

Integrated Laboratory Network Management System

Takao Shimomura
University of Tokushima
Dept. of Info Sci. & Intel. Syst.
Tokushima
JAPAN

Quan Liang Chen
University of Tokushima
Course of Info Sci. & Intel. Syst.
Tokushima
JAPAN

Nhor Sok Lang
University of Tokushima
Course of Info Sci. & Intel. Syst.
Tokushima
JAPAN

Kenji Ikeda
University of Tokushima
Dept. of Info Sci. & Intel. Syst.
Tokushima
JAPAN

Abstract: This paper presents a Web-based system that automates some processes to connect machines to a network, create accounts, mount remote home directories, set mailing lists, and so on by cooperating with multiple servers, and describes its implementation. By introducing this novel system, a lot of task has been reduced compared with the conventional administrative tasks, and it has become easier for users to create and change their own accounts and connect their machines to the network without login.

Key-Words: Account, Administration, AJAX, Network, Web

1 Introduction

There are some tools that help system administrators administer machines and networks using graphical user interface and Web interface, such as Webmin, Nagios, iDNS-MS, DNS Ontology, Friendly-RoboCopy, and Digital Evidence Bag. Webmin [1] is a Web-based interface for system administration for Unix. Using a Web browser, we can setup user accounts, Apache, DNS, file sharing and so on. It is a convenient tool that can be used to make a variety of settings after an operating system and several servers are installed on a machine. A Webmin server runs with the privilege of the system administrator (root), and directly updates system files. User accounts are created by the system administrator (or a Webmin user). As a result, when the system administrator creates a new account for a user, he needs to set a temporary password for that new account, and then he needs to inform the user of the temporary password in some way. After that, the user also needs to change the temporary password to set his own password. In Webmin, all accounts included in “/etc/password” file are administered, and therefore it cannot classify user accounts according to the groups of a laboratory. While NisWeb system this paper presents is user-oriented, Webmin is administrator-oriented, and does not have

the concept that each user can administer his or her own account. Nagios [2] is a monitoring tool for machines, services and networks. We can examine the status of networks, resources of machines, and performance of services using a Web browser. iDNS-MS [3] is a unifying environment for providing plausible answers to help solve the complex DNS management problems or alleviate these DNS administration loadings. It is developed by using web interface and expert system technology. DNS Ontology [4] is a unifying framework for supporting intelligent DNS management using web interface and expert system technology to help inexperienced administrators in insuring the smooth operation of their DNS systems. RoboCopy [5] is a tool for the extraction and forensic preservation of a subset of data on target computer systems. FriendlyRoboCopy provides an effective, user-friendly interface to RoboCopy. Digital Evidence Bag [6] is a universal container for digital evidence from any source, and used to diagnose system behaviors. It allows the provenance to be recorded and continuity to be maintained throughout the life of the investigation.

This paper presents a Web-based system that automates some processes to connect machines to a network, create accounts, mount remote home directories, set mailing lists, and so on by cooperating with

multiple servers, and describes its implementation. By introducing this novel system, a lot of tasks have been reduced compared with the conventional administration, and it has become easier for users to create their own accounts and connect their machines to the network.

2 Requirements

In laboratories at university, the machines students can use are arranged in student rooms, computer rooms, and laboratory rooms, and those machines are connected with each other through a network. Students use their machines in student rooms to develop software. They use machines in computer rooms to demonstrate software to other students and visitors, and use machines in laboratory rooms to use them in specific environments. It would be better for students to log in any machine in the same way. That is, a student should log in any machine with the same account and password, and use the same home directory although this home directory might exist on another machine (Requirement 1). The file system that is used as a home directory may exist on either a student's machine or a shared machine. In our department, account names are also used as the user names of mail addresses that have the common domain name of the department (is.tokushima-u.ac.jp). That is, the mail address of a student who has account "venus" becomes "venus@is.tokushima-u.ac.jp". Therefore, account names should be unique among not only a laboratory but also the department (Requirement 2). Previously, the system administrator created accounts for new students by using administrative commands. To reduce the loads of the system administrator, a new student should create his or her own account and set their passwords (Requirement 3). To fulfill these requirements, we have developed a Web-based laboratory management system "NisWeb". The NisWeb system cooperates with DHCP, DNS, NIS, NFS, AutoFS, Web, DB and Mail servers to automate the processes that create accounts, set mailing lists, connect machines to the laboratory network, and mount remote home directories.

On sysM machine in the computer room, DHCP, DNS, NIS, NFS servers and the NisWeb system that contains Web server, DB server and a system daemon are running. On sysS machine in the computer room, the slave servers of DHCP, DNS, and NIS, and mail servers such as STMP, POP are running.

3 Implementation

3.1 Flexible home directory mount

We would like to enable a student to log in any machine with the same account and password, and to use the same home directory even if this home directory exists on another machine. For example, suppose that student stdX wants to mount as his home directory the default home directory "/exportb2lab/local/stdX" that sysM machine provides even if he logs in any machine. Student stdY wants to mount the home directory "/home/stdY" of her own machine stdY as her home directory even if she logs in any machine. As shown in Fig. 1, when student stdX logs in a machine, his home directory will be "/b2lab/local/stdX", and the default home directory "/exportb2lab/local/stdX" that sysM machine provides will be mounted at "/b2lab/local/stdX". When student stdY logs in a machine, her home directory will be "/b2labremote/stdY", and the home directory "/home/stdY" of her own machine stdY will be mounted at "/b2labremote/stdY". To realize these functions, the NisWeb system makes use of NIS and AutoFS servers and automates these settings (Requirement 1).

The NisWeb system creates NIS maps for the NIS master server on sysM machine as shown in Fig. 1. It specifies mount points "b2lab" and "b2labremote" in "/etc/auto.master" file. It defines "/etc/auto.home" file so that the default home directory "/exportb2lab/local" that sysM machine provides will be automatically mounted at "b2lab/local". It defines "/etc/auto.remote" file so that the home directory "/home/stdY" of machine stdY will be automatically mounted at "b2labremote/stdY". This line of "stdY -rw stdY:/home/stdY" will be dynamically added to "/etc/auto.remote" file when student stdY creates her own account. In this situation, we cannot use "/home/stdY", which is commonly used as a mount point, instead of "b2labremote/stdY". The reason is because the file system will be recursively referred to if stdY machine joins in the NIS service as a NIS client.

3.2 NisWeb system configuration

Figure 2 shows the NisWeb system configuration. NisWeb server is running on sysM machine. Because NisWeb server is a Web server, it is running with the privilege of an ordinary user. It cannot deal with such processes as creating accounts that require the privilege of the system administrator (root). To execute such processes, we have determined to run a NisWeb daemon. The NisWeb daemon is ar-

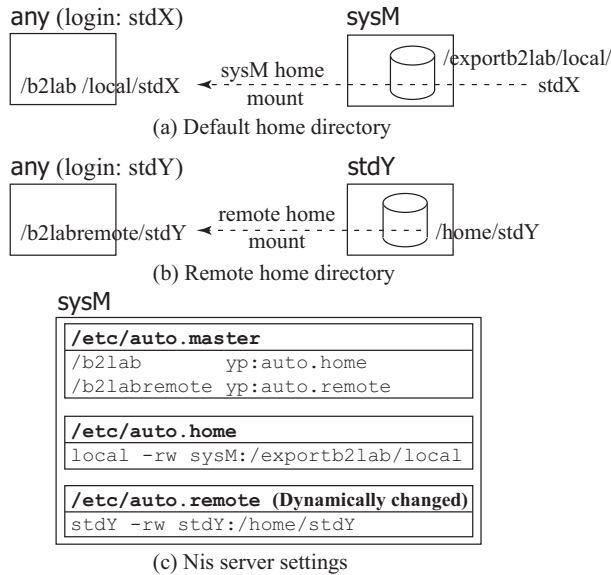


Figure 1: Flexible home directory mount

ranged in “/etc/rc.d/init.d” directory, and is automatically started at the system boot time. NisWeb server asks NisWeb daemon to perform some processes that require the privilege of the system administrator such as creating and deleting accounts.

Students can log in any machine, and access NisWeb server on sysM machine by using Web browsers. When a Web browser sends NisWeb server a request for creating an account, NisWeb server will ask NisWeb daemon to create the account through the socket communication. By executing various kinds of scripts, NisWeb daemon will perform such processes as creating accounts, mounting remote home directories, and setting mailing lists.

The following procedure shows how to create an account for a user.

- (1) Obtain an encrypted password from an entered plain password by using MD5 algorithm.
- (2) By executing “/usr/sbin/useradd” command, add an account name, the encrypted password, and a home directory name to the “/etc/passwd” file (See Fig. 3 (c)).
- (3) By executing addMount script to mount a remote home directory, add a mount point and a remote file system to the “/etc/auto.remote” file.
- (4) By executing makeNis script, update the Nis maps and reload the AutoFS server.
- (5) By executing addLabML script, add the account name to “/etc/postfix/labML” mailing list on sysM machine.
- (6) Add the account to account DB table (See Sec. 3.4).

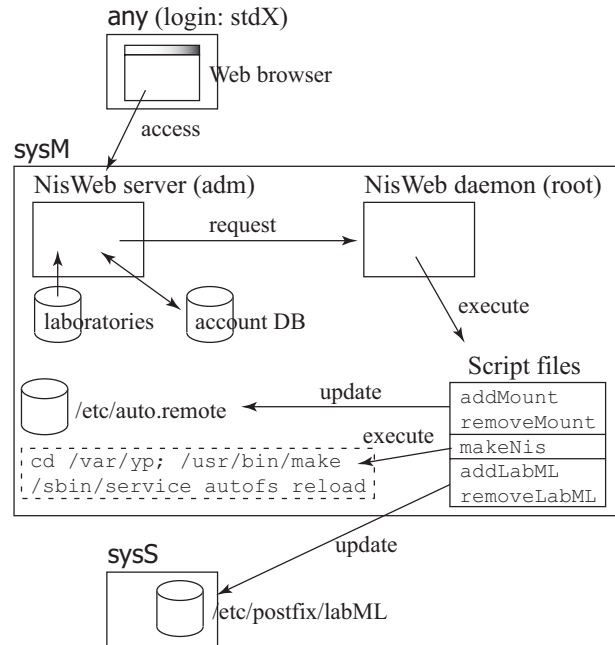


Figure 2: NisWeb system configuration

A mail server Postfix is running on sysS machine. The mailing list of our laboratory is administered at “/etc/postfix/labML” file on sysS machine. When the account of a new student stdX is created, the account name stdX will be added to the “/etc/postfix/labML” file so that a mail that is sent to labML@is.tokushima-u.ac.jp can reach the student stdX.

3.3 Introduction of account administrative type

A laboratory has multiple professors, and each of them instructs multiple students in their research. To easily see which student is studying under which professor, we have determined to show a list of students’ accounts so that they will be classified according to their professors. To do this, we have prepared “laboratories” configuration file as shown in Fig. 3 (a), which defines professors’ names (name) and the titles of the professors’ laboratories (title). The list of students’ accounts will be shown according to the definition of this “laboratories” configuration file. In addition, we have defined the following account administrative types of professors so that professors can correct students’ erroneous accounts and remove the accounts of the students who have graduated or finished their courses.

- (1) “lab” type
Professors can freely change and remove the accounts of the students they instruct.
- (2) “adm” type

name	type	title
simomura	adm	下村研究室 (Shimomura Lab.)
ikeda	lab	池田研究室 (Ikeda Lab.)
.....
guest	guest	ゲスト (Guests)

(a) laboratories configuration file

name	account	host	home
simomura	simomura	simoln	/home/simomura
simomura	azusa	sysM	/b2lab/local/azusa
simomura	quan	sysM	/b2lab/local/quan
ikeda	ikeda	sysM	/b2lab/local/ikeda
.....

(b) account DB table

```

simomura:X:6111:6100:Takao Shimomura:
                        /b2labremote/simomura:/bin/bash
azusa:x:7033:6500:Azusa Imai:
                        /b2lab/local/azusa:/bin/csh
quan:x:6943:6500:Quan Liang Chen:
                        /b2lab/local/quan:/bin/csh
.....
    
```

(c) /etc/passwd file

Figure 3: Configuration files and a database table

Professors can freely change and remove the accounts of all students.

(3) “guest” type

Any professor can change and remove the accounts of the students who study under the professor whose administrative type is “guest”.

The privilege of “adm” administrative type is given to the NisWeb system administrator. When anyone temporarily needs accounts for demonstrations, exhibitions, and experiments, they can make the accounts under the privilege of “guest” administrative type.

3.4 Database table configuration

The “/etc/passwd” system file contains a lot of accounts other than students’ accounts. We would like to show only the accounts of professors and students among them. In addition, the students’ accounts should be classified according to the professors under whom they study. To do this, the information that indicates which student’s account belongs to which professor needs to be recorded. Moreover, the information that indicates whether a student uses either the default home directory that sysM machine provides or the home directory of the machine the student owns as his or her home directory also needs to be recorded.

For these reasons, we have created an account DB table that is shown in Fig. 3 (b) to record these pieces of information permanently. The name field of the table indicates the account names of professors; the account field indicates the account names of the students who belong to the corresponding professors; and the host field indicates the machines on which their home

directories exist. When a student uses the default home directory that sysM machine provides, the home field will record “/b2lab/local/accountName”; and when a student uses the home directory of the machine the student owns, this field will record the student’s home directory on the machine. The NisWeb home page will show only the accounts that are recorded in this account DB table as a list of accounts. In this way, the other accounts included in the “/etc/passwd” system file can be excluded.

4 NisWeb system

4.1 NisWeb home page

Figure 4 (b) shows an example of the NisWeb home page. Its left frame contains some links to a help page and several professors’ laboratories, and below them, a list of registered accounts, a list of registered user IDs, how to connect machines to the network, and a list of host names. Its right frame shows a list of students’ accounts that are classified according to the professors under whom students study. When new students come to the laboratory of this research group, they can create their accounts by clicking on the “Create New Account” button on the right of the corresponding professors’ laboratory titles (Requirement 3). When they want to change or delete their accounts, they have only to click on the “Change” button on the right of their account names. When professors want to change or delete their students’ accounts by the privilege of “lab” administrative type, they have only to click on the “Manager Login” button on the right of their laboratory titles.

4.2 Creating, changing, and deleting accounts

When a new student comes to the laboratory and clicks on the “Create New Account” button on the right of his professor’s laboratory title, a pop-up window will appear as shown in Fig. 5. Only by entering an account name (venus), password (*****), and the student’s name (Venus de Milo), a new account can be created. The other options will be automatically set by default (See Fig. 5 (b) and (c)). A group ID will be automatically set, which is b2staff (6100) for a professor, and student (6500) for a student.

When student stdY wants to use the home directory “/home/stdY” of her own machine stdY as her home directory even if she logs in any machine, she will check the “Remote mount” radio button, and specify “stdY” for the “Machine name” field, and “/home/stdY” for the “Directory” field. In this

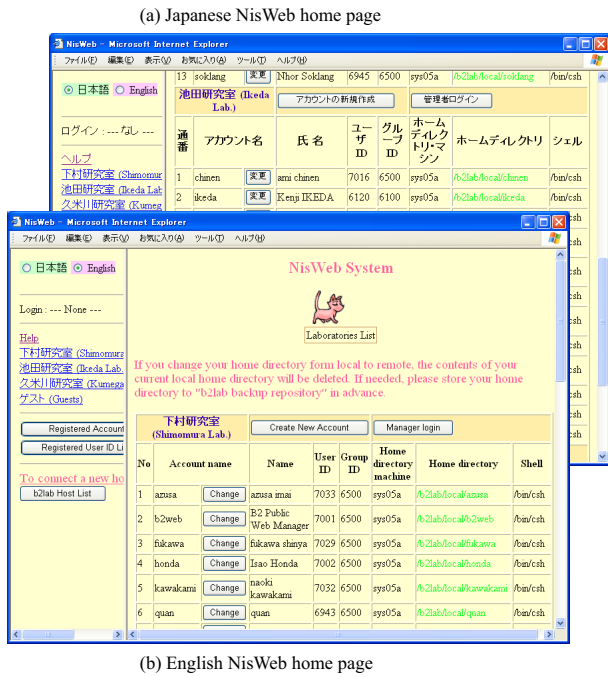


Figure 4: Examples (English and Japanese) of NisWeb home page

case, she will need to add the following line to the “/etc/exports” file on her stdY machine to make her home directory “/home/stdY” public to the laboratory network.

/home/stdY 192.168.0.0/24(rw)

For example, suppose that student stdX wants to mount as his home directory the default home directory “/exportb2lab/local/stdX” that sysM machine provides even if he logs in any machine, and that student stdY wants to mount the home directory “/home/stdY” of her own machine stdY as her home directory even if she logs in any machine. In this case, their accounts will be shown in the NisWeb home page as illustrated in Table 1 (See also Fig. 5 (d)).

When students click on the “Change” button on the right of their account names, and then enter their account names and passwords to log in the system, they can change or delete their accounts. The user authentication is performed by encrypting an entered password with the MD5 algorithm, and comparing the encrypted password with that of the “/etc/passwd” file.

4.3 Unique account name input method

In our department, account names are also used as the user names of mail addresses that have the common domain name of the department (is.tokushima-u.ac.jp). That is, the mail address of a student who

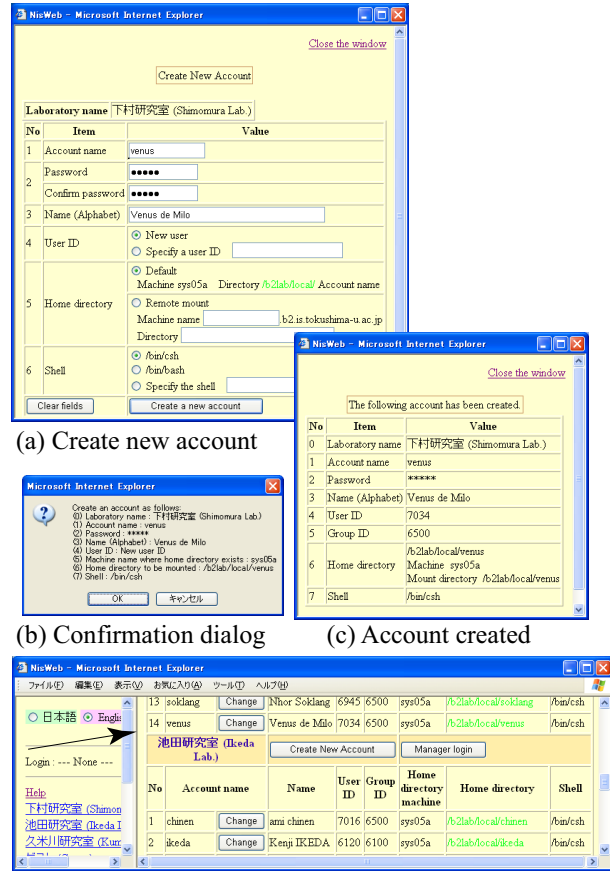


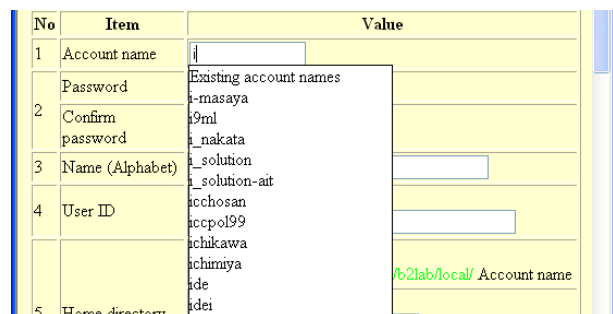
Figure 5: Account creation page

has account “venus” becomes “venus@is.tokushima-u.ac.jp”. Therefore, account names should be unique among not only a laboratory but also the department. All mail addresses of the department are managed in the “aliases” file on IS machine of the department. To facilitate entering a unique account name, we have determined to show a list of account names that already exist in the department by using the AJAX mechanism each time a new account name is being entered (Requirement 2). While a new account name is being entered, the Web browser keeps sending the prefix of the account that has been entered so far to the NisWeb server. Then, the NisWeb server receives all latest account names of the department from IS machine, and returns only the account names that start with the prefix to the Web browser.

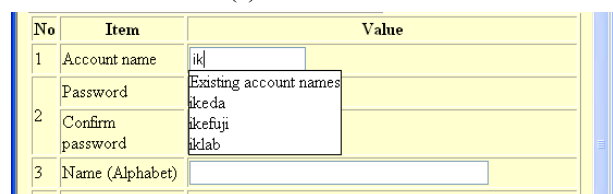
Let’s try to enter an account name “ikeda” in the account creation page in Fig. 5. Figure 6 (a) shows an example of the account creation page when “i” is first entered. Figure 6 (b) shows an example of the account creation page when “ik” has been entered.

Table 1: A part of account list

Account name	Name	User ID	Group ID	Home directory machine	Home directory	Shell
stdX	"Change"	Student X	7001	6500	sysM	/b2lab/local/stdX
stdY	"Change"	Student Y	7002	6500	stdY	/b2labremote/stdY (/home/stdY)



(a) "i" is entered



(b) "ik" is entered

Figure 6: Examples of facilitating entering a unique account name

5 Evaluation

It has been easier to administer the accounts in the laboratory because we can easily see who are studying in the laboratory and which student account belongs to which professor. Professors can easily remove the accounts of the students who have left their laboratories. There will be no garbage left in the laboratory network because not only their accounts but also their home directories, their mailing-list entries, and their mail spools will be automatically deleted. Every year, several foreign students come to the laboratory, and they also use this system without circumstance.

6 Conclusion

We have developed a Web-based NisWeb system that cooperates with several servers to facilitate installing and connecting machines, and automate creating students' accounts. This paper has presented an administrative method that makes a Web-based NisWeb server communicate a system daemon. Because the NisWeb

server is running with the privilege of an ordinary user, it asks a NisWeb daemon to perform the processes that require the privilege of the system administrator (root). Java serialization mechanism is used in this communication. If its port number and the contents of the serialized objects are revealed, illegal accesses could be possible. Especially, if the NisWeb server and the NisWeb daemon are running on different machines, it might cause a serious problem for security. This problem should be solved by encrypted secure communication.

References:

- [1] Jamie Cameron. *Webmin*. <http://www.webmin.com/>, 4 2007.
- [2] Ethan Galstad. *Nagios*. <http://www.nagios.org/>, 4 2007.
- [3] Chien-Liang Liu, Shian-Shyong Tseng, and Chang-Sheng Chen. Design and implementation of an intelligent dns management system. *Expert Systems with Applications*, Vol. 27, No. 2, pp. 223–236, 8 2004.
- [4] Chang-Sheng Chen, Shian-Shyong Tseng, and Chien-Liang Liu. A unifying framework for intelligent dns management. *International Journal of Human-Computer Studies*, Vol. 58, No. 4, pp. 415–445, 4 2003.
- [5] Claire LaVelle and Almudena Konrad. Friend-lyrobocopy: A gui to robocopy for computer forensic investigators. *Digital Investigation*, Vol. 4, No. 1, pp. 16–23, 3 2007.
- [6] Philip Turner. Applying a forensic approach to incident response, network investigation and system administration using digital evidence bags. *Digital Investigation*, Vol. 4, No. 1, pp. 30–35, 3 2007.