

Переводим домен Active Directory на лицензионную основу



Александр Емельянов

В свете событий последних полутора-двух лет, касающихся преследования правоохранительными органами за использование «пиратского» софта, многие организации стараются перейти на лицензионное программное обеспечение либо использовать его свободные аналоги. Хорошо, когда организация находится в стадии становления и ее IT-инфраструктура еще не построена. Но как быть в этом случае с уже настроенным и работающим доменом Active Directory вашей компании?

Предположим ситуацию. Вы администратор небольшой сети (скажем, с парком машин на 50-60), в которой серверное ПО производства компании Microsoft не имеет ни единой лицензии. На досуге, бороздя просторы Интернета, вы ознакомились с российским законодательством и осознали, что грозит вам как администратору локальной сети и вашему руководству за использование данных программных продуктов в коммерчес-

ких интересах фирмы. Вы идете в кабинет с табличкой «Директор» и доносите до сидящего в нем человека понятным ему языком, что вам необходимо встать в стройные ряды пользователей лицензионного софта от Microsoft (и не только). И что в противном случае существует риск получить проблемы с законом. При удачном исходе беседы через некоторое время ваша организация разорвется (иначе не назовешь) на покупку ПО и соответствующ-

щих лицензий, а перед вами стоит задача безболезненно перевести домен компании на легальную основу. Попробуем разобраться.

Я не буду затрагивать программы лицензирования Microsoft, потому что они хорошо были освещены в серии статей «Как купить ПО от Microsoft? Особенности приобретения и использования OEM-версий» Дмитрия Бутянова (см. №12 за 2006 г., №1 и 3 за 2007 г.).

Сразу же скажу, что будет описан только предполагаемый план действий для решения поставленной задачи, а не пошаговое руководство по выполнению стандартных операций. Также будут рассмотрены возможные «подводные камни». Все вопросы, касающиеся технической стороны дела, вы можете задать на интернет-форуме журнала (www.samag.ru/forum).

Хочется отметить, что в Интернете мне встречались некоторые описания по «ускоренному» лицензированию серверных операционных систем Microsoft. Зачастую они требовали либо определенных манипуляций с реестром (например, для преобразования Windows 2003 Server Enterprise Edition в Standard Edition), либо использования стороннего ПО (для подмены ключа на лицензионный).

Но, во-первых, такие действия, даже если они с успехом проходят на виртуальной машине, я не рискнул бы выполнять на работающем контроллере домена. А, во-вторых, количество рабочих станций, как правило, намного больше числа серверов в офисе, и для них можно использовать пакет лицензирования Get Genuine Kit, который как раз позволяет заменить «серый» ключ на лицензионный и успешно активировать систему.

Как я уже говорил, предлагаемый ниже способ перехода на лицензии требует совершения ряда стандартных действий с серверами в домене и в определенной степени гарантирует отказоустойчивость при проведении операций. Во многом именно поэтому он представляется мне наиболее корректным.

Построение сети каждой организации имеет индивидуальный характер. Поэтому я буду рассматривать гипотетическую сеть со стандартными сервисами. Предположим, у нас, точнее у вас, есть домен Active Directory с DNS, DHCP, почтовым, терминальным, файловым и прокси-серверами, работающими под управлением Windows Server 2003 SE (EE).

Наши исходные данные:

- **Сервер Main1** – контроллер домена, DNS-сервер, DHCP-сервер, сервер лицензий служб терминалов, обладатель ролей FSMO.
- **Сервер Main2** – контроллер домена, DNS-сервер, файловый сервер.

■ **Сервер TS** – сервер терминалов (на нем может работать какая-нибудь бухгалтерская программа, например 1С:Бухгалтерия или Инфо-Бухгалтер).

■ **Сервер SMail** – почтовый сервер предприятия (предположим, что в сети используется офисный сервер, отличный от Exchange, например, Kerio Mail Server, MDAemon Mail Server, Office Mail Server или другие аналоги), прокси-сервер.

Дополнительные данные: сетевые настройки все машины получают от DHCP-сервера, авторизация на прокси-сервере доменная. Что защищает вашу сеть от вторжений из Интернета, в данном случае не берем в расчет (тем более если это отдельно стоящий «железный» фаервол).

Наша задача – получить в итоге ту же картину, но с лицензионными системами «на борту», либо сократить число серверов (все зависит от количества купленных лицензий).

Этап 1. Лицензируем сервер терминалов

Выбираем период, когда пользователи не используют терминальный доступ. Это может быть время после рабочего дня либо выходной день. Выводим сервер TS из домена, устанавливаем на нем операционную систему и вводим в домен под тем же именем.

Все, казалось бы, просто, если бы не одно «но». Пользователи могут хранить важные данные в терминальном профиле, помимо этого у них могут быть настроены ярлыки на запуск программ (например, для запуска конкретной базы 1С от имени определенного пользователя). Вряд ли пользователям, да и вам, захочется их потерять. Хорошо, если профили пользователей хранятся у вас на другом сервере (предположим на машине Main2) и в групповых политиках определен путь для них. Зачастую это используется при наличии нескольких серверов терминалов в сети. Однако положим, что вы сделали это для обеспечения отказоустойчивости. Если же пользователи при входе на сервер терминалов используют локальные профили, то вы можете руками сохранить все важные данные. Но, вероятнее всего, вам потом придется заново

настраивать профиль для каждого пользователя. Чтобы этого избежать, используйте групповую политику для задания папки для хранения перемещаемых профилей сервера терминалов на сервере Main2, где будут сохраняться пользовательские данные и настройки.

Перед тем, как вы будете переустанавливать систему, нужно будет проследить, чтобы пользователи корректно вышли из терминального сеанса, а не оставили его в состоянии «отключен». В этом случае все изменения профиля скопируются на сервер Main2.

Итак, вводим сервер TS в домен и назначаем ему роль терминального сервера. Все подробные руководства вы можете без труда найти в Интернете. И если пути к программам остались как на старом терминале, то для пользователей все ваши действия окажутся абсолютно «прозрачными».

Если по каким-то причинам (например, намеченный апгрейд терминального сервера) вам нужно временно передать роль сервера терминалов для обеспечения работы офиса другому серверу, вы можете использовать сервер Main2. Но для этого его нужно предварительно освободить от роли контроллера домена (из соображений безопасности не рекомендуется совмещать роли Domain Controller и Terminal Server).

Далее необходимо будет перенести программы с сервера TS (желательно, чтобы абсолютный путь к ним был как на сервере TS) и создать на DNS-сервере в зоне прямого просмотра вашего домена псевдоним для сервера Main2 (создаем запись CNAME, псевдоним будет TS, а реальный сервер Main2). Это делается для того, чтобы не перенастраивать RDP-файлы на рабочих станциях для каждого пользователя (Remote Desktop Protocol, протокол подключения к удаленному рабочему столу).

После того как вы «поднимете» сервер TS, псевдоним на DNS-сервере нужно будет убрать. В конечном итоге перед вторым этапом мы имеем следующую картину:

- два нелицензированных контроллера домена;
- лицензированный сервер терминалов;

- нелегитимизированный почтовый/прокси-сервер.

Этап 2. Лицензируем почтовый (прокси) сервер и контроллер домена

Касательно лицензирования сервера SMail некие общие рекомендации давать сложно, потому как почтовых и прокси-серверов существует изрядное количество. В целом если вы используете, например, ISA Server для защиты корпоративной сети из 50 машин (судя по сообщениям на форумах, таких людей немало), то приобретение еще одной серверной лицензии вкупе со стоимостью самого ISA-сервера не иначе как расточительство. Возможно, есть смысл посмотреть в сторону таких решений, как, например, Traffic Inspector (www.smart-soft.ru) или Eproxу (www.eserv.ru). Стоимость их в разы меньше стоимости ISA Server, оба продукта имеют российское гражданство, а значит, вы сможете получить техподдержку от производителя, в каждом поддерживается авторизация по доменному имени. Помимо этого, они могут быть установлены на машину с ОС Windows XP. Конечно, оба продукта уступают по функционалу ISA-серверу. Однако в небольших организациях все его широчайшие возможности, как правило, не нужны.

Что касается почтового сервера, здесь также все индивидуально. Я думаю, с сохранением почтового архива и конфигурационных файлов вашего почтового сервера у вас не возникнет затруднений. Я использую уже не один год в своей работе Office Mail Server, и для обеспечения его запуска на новой лицензированной машине мне потребовалось бы несколько секунд.

Собственно, выбор почтового или прокси-сервера не самоцель статьи, поэтому так или иначе конечное решение за вами. Порядок действий на этом этапе предельно прост: бэкап почты и конфигурации почтовика, настроек прокси-сервера; установка операционной системы и восстановление работы сервисов данного сервера SMail в исходное состояние.

На этом же этапе лицензируем сервер Main2. Так как он является у нас файловым сервером, отключать его в рабочее время нежелательно. Но поскольку для его перевода требуется ми-

нимум вмешательства администратора (основное время будет потрачено на репликацию при понижении роли и установку системы), это можно делать одновременно с вашим почтовым сервером. Понижаем его до рядового сервера, выводим из домена, устанавливаем систему, вводим в домен и снова делаем его контроллером домена. Однако если вы используете разграничение доступа к файлам на сервере Main2 при помощи разрешений NTFS, все эти разрешения будут потеряны при переустановке системы, поэтому вы можете заранее перенести файловое хранилище на другой сервер с сохранением разрешений (Total Commander позволяет это делать) либо сделать резервную копию разрешений, используя скрипт NTFSBKP.bat [1] в совокупности с утилитой subinacl.exe [2], и затем восстановить её.

В итоге на подходе к третьему этапу мы имеем нелегитимизированный контроллер домена, лицензированный контроллер и две машины с лицензионной операционной системой «на борту».

Этап 3. Лицензируем контроллер домена (обладатель ролей FSMO)

Все действия в принципе можно проводить в рабочее время. Для этого нужно на сервере Main2 установить DHCP-сервис и создать область, аналогичную области на Main1, но DHCP-сервер Main2 не авторизовать в Active Directory, тогда он не будет выдавать адреса клиентам. В конце рабочего дня можно освободить Main1 от роли DHCP-сервера и авторизовать DHCP-сервер Main2. Вдобавок, если на DNS-сервере Main1 настроена пересылка запросов на разрешение имен на DNS-провайдера, такую обязанность нужно назначить Main2, при условии если этого еще не сделано. Для этого в консоли DNS нужно открыть свойства вашего сервера и найти вкладку «Пересылка запросов» или «Forwarding» и проставить там IP-адрес DNS-сервера провайдера. Также нужно разрешить Main2 на прокси-сервере доступ к DNS-серверу провайдера. Таким образом, на следующий день рабочие станции вашей сети смогут получать сетевые настройки с сервера Main2.

Теперь можно спокойно проводить с Main1 дальнейшие манипуляции.

Мы помним, что Main1 – сервер лицензий сервера терминалов. Поэтому перед его отключением нужно Main2 назначить роль сервера лицензий и установить купленные вами лицензии на терминальный доступ.

Далее нужно сделать контроллер Main2 обладателем ролей FSMO. Сделать это можно при помощи оснасток «AD → Users and Computers», «AD → Domains and Trusts» и «Схема Active Directory». Последнюю нужно дополнительно подключить через консоль mmc, но перед этим необходимо выполнить команду «regsvr32 schmmgmt.dll» в командной строке.

Аналогично передать роли с одного контроллера на другой можно, используя утилиту командной строки Ntdsutil.exe с ключом /roles. Не помешает после этих операций прогнать тест dcdiag на предмет ошибок.

После всего этого выводим Main1 из домена, предварительно сделав его рядовым сервером. Устанавливаем систему, вводим Main1 в домен и «поднимаем» его до контроллера домена.

Вы можете передать Main1 роли сервера DHCP, обладателя ролей FSMO и DNS-сервера, а можете оставить все как есть. Многое будет зависеть от нагрузки на ваши серверы и от потребностей вашей организации.

Заключение

Естественно, наличие установленного серверного ПО зависит от задач, решаемых на предприятии. В рамках статьи не были рассмотрены такие продукты, как SharePoint Server, сервер MOM (Microsoft Operations Manager), почтовый сервер Exchange, сервер обновлений Windows Server Update Services, сервер баз данных SQL Server и другие. Но правильный переход на легальную основу любого из таких сервисов во многом зависит от хорошего понимания администратором принципов работы и взаимодействия всех компонентов каждого отдельно взятого серверного программного продукта. 

1. <http://www.jsifaq.com/SF/Tips/Tip.aspx?id=9945>.
2. <http://www.microsoft.com/downloads/details.aspx?FamilyID=e8ba3e56-d8fe-4a91-93cf-ed6985e3927b&displaylang=en>.