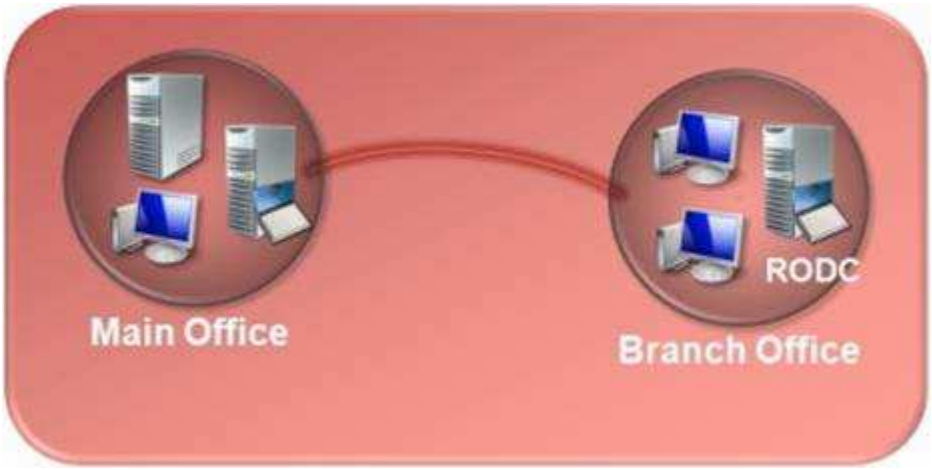
Работа с контроллерами домена Read-Only (RODC)

http://winitpro.ru/index.php/2010/11/21/rabota-s-kontrollerami-domena-read-only-rodc-chast-1/

Contents

Введение

В Windows Server 2008, Microsoft решила вернуть функцию, которую мы не видели со времен Windows NT: это технология контроллеров домена, доступных только для чтения. В этой статье я расскажу про технологию Read Only Domain Controllers и ее преимущества. Я ранее не раз упоминал об этой технологии в своих статьях, например в статье про использование утилиты adprep в Windows 2008.



Хорошим примером циклического характера развития IT технологий является новая функция Windows Server 2008, которая называется Read Only Domain Controller, или RODC. Ведь эта технология впервые появилась уже давно, однако протяжении последних 10 лет практически не применялась.

Windows NT была первой серверной ОС от Microsoft. Как и современные операционные системы Windows Server, Windows NT полностью поддерживала технологию доменов. Одним отличием был тот факт, что только один контроллер домена в каждом домене был доступен для записи. Этот контроллер домена, называемый Primary Domain Controller или PDC, был единственным контроллером домена, в который администратор мог вносить изменения. Основной контроллер домена затем передавал обновления на другие контроллеры домена в домене. Эти контроллеры домена назывались резервными контроллерами домена (backup domain controllers или BDC), и информация на них обновлялась только при обновлении основного контроллера домена, для клиентов домена они были доступны только на чтение.

И хотя эта доменная модель была полностью работоспособной, у нее были и существенные недостатки. В частности, проблемы с основным контроллером домена могли парализовать работу

всего домена целиком. Как вы знаете, Microsoft внесла значительные изменения в доменную модель, которую они внедрили в свою новую серверную ОС Windows 2000 Server. В Windows 2000 Server появились две новые технологии для контроллеров доменов, и оба этих нововведения используются и по сей день: это Active Directory и модель с несколькими основными контроллерами (multi master модель).

И хотя роль PDC все еще сохранялась, остальные контроллеры домена в мульти-мастерной конфигурации были доступными на запись. Это означало, что администратор может внести изменения на любом контроллере домена, и эти изменения в виде обновлений в конечном итоге будут распространены на все другие контроллеры домена в сети.

Затем мульти-мастерная модель была сохранена и в Windows Server 2003 и в Windows Server 2008. Однако, в Windows Server 2008 появилась возможность создавать контроллеры домена только для чтения (Read Only Domain Controllers). RODC – это контроллер домена, информация в котором не может быть изменена непосредственно даже администраторами. Единственный способ обновления этих контроллеров домена — применить изменения на PDC, а затем эти изменения должны быть распространены (реплицированы) на RODC. Ничего не напоминает?

Как вы видите, RODC, являются не чем иным, как пережитком времен Windows NT. Безусловно, Microsoft не вернула бы технологию RODC, если бы не усмотрела бы в их применении существенных преимуществ.

Прежде чем приступить к объяснению того, почему Microsoft решила вновь вернуться к RODC, позвольте мне пояснить, почему использование RODC не является обязательным условием работы с доменами Active Directory в 2008 Server. Если вы хотите, чтобы каждый контроллер домена в вашем лесу был доступен для записи, вы, безусловно, может сделать это.

Я хочу вкратце упомянуть, что несмотря на то, что RODC, очень похожи на резервные контроллеры домена (BDC) в NT, они претерпели ряд изменений. Есть несколько вещей, которые являются новинками в технологии RODC, и я хочу о них рассказать.

Итак, почему Microsoft решила вернуть RODC? Это связано с проблемами поддержки филиальной сети (подразделений и филиалов). Офисы филиалов традиционно достаточно трудно сопровождать и поддерживать из-за их удаленности и особенностей связи между головным офисом и филиалом.

Традиционно применялось несколько различных способов управления филиалами, но каждый из них имел свои собственные преимущества и недостатки. Одним из наиболее распространенных способов организации филиальной сети является установка всех серверов в главном офисе, и предоставление доступа к ним пользователей филиала через глобальную сеть (WAN).

Конечно, наиболее очевидным недостатком такого метода является то, что если канал WAN нестабилен или отвалился, то пользователи, которые находятся в филиале, не в состоянии нормально работать, т.к. они полностью отрезаны от всех ресурсов центрального офиса. Даже если сетевое соединение с головным офисом стабильно, зачастую производительность WAN соединения может быть невысока из-за нагрузки на канал или непосредственно скорости соединения

Другим распространенным вариантом при работе с удаленными филиалами является подход, предусматривающий установку по крайней мере одного контроллера домена в филиал. Часто, этот контроллер домена также выступает в качестве сервера DNS и сервера глобального каталога. Таким образом, даже если WAN подключение разрывается, то пользователи в филиале, по крайней мере, имеют возможность войти в сеть. В зависимости от характера работы организации, в филиальном подразделении могут устанавливать и другие сервера.

Хотя это решение, как правило, работает довольно неплохо, и у него есть ряд недостатков. Основным недостатком является стоимость. Размещение серверов в филиалах требует от предприятия вкладывать деньги в серверное оборудование и лицензии на программное обеспечение. Существенно увеличиваются также затраты на поддержку. Организация должна определить, нужен ли в филиале штат собственных ИТ-специалистов, или в случае неполадок, она готова ждать пока ИТ-персонал из центрального офиса доберется в филиал.

Еще один нюансом при установке собственных серверов в филиале, является вопрос безопасности. В моем опыте нередки случаи, при которых сервера, которые расположены за пределами центрально датацентра, оставались банально без присмотра. Часто сервера просто закрывают в шкафу на ключ!

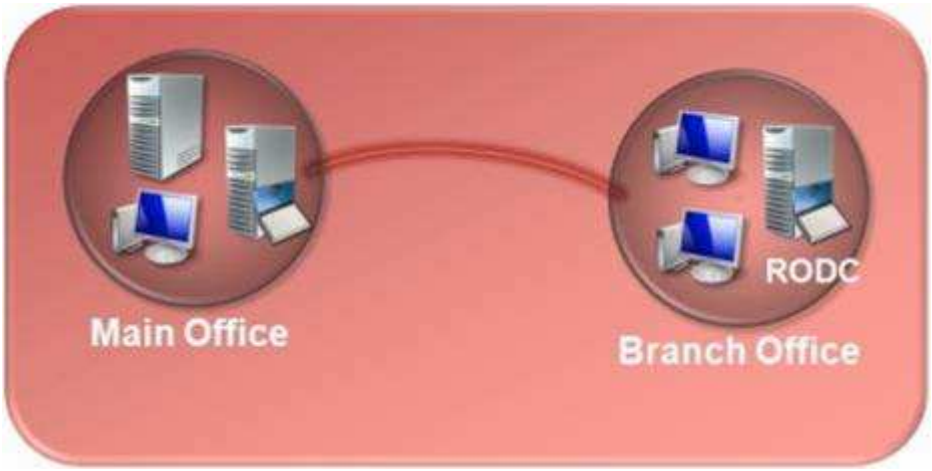
Как я упоминал ранее, WAN соединения часто бывают медленным и ненадежным. В этом кроется еще одна проблема с размещением серверов в филиале. Трафик репликации контроллеров домена может существенно загрузить такое соединение

Вот это как раз тот случай, когда можно использовать RODC. Размещение RODC в филиал не избавляет совсем от трафика репликации Active Directory, но существенно снижает нагрузку на bridgehead сервера, т.к. они получают только входящий трафик репликации.

RODC могут также способствовать повышению безопасности, ведь персонал в офисе филиала не сможет внести изменения в базу данных Active Directory. Кроме того, никакой информации обо всех пользователях домена и их учетках, не передаются на RODC. Это означает, что если кто-то украл сервер RODC, он не сможет воспользоваться информацией, полученной в результате взлома паролей пользователей.

В следующих статьях этой серии, мы обсудим процесс планирования и развертывания контроллеров домена, доступных только для чтения.

В моей предыдущей статье я объяснил основные причины, по которым Microsoft решила вернуться к технологии RODC в Windows Server 2008. Эта статья продолжает серию, и мы перейдем к изучению некоторых практических аспектов работы с Read Only Domain Controllers.



Учетные данные пользователя

В предыдущей статье я сказал, что на RODC контроллеры домены не передается вся информация обо всех пользователях домена. На самом деле информация о учетных записях пользователей все-таки хранится на RODC, на такой контроллер домена просто не выполняется репликация паролей пользователей. И если кто-то украдет контроллер домена из филиала, он не сможет использовать информацию из базы данных Active Directory для получения паролей пользователей.

Атрибуты пользователей

По умолчанию пароли, это единственный атрибут пользователей, который не реплицируются на Read Only Domain Controller. Тем не менее, существует возможность ручной настройки Windows, позволяющей запретить реплицироваться и другие атрибуты пользователей.

Так в каких случаях можно использовать эту функцию? Если вы используете Active Directory только в качестве механизма аутентификации, то вероятнее всего, вам она не понадобится. Однако имейте в виду, что есть организации, которые сильно зависят от базы Active Directory, которая применяется не только для аутентификации.

Достаточно часто в крупных организация, в которых используются различные пользовательские приложения и базы данных, для уменьшения количества ошибок и дублирования пользовательской информации, предпочитают использовать единое место хранения всей информации о сотрудниках (телефоны, адреса, контакты и т.д.), и отличным местом для этого является Active Directory.

Например, я знаю одну организацию, которая разработала приложение для управления кадрами, которое они применяют внутри своего периметра. И хотя основная часть данных хранится в базе данных SQL, но такие вещи, как имена сотрудников, должности, номера телефонов и т.д. хранятся в Active Directory, в качестве атрибутов учетной записи. А в базе SQL Servera хранятся такие данные, как номера ИНН, информация о зарплате, и в этой базе не содержатся имена сотрудников. Единственно, что связывает базы данных AD и SQL – это номер сотрудника, который присутствует в обеих базах данных.

Я привел вам этот пример для того, чтобы было понятно, что в ряде организаций в атрибутах пользователя AD может содержаться конфиденциальная информация. И в том случае, если такая информация не требуется в филиале, вы можете заблокировать ее репликацию на контролер домена филиала.

Еще одной особенностью технологии Read Only Domain Controller является то, что такой контроллере также может быть настроен как DNS сервер, доступный только на чтение. По существу это означает, что если злоумышленник получит доступ к серверу Read Only Domain Controller, он не сможет парализовать работу корпоративного DNS.

Административные вопросы

Я уверен, что к настоящему времени у вас появилось множество вопросов об администрировании rodc. Попробую сразу ответить на часть из них.

Как же аутентифицируются пользователей, если на контроллере домена нет информации об их паролях?

Здесь есть хитрость. Как вы знаете, и с учетной записью пользователя и с учетной записью компьютера ассоциирован пароль. По умолчанию, Read Only Domain Controller хранит только свой собственный пароль (пароль учетки компьютера) и пароль специального аккаунта, под названием «krbtgt», который используется протоколом Kerberos.

Т.к. пароли локально не хранятся, все запросы на аутентификацию перенаправляются на обычный контроллер домена, запись на который разрешена. В том случае, если вы хотите, чтобы пользователи могли зайти в системы, даже если ни один обычный контроллер не доступен, вам необходимо включить функцию кэширования паролей. При включенном кэшировании в кэше будут храниться пароли только тех учеток, которые прошли проверку подлинности на контроллере домена. И даже если ваш домен контроллер будет скомпрометирован, вы с другого

контроллера можете всегда выявить те учетные записи, пароли которых были кэшированы на rodc.

Административная работа с rodc

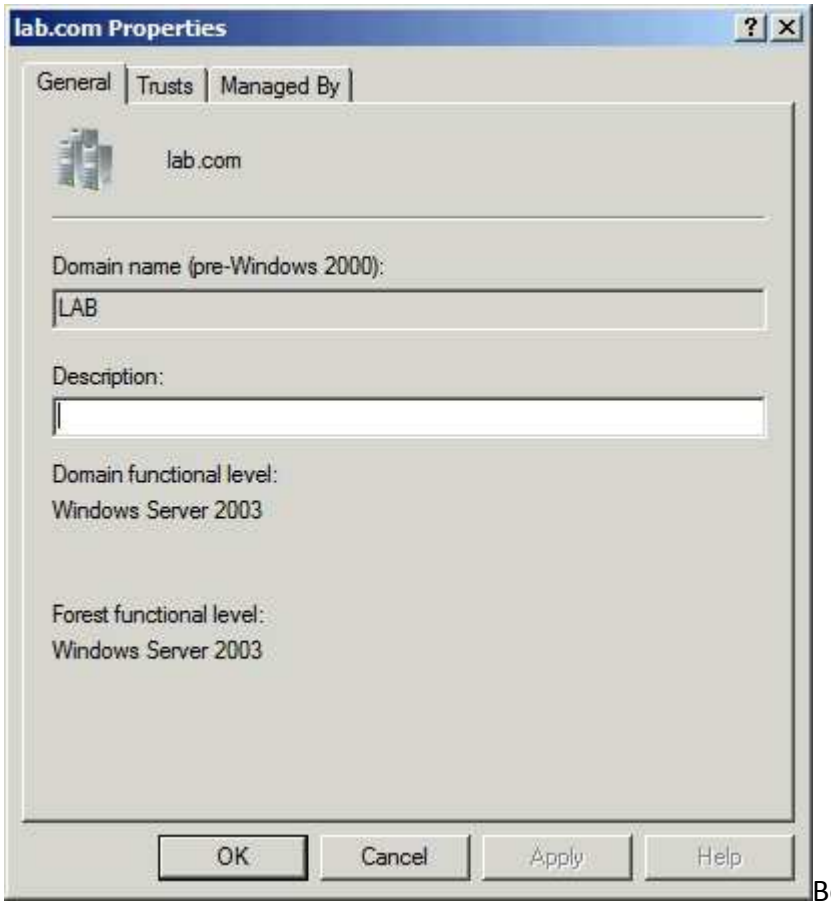
Во многих филиальных офисах зачастую контроллер домена используется еще и в качестве сервера приложений. И в том случае, если в таком офисе нет отдельного ИТ специалиста, вы можете назначить кого-то из сотрудников офиса в качестве администратора rodc контроллера, не предоставляя ему прав администратора всего домена (можете почитать пост о делегировании прав управления контроллером домена rodc). Таким образом, он будет иметь права только на локальное администрирование такого сервера, и не будет иметь возможности что-то изменить или испортить в Active Directory. В результате такой пользователь будет иметь права на установку обновлений ПО и выполнение других повседневных задач по администрированию и обслуживанию сервера. Назначение кого-то администратором Read Only Domain Controller похоже на процедуру назначения определенного пользователя или группы в качестве локального администр В прошлых статьях этого цикла (rodc часть 1, и работа с rodc часть 2) вы поговорили о теории и преимуществах новой технологии от Microsoft, которая называется Read Only Domain Controller. В этой статье я расскажу о процедуре развертывания такого контроллера домена.

Перед началом работы

В начале на свой сервер, который вы планируете использовать в качестве RODC, вы должны установить ОС Windows Server 2008 и присоединить его к домену AD. Технически возможно создать Read Only Domain Controller из сервера, который первоначально не включен в домен, однако в своей статье я описываю случай, когда этот сервер уже является рядовым сервером домена.

Функциональный уровень леса

Прежде чем начать, вы должны убедиться, что функциональный уровень леса у вас Windows Server 2003 или выше. Для этого откройте оснастку «Active Directory Domains and Trusts». В окне консоли щелкните правой кнопкой мыши по вашему лесу Active Directory, и выберите команду «Properties» из появившегося контекстного меню. На рисунке видно, что функциональный уровень леса отображен на вкладке «General».



Возможно в вашем случае придется [подготовить домен для установки Windows Server 2008/R2](). Если уровень леса является недостаточным, вы должны поднять его. Имейте в виду, что это означает, что вы больше не сможете использовать контроллеры домена Windows 2000 в своем лесу.

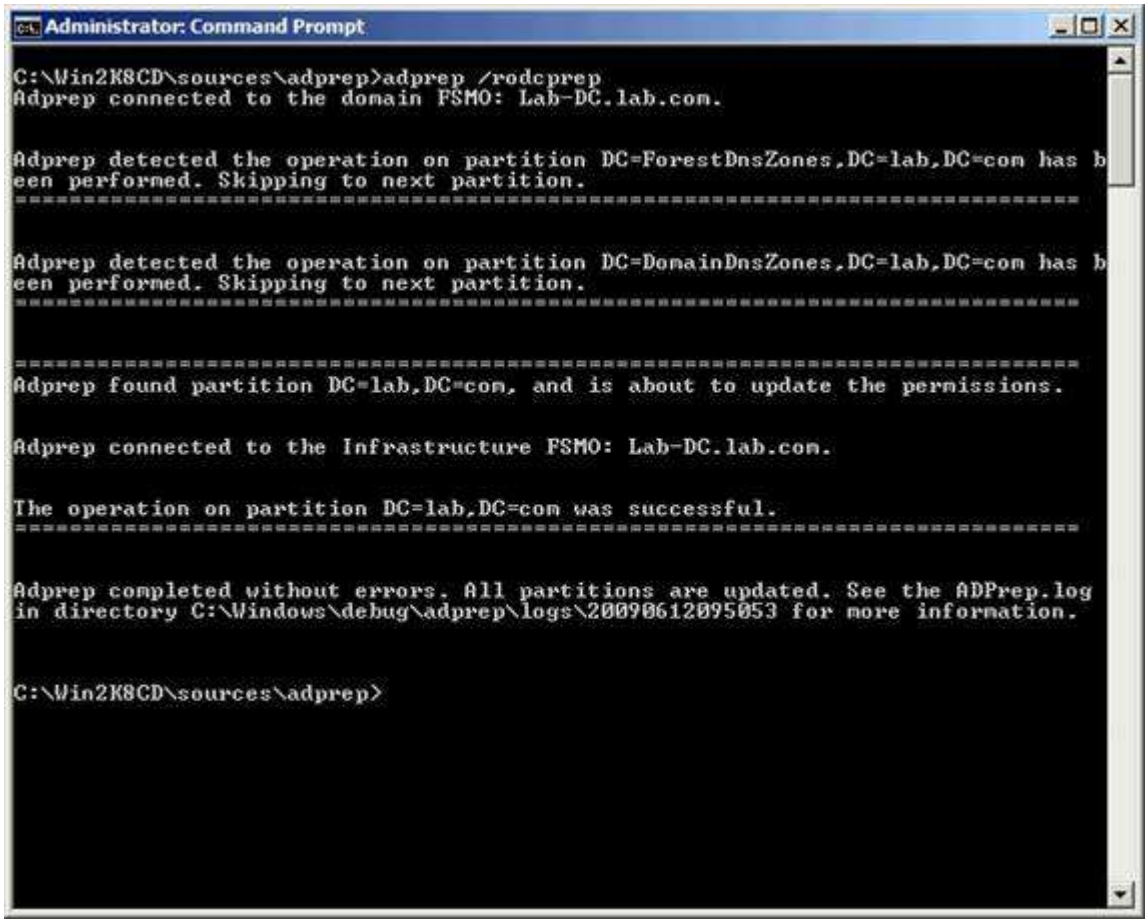
Итак, чтобы повысить уровень леса AD, еще раз нажмите правой клавишей по своему лесу и выберите команду «Raise Forest Functional level», в появившемся окне выберите «Windows Server 2003» и нажмите кнопку Raise.

Обновление разделов Application Directory

На следующем этапе вы должны обновить разрешения на все ветки приложений (application directory) в вашем лесу. В результате чего появится возможность управления репликацией этих разделов на Read Only Domain Controller.

Для этого вставьте ваш дистрибутив с Windows Server 2008 в контроллер домена, который был назначен в качестве хозяина схемы (schema master). Далее, скопируйте с дистрибутива папку \Sources\Adprep в любую папку на жестком диске сервера. Наконец, откройте окно командной строки и перейдите в только что созданную папку ADPREP, и выполнить следующую команду:

ADPREP /RODCPREP



Повышение сервера до контроллера домена

Процесс преобразования простого сервера в Read Only Domain Controller очень похож на процедуру создания обычного контроллера домена.

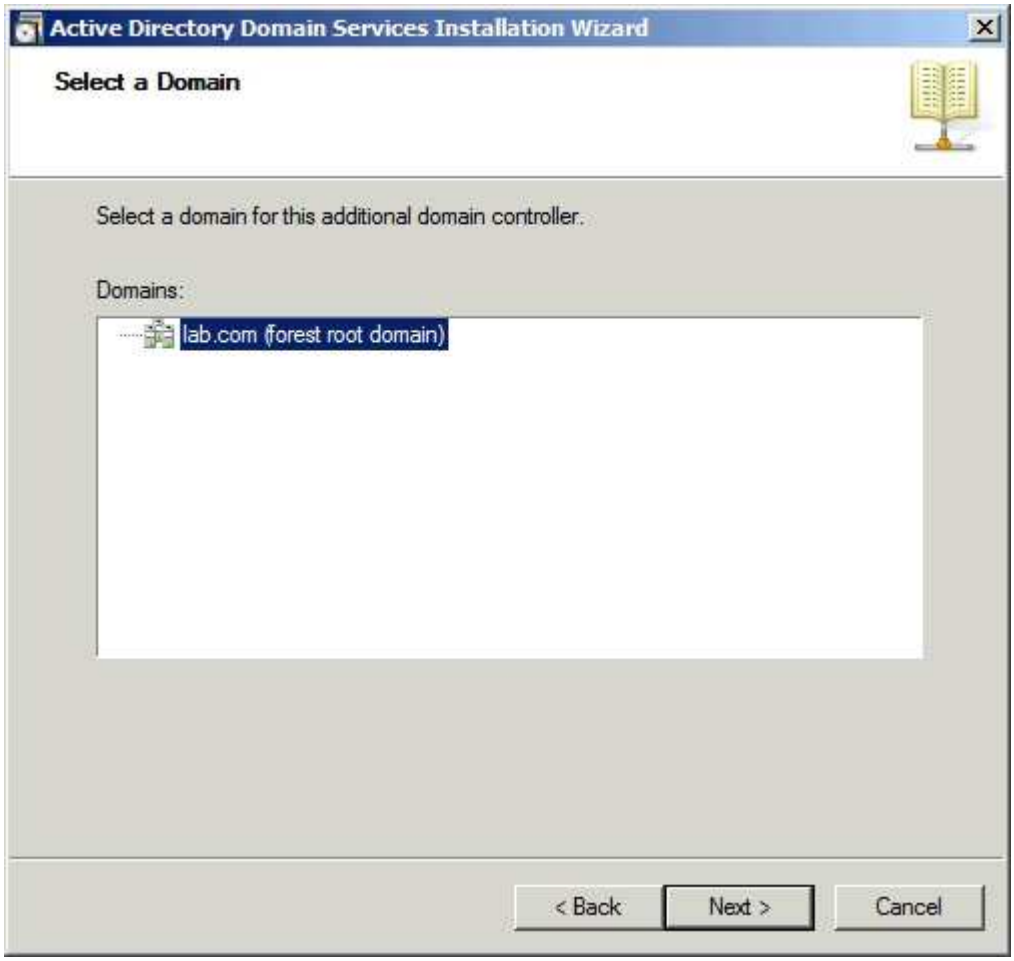
Сначала зайдите на сервер с учетной записью, которая является членом группы администраторов домена (Domain Admins). В командной строке наберите DCPROMO. В результате запустится мастер установки Active Directory Domain Services.

На первом экране мастера отметьте галочкой флажок «Use Advanced Mode Installation» и нажмите «Далее».

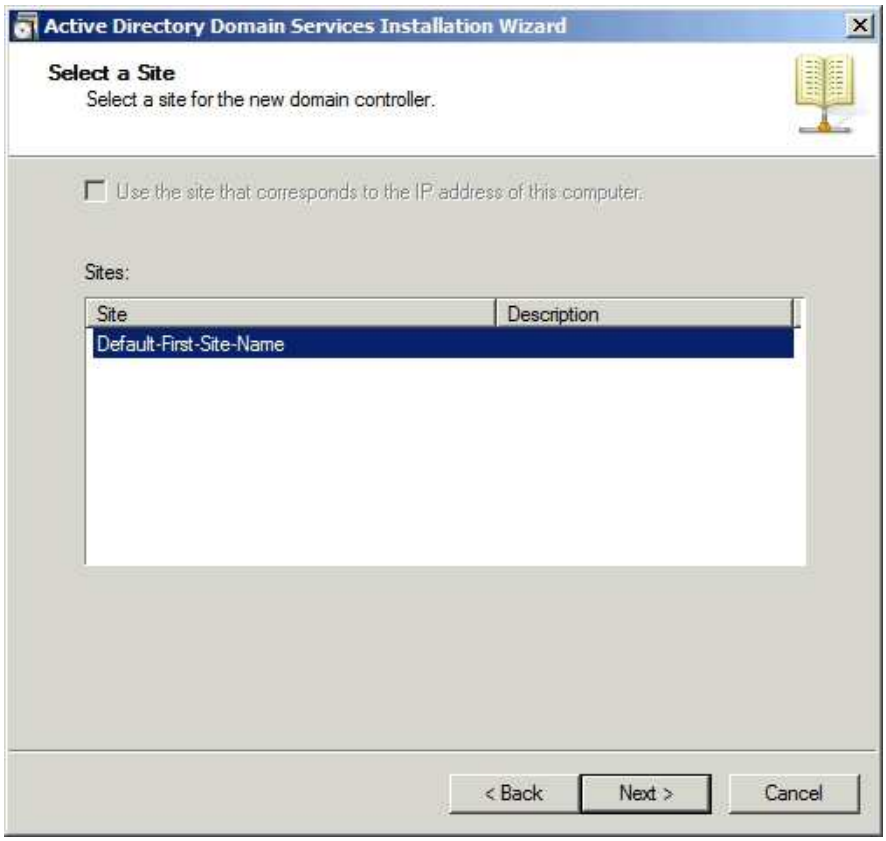
Мастер спросит вас о том, для какого домена вы планируете установить контроллер. Выберите опцию – добавить контроллер домена в существующий домен (add the domain controller to an existing domain).

Нажмите кнопку «Далее», и мастер попросит вас указать имя домена, в который вы планируете добавить контроллер домена. Введите имя вашего домена в соответствующее окно.

Следующее окно является немного избыточным, в нем вы подтверждаете выбор домена.

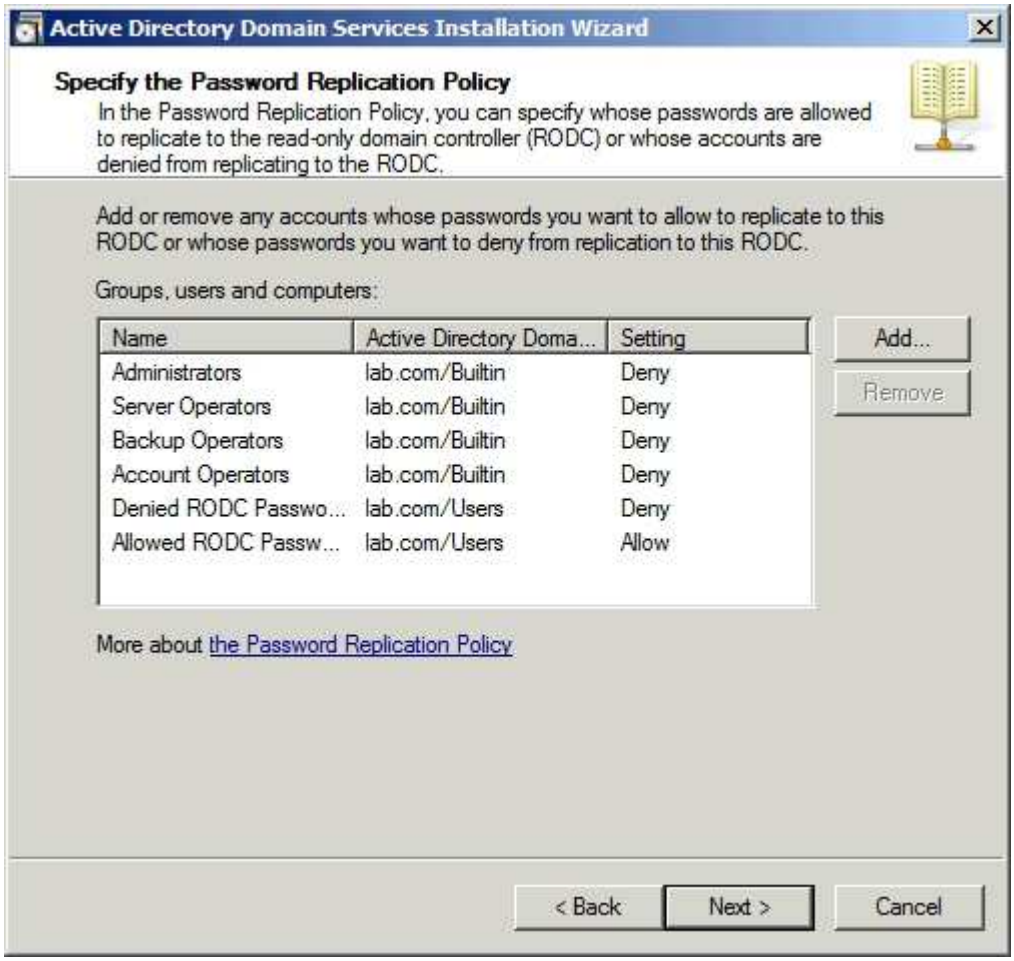


В следующем окне мастера вам нужно будет указать сайт AD, в который вы хотите поместить новый контроллер домена. Данное окно особо важно при размещении нового контроллера домена в филиале, ведь, как правило, филиалы находятся в отдельных сайтах Active Directory.



Далее вам будет предложено выбрать дополнительные опции для контроллера домена. Очевидно, что вам нужно отметить галочкой опцию «Read Only Domain Controller», но также было бы неплохо сделать этот контроллер DNS сервером и сервером глобального каталога.

В следующем окне мастера установки контроллера домена вам будет необходимо выбрать политику репликации паролей, здесь вы должны указать какие пароли могут быть реплицированы на Read Only Domain Controller. Вы можете указать свои настройки, но обычно настройки по умолчанию, достаточно правильны.



Нажмите далее, и вам будет предоставлена возможность делегировать пользователю или группе права на управление сервером RODC (процедуру делегирования прав на rodc можно выполнить и позже).

На следующем экране вы сможете указать хотите ли выполнить репликацию данных по сети с ближайшего контроллера домена или вы хотите создать базу данных Active Directory из файла. Создание базы данных Active Directory из файла удобно в случаях, если у вас достаточно большая база данных и медленное соединение.

В следующем окне будет предложено выбрать партнера репликации для контроллера домена. Как правило, система автоматически выберет оптимального партнера по репликации.

После нажатия кнопки «Next», вы попадете в знакомый вам экран, в котором необходимо выбрать местохранения базы данных Active Directory. Выберите необходимый путь к БД и нажмите кнопку «Далее».

Далее вам будет предложено указать пароль для режима восстановления службы каталогов (Directory Services Restore Mode). Введите пароль и нажмите кнопку Далее.

Следующее окно будет результирующим, на нем вы сможете просмотреть все указанные вами настройки. После нажатия кнопки Next начнется процесс установки контроллера домена. После его окончания вам будет предложено перезагрузить сервер.

Вот и все контроллер домена RODC установлен и работоспособен! Теперь после установки первого сервера RODC, вы можете установить дополнительные контроллеры RODC, но прежде чем приступить к этому процессу вы должны дождаться цикла репликации AD, в противном случае вы получите массу различных ошибок в Active Directory.