IRAM-COMP-011

Revision: 0
2004-11-02

Contact Author

Institut de RadioAstronomie Millimétrique

Proposition to deploy a Windows Directory Service

Owner Sebastien Blanchet

Keywords: Windows Directory Service, Windows Server, Active Directory

Approved by:	Date:	Signature:
	Nov 2004	

Change Record

REVISION	DATE	AUTHOR	SECTION/PAGE AFFECTED	REMARKS

Content

1 Current IRAM status and expectation

On Nov 16th 2004, there were 133 computer running Windows, (any versions). All these computers are totally autonomous. On one hand, they don't depend on a server, but on the other hand they require many manual intervention because no automatically procedure are available.

1.1 Drawbacks of the actual situation

- The client computers have static configurations
- The client computers have different software versions, according to their installation date.
- The software upgrades / updates are very long to deploy

For example, if I want to execute a script on every computer, a computer group member must login on every system to run it.

1.2 Expected benefits of a new infrastructure

- Provide a centralized framework software installation
- Centralize account management
- Increased security by forcing user to use best practices, like strong password
- Be 100%-compatible with the current network services, hosted on Linux computers
- Save time and efforts for users and computer group.

The main drawback is that we become slightly more dependent from Microsoft.

2 Active Directory

2.1 Overview

Active Directory is a **distributed directory service** that is included with Windows Server 2003. Active Directory enables centralized, secure management of an entire network, which might span a building, a city, or multiple locations throughout the world.

2.2 General Prerequisites

Active Directory works only on the Windows Server Family. We have chosen to install Windows Server 2003 Standard Edition, the lastest and more secure operating system of this family.

Install the operating system from the CDROM, then install the drivers, Norton anti-virus, etc.

2.3 Active Directory installation

Active Directory needs **absolutely** the Microsoft DNS server to work. In particular, it needs several *Forwarder Lookup Zones* in the Microsoft DNS configured with the "*Active Directory Integrated*" attribute. It is safer to let Active Directory Wizard configure the DNS Server. But if you have already installed the DNS Server before installing Active Directory, the wizard will fail and only a subset of Active Directory functionality will work normally.

Installation procedure
Execute in a command window: *dcpromo.exe* (domain controller promotion),

Domain Controller Type
(x) Domain Controller for a new domain

Create New Domain
(x) Domain in a new forest

New Domain Name
Full DNS name for new domain: iram.wintest

NetBIOS Domain Name
NetBIOS domain name: IRAMWIN

Database and Log Folders
Database folder: C:\WINDOWS\NTDS
Log folder: C:\WINDOWS\NTDS

Shared System Volume
Folder location: C:\WINDOWS\SYSVOL

DNS Registration Diagnostics
(x) Install and configure the DNS server on this computer

Permissions
(x) Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems

Directory Services Restore Mode Administrative Password
Set the same password as the system administrator

Note:
- the DNS and Netbios domain name should be restricted to the Intranet. Therefore, choose a DNS suffix which doesn't exist on Internet, is a good idea and a good pratice.
- The *Directory Services Restore Mode Administrative Password* is mandatory to restore Active Directory from a backup after a major crash. Don't loose it.

Wait few minutes, while the wizard install Active Directory and the DNS server. At the end of the installation, you have to restart the computer.

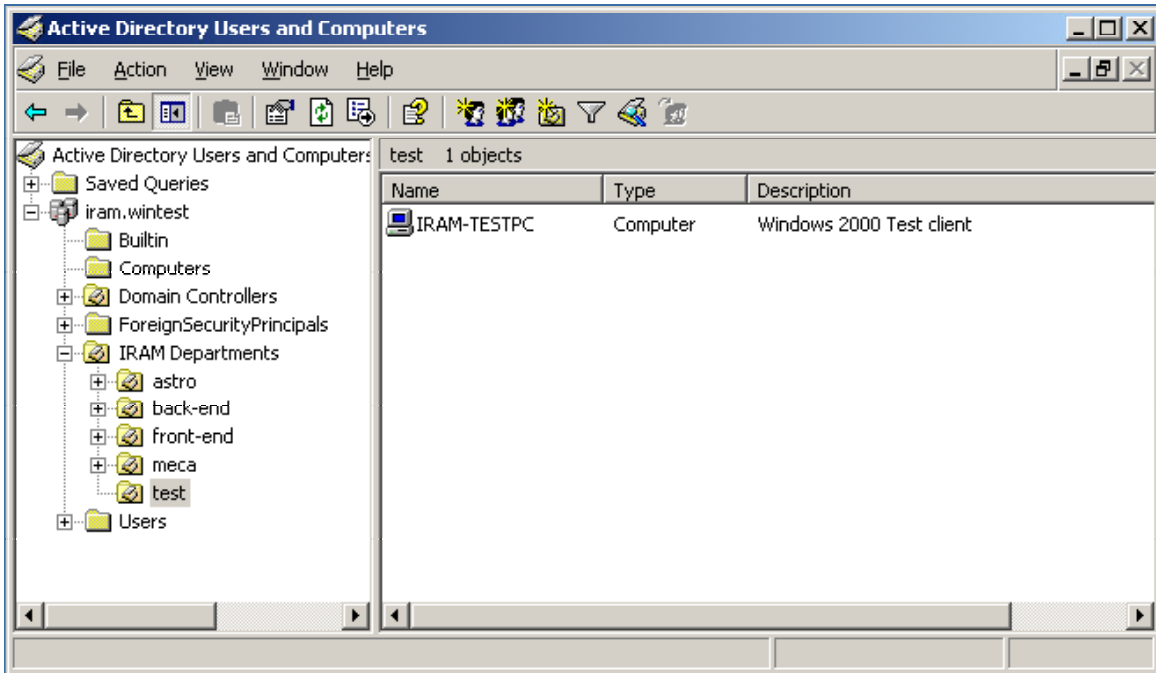
Installation of an additional tool
Install Microsoft Group Policy Management Console (download from Microsoft the gpmc.msi file)
This tool simplifies policy management; therefore it is worth installing it.

Configuration
Start > Administrative Tools > Active Directory Users and Computers

The default categories are:
- *Built-in*: it holds the built-in users needed by the server's services
- *Compute:* it holds the new computers that have just joined the domain
- *Domain Controllers*: this Organization Unit holds the Domain Controllers
- *ForeignSecurityPrincipals*: empty by default
- *Users*: it holds others built-in users needed by the server.

Create Organizational Units, and users. In the following example, we have created an Organizational Unit *Department* to group together all the IRAM departments (admi, astro, backend, etc.) We have also create a test account user, in the *test* Organizational Unit.

To create an organisation unit use *Action* | *New* | *Organizational Unit*.



2.4 Client computer configuration

Now a Windows 2000 Pro PC client will be configured to join the domain. The client IP address can be in any networks. The only requirement is that it must be able to resolve any domain names. The safer way to ensure that, it is configure the client computer to use iram.wintest DNS as first as first DNS. In this case you have to specify the Microsoft DNS IP address in the client IP configuration.

Note: Windows XP Home Edition can not join a domain.

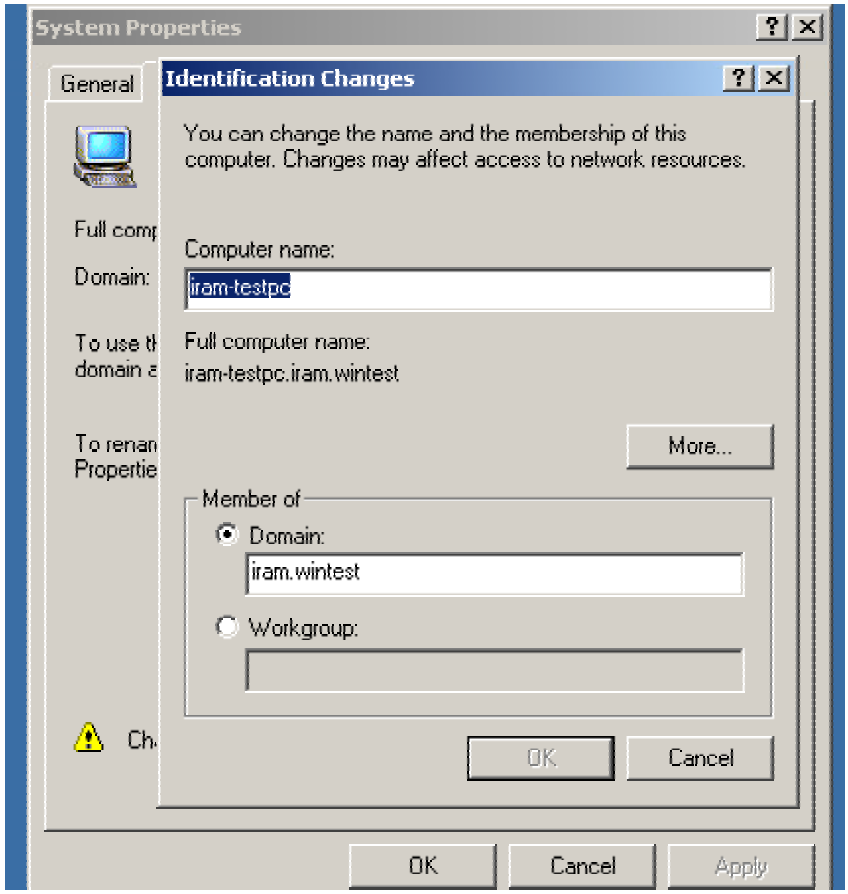
Control Panel > Network and Dial-Up connections
Right-click on Local Area Connection > Properties

Internet Protocol (TCP/IP) > Properties

TCP/IP configuration:
(x) Obtain an IP address automatically

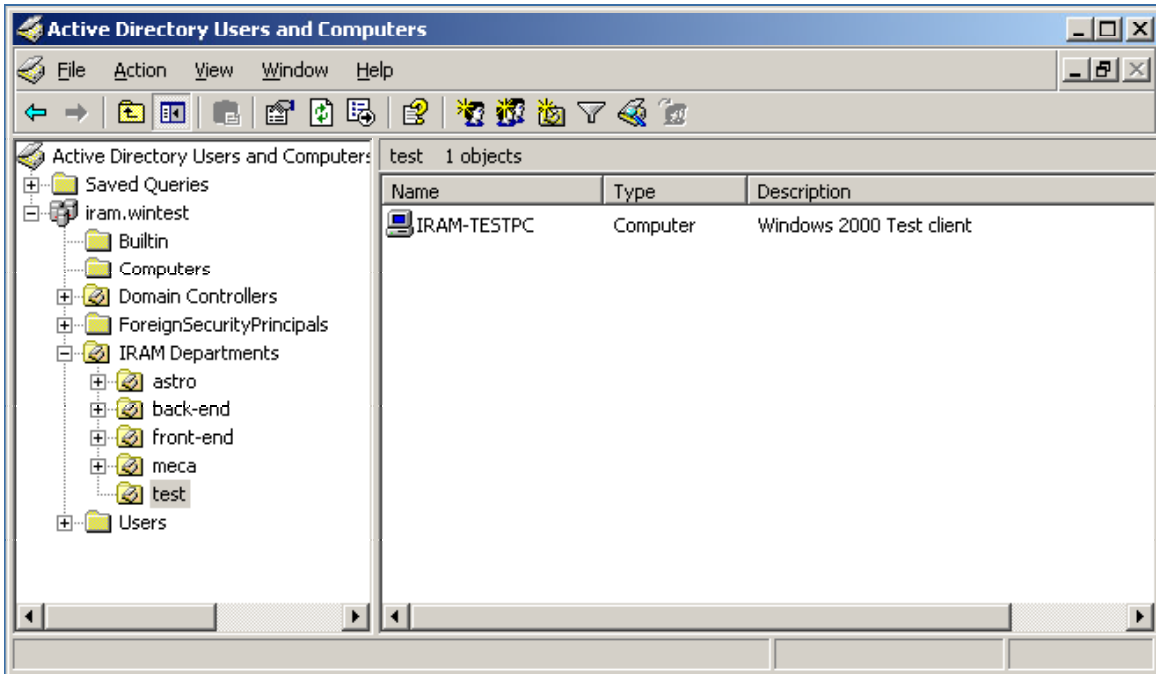
use the following DNS server addresses:
1st DNS: 192.168.192.2 (Windows Server's IP address)
2nd DNS: 193.48.252.22 (IRAM standard DNS)

Join the domain
Control Panel > System > Network Identification > Properties



For the domain name you can use either the netbios name (IRAMWIN) or the DNS name (iram.wintest). Use the DNS name is the best practice: if it fails it means that the DNS configuration on the client computer is invalid.

The new computers appear in Active Directory in iram.wintest/Computers, so they must be moved to the appropriate Organizational Unit. In the following example we have moved our Windows XP test PC to iram.wintest /IRAM Departments/test.



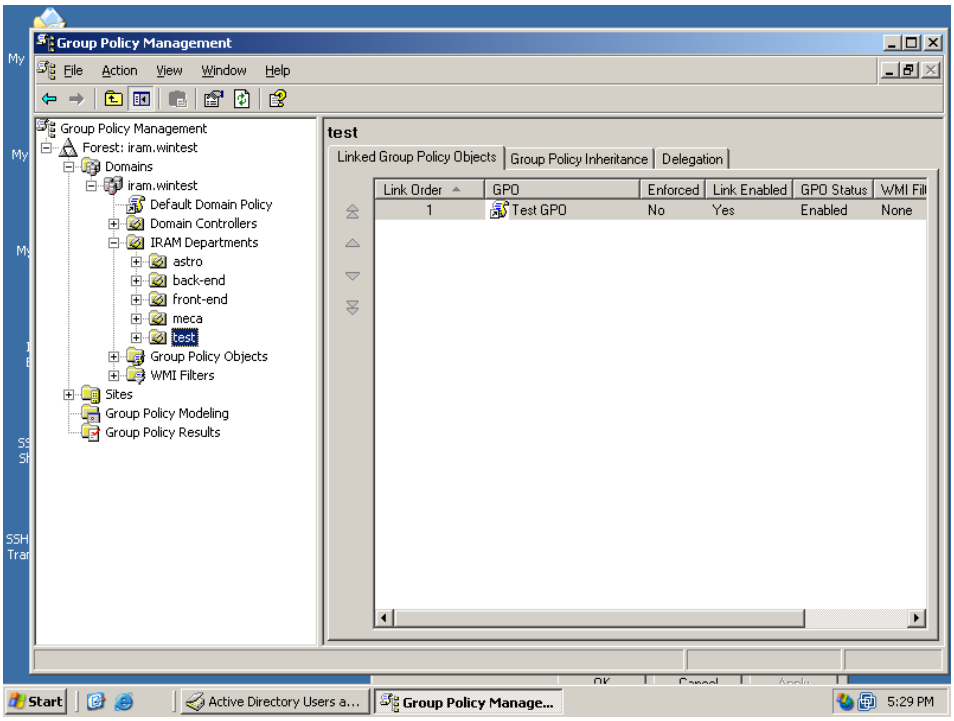
After the client reboot, you should also see a new entry for the client hostname in the DNS. If not, it means that the client DNS configuration is invalid. This problem should be fixed immediately, otherwise the client computer can not be managed rightly with Active Directory.

2.5 Group policy

Now we will define a group policy to define the settings for the Organizational Unit members.

Start > Administrative Tools > Group Policy Management

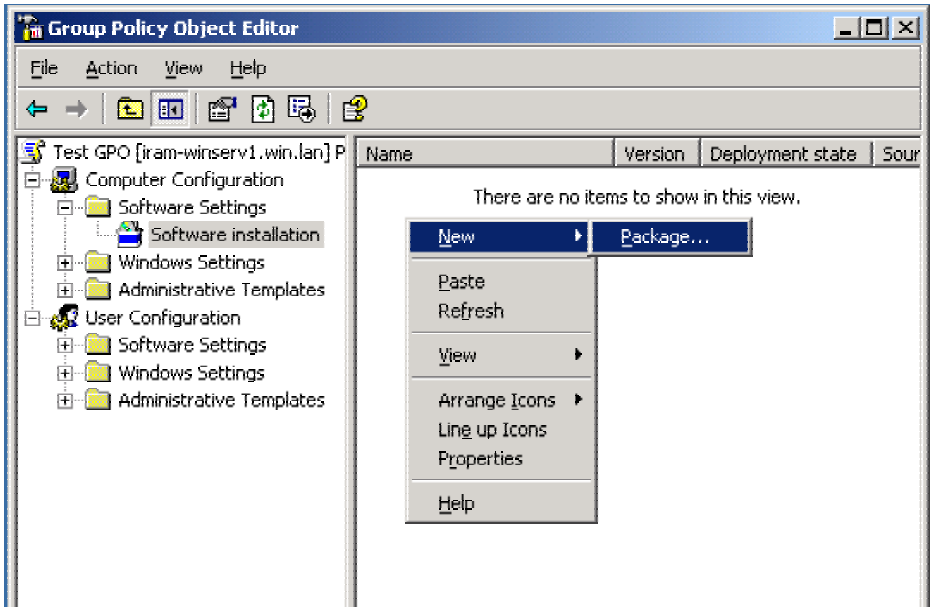
Select Forest: iram.wintest → Domains → iram.wintest → IRAM Departments → test
Menu Action | Create and Link a GPO Here
GPO Name: Test GPO



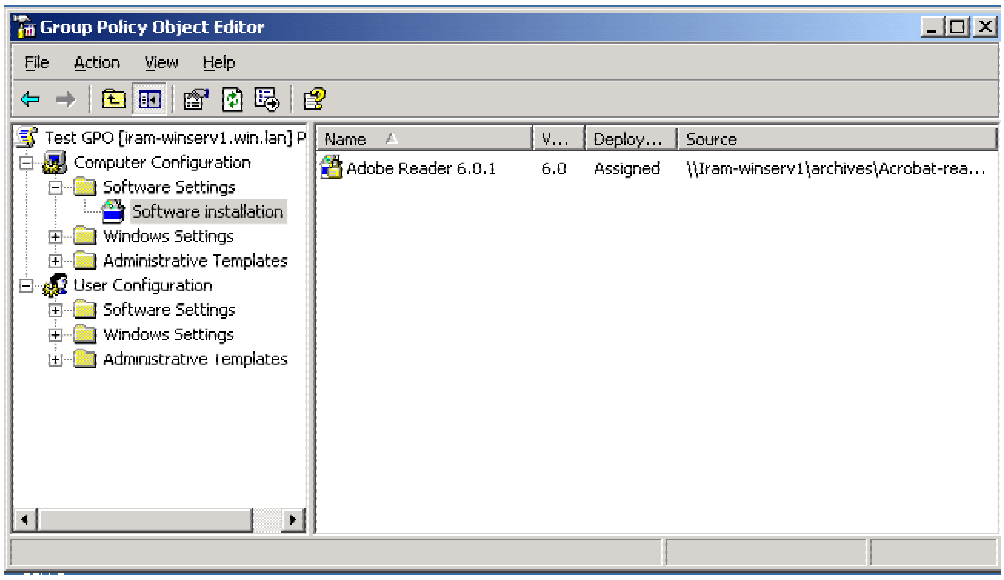
Example of policy
Right-click on Test GPO and select “Edit”

All settings made on this GPO will be applied to computers and users managed with this policy.

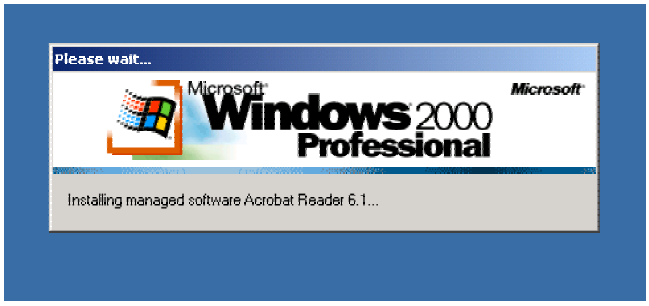
1st Example: Install Acrobat Reader 6.1 to all computers



Select “acrobat_reader_6.1.msi”
Note 1: To know how to generate a .msi package, see the appropriate chapter of this document.
Note 2: the .msi package must be located in a shared folder.

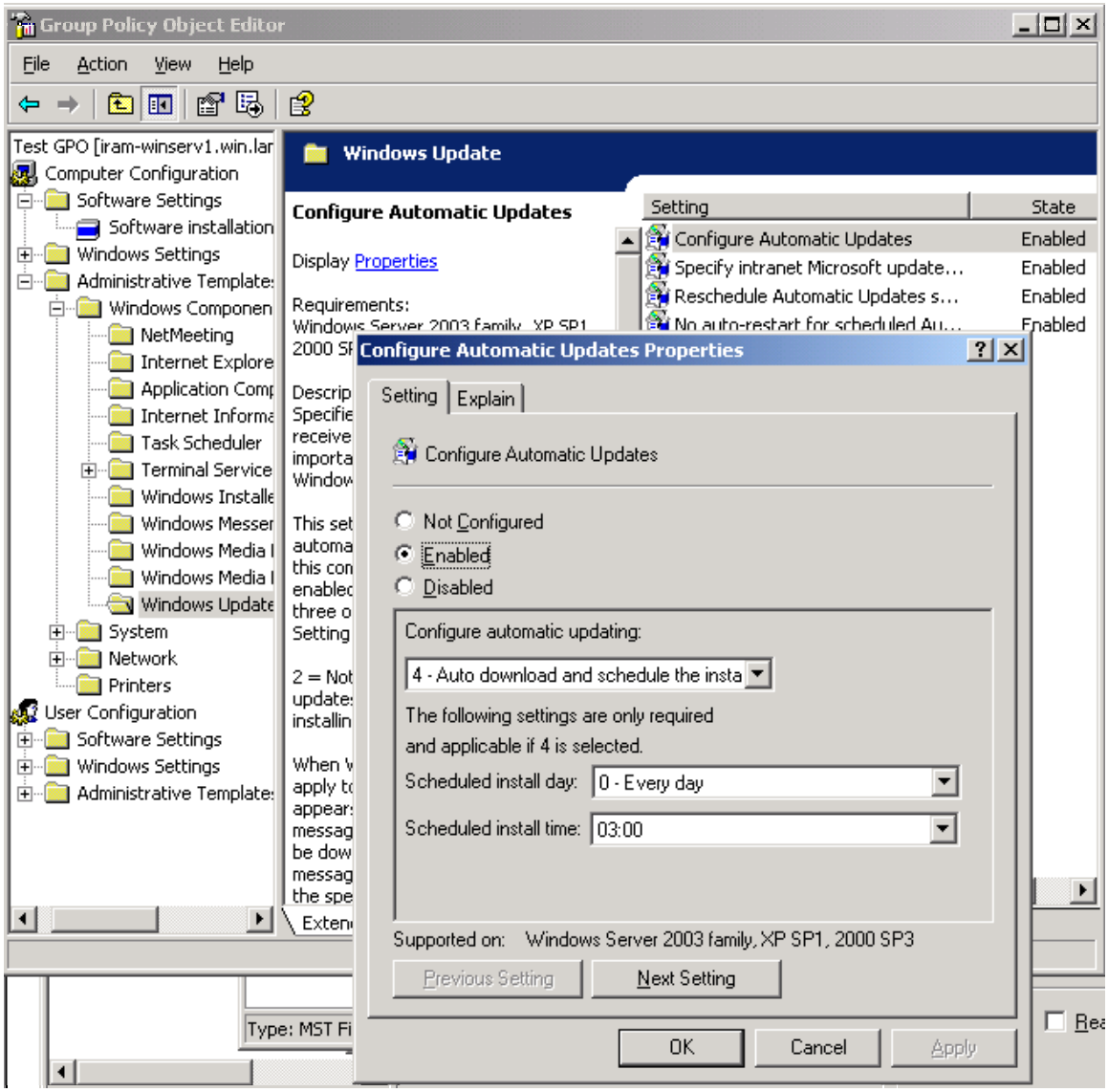


The software will be automatically installed on the client computer on the next reboot.



2nd Example: Activate software update service from windowsupdate.iram.fr

Test GPO→Computer Configuration→Administrative Templates→Windows Update, then setup the wanted parameters.



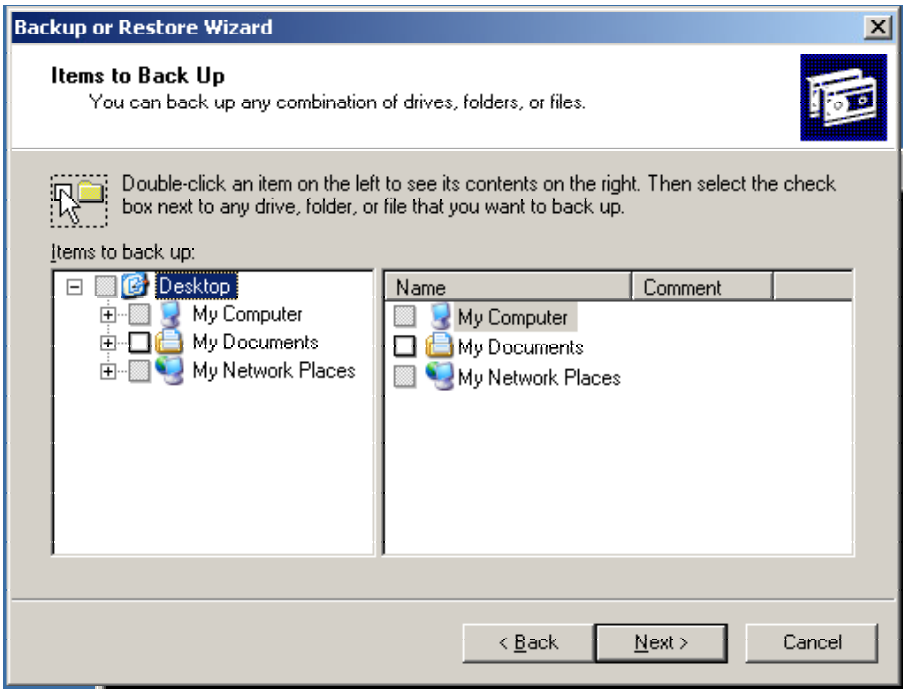
Many others interesting features can be controlled by the Global Policy.

3 Failure management

If the server is down, the user can still login, thank to the authentication cache. They will use the IRAM standard DNS to continue surfing on Internet and receiving their emails.

3.1 Backup and recovery

To backup the server, use “ntbackup” which is provided with Windows 2003 server. It is an easy tool, with a wizard to help you.
Store the backup on another hard disk or on a file server.
To restore a backup, use “ntbackup” again. Don’t forget to reboot.



3.2 Redundancy

A Windows Domain Control can work with secondary server to provide load-balancing and redundancy.

To create a secondary controller, execute dcpromo.exe on a windows 2003 server belonging to the domain

Domain Controller Type
(x) Additional domain controller for an existing domain

Network Credentials
User name: administrator
Password: ••••••••••
Domain: iram.wintest

Additional Domain Controller
Domain name: iram.wintest

Database and Log Folders
Database folder: C:\WINDOWS\NTDS
Log folder: C:\WINDOWS\NTDS

Shared System Volume
Folder location: C:\WINDOWS\SYSVOL

Directory Services Restore Mode Administrative Password
Set the same password as the system administrator

Restart at the end of the process

The server replication is automatically enabled (every 180 minutes). It can be modified with *Administrative Tools | Active Directory Site and Service*

4 Software deployment

To deploy a software on a set of computer clients with Active Directory, the application must be packaged in a .msi file.

Ideal case: a recent application which follow all Microsoft recommendations
In this case the application provides an .msi package (customisable or not) to install silently the application. Today, only Microsoft takes care to provide its software in this convenient format.

1st Example: Deploy Acrobat Reader 6.0.1
1- On a workstation, download the full version of Acrobat Reader from www.adobe.com.
2- Run the executable;
3- When the first setup screen appears, go to c:\windows\cache to get the installation files ; copy them in a shared folder on the server
4- Publish the .msi file in the Active Directory
5- Test if it works. In case of problem, it is possible to modify the companion files

2nd example: deploy Microsoft Office 2000
- create an administrative package, i.e. a .msi specially designed for network deployment with *setup.exe /a*
- create a modification file (.MST) with the Office Resource Kit (download it from www.microsoft.com) to record the installation parameter
- import the .msi and the .mst in to the group policy

If two groups need different installation parameter, you have just to create 2 .MST files.

Worst case
Unfortunately many applications don't provide yet .msi files to install them. In this case you have to use WinInstall LE 2003 (download it from http://www.ondemandsoftware.com, it is a freeware) to create a new msi package. You can also use WinInstall LE 2000 which is located on the Windows 2000 Server cdrom.
In few words: this tool works by comparing a snapshot before the installation and after it, to generate an incremental package. See the manual of this software for more details.
Note: these kind of msi package are expected to work with only the operation system version on which they have been built. Therefore it would be a good idea if we have a GPO for Windows 2000 and another for Windows XP, because the .msi made with WinInstall LE are OS dependent.

5 Printers

A print server is required to provide a unified printer configuration to all users.
The printer must be installed on the server, and then, it must be shared.

When a user try to print on this shared printer, the driver is automatically installed. The connection can be automatically pre-defined with a logon script. See the section about scripting for more details.

6 Server administration

The server can obviously be remotely managed with Terminal Service (RDP protocol).

7 Integration with Unix

Service for Unix (SFU) is a Microsoft software to easily integrated Windows into existing Unix environment.
With SFU you can:

- Use NFS to share files between Windows and Unix computers
- Manage user account on Windows and Unix system with NIS
- Synchronize password to provide a "single sign-on" capability to Windows and Unix users
- Run Unix shell scripts on Windows-based computer in a full-featured Unix environment

In your case, we are interested only the password synchronization with Linux.

SFU Installation
Download SFU 3.5 from www.microsoft.com and uncompress the archive in C:\SFUdecomp, on the windows server, and run "setup.exe".

Install SFU in C:\SFU
After the installation, run the program and read the help included.

Windows configuration
Administrative Tools > Service For Unix Administration

Microsoft Windows Services for Unix > Password Synchronization:
On the default page:

- Check both cases for a bi-directional synchronization.
- Click on "New Key" to generated a new encryption key.
- Click "Apply"

On the advanced page:

- Add to the list the Unix computers you want to synchronize

Linux configuration
Copy the content of C:\SFUdecomp\unix\bins on the Linux machine in ~root/sso and login as root

```
# cd ~/sso
# cp ssod.rhl /usr/bin/ssod
# cp sso.cfg /etc/sso.conf
# cp pam_sso.rhl /lib/security/pam_sso.so.1
# cp /etc/pam.d/system-auth /etc/pam.d/ssod
```

edit /etc/sso.conf

- enter the value for ENCRYPT_KEY=, as display on the windows server
- enter the name of you domain controller in SYNC_HOSTS=

Example:

```
ENCRYPT_KEY=12345!qf
SYNC_HOSTS=(iram-winserv1.win.lan)
```

Note: don't forget the parenthesis around the hostnames.

edit /etc/pam.d/system-auth

- Locate the line "`password required /lib/security/pam_cracklib.so retry=3`"
- Add after this line "`password required /lib/security/pam_sso.so.1`"
- Comment (add a #) the line "`password required /lib/security/pam_deny.so`"

Run ssod, check that it is running with "ps –edf" and test password synchronization.
Add "/usr/bin/ssod" at the end of /etc/rc.local to start automatically the sso daemon.

Note:

- The Linux binary was designed for RedHat 8.0, but they work on RedHat 9.0. Otherwise you can rebuild them, because the source code is provided by Microsoft, in C:\SFUdecomp\unix\srcs.
- The accounts must have be created before with the same name on both systems.

8 Scripting

It is possible to execute automatically administrative task by writing scripts. The standard scripting technology in Windows is "Windows Script Host". These scripts are written in Jscript (.js) or Vbscript (.vbs). They can be run locally, remotely, at the PC startup (via the GPO), etc.

http://tiger.la.asu.edu/WSH/wsh_tutorial.htm

For example, a logon script to connect the shared printer:

```
// script to install the printer

var WshNetwork = WScript.CreateObject("WScript.Network");
var PrinterPath =" \\\\iram-winserv1\\laser7-ps";
WshNetwork.AddWindowsPrinterConnection(PrinterPath);
```

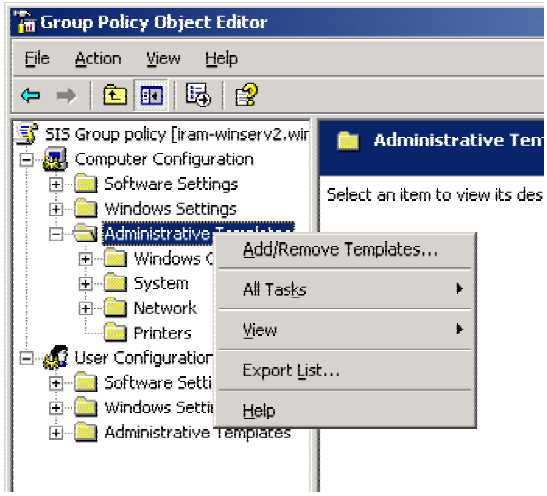
On the server, there are many way to manage Active Directory by scripting.

For example, you can use the following command line in a batch (.bat) to edit Active Directory

- dsadd
- dsmod
- dsquery
- dsget
- dsmove
- dsrm

9 Global Registry Modification

To modify a value in the registry of every computer, the domain administrator had rather use a GPO than a script. Many parameters are pre-defined in the standard GPO. It is possible to defined new parameters by writing and adding an ADM file (a little text file which defined registry key).



Tips: On the client computer, you can use *rsop.msc* (Resultant Set of Policy) to check the GPO result.

10 VMware

Quote from VMware website:

> *VMware Workstation is powerful virtual machine software for developers and system administrators who want to revolutionize software development, testing and deployment in their enterprise.*

It is true: VMware is very useful to accelerate application deployment. With this tool, we can have as many as wanted virtual computers with specific configurations, we can rollback to a previous snapshot, clone a fresh installation to begin with a blank configuration, etc.

I think that it is a must-have software, because at least 4 machines are needed.

- a Windows 2000 test machine
- a blank Windows 2000 machine to build .msi file
- a Windows XP test machine
- a blank Windows XP machine to build .msi file

The main VMware drawback is that it needs a lot of computer resources:

- 1 GB of RAM is not luxury to run simultaneously 2 virtual machines.
- a big dedicated hard disk (40 GB) is precious to store all the virtual disk of these virtual computer.
- a 2Ghz or more processor is welcome to run application smoothly.

11 Costs

Hardware

Computer	Description	Price
A strong computer to run Windows 2003 Server master	2Ghz/ 768 Mo/ 2x 40 GB (a disk will be dedicated disk for the software repository)	
A strong computer to run Windows 2003 Server slave ??	idem	
A strong computer to run VMware	2Ghz/ 1GB/ 80 GB hard disk	

Options ??
Raid1 SATA hard disk ?

Software

Sofware	Number of license	Price
VMware Workstation 4.5.2 for Linux	1 (or more)	??? euros / license
Windows 2003 Server	150 client license ?	???

And, obviously, a small period of time to become with this new computer and network environment.

12 Migration planning

13 Bibliography

http://www.microsoft.com

http://www.laboratoire-microsoft.org

http://www.forum-microsoft.org/

“Microsoft Windows 2000 Server au Quotidien Expert” by Russel & Crawford (IRAM library)