Основные сведения о доменах Active Directory

(Взято с http://www.windowsfaq.ru/content/view/465/46/**)**

Домены на базе Active Directory позволяют централизованно администрировать все ресурсы, включая пользователей, файлы, периферийные устройства, доступ к службам, сетевым ресурсам, веб-узлам, базам данных и так далее. AD поддерживает иерархическое пространство имён для учётной информации о пользователях, группах и компьютерах, а так же о других каталогах, что в конечном счёте позволяет снизить административные издержки, связанные с поддержкой нескольких пространств имён. Короче говоря, AD позволяет использовать единую точку администрирования для всех публикуемых ресурсов. В основе AD используется стандарт именования X.500, система доменных имён – Domain Name System (DNS) для определения местоположения, и в качестве основного протокола используется Lightweight Directory Access Protocol (LDAP).

AD объединяет логическую и физическую структуру сети. Логическая структура AD состоит из следующих элементов:

- **организационное подразделение (organizational unit)** – подгруппа компьютеров, как правило, отражающая структуру компании;
- **домен (domain)** – группа компьютеров, совместно использующих общую базу данных каталога;
- **дерево доменов (domain tree)** – один или несколько доменов, совместно использующих непрерывное пространство имен;
- **лес доменов (domain forest)** – одно или несколько деревьев, совместно использующих информацию каталога.

К физической структуре относятся следующие элементы:

- **подсеть (subnet)** – сетевая группа с заданной областью IP-адресов и сетевой маской;
- **сайт (site)** – одна или несколько подсетей. Сайт используется для настройки доступа к каталогу и для репликации.

В каталоге хранятся сведения трех типов: данные домена, данные схемы и данные конфигурации. AD использует только контроллеры доменов. Данные домена реплицируются на все контроллеры домена. Все контроллеры домена равноправны, т.е. все вносимые изменения с любого контроллера домена будут реплицированы на все остальные контроллеры домена. Схема и данные конфигурации реплицируются во все домены дерева или леса. Кроме того, все объекты индивидуального домена и часть свойств объектов леса реплицируются в глобальный каталог (GC). Это означает, что контроллер домена хранит и реплицирует схему для дерева или леса, информацию о конфигурации для всех доменов дерева или леса и все объекты каталога и свойства для собственного домена.

Контроллер домена, на котором хранится GC, содержит и реплицирует информацию схемы для леса, информацию о конфигурации для всех доменов леса и ограниченный набор свойств для всех объектов каталога в лесу

(который реплицируется только между серверами GC), а также все объекты каталога и свойства для своего домена.

Контроллеры домена могут иметь разные роли хозяев операций. Хозяин операций решает задачи, которые неудобно выполнять в модели репликации с несколькими хозяевами.

Существует пять ролей хозяина операций, которые могут быть назначены одному или нескольким контроллерам доменов. Одни роли должны быть уникальны на уровне леса, другие на уровне домена.

В каждом лесе AD существуют следующие роли:

- **Хозяин схемы (schema master)** – управляет обновлениями и изменениями схемы каталога. Для обновления схемы каталога необходим доступ к хозяину схемы. Чтобы определить, какой сервер в данное время является хозяином схемы в домене, нужно в окне командной строки набрать команду *dsquery server -hasfsmo schema*
- **Хозяин именования доменов (domain naming master)** – управляет добавлением и удалением доменов в лесу. Чтобы добавить или удалить домен требуется доступ к хозяину именования доменов. Чтобы определить, какой сервер в данное время является хозяином именования доменов, в окне командной строки введите *dsquery server -hasismo name*

Эти роли, общие для всего леса в целом и являются в нем уникальными.

В каждом домене AD обязательно существуют следующие роли:

- **Хозяин относительных идентификаторов (relative ID master)** – выделяет относительные идентификаторы контроллерам доменов. Каждый раз при создании объекта пользователя, группы, или компьютера, контроллеры назначают объекту уникальный идентификатор безопасности, состоящий из идентификатора безопасности домена и уникального идентификатора, который был выделен хозяином относительных идентификаторов. Чтобы определить, какой сервер в данное время является хозяином относительных идентификаторов домена, в командной строке введите *dsquery server -hasfsmo rid*
- **Эмулятор PDC (PDC emulator)** – в смешанном или промежуточном режиме домена действует как главный контроллер домена Windows NT. Он аутентифицирует вход в Windows, обрабатывает изменения пароля и реплицирует обновления на BDC, если они есть. Чтобы определить, какой сервер в данное время является эмулятором PDC домена, в командной строке введите *dsquery server -hasfsmo pdc*
- **Хозяин инфраструктуры (infrastructure master)** – обновляет ссылки объектов, сравнивая данные своего каталога с данными GC. Если данные устарели, он запрашивает из GC обновления и реплицирует их на остальные контроллеры домена. Чтобы определить, какой сервер в данное время является хозяином инфраструктуры домена, в командной строке введите *dsquery server -hasfsmo infr*

Эти роли, общие для всего домена и должны быть в нем уникальны.

Роли хозяев операций назначаются автоматически первому контроллеру в домене, но могут быть в дальнейшем переназначены вами. Если в домене только один контроллер, то он выполняет все роли хозяев операций сразу.

Не рекомендуется разносить роли хозяина схемы и хозяина именования доменов. По-возможности назначайте их одному контроллеру домена. Для наибольшей эффективности желательно, чтобы хозяин относительных идентификаторов и эмулятор PDC также находились на одном контроллере, хотя при необходимости эти роли можно разделить. В большой сети, где большие нагрузки снижают быстродействие, хозяин относительных идентификаторов и эмулятор PDC должны быть размещены на разных контроллерах. Кроме того, хозяин инфраструктуры не рекомендуется размещать на контроллере домена, хранящем глобальный каталог.

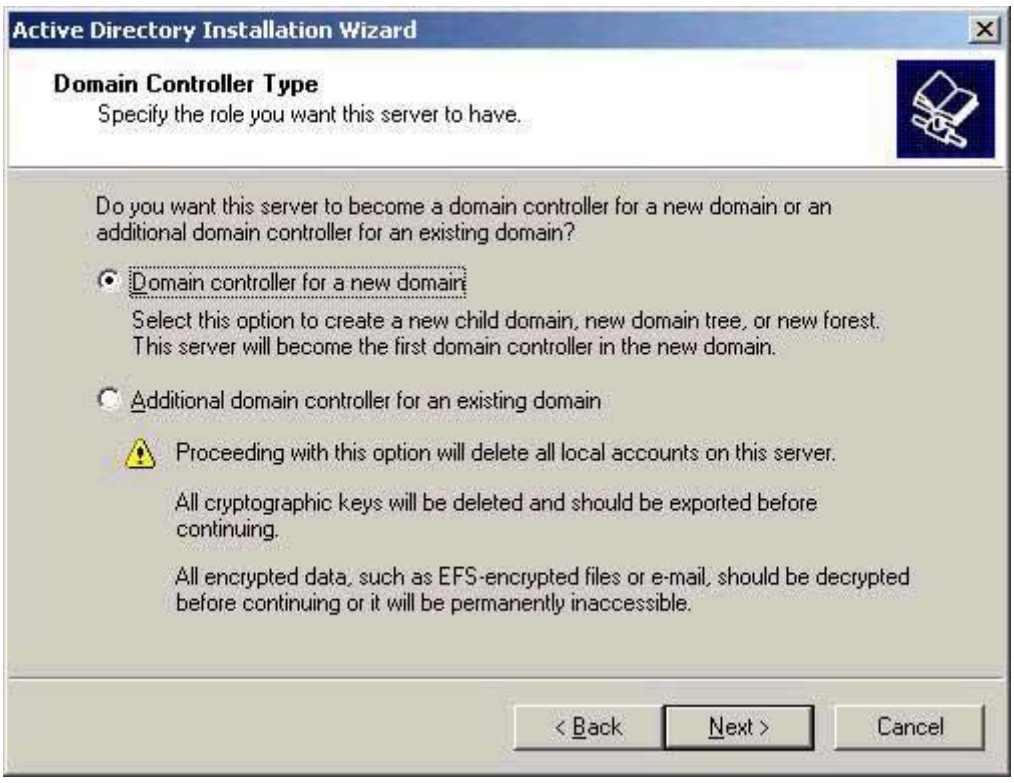
Инсталляция контроллера домена (DC) на базе Windows Server 2003 с помощью мастера установки Active Directory

Установка контроллера домена производится с помощью мастера Active Directory Installation Wizard. Чтобы повысить статус сервера до контроллера домена необходимо убедиться в выполнении всех необходимых для этого требований:

1. На сервере должен быть хотя бы один раздел NTFS для размещения системного тома SYSVOL.
2. Сервер должен иметь доступ к DNS серверу. Желательно установить службу DNS на этом же сервере. Если используется отдельный сервер, то необходимо убедиться, что он поддерживает ресурсные записи Service Location (RFC 2052) и протокол Dynamic Updates (RFC 2136).
3. Необходимо иметь учётную запись с правами локального администратора на сервере.

Рассмотрим подробно повышение роли сервера до контроллера домена Active Directory по шагам:

1. Чтобы запустить мастер повышения статуса сервера необходимо в меню **Start** (Пуск) выбрать **Run...** (Выполнить…), ввести *dcpromo* и нажать OK.
2. После запуска мастера установки Active Directory нажмите *Next* (Далее).
3. На странице **Domain Controller Type** (Тип контроллера домена) выберите вариант **Domain controller for a new domain** (Контроллер домена в новом домене). Нажмите *Next*.



Тип контроллера домена

4. На странице **Create New Domain** (Создать новый домен) выберите вариант **Domain in a new forest** (Новый домен в новом лесу). Нажмите *Next*.
5. На странице **New Domain Name** (Новое имя домена) введите полное (FQDN) DNS-имя для создаваемого нового домена леса Active Directory (например, mydomain.local). Не рекомендуется использовать одиночное (single label) имя домена (например, mydomain). Нажмите *Next*.
6. Проверьте NetBIOS-имя на странице **NetBIOS Domain Name** (NetBIOS-имя домена). Хотя домены Active Directory обозначаются в соответствии со стандартами именования DNS, необходимо так же задать NetBIOS-имя. NetBIOS-имена по возможности должны совпадать с первой меткой DNS-имени домена. Если первая метка DNS-имени домена Active Directory отличается от его NetBIOS-имени, в качестве полного доменного имени используется DNS-имя, а не NetBIOS-имя. Нажмите *Next*.
7. На странице **Database and Log Folders** (Папки базы данных и журналов) введите путь, по которому будут располагаться папки базы данных и журналов, или нажмите кнопку *Browse* (Обзор), чтобы указать другое расположение. Убедитесь, что на диске достаточно места для размещения базы данных каталога и файлов журналов, чтобы избежать проблем при установке или удалении Active Directory. Мастеру установки Active Directory необходимо 250 МБ дискового пространства для установки базы данных Active Directory и 50 МБ для файлов журналов. Нажмите *Next*.
8. На странице **Shared System Volume** (Общий доступ к системному тому) укажите расположение, в которое следует установить папку SYSVOL, или нажмите кнопку *Browse* (Обзор), чтобы выбрать расположение. Папка SYSVOL должна находиться на томе NTFS, так как в ней находятся файлы, реплицируемые между контроллерами домена в домене или лесу. Эти файлы содержат сценарии, системные политики для Windows NT 4.0

и более ранних версий, общие папки NETLOGON и SYSVOL и параметры групповой политики. Нажмите *Next*.

9. На странице **DNS Registration Diagnostics** (Диагностика регистрации DNS) проверьте правильность установки параметров. Если в окне **Diagnostic Results** (Результаты диагностики) отображается сообщение об ошибках диагностики, нажмите кнопку *Help* (Справка) для получения дополнительных инструкций по устранению ошибки. Нажмите *Next*.
10. На странице **Permissions** (Разрешения) выберите требуемый уровень совместимости приложений с операционными системами pre-Windows 2000, Windows 2000 или Windows Server 2003. Нажмите *Next*.
11. На странице **Directory Services Restore Mode Administrator Password** (Пароль администратора для режима восстановления) введите и подтвердите пароль для учетной записи администратора режима восстановления Active Directory для данного сервера. Этот пароль необходим для восстановления резервной копии состояния системы данного контроллера домена в режиме восстановления Active Directory. Нажмите *Next*.
12. Проверьте сведения на странице **Summary** (Сводка) и нажмите *Next*.
13. После завершения установки нажмите кнопку *Finish* (Готово). Для перезагрузки компьютера нажмите кнопку *Restart Now* (Перезагрузить сейчас), чтобы изменения вступили в силу.

Основы управления доменом Active Directory

Ряд средств в оснастках Microsoft Management Console (MMC) упрощает работу с Active Directory.

Оснастка **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) является консолью управления MMC, которую можно использовать для администрирования и публикации сведений в каталоге. Это главное средство администрирования Active Directory, которое используется для выполнения всех задач, связанных с пользователями, группами и компьютерами, а также для управления организационными подразделениями.

Для запуска оснастки Active Directory Users and Computers (Active Directory – пользователи и компьютеры) выберите одноименную команду в меню **Administrative Tools** (Администрирование).

По умолчанию консоль Active Directory Users and Computers работает с доменом, к которому относится Ваш компьютер. Вы можете получить доступ к объектам компьютеров и пользователей в этом домене через дерево консоли или подключиться к другому домену. Средства этой же консоли позволяют просматривать дополнительные параметры объектов и осуществлять их поиск.

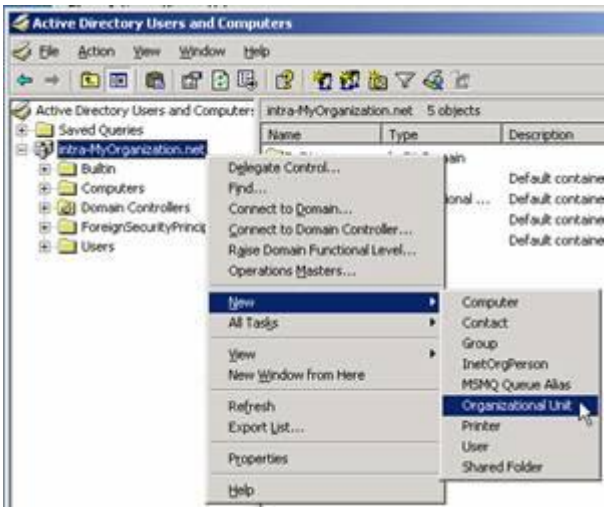
Получив доступ к домену вы увидите стандартный набор папок:

- **Saved Queries** (Сохраненныезапросы) – сохраненные критерии поиска, позволяющие оперативно повторить выполненный ранее поиск в Active Directory;
- **Builtin** – список встроенных учетных записей пользователей;
- **Computers** – контейнер по умолчанию для учетных записей компьютеров;
- **Domain Controllers** – контейнер по умолчанию для контроллеров домена;
- **ForeignSecurityPrincipals** – содержит информацию об объектах из доверенного внешнего домена. Обычно эти объекты создаются при добавлении в группу текущего домена объекта из внешнего домена;
- **Users** – контейнер по умолчанию для пользователей.

Некоторые папки консоли по умолчанию не отображаются. Чтобы вывести их на экран, выберите в меню *View* (Вид) команду *Advanced Features* (Дополнительные функции). Вот эти дополнительные папки:

- **LostAndFound** – потерявшие владельца, объекты каталога;
- **NTDS Quotas** – данные о квотировании службы каталогов;
- **Program Data** – сохраненные в службе каталогов данные для приложений Microsoft;
- **System** – встроенные параметры системы.

Вы можете самостоятельно добавлять папки для организационных подразделений в дерево AD.



OU

Рассмотрим пример создания учётной записи пользователя домена. Чтобы создать учётную запись пользователя щелкните правой кнопкой контейнер, в

который вы хотите поместить учетную запись пользователя, выберите в контекстном меню *New* (Создать), а затем – *User* (Пользователь). Откроется окно мастера *New Object – User* (Новый объект – Пользователь):

1. Введите имя, инициал и фамилию пользователя в соответствующих полях. Эти данные потребуются для создания отображаемого имени пользователя.
2. Отредактируйте полное имя. Оно должно быть уникальным в домене и иметь длину не более 64 символов.
3. Введите имя для входа. С помощью раскрывающегося списка выберите домен, с которым будет связана учетная запись.
4. При необходимости измените имя пользователя для входа в системы с ОС Windows NT 4.0 или более ранними версиями. По умолчанию в качестве имени для входа в системы с предыдущими версиями Windows используются первые 20 символов полного имени пользователя. Это имя также должно быть уникальным в домене.
5. Щёлкните *Next* (Далее). Укажите пароль для пользователя. Его параметры должны соответствовать вашей политике паролей;
   Confirm Password (Подтверждение) – поле, используемое для подтверждения правильности введенного пароля;
   User must change password at next logon (Требовать смену пароля при следующем входе в систему) – если этот флажок установлен, пользователю придется изменить пароль при следующем входе в систему;
   User cannot change password (Запретить смену пароля пользователем) – если этот флажок установлен, пользователь не может изменить пароль;
   Password never expires (Срок действия пароля не ограничен) – если этот флажок установлен, время действия пароля для этой учетной записи не ограничено (этот параметр перекрывает доменную политику учетных записей);
   Account is disabled (Отключить учетную запись) – если этот флажок установлен, учетная запись не действует (параметр удобен для временного запрета использования кем-либо этой учетной записи).

Учётные записи позволяют хранить контактную информацию пользователей, а так же информацию об участии в различных доменных группах, путь к профилю, сценарий входа, путь домашней папки, список компьютеров, с которых пользователю разрешён вход в домен и т.д.

Сценарии входа определяют команды, выполняемые при каждом входе в систему. Они позволяют настроить системное время, сетевые принтеры, пути к сетевым дискам и т.д. Сценарии применяются для разового запуска команд, при этом параметры среды, задаваемые сценариями, не сохраняются для последующего использования. Сценариями входа могут быть файлы сервера сценариев Windows с расширениями .VBS, .JS и другие, пакетные файлы с расширением .BAT, командные файлы с расширением .CMD, программы с расширением .EXE.

Можно назначить каждой учетной записи свою домашнюю папку для хранения и восстановления файлов пользователя. Большинство приложений по умолчанию открывают домашнюю папку для операций открытия и сохранения файлов, что упрощает пользователям поиск своих данных. В командной строке домашняя папка является начальным текущим каталогом. Домашняя папка

может располагаться как на локальном жестком диске пользователя, так и на общедоступном сетевом диске.

К доменным учётным записям компьютеров и пользователей могут применяться групповые политики. Групповая политика упрощает администрирование, предоставляя администраторам централизованный контроль над привилегиями, разрешениями и возможностями пользователей и компьютеров. Групповая политика позволяет:

- создавать централизованно управляемые специальные папки, например My Documents (Мои документы);
- управлять доступом к компонентам Windows, системным и сетевым ресурсам, инструментам панели управления, рабочему столу и меню Start (Пуск);
- настроить сценарии пользователей и компьютеров на выполнение задачи в заданное время;
- настраивать политики паролей и блокировки учетных записей, аудита, присвоения пользовательских прав и безопасности.

Помимо задач управления пользовательскими учётными записями и группами существует масса других задач управления доменом. Для этого служат другие оснастки и приложения.

Оснастка **Active Directory Domains and Trusts** (Active Directory – домены и доверие) служит для работы с доменами, деревьями доменов и лесами доменов.

Оснастка **Active Directory Sites and Services** (Active Directory – сайты и службы) позволяет управлять сайтами и подсетями, а так же межсайтовой репликацией.

Для управления объектами AD существуют средства командной строки, которые позволяют осуществлять широкий спектр административных задач:

- **Dsadd** – добавляет в Active Directory компьютеры, контакты, группы, организационные подразделения и пользователей. Для получения справочной информации введите *dsadd <имя_объекта> /?*, например *dsadd computer/?*
- **Dsmod** – изменяет свойства компьютеров, контактов, групп, организационных подразделений, пользователей и серверов, зарегистрированных в Active Directory. Для получения справочной информации введите*dsmod <имя_объекта> /?*, например *dsmod server /?*
- **Dsmove** – перемещает одиночный объект в новое расположение в пределах домена или переименовывает объект без перемещения.
- **Dsget** – отображает свойства компьютеров, контактов, групп, организационных подразделений, пользователей, сайтов, подсетей и серверов, зарегистрированных в Active Directory. Для получения справочной информации введите *dsget <имя_объекта> /?*, например *dsget subnet /?*
- **Dsquery** – осуществляет поиск компьютеров, контактов, групп, организационных подразделений, пользователей, сайтов, подсетей и серверов в Active Directory по заданным критериям.
- **Dsrm** – удаляет объект из Active Directory.

- **Ntdsutil** – позволяет просматривать информацию о сайте, домене или сервере, управлять хозяевами операций (operations masters) и обслуживать базу данных Active Directory.

Так же существуют средства поддержки Active Directory:

- **Ldp** – Осуществляет в Active Directory Administration операции по протоколу LDAP.
- **Replmon** – Управляет репликацией и отображает ее результаты в графическом интерфейсе.
- **Dsacls** – Управляет списками ACL (списками управления доступом) для объектов Active Directory.
- **Dfsutil** – Управляет распределенной файловой системой (Distributed File System, DFS) и отображает сведения о её работе.
- **Dnscmd** – Управляет свойствами серверов, зон и записей ресурсов DNS.
- **Movetree** – Перемещает объекты из одного домена в другой.
- **Repadmin** – Управляет репликацией и отображает её результаты в окне командной строки.
- **Sdcbeck** – Анализирует распространение, репликацию и наследование списков управления доступом.
- **Sidwalker** – Задает списки управления доступом для объектов, в прошлом принадлежавших перемещенным, удаленным или потерянным учетным записям.
- **Netdom** – Позволяет управлять доменами и доверительными отношениями из командной строки.

Как видно из этой статьи объединение групп компьютеров в домены на базе Active Directory позволяет существенно снизить издержки административных задач за счёт централизации управления доменными учётными записями компьютеров и пользователей, а так же позволяет гибко управлять правами пользователей, безопасностью и массой других параметров. Более подробные материалы по организации доменов можно найти в соответствующей литературе.