Визитка

ЕВГЕНИЙ БУШКОВ, системный администратор в Passware

Использование pGina
для аутентификации в системах MS Windows

Проект pGina с подключаемыми плагинами позволяет взаимодействовать системам MS Windows с разными Open Source-сервисами аутентификации, включая систему каталогов OpenLDAP

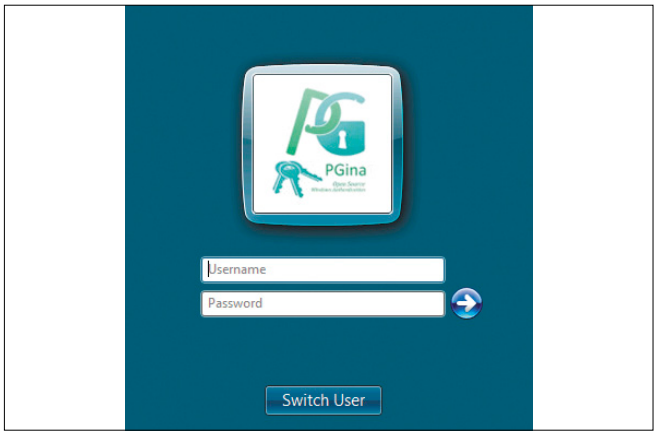
В настоящее время наибольшее распространение получили компьютерные системы, состоящие из рабочих станций и серверов с установленными операционными системами Microsoft. Порой продукты этой компании вынуждены потесниться, уступая место программным средствам Open Source. Как организовать взаимодействие между разными операционными системами (ОС) унифицированно? Это большая проблема для системных администраторов.

В статье я буду описывать pGina 2.x, в конце кратко упомяну первую версию 1.x программы, для тестирования Windows-сервера буду использовать Windows Server 2008 x86 SP2, а в качества всех Linux-серверов – систему Gentoo [1]. Читателю нужно уметь работать с OpenLDAP [2], реестром Windows, иметь базовые знания по администрированию GNU Linux и Windows-систем. Все, что здесь написано о Gentoo, должно работать и на других дистрибутивах Linux, а также BSD-системах, например, FreeBSD [3].

Немного истории

Интересно проследить, как за последние 15 лет менялась ситуация на рынке серверных ОС.

Рисунок 1. Приглашение для ввода логина и пароля pGina



Основная борьба между системами каталогов происходила между Novell eDirectory и Microsoft NT Domain, а впоследствии и Active Directory (AD). Novell Netware, очень популярная когда-то ОС, в результате конкуренции постепенно стала уступать свои позиции системам Microsoft. Повсеместное использование и внедрение систем Windows и доменов NT/AD начало вытеснять систему каталогов eDirectory.

Тем временем в мире Open Source неспешно развивалась своя система каталогов – OpenLDAP (далее просто LDAP). Конечно, конкуренцию таким гигантам, как Microsoft или Novell, она не могла составить. Меня, как и многих других администраторов, интересовало, как можно облегчить жизнь пользователям и упростить администрирование гетерогенных сетей (синхронизация паролей, возможности SSO и т.п.), включающих эти три системы каталогов.

Одним из способов решения данной проблемы было использование появившегося в начале 2000-х технологии Novell DirXML Password Synchronisation for Windows. Решение было не бесплатным, внедрение не выглядело таким уж простым. Также не были понятны тенденции развития существующих каталогов и конкуренции упомянутых выше гигантов. Жизнь сама расставила все по своим местам. Развивать и поддерживать систему с несколькими каталогами многим предприятиям стало не только сложно, но и дорого.

В настоящее время проблемы взаимодействия Microsoft AD и LDAP становятся все более актуальными в работе администраторов. В данной статье я не стану рассказывать, как использовать Winbind [4] для аутентификации Windows-пользователей на Linux-серверах, – эта тема достаточно подробно освещена в Интернете.

Интереснее и актуальнее рассмотреть возможность аутентификации Linux-пользователей на серверах и рабочих станциях Windows. То есть достаточно иметь LDAP-аккаунт для того, чтобы подключаться по протоколу RDP к рабочим станциям и серверам Windows с любого компьютера (Linux, Windows, Mac OS, FreeBSD). При этом аутентификация прозрачно для пользователя проходит на LDAP-сервере.

Этимология слова, и что из нее можно узнать

Настало время поближе познакомиться с pGina. Почему так называется продукт?

GINA – это акроним от Microsoft Graphical Identification and Authentication. Соответственно Msgina.dll – библиотека Windows, подгружаемая процессом Winlogon для вывода графического интерфейса (GUI) и участвующая в процессе аутентификации совместно с сервисом LSA [5].

Более подробно о взаимодействии Winlogon, GINA, LSA можно почитать, например, здесь [6].

Всем знакомо окошко с просьбой нажать комбинацию клавиш <Ctrl> + <Alt> + <Del> и ввести логин и пароль – за его вывод как раз и отвечает библиотека GINA. На рабочих станциях и серверах Windows с установленным Netware Novell client вместо Msgina.dll используется nwgina.dll. Как видим, многое можно узнать из названия продукта. Но это еще не все!

GINA использовалась в системах Windows 2000, XP, Server 2003. С выпуском MS Vista и последующих ОС (Windows 7, Server 2008) функции GINA стала выполнять другая библиотека – Credential Providers, призванная упростить, а также улучшить безопасность ОС Windows [7].

Хорошей новостью является то, что сегодня pGina поддерживает обе разновидности систем аутентификации, для этого есть соответственно версии 1.x (только поддержка ОС младше MS Vista) и 2.x (поддержка ОС MS Vista и более поздних).

Между этими версиями значительная разница в коде, но вам не нужно об этом беспокоиться, внешне интерфейсы различных версий программы мало отличаются, технологии их настройки очень похожи. Сервис pGina сам по себе не осуществляет аутентификацию, тем не менее он позволяет подключать различные плагины и может использовать их для аутентификации в LDAP, RADIUS, SSH, FTP, SMTP, POP3 и др. [8].

Я рассмотрю возможность работы pGina с LDAP и SSH, такую функциональность обеспечивают соответственно плагины LDAP Auth и SSHAuth.

Настройка pGina

Определитесь, на каком компьютере будете настраивать аутентификацию, у меня это Windows Server 2008, поэтому использую pGina версии 2.x. Вы можете использовать любую Windows-систему начиная с Vista. Для Windows XP используйте pGina 1.x (работу с pGina 1.x я кратко описываю ниже).

Скачиваем программу [9] и устанавливаем на выбранном компьютере под управлением Windows, куда будет осуществляться терминальный доступ. Здесь нет ничего сложного, остается внести нужные нам настройки.

Чтобы запустить программу изменения конфигурации, выберите в меню «Пуск → Configure pGina». Настройки безопасности Windows Server 2008 по умолчанию не позволяют нам выполнить файл ConfigApp.exe. Щелкаем правой кнопкой мышки на Configure pGina и выбираем Properties («Свойства»). Выбираем в свойствах закладку Compatibility и отмечаем Run this program as administrator. Теперь программа запускается.

Думаю, что в настройках несложно разобраться: можно изменить текст приглашения при вводе пароля, вставить картинку (лого) своей организации, разрешить подключение сетевых дисков при входе в систему, указать ограничение времени для сеансов терминальной связи, настроить автоматическое выполнение скриптов и кое-что еще. Опишу наиболее важные, с моей точки зрения, пункты.

На вкладке Profile есть пункт Keep user profiles persistent... Если его отметить галочкой, пользовательские профили будут сохраняться при закрытии сессии, в противном случае станут удаляться, так что можете решать сами, что предпочесть.

На этой же вкладке есть параметр Replace plugin authentification password with local password (if account exists). Если в системе Windows уже есть учетная запись, совпадающая по имени с аккаунтом из LDAP, то pGina будет автоматически изменять ее пароль локально. В противном случае пользователь сможет заходить в систему под обоими паролями, что, на мой взгляд, может привести к путанице и ухудшению безопасности системы.

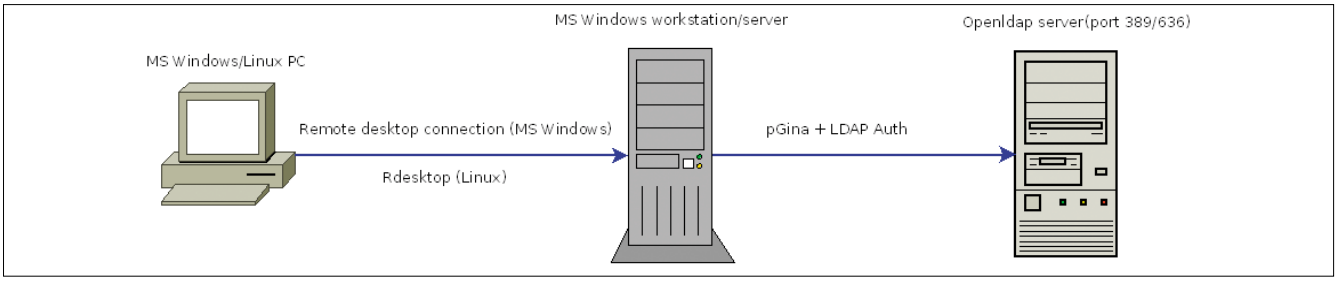
Загляните на вкладку Log settings. В поле Full path to file which log will be written to... можно прописать свой путь к файлу журнала событий вручную либо нажать кнопку Browse и выбрать его с помощью мышки. Если что-то не будет работать, можно почитать последние записи данного журнала (не надо забывать, конечно, и системный Event Viewer), там же можно изменить уровень важности записываемых событий (Log Level) и другие настройки записи событий pGina.

Настройка плагина LDAP Auth

Вот мы добрались наконец до настройки плагина. Откройте закладку Plugin. По умолчанию в системе pGina используется плагин-заглушка DummyPlugin.dll, требуется указать нужный нам плагин.

Для этого скачайте LDAP Auth [10], распакуйте в папку установки pGina, по умолчанию это C:\Program Files\pGina\

Рисунок 2. Взаимодействие связки pGina + LDAP Auth с клиентами и LDAP-сервером



plugins, хотя путь может быть и другой, это не так важно. Нажмите кнопку Browse и укажите путь к файлу ldapauth_plus.dll. Теперь нажмите Configure, откроется окно с настройками LDAP. Сейчас нас интересует только первая закладка LDAP Configuration: здесь можно найти все необходимое для настройки соединений с LDAP.

В первую очередь нужно определиться с методом поиска записей пользователей в дереве LDAP.

Напомню, что такое контекст объекта в дереве LDAP. Каждый элемент в каталоге имеет уникальное характерное имя (или DN – Distinguished Name), состоящее из пар «атрибут=значение», разделенных запятыми. Часть характерного имени без крайней пары значений и есть контекст данного элемента. Например, элемент с DN uid=username, ou=People,dc=domain,dc=ru имеет контекст ou=People, dc=domain,dc=ru.

Если у ваших пользователей разные контексты, то нужно применить методы Search Mode или MultiMap Mode, после чего необходимо ниже добавить нужные контексты. Если у вас, как у меня, только один контекст для всех пользователей, то выбирайте Map Mode, в этом случае этот контекст можно прописать в пункте Append: (см. рис. 3).

Далее следует указать префикс пользовательских записей, в LDAP это uid, поэтому в поле PrePend: прописываем uid= (это поле не используется в режиме Search Mode). Далее нужно прописать адрес сервера, который будет использоваться для аутентификации в пункте LDAP Server.

Возможность использования групп LDAP рассмотрим позже, поэтому пока поле Group Attr: я оставил пустым.

Если вы не хотите использовать SSL для безопасной передачи паролей на сервер LDAP, то укажите номер порта 389 в пункте Port:, и на этом все – можно тестировать наши настройки.

Для тех, кто будет использовать SSL, укажите 636-й порт и читайте следующую часть.

Настройка SSL для LDAP

В последних версиях LDAP по умолчанию используется порт 389 для всех соединений, включая шифрованные TLS/SSL. После подключения клиентской программы к данному TCP-порту и установки нешифрованного сеанса связи выполняется стандартная LDAP-операция StartTLS, а затем используется протокол TLS/SSL.

StartTLS – это расширение протокола передачи данных, позволяющее инициализировать TLS-сессию поверх незащищенного соединения, не используя для этого отдельный порт TCP [11]. Проблема в том, что плагин LDAP Auth не умеет работать с методом StartTLS, поэтому нам придется настроить LDAP для работы с LDAPS (LDAP over TLS/SSL) с соединениями на отдельный порт (по умолчанию 636) [12]. Для Gentoo достаточно раскомментировать следующую строчку в файле /etc/conf.d/slapd:

```
OPTS="-h 'ldaps:// ldap:// ↵
       ldapi://%2fvar%2frun%2fopenldap%2fslapd.sock'"
```

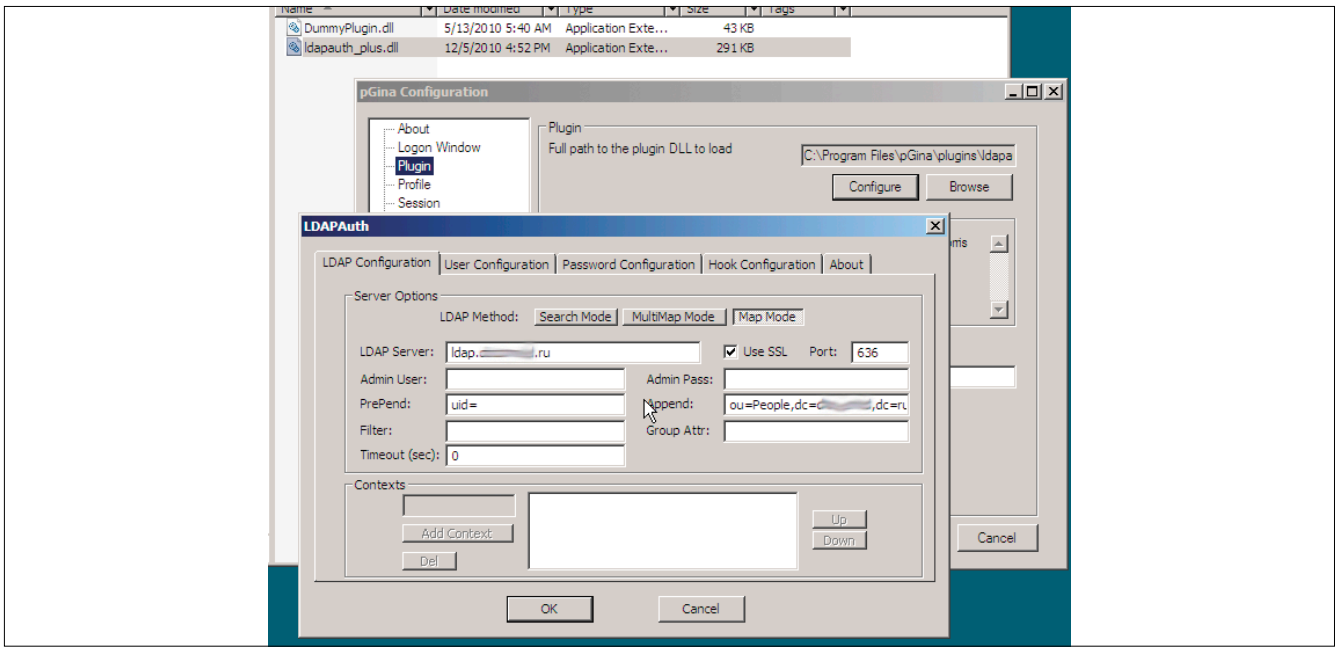
Осталось перезапустить LDAP-сервис. Следующей командой можно проверить, задействованы ли нужные нам порты:

```
netstat -nap|egrep '0.0.0.0:(389|636)'
```

Со стороны сервера Linux мы выполнили все, что требуется для работы плагина LDAP Auth. Скорее всего в своей организации вы используете собственный центр сертификации (Certificate Authority или CA, смотрите врезку) для выдачи и подписи сертификатов различных сервисов вашей сети, устанавливающих SSL/TLS-соединения, в том числе и LDAP. Это нормальная ситуация, только вот системы Windows отказываются работать с серверами, использующими такие сертификаты.

В журнале событий LDAP на сервере можно получить подобную запись:

Рисунок 3. Окно основных настроек соединения с LDAP



```
Dec  5 17:19:14 ldapserver slapd[8172]: conn=50674 fd=63
ACCEPT from IP=192.168.0.112:49162 (IP=0.0.0.0:636)
Dec  5 17:19:14 ldapserver slapd[8172]: conn=50674 fd=63
closed (TLS negotiation failure)
Dec  5 17:19:25 ldapserver slapd[8172]: conn=50673 fd=61
closed (connection lost)
```

Эта проблема решаема, достаточно установить сертификат вашего CA на компьютере Windows в хранилище доверительных центров сертификации.

Для этого скопируйте сертификат любым доступным способом на нужный компьютер, щелкните на файле пару раз мышкой – откроется окно с информацией о сертификате. Если не открылось, проверьте, что расширение у сертификата .crt, и, если нет, переименуйте.

Кстати, установку сертификата можно выполнить и через стандартную оснастку Certificates в консоли mmc. Нажмите кнопку Install Certificate, здесь нужно правильно указать хранилище сертификатов, поэтому не используйте автоматический выбор хранилища.

Посмотрите на рис. 4, там я показал, какой пункт меню нужно выбрать для правильной установки сертификата, а именно: отметьте Show physical stores, выберите из списка Trusted Root Certification Authorities и Local Computer. Готово, можно проверять работу SSL-соединений.

Создание собственного центра сертификации и генерирование сертификата для LDAP-сервера

Организация собственного центра сертификации позволяет подписывать сертификаты различных серверов и сервисов вашей организации, не прибегая к услугам сторонних (как правило, небесплатных) CA. Подписание сертификатов с помощью CA гарантирует, что данный сервер/сервис является тем, за кого он себя выдает, и ему можно доверять внутри вашей организации.

Сам CA представляет собой два файла – сертификат и защищенный паролем ключ. Пароль для ключа необходимо задать достаточно сложный, чтобы максимально уменьшить вероятность его подбора злоумышленниками, для этого можно использовать генератор паролей (например, в Gentoo для этого есть утилита pwgen).

Создание CA

Проводим генерацию ключа CA:

```
$ openssl rsa -noout -text -in ca.key 1024
```

В ответ на запрос введите сгенерированный пароль.

Создаем сертификат CA:

```
$ openssl req -new -x509 -nodes -sha1 -days 1825 ↵
        -key ca.key out ca.crt
```

Здесь число 1825 – срок в днях, в течение которого сертификат будет действителен (365 x 5 = 1825), то есть пять лет, но у вас этот срок может быть другим. В ответ на команду вас попросят ввести информацию о сертификате:

```
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:
Moscow region
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Company ltd.
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:Company CA
Email Address []:mail@domain.ru
```

Вместо использованных мною значений задействуйте данные своей организации.

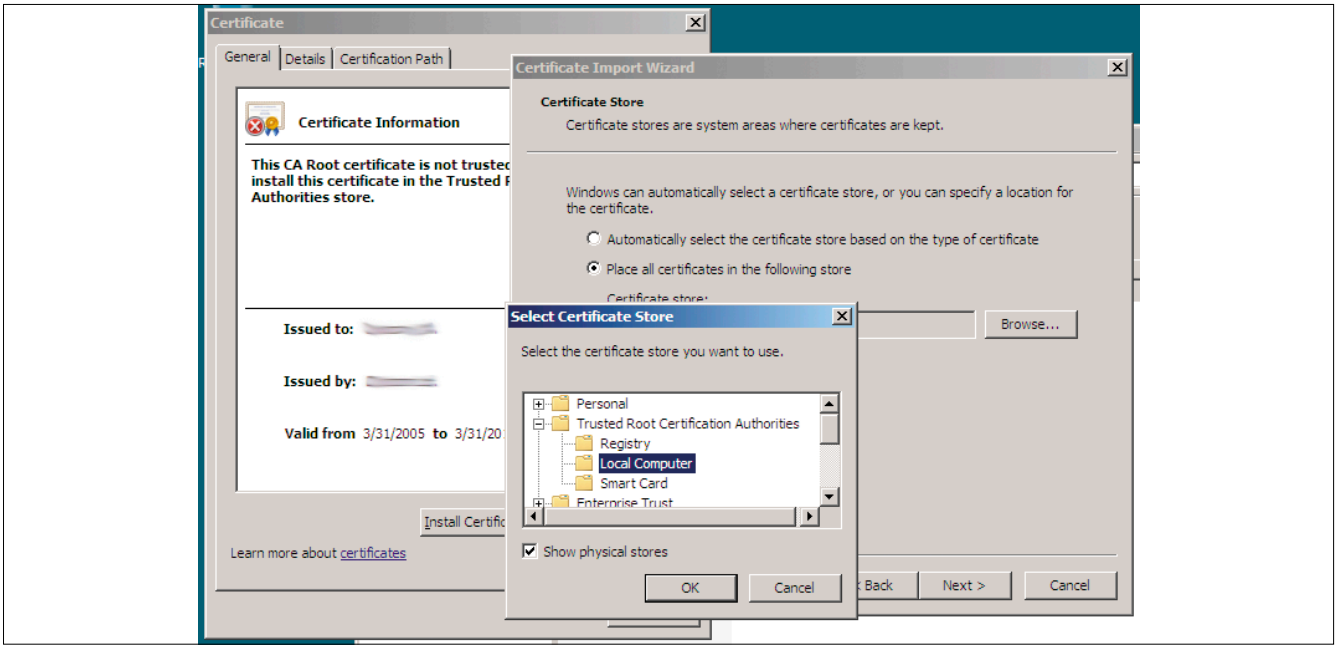
Сертификат готов, можно вывести информацию о нем командой:

```
$ openssl x509 -noout -text -in ca.crt
```

Генерирование сертификата для LDAP-сервера

Создаем закрытый ключ:

Рисунок 4. Выбор хранилища для нашего сертификата



```
$ openssl genrsa -des3 -out ldap.key 1024
```

В ответ на запрос введите новый пароль для этого ключа.

Часто необходимо в разных сервисах использовать незашифрованный ключ. Чтоб получить такой ключ, выполните команды:

```
$ openssl rsa -in ldap.key -out ldap.key.unsecure
$ chmod 440 ldap.key.unsecure
$ chown ldap:ldap ldap.key.unsecure
```

Команды chmod и chown ограничивают доступ к этому ключу только сервисом OpenLDAP.

Создаем запрос на подписание сертификата:

```
$ openssl req -new -key ldap.key -out ldap.csr
```

В ответ на команду введите информацию о сертификате:

```
Country Name (2 letter code) [AU]:RU
State or Province Name (full name) [Some-State]:
Moscow region
Locality Name (eg, city) []:Moscow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Company ltd.
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:ldap.domain.ru
Email Address []:mail@domain.ru
```

Самый важный пункт здесь – Common Name, убедитесь, что имя корректно разрешается в IP-адрес и соответствует серверу, на который будет установлен сертификат. Если ошибетесь в имени, то при TLS-соединении с вашим LDAP-сервером получите ошибку, и нужно будет создавать запрос снова.

Теперь можно подписать сертификат, используя полученный файл ldap.csr:

```
$ openssl x509 -req -in ldap.csr -days 1080 -CA ca.crt ↵
        CAkey ca.key -CAcreateserial -out ldap.crt
```

Для подписи запроса потребуется ввести пароль ключа CA. После ввода пароля получаем готовый сертификат ldap.crt.

Полученные файлы ключа, сертификата LDAP и сертификата CA разместите в используемых вашей системой каталогах, после чего пропишите их в файле конфигурации LDAP /etc/openldap/slapd.conf с помощью следующих директив:

```
TLSCertificateKeyFile    /etc/openldap/ssl/ldap.key.unsecure
TLSCertificateFile       /etc/openldap/ssl/ldap.crt
TLSCACertificateFile     /etc/ssl/certs/ca.crt
```

Использование pGina 1.x

Для установки pGina на Windows XP понадобится первая версия программы. Скачайте ее [13] и распакуйте в выбранный каталог на жестком диске. Если не запускается конфигуратор, то в вашей системе не хватает некоторых необходимых для его работы библиотек Visual Studio. В этом случае понадобится выполнить из только что распакованных файлов vcredist_x86(vcredist_x64). Устанавливать библиотеки можно до или после инсталляции pGina.

Настройки плагина LDAP Auth ничем не отличаются от описанных выше про вторую версию pGina. Конфигураторы pGina версий 1.x и 2.x отличаются только интерфейсом, названия и значения всех параметров очень похожи, и в них несложно разобраться, поэтому я не стану здесь подробно описывать их отличия.

Использование реестра

Все описанные настройки можно менять непосредственно в реестре (ветка HKEY_LOCAL_MACHINE\SOFTWARE\pGina и подраздел ldapauth), более того, описание настроек в документации плагина LDAP Auth использует именно имена параметров из реестра. Тем не менее использование графического конфигуратора выглядит более удобным. Более полезным примером использования редактора реестра является экспорт ветки настроек pGina для последующего импортирования на других компьютерах. Экспорт можно сделать непосредственно в редакторе реестра (regedit), а можно из командной строки:

```
reg export "hklm\software\pGina" c:\path\pgina.reg
```

Прежде чем переносить полученный файл на другие машины, неплохо открыть его на редактирование в Wordpad или в любом другом текстовом редакторе и подправить, оставив только необходимые строчки. Например, можно удалить пути к файлам (в случае если установка выполняется на другой диск или в другую папку): logFile, logo, pathPlugin и т.п.

После установки на другом компьютере pGina можно выполнить pgina.reg, разрешить системе внесение изменений в реестр, и нужные нам настройки добавятся в реестр.

***

Как видим, существуют решения Open Source, позволяющие использовать каталоги OpenLDAP и единую систему аутентификации пользователей в сети для работы не только с GNU Linux, но и с широко распространенными рабочими станциями и серверами MS Windows.

Предложенное решение не претендует на то, чтобы полностью заменить AD в крупной организации. Оно может быть применимо в небольшой компьютерной системе либо если OpenLDAP является единственным каталогом вашей сети. В этих случаях есть возможность отказаться от использования связки AD и не всегда надежного Winbind- средства.

В следующей части статьи я более подробно опишу вопросы управления доступом pGina, конфигурирования LDAP и использования другого плагина SSHAuth.

Успехов в освоении pGina! EOF

1. http://www.gentoo.org.
2. http://www.openldap.org.
3. http://www.freebsd.org.
4. http://smb-conf.ru/winbindd.html.
5. http://msdn.microsoft.com/en-us/library/aa380543%28VS.85%29.aspx.
6. http://technet.microsoft.com/ru-ru/library/cc780332%28WS.10%29.aspx.
7. http://msdn.microsoft.com/en-us/magazine/cc163489.aspx.
8. http://www.pgina.org/index.php/Main_Page.
9. http://www.pgina.org/index.php/PGina_2.x_Downloads.
10. http://www.pgina.org/index.php/Plugins:LDAP_Auth.
11. http://www.ietf.org/rfc/rfc2830.txt.
12. http://www.openldap.org/faq/data/cache/185.html.
13. http://www.pgina.org/index.php/PGina_1.x_Downloads.