KAK - Работаем с Windows Server 2008 без ошибок в AD

http://www.osp.ru/win2000/2012/04/13016766/

Ошибки Adprep и Dcpromo не застанут врасплох

Джастин Холл

Иногда при установке служб Microsoft Active Directory Domain Services (AD DS) в среде Windows Server 2008 или Server 2008 R2 возникают две проблемы. Одна из них относится к процессу установки; другая связана с рекомендациями компании Microsoft по запуску контроллеров домена (DC) на виртуальных машинах.

Эти проблемы известны опытным администраторам. Но начинающим специалистам, которым необходимо заменить операционную систему контроллера домена с Windows Server 2003 на Server 2008 R2, будет очень полезна эта статья, в которой я планирую рассмотреть все возможные трудности и пути их преодоления.

Ошибки, связанные с Adprep

Adprep — утилита для подготовки существующей среды Active Directory (AD) для первого DC, функционирующего с новой операционной системой, например Server 2008 R2. Если все контроллеры домена в среде AD работают с Server 2008 или Windows 2003 и требуется добавить первый DC с операционной системой Server 2008 R2, необходимо выполнить определенные команды Adprep.

1. Выполните adprep/forestprep на хозяине схемы.
2. Выполните adprep/domainprep на каждом хозяине инфраструктуры домена.
3. Если предполагается установить доступный только для чтения DC (RODC — новшество Server 2008), следует также выполнить adprep/rodcprep для каждого домена с RODC.

Этот достаточно простой процесс подробно описан в Интернете, но тем не менее у администраторов часто возникают вопросы:

- какие именно действия выполняет Adprep?
- как убедиться, что все необходимые команды Adprep выполнены успешно?
- как исправлять возникающие ошибки?

В статье Microsoft «Running Adprep.exe» (technet.microsoft.com/en-us/library/dd464018%28WS.10%29.aspx) эти вопросы разъясняются, а также описываются общее назначение утилиты, процесс запуска необходимых команд и методы проверки результатов работы программы. Чтобы выяснить, какие именно изменения вносит Adprep при подготовке существующей AD, можно прочитать статьи Microsoft «Windows Server 2008: Appendix of Changes to Adprep.exe to Support AD DS» (technet.microsoft.com/en-us/library/cc770703%28WS.10%29.aspx) и «Windows Server 2008 R2: Appendix of Changes to Adprep.exe to Support AD DS» (technet.microsoft.com/en-us/library/dd378876%28WS.10%29.aspx).

При запуске Adprep необходимо учитывать следующие важные факторы.

- ***Учетные данные.*** Приготовьтесь указать необходимые учетные данные для каждой команды Adprep. В зависимости от команды, требуются данные для учетной записи, которая является членом группы Schema Admins, Enterprise Admins или Domain Admins.
- ***Роли хозяина операции FSMO.*** Необходимо выполнить Adprep на хозяине схемы леса и на хозяине инфраструктуры в домене, в котором устанавливается новый DC. Обратите внимание, что команду следует запускать с диска DVD с новой операционной системой на хозяине операций или скопировать утилиту Adprep и содержимое ее папки с диска DVD перед ее запуском. Во врезке «Особенности Adprep» содержится предупреждение относительно хозяина схемы. В состав Server 2008 R2 входят как 32-, так и 64-разрядная версии Adprep (в папке \support\adprep на диске операционной системы). По умолчанию запускается 64-разрядная версия. При работе с 32-разрядной операционной системой следует использовать Adprep32.exe.
- ***Репликация.*** Убедитесь, что репликация работает во всем лесу. Дополнительные сведения о диагностике репликации AD приведены в статьях «Troubleshooting Active Directory Replication» (www.windowsitpro.com/article/activedirectory/troubleshooting-activedirectory-replication) и «Active Directory Replication In Depth» (www.windowsitpro.com/article/activedirectory/gain-a-better-understandingof-exactly-how-active-directoryreplication-works-135815).

Если подготовиться к возможным проблемам и выполнять рекомендации, приведенные в указанных выше статьях, то, скорее всего, сбоев удастся избежать. Однако в некоторых случаях в ходе выполнения Adprep могут возникать следующие ошибки.

- Сбой Rodcprep, если хозяин инфраструктуры раздела DNS назначен не имеющему прав или недействительному владельцу FSMO. У каждого раздела каталога приложений леса есть хозяин инфраструктуры, и команда Rodcprep обращается к каждому из них. Ошибка Rodcprep возникает, если хозяин инфраструктуры назначается удаленному DC. Например, DC мог быть переведен в состояние рядового сервера, но при этом не учтено, что ему назначена роль хозяина инфраструктуры раздела приложения. Это обнаружится, когда при выполнении Rodcprep возникнет ошибка. В статье Microsoft «Error message when you run the 'Adprep/rodcprep' command in Windows Server 2008: 'Adprep could not contact a replica for partition DC=DomainDnsZones, DC=Contoso, DC=com'» (support.microsoft.com/kb/949257) приведен скрипт для устранения этой ошибки.
- Ошибка «Атрибут с таким идентификатором ссылки уже существует» может возникнуть при выполнении команды adprep/forestprep на компьютере Windows 2003. Эта ошибка случается, если попытаться добавить с помощью команды adprep/forestprep новый объект к разделу схемы с использованием идентификатора ссылки, уже назначенного существующему объекту в этом разделе. Решение данной проблемы описано в статье Microsoft «An error occurs when you run the ADPREP/FORESTPREP command on a Windows Server 2003-based computer: 'An attribute with the same link identifier already exists'» (support.microsoft.com/kb/969307).

В целом процесс модернизации Server 2008 или Server 2008 R2 описан в статье Microsoft «Upgrade Domain Controllers: Microsoft Support Quick Start for Adding Windows Server 2008 or Windows Server 2008 R2 Domain Controllers to Existing Domains» по адресу technet.microsoft.com/en-us/library/upgrade-domaincontrollers-to-windows-server-2008-r2(WS.10).aspx.

Ошибка делегирования DNS

После успешного завершения Adprep можно установить в существующей среде AD первый DC, работающий с Server 2008 или Server 2008 R2. Если определить роль сервера DNS в ходе установки DC, можно увидеть предупреждение, показанное на экране 1: «Делегирование для этого DNS-сервера невозможно, поскольку полномочная родительская зона не найдена или не использует DNS-сервер Windows. При объединении с существующей инфраструктурой DNS следует вручную создать делегирование для этого DNS-сервера в родительской зоне, чтобы обеспечить надежное разрешение имен за пределами домена ‘treyresearch5.net’. В противном случае никаких действий не требуется».

Экран 1. Ошибка делегирования DNS

До появления Server 2008 многие проблемы с AD были вызваны внутренними неполадками в инфраструктуре DNS, в частности отсутствующими или неправильными записями делегирования DNS. Одной из целей специалистов Microsoft при совершенствовании установки служб AD DS в Server 2008 было помочь потребителям в начальной настройке правильной инфраструктуры DNS, а затем облегчить обслуживание данной конфигурации.

С этой целью мастер установки служб AD DS (Dcpromo) в Server 2008 и более новых версиях автоматически пытается создать делегирование DNS при построении нового леса. Делегирование DNS помогает клиентам из других доменов распознавать имена узлов в домене нового DC. Если возможность пользователей в других доменах и в Интернете распознавать запросы имен DNS для компьютеров в локальном домене не важна, можно игнорировать сообщение, используемое Dcpromo для создания делегирования DNS; просто нажмите кнопку Yes при появлении сообщения.

Сообщение появляется, когда выполняются три условия:

- утилита Dcpromo настроена для установки роли DNS-сервера;

- слишком мало отношений делегирования существует между DNS-серверами и непосредственной родительской зоной DNS и поддоменом, в котором устанавливается новый DC;
- устанавливаемый DC не может создать делегирование поддомену DNS на DNS-сервере для родительской зоны.

Dcpromo пытается создать делегирование, чтобы компьютеры в других доменах могли распознавать запросы DNS для узлов, в том числе контроллеров домена и компьютеров — членов домена, в поддомене DNS. Dcpromo может автоматически создавать такие отношения делегирования только на DNS-серверах Microsoft; попытка завершится неудачей, если родительская зона домена DNS находится на сторонних DNS-серверах, таких как BIND.
Эта ошибка появляется при установке контроллеров домена в корневых доменах леса с именами, которые состоят из двух или трех частей (например, contoso.com или corp.contoso.com) и находятся в отношениях непосредственного подчинения с интернет-доменами верхнего уровня, такими как. com, .gov, .biz, .edu, или доменами с двухбуквенными обозначениями стран, такими как .nz и .au. Если домен AD предстоит зарегистрировать в Интернете ко времени его продвижения, появление этой ошибки может указывать на то, что интернет-провайдер или поставщик DNS-хостинга пока не создал необходимого делегирования для поддомена AD.
Эта ошибка также возможна при создании контроллеров домена в корневом домене леса, подчиненного пространству имен существующей корпоративной распределенной сети. Например, если DNS-серверы BIND владеют внутренним доменом contoso.com, то данная ошибка возникнет, когда Dcpromo попытается создать делегирование из contoso.com в поддомен corp.contoso.com корневого домена леса AD.
Чтобы организовать делегирование на полномочных DNS-серверах в родительском домене, должны быть выполнены следующие условия.

- На родительском DNS-сервере должна функционировать служба Microsoft DNS Server.
- DNS-сервер Microsoft в родительском домене должен быть подключен к сети и доступен с устанавливаемого контроллера домена.
- Пользователь, запускающий утилиту Dcpromo на устанавливаемом контроллере домена, должен иметь учетные данные Domain Admins, Enterprise Admins или DNS Admin в родительской зоне DNS.

Учитывая, что многие домены AD не числятся в реестре Интернета, а DNS-серверы для доменов верхнего уровня (TLD) работают с BIND, можно спокойно игнорировать это сообщение об ошибке и нажать кнопку Yes, продолжив повышение уровня.
Если между родительским доменом и повышаемым поддоменом должно существовать делегирование, можно создать и проверить делегирование до и после повышения. Нет оснований откладывать повышение уровня нового DC, который выдает ошибку. Чтобы избежать сообщений об ошибках при будущих операциях повышения уровня, выполните одно из перечисленных ниже действий.

- Заранее создайте делегирование на сторонних DNS-серверах в непосредственном родительском домене.
- Убедитесь, что повышаемые контроллеры домена подключены к сети и располагают необходимыми административными учетными данными для создания делегирования зоны на DNS-серверах Microsoft, на которых размещается родительская зона DNS.
- Укажите аргумент /CreateDNSDelegation: No в командной строке Dcpromo или файле ответов.

Дополнительные сведения о делегировании DNS можно найти в статье Microsoft «Understanding Zone Delegation» (technet.microsoft.com/en-us/library/cc771640.aspx). Если делегирование зоны в конкретной ситуации невозможно, рассмотрите иные методы разрешения имен из других доменов для узлов в своем домене. Например, администратор DNS другого домена может настроить условное перенаправление, зоны-заглушки или вторичные зоны для разрешения имен в вашем домене. В следующих статьях Microsoft эти методы разъясняются подробнее:

- «Understanding Zone Types» (go.microsoft.com/fwlink/?linkid=157399);
- «Understanding stub zones» (go.microsoft.com/fwlink/?linkid=164776);
- «Understanding forwarders» (go.microsoft.com/fwlink/?linkid=164778).

Виртуальные DC и возврат USN
Компания Microsoft опубликовала рекомендации по запуску контроллеров домена на виртуальных машинах (см. статью «Running Domain Controllers in Hyper-V» по адресу technet.microsoft.com/en-us/library/virtual_active_directory_domain_controller_virtualization_hyperv%28WS.10%29.aspx), но некоторые администраторы, запускающие виртуальные контроллеры домена, испытывают затруднения при возврате

номера последовательного обновления USN. Эти проблемы часто бывают вызваны неправильным восстановлением виртуальной машины. Например, установлено, что ошибки репликации связаны с возвратом USN, который получился в результате восстановления из моментального снимка виртуального контроллера домена.
Только поддерживаемые решения резервного копирования, такие как Windows Server Backup, могут быть использованы для восстановления контроллера домена. Недавно компания Microsoft пересмотрела рекомендации по запуску контроллеров домена на виртуальных машинах, в частности объяснено функционирование USN и способы предотвращения возврата USN. Благодаря этим изменениям информация представлена в более краткой и ясной форме, и администраторам будет проще избежать проблем.

Ошибка The Specified User Already Exists

В некоторых случаях установка AD на сервере рабочей группы может закончиться сбоем, а на странице Summary появится следующее сообщение об ошибке: «Не удалось выполнить операцию: не удалось присоединить этот компьютер к <целевому домену>. ‘Указанный пользователь уже существует’».
В этой ситуации в файле dcpromoui.log, сохраненном в папке \%windir%\debug, содержится текст, показанный в листинге 1.
Чаще всего эта ошибка указывает на то, что имя узла повышаемого сервера — такое же, как у другого контроллера домена. Для устранения этой проблемы выполните следующие шаги.

1. Если выполняется замена ранее пониженного DC новым контроллером домена с тем же именем, обязательно удалите метаданные старого DC. В Server 2008 и более новых версиях самый простой способ удаления метаданных — через оснастки AD. При необходимости можно воспользоваться и старым методом — Ntdsutil.
2. Если по-прежнему происходят сбои Dcpromo с этой ошибкой, выясните в файле dcpromoui.log имя исходного DC (он же вспомогательный DC), используемого новым DC для репликации. Найдите в файле раздел, который начинается с метки A в листинге 2. Имя исходного DC показано во фрагменте с меткой B.
3. Убедитесь, что исходный DC выполнил входящую репликацию удаления метаданных DC (то есть конфликтующих учетной записи компьютера DC и объектов параметров NTDS). Если учетная запись контроллера домена все еще существует, определите причину:

- простая задержка репликации; например, DC находится на расстоянии нескольких переходов от DC, запустившего операцию очистки метаданных;
- сбой входящей репликации на вспомогательном DC или на исходном DC, с которого вспомогательный DC получает изменения;
- вспомогательный DC в «сайте задержки» преднамеренно настроен на входящую репликацию изменений в AD с задержкой.

У ошибки могут быть и другие причины, кроме конфликта учетных записей компьютера. В следующих статьях Microsoft рассматриваются некоторые из них:

- «'Computer <name> is already in use' error message when you add user names in Windows 2000 or Windows Server 2003» (support.microsoft.com/kb/266633);
- «Error Message 'lsass.exe-System Error' After Running the Dcpromo.exe Program» (support.microsoft.com/kb/273875);
- «You cannot add a user name or an object name that only differs by a character with a diacritic mark» (support.microsoft.com/kb/938447).

Иногда сбой Dcpromo происходит при попытке создать объект NTDS для DC. В этом случае несколько ошибок могут приводить к отображению одного и того же сообщения; истинную причину можно выявить с помощью расширенной информации об ошибке. Ищите текст «Не удалось выполнить операцию…» или «Active Directory не удается создать объект NTDS…».
Например, сбой Dcpromo может сопровождаться следующим сообщением на экране: «Не удалось выполнить операцию: Active Directory не удается создать объект NTDS для данного контроллера домена <путь DN объекта NTDS> на удаленном контроллере домена <полное имя компьютера исходного контроллера домена>. Убедитесь, что заданные сетевые учетные данные обладают достаточными разрешениями. <%Расширенная строка ошибки%>». Учтите, что шаблонный текст «Убедитесь, что заданные сетевые учетные данные обладают достаточными разрешениями» может ввести в заблуждение; невозможность создать объект NTDS не обязательно связана с недостаточными правами учетной записи. В таблице 1 перечислены возможные расширенные строки ошибок для этого сообщения.

Таблица 1. Возможные строки расширения ошибок

Строка ошибки	Код ошибки в десятичном формате	Код ошибки в шестнадцатеричном формате	Устранение
Отказано в доступе	5	5	Проверьте системное время, в том числе ГГ, ММ, ДД, АМ/ РМ + часовой пояс, для точного соответствия между новой репликой, Центром распространения ключей (KDC) и вспомогательным DC. Исправьте время, перезагрузите повышенный DC и повторите операцию. Также проверьте назначение прав пользователей
Сделана попытка добавить к каталогу объект с уже существующим именем	8305	0x2071	См. статью Microsoft «Error message when you re-install ISA Server 2004 and CSS on a computer that is a member of an ISA Server array» по адресу support.microsoft.com/kb/925883
Не удается найти контроллер домена	1908	0x774	KDC отключен. Проверьте, что служба KDC работает и настроена на автоматический запуск. Перезагрузитесь в правильной конфигурации. См. статью Microsoft «How to force Kerberos to use TCP instead of UDP in Windows» по адресу support.microsoft.com/kb/244474
Службе каталогов не удается выполнить запрошенную операцию, поскольку выполняется операция переименования домена	Неприменимо	Неприменимо	Проблема может быть вызвана недавно завершенной или текущей операцией переименования домена. См. статью Microsoft «Error message when you use the Active Directory Installation Wizard to add a member server in a Windows Server 2003 SP1 domain» по адресу support.microsoft.com kb/936918

Еще одна распространенная причина сбоя установки AD заключается в том, что группе Administrators не назначено право Enable computer and user accounts to be trusted for delegation («Разрешение доверия к учетным записям компьютеров и пользователей при делегировании»). Это право — параметр групповой политики, включенный для группы Administrators по умолчанию в политике контроллеров домена. Если DC выбран в качестве партнера репликации в ходе повышения уровня реплицируемого DC, выбранному DC требуется доступ к ресурсам повышаемого компьютера. Если право Enable computer and user accounts to be trusted for delegation не назначено группе безопасности Administrators, то каждый запрос доступа к ресурсу завершается неудачей с пояснением «отказано в доступе», как показано на экране 2.

Экран 2. Ошибка «отказано в доступе»

Чтобы устранить ошибку, используйте консоль управления групповой политики (GPMC) и инструмент Group Policy Results (Gpresult) для проверки, назначено ли группе Administrators право Enable computer and user accounts to be trusted for delegation в политике Default Domain Controllers Policy. Путь в редакторе групповой политики — \Computer Configuration\Policies\Windows Settings\SecuritySettings\Local Policies\UserRights Assignment\Enable computer and user accounts to be trusted for delegation.

После того как DC начинает работать с 2008 R2, можно запустить анализатор AD DS Best Practices Analyzer (BPA) для обнаружения любых ошибок в настройках политики. Соответствующее правило BPA не входит в изначальный набор правил, но имеется в дополнительном наборе правил, поставляемом через службу Windows Update. Это правило применяется к DC, работающему с Server 2008 R2.

При запуске AD DS BPA другое правило из того же дополнительного набора поможет предотвратить две типичные ошибки в настройках групповой политики, которые являются коренными причинами отказа репликации DC: непредоставление права Access this computer from the network («Доступ к компьютеру из сети») группам безопасности Administrators, Enterprise Domain Controllers или Authenticated Users либо назначение группам безопасности Enterprise Domain Controllers, Everyone, Administrators или Authenticated Users права Deny access to this computer from network («Запрет доступа к компьютеру из сети»). Отказ может случиться на любом DC, пытающемся выполнить репликацию из DC с одной из упомянутых выше настроек. Пользователи и компьютеры также могут столкнуться с отказами при применении объектов групповой политики (GPO).
Чтобы устранить эту ошибку, убедитесь в анализаторе BPA, что контроллеры домена назначили это право соответствующему участнику безопасности. Используйте настройки GPMC и Gpresult из таблицы 2, чтобы проверить правильность параметров групповой политики.

Таблица 2. Параметры GPMC и Gpresult

Параметр	Участники безопасности
Доступ к компьютеру из сети (включен по умолчанию политикой контроллера домена по умолчанию)	Должен охватывать: • администраторов; • контроллеры домена предприятия; • прошедших проверку пользователей
Запрет доступа к данному компьютеру из сети (не определен по умолчанию политикой контроллера домена по умолчанию)	Если включен, не должен охватывать: • контроллеры домена предприятия; • всех; • администраторов; • прошедших проверку пользователей

Особенности Adprep

Когда в Windows Server 2003 впервые появилось требование выполнения команды adprep/forestprep, компания Microsoft и некоторые партнеры рекомендовали в целях предосторожности изолировать хозяина схемы (например, временно поместить его в отдельную сеть) для лучшего управления процессом обновления схемы. С тех пор специалисты службы поддержки пользователей Microsoft пришли к выводу, что в большинстве компаний такой подход скорее вызывает проблемы, чем устраняет. Поэтому специалисты Microsoft больше не рекомендуют отключать от сети хозяина схемы перед запуском adprep/forestprep.

Листинг 1. Текст ошибки в файле dcpromoui.log

```
dcpromoui Enter ComposeFailureMessage
dcpromoui Enter GetErrorMessage 80070524
dcpromoui  Enter  State::GetOperationResultsMessage  The  attempt  to  join  this
computer
   to the <target DNS domain> domain failed.
dcpromoui Enter State::GetOperationResultsFlags 0x0
dcpromoui Enter State::SetFailureMessage The operation failed because:
The attempt to join this computer to the <target DNS domain> domain failed.
"The specified user already exists."
```

Листинг 2. Поиск имени вспомогательного DC в файле dcpromoui.log

```
Начало фрагмента A
dcpromoui Enter DS::JoinDomain
Конец фрагмента A
dcpromoui Enter MassageUserName administrator
dcpromoui z.com\administrator
Начало фрагмента B
dcpromoui Enter MyNetJoinDomain contoso.com\DC1.contoso.com
Конец фрагмента B
dcpromoui Calling NetJoinDomain
dcpromoui lpServer : (null)
dcpromoui lpDomain : contoso.com\DC1.contoso.com
dcpromoui lpAccountOU : (null)
dcpromoui lpAccount : contoso.com\administrator
dcpromoui fJoinOptions : 0x27
dcpromoui HRESULT = 0x80070524
```

Джастин Холл (justinha@microsoft.com) — старший технический писатель в компании Microsoft, редактор статей об Active Directory