Взято: http://www.deltann.ru/10/d-052008/p-111

Игорь Полянский

В данной статье речь пойдет о том, как управлять единой учетной записью пользователя посредством MS Active Directory вне зависимости от того, на какой платформе он работает, будь то Windows или UNIX-подобные системы. Забегая вперед, скажу, что если с Windows-клиентами все ясно, то интеграция с каталогом от Microsoft тем способом, который будет здесь описан, подходит не для всех UNIX-подобных операционных систем. Так уж сложилось – все они разные, да и Active Directory вовсе не идеальная среда для интеграции разнородных систем. Тогда зачем я все это пишу? А за тем, что очень многие организации изначально ориентированы на платформу Windows и в качестве каталога применяют Active Directory, а когда в сети начинает появляться UNIX, то встает вопрос об интеграции, и не всегда хорошие коммерческие решения подходят, либо из-за стоимости, либо в силу других причин. Я изначально рассматривал вариант с ведением второго каталога для UNIX-клиентов на базе OpenLdap, но хотелось все-таки управлять учетными записями из единой точки, а именно из Active Directory, потому что этот каталог широко используется у нас в сети.

Вариант Samba + winbind меня не устраивал, поскольку по роду задач samba вообще не нужна, к тому же это лишние службы на каждой машине, использование которых все-таки не решает проблем с централизованным управлением пользовательскими данными, поэтому это решение мне показалось неразумным и неизящным.

Более всего привлекал вариант с использованием сервера NIS, который входит в продукт, известный как Services For Unix от компании Microsoft и синхронизация записей Active Directory to NIS. Зайдя на microsoft.com в надежде скачать SFU3.5, которая в отличие от предыдущей версии SFU3.0 бесплатна, я набрел на ряд интересных статей, прочитав которые, пошел по другому пути.

Как уже говорилось в начале, не все UNIX-подобные системы могут проходить аутентификацию и запрашивать данные о пользователе в Active Directory описанным здесь способом, а только те, которые умеют работать с PAM и pam-модулями. Как вы, наверное, догадались, я буду описывать способ взаимодействия с ldap-сервером,

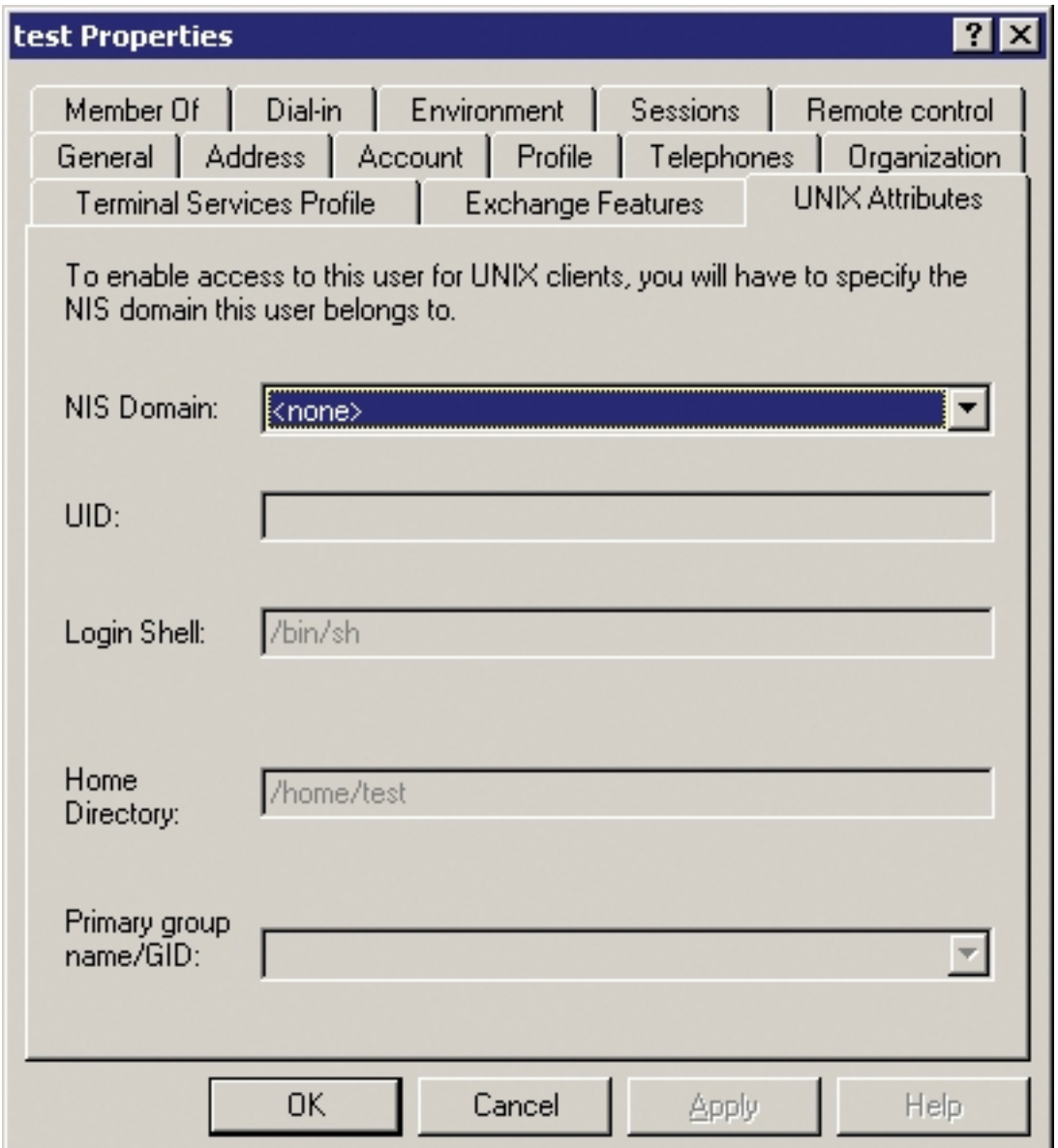
входящим в Active Directory через модули pam_ldap и nss_ldap.

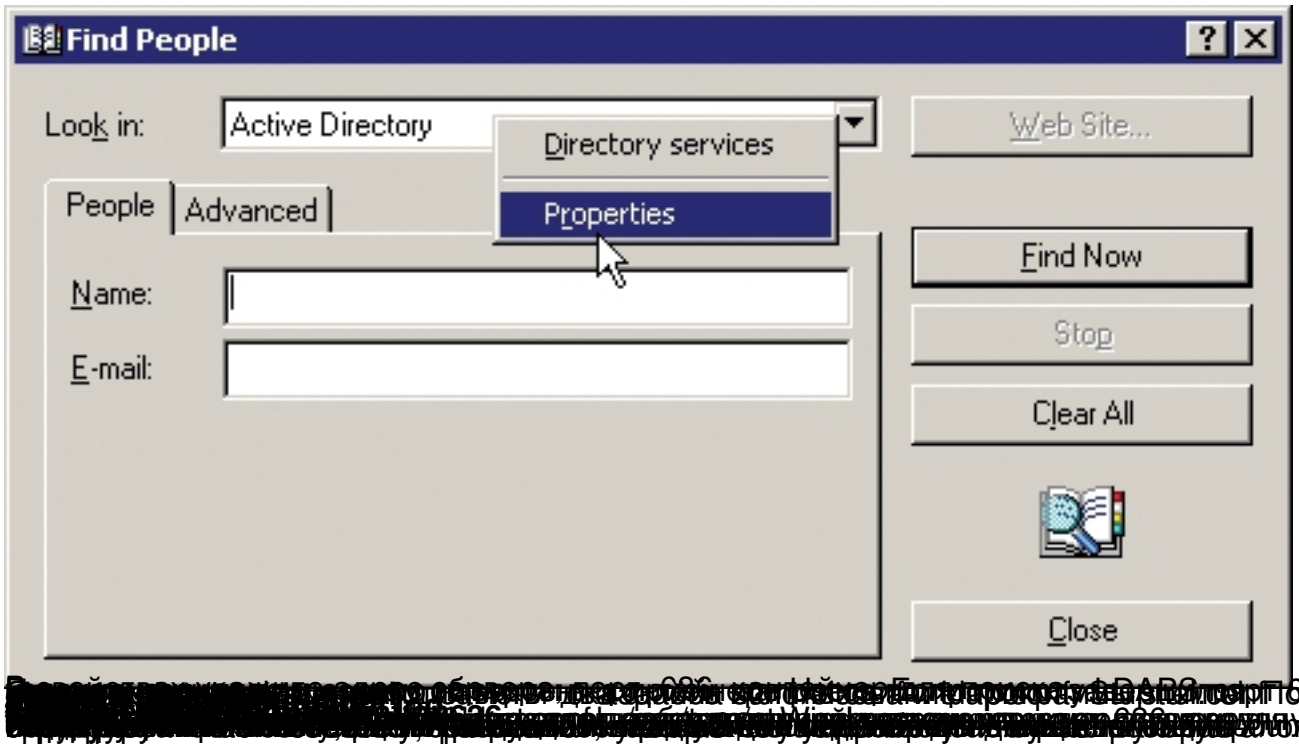
Итак, начнем. В качестве подопытных будут выступать MS Windows 2000 Server Standart с установленной Active Directory (в дальнейшем AD), Linux Manrdake 10.0, Solaris 9 x86, FreeBSD 4.10. Над Windows 2000/XP опыты ставить бессмысленно – все и так работает. Как минимум понадобится DNS-сервер, который может быть установлен на том же Windows 2000 Server. Свежеустановленная AD не имеет традиционной ldap-схемы для UNIX: userid, grouid, login shell, home directory. Нам нужно её расширить, и для этого я воспользуюсь SFU3.5. Вообще-то существует несколько способов это сделать: вручную создав ldif-файл с нужной схемой и импортировав его при помощи каких-либо программ сторонних разработчиков, например такой, как AD4Unix (www.padl.com/download/MKSADPlugins.msi), или с помощью SFU от Microsoft. Первый способ я оставляю гуру, вышеозначенную программу MKSADPlugins.msi вам установить вряд ли удастся, если Windows 2000 Server работает с альтернативной локалью, отличной от US, что для России уместно. В пользу же SFU, на мой взгляд, говорит то, что она сделана в том же КБ, где Windows и AD, плюс в своем составе имеет много утилит от UNIX.

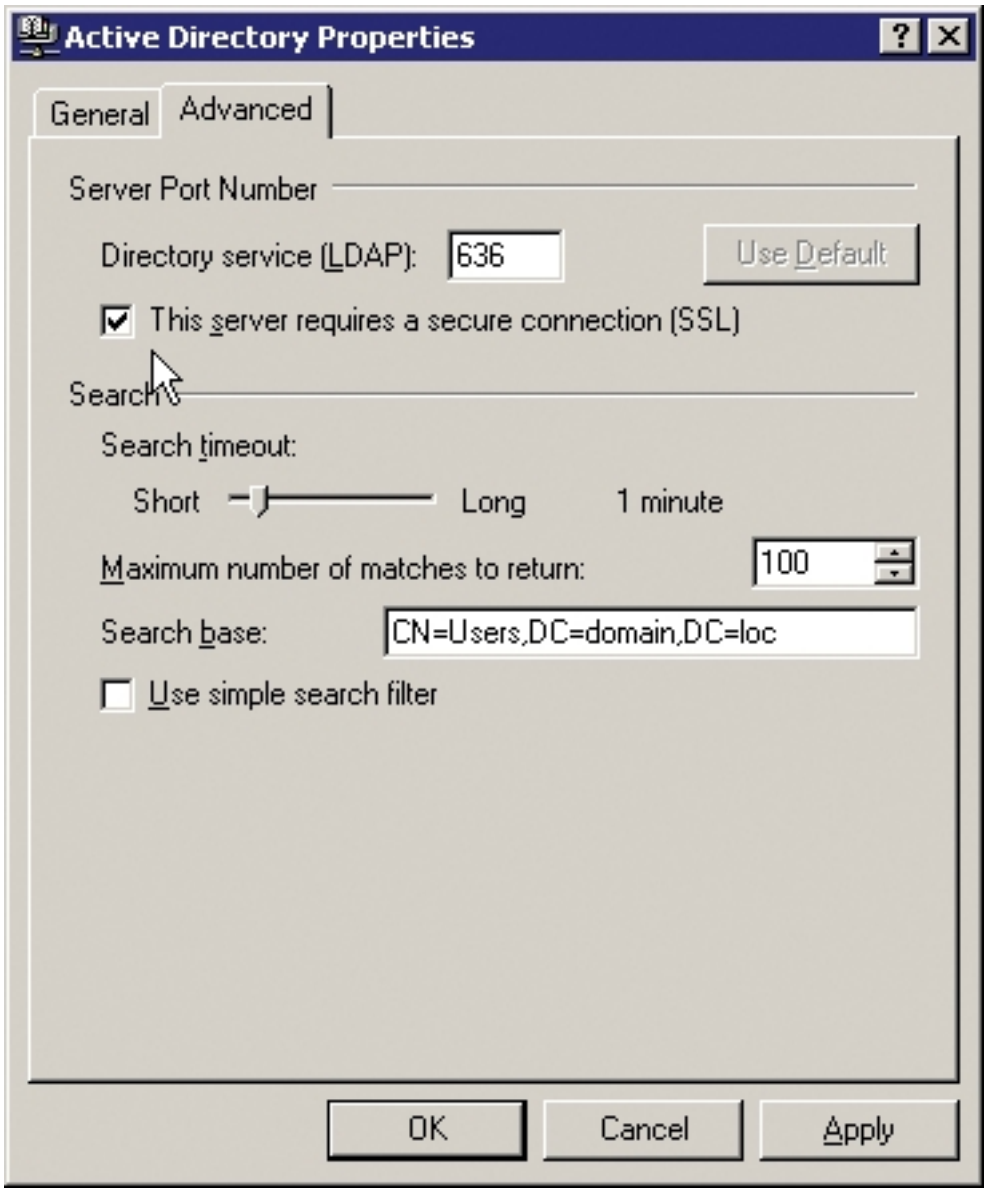
Пройдя добровольно-принудительную процедуру получения .NET Passport, вы сможете бесплатно скачать и использовать SFU3.5 (www.microsoft.com/windows/sfu). Размер программы примерно 230 Мб. Прежде чем устанавливать SFU, нужно инсталлировать Active Directory Schema MMC snap-in следующей командой:

regsvr32 c:WINNTsystem32schmmgmt.dll

Для расширения схемы AD достаточно установить только NIS-сервер из состава SFU. Для успешного завершения установки необходимо быть либо членом групп Domain Admins и Schema Admins, либо работать с правами Администратора. После установки будет предложено перегрузить машину. NIS-сервер как таковой не понадобится и его можно остановить и благополучно забыть о нём. В свойствах пользователя, группы, компьютера в Active Directory Users and Computers добавится вкладка UNIX Attributes.


test Properties
Member Of
Dial-in
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Terminal Services Profile
Exchange Features
UNIX Attributes
To enable access to this user for UNIX clients, you will have to specify the NIS domain this user belongs to.
NIS Domain:
<none>
UID:
Login Shell:
/bin/sh
Home Directory:
/home/test
Primary group name/GID:
OK
Cancel
Apply
Help


Find People
Look in:
Active Directory
Directory services
Properties
Web Site...
People
Advanced
Find Now
Name:
Stop
E-mail:
Clear All
Close


Active Directory Properties
General
Advanced
Server Port Number
Directory service (LDAP):
636
Use Default
This server requires a secure connection (SSL)
Search
Search timeout:
Short
Long
1 minute
Maximum number of matches to return:
100
Search base:
CN=Users,DC=domain,DC=loc
Use simple search filter
OK
Cancel
Apply