	Kancelář	Porty	Prohlížet	Upravit	Změněno	Změnil
Cíperka 2	OKV	P. Dádák	Switch Cisco Catalyst 3750	ne	ano	Q1.36					06.03.2005	A. Vincenc
JAK-Q-3750	OKM	P. Fortelny	Switch Cisco Catalyst 3750	ne	ne	JAK-Q***					15.10.2004	P. Fortelny
JAK-3750	OKV	P. Dádák	Switch Cisco Catalyst 3750	ne	ne	JAK-B***					06.03.2005	A. Vincenc
Kraken	ÚI	P. Serafinová	Switch Cisco Catalyst 3750	ano	ano	Q1.58					03.11.2004	P. Serafinová

Therefore, it is impossible for the end users to change the connection of their workstations and, subsequently, create discrepancies between the documentation in the information system and the reality.

```

Aršík
T- 3441/3442: root@is.mendelu.cz LOG: refresh-budovy-q -- (76)
From root@is.mendelu.cz Sun May 15 10:49:55 2005
From: root@is.mendelu.cz
Subject: LOG: refresh-budovy-q
Date: 15 May 2005 10:49:52 -0000
To: dadak@ulkt.mendelu.cz, fiser@mendelu.cz, kacer@ulkt.mendelu.cz,
seda@mendelu.cz, sorm@ulkt.mendelu.cz, xforteln@ulkt.mendelu.cz

DHCPD generovani:
DHCPD konfigurace je v poradku
Shutting down dhcpcd-q: [ OK ]
Starting dhcpcd-q: [ OK ]
DHCPD konec
DNS generovani:
Seriozne cislo pro tento DNS generovani => 2005051550
Automaticky generovane VLAN: 11, 15, 16, 17, 181, 201, 209, 210, 211, 213, 301, 313, 314, 701, 709, 713, 74, 76, 79, 80, 809
Generuj reverzní zone soubor 219.113.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 254 zaznamu.
Generuj reverzní zone soubor 216.113.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 253 zaznamu.
Generuj reverzní zone soubor 217.113.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 177 zaznamu.
Generuj reverzní zone soubor 218.113.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 39 zaznamu.
Generuj reverzní zone soubor 72.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 85 zaznamu.
Generuj reverzní zone soubor 73.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 74 zaznamu.
Generuj reverzní zone soubor 74.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 133 zaznamu.
Generuj reverzní zone soubor 76.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 143 zaznamu.
Generuj reverzní zone soubor 77.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 60 zaznamu.
Generuj reverzní zone soubor 78.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 37 zaznamu.
Generuj reverzní zone soubor 79.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 197 zaznamu.
Generuj reverzní zone soubor 80.178.195.in-addr.arpa
Nacitam z databaze evidovane IP adresy => 180 zaznamu.
Generuj dopredny zone soubor q.mendelu.cz
Nacitam udaje z databaze => 1749 zaznamu
Reloading DNS configuration[ OK ]
DNS konec
Konfigurovani switchu v budove Q:
Switch A-AB:
Switch A-Ba:
Switch A-Ca:
Switch A-Cb:
Switch A-ICa:
Switch A-Ma:
Switch A-Mb:
q:Konec -:Pfstr <Space>:Distr v:Přílohy d:Smažat r:Odepsat j:Další ?:Nápoře

```

The constructed solution not only helps to keep the register of linked computers organized, but also increases the safety of the computer network (only the registered computers are permitted to link to the network). Nevertheless, for its construction it is necessary to set up a homogenous environment consisting exclusively of Cisco switches supporting Cisco IOS.

The homogeneity facilitates both smooth generation of all files, necessary for administering the network operation (DNS, DHCP, firewall rules, WINS), and executing atomically any changes in the network topology from one spot (from the information system). The system helped to solve the problems with uncovered plugs for teachers' laptops, conferences with foreign participants and helped to design a methodology of transition from unrestricted operation to restrictive conditions imposed by Cisco switches technology.

A thoroughly administered topology helps to locate the problem user quickly, ensures his rapid disconnection or implementing limited net services for computer library (a teacher can permit or forbid his students to access the Internet at his lectures through UIS, etc.).

## 5 Self monitoring tools

The last principle to be mentioned is the preparation of the tools which monitor non-stop and supervise all active elements and servers at the university. Their function is also going to be to notify the supervising systems, e-mails and mobile phones of problems and in case of increasing number of problems to report to the head officers.

```

Arsik
-N - 3442/3442: root@big.is.mendelu. Log server [brucoun] -- ACTIV -- (all)
From root@big.is.mendelu.cz Sun May 15 10:50:14 2005
To: root@big.is.mendelu.cz
Subject: Log server [brucoun] -- ACTIVE SYSTEM ATTACK!
Date: 15 May 2005 10:50:12 -0000
To: uis-roots@ukt.mendelu.cz

-----
Syslog Report on arsik
Security Violations
=====

May 15 12:40:25: arsik spamd: Cannot open bayes databases /root/.spamassassin/bayes_* R/W: lock failed: Přerušené volání systému

-----
syslog Report on taktika
Active System Attack Alerts
=====

q:Konec - :Přestr <Space>:Dlstr v:Přílohy d:Smažat r:Odepsat j:Další ?:Nápově

```

These tools process thousands of data every minute, analyse them and require the help of the administrators only in case of error or non-standard operation. Simultaneously, the tools for automatic upgrade, back-up and synchronization of all servers and active elements were put into operation. As a result, the number of administrators could be reduced to 5 despite the 3,000 connected devices.

At the university we make use of the standard syslog programme with a distant logging at several logging servers. In these servers we have installed the logcheck programme which continuously analyses the incoming messages and on

the basis of a large regulations database evaluates the attack warnings, active risks, and corruptions in system safety and non-standard operations executed in the university computer network. The results are sent by electronic mail both to the administrators of the individual servers, the heads (in the case of problem escalation) and on the mobile phones of the emergency services staff.

## 6 Conclusion

The paper describes the process of gradual introduction of new technologies into the University Information System, which minimizes the administrators' tasks (account administration, reconfiguration of network set-up and services, security and system watch, upgrade) by transforming them into fully automatic software.

This procedure requires only 5 administrators (1 person attending to operation of remote locations, the rest executing the remaining manual tasks) in the central office to ensure a daily running of our university (3,000 connected devices, app. 100 servers and several geographically remote locations).

## Acknowledgements

Since June 2003 the development of the UIS has been supported by the Department of Conceptions and Development at the Institute of Information and Communication Technology at Mendel University in Brno, Czech Republic. Our thanks belong to our great team-mates in the development team. This paper is also supported by the Research program of Czech Ministry of Education, VZ MSM 6215648904/03.

## References

- [1] Šorm, M., Dadák, P., Netrefová H. Central account management carried out by LDAP generating. In *Proceedings of the 9th International Conference of European University Information Systems*. Amsterdam: UvA, 2003. pp. 503–506. ISBN 90-9017079-0.
- [2] Dadák, P. Hardwarové vybavení UIS. In *Univerzitní informační systém I*. Brno: Konvoj, 2003, pp. 12-14. ISBN 80-7302-058-0.
- [3] Dadák, P. Systém jednotné autentizace. In *Univerzitní informační systém I*. Brno: Konvoj, 2003, pp. 9-11. ISBN 80-7302-058-0.
- [4] Šorm, M. et al. University information system documentation and publications.  
[http://is.mendelu.cz/dok\\_server/slozka.pl?id=14210;zobraz=1](http://is.mendelu.cz/dok_server/slozka.pl?id=14210;zobraz=1)