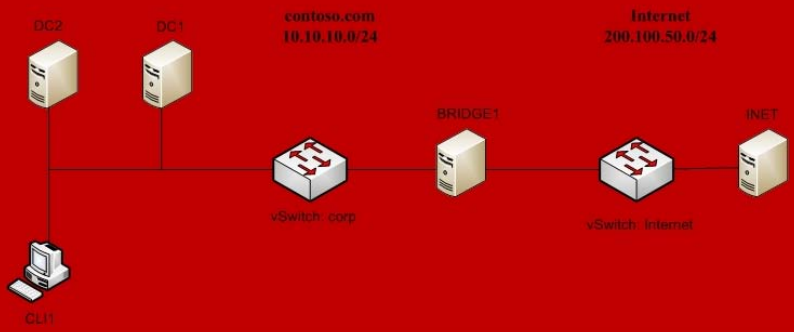
Д. В. Дюгуров

Операционные системы



Ижевск
2019

Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт математики, информационных технологий и физики

Д. В. Дюгуров

Операционные системы

Учебно-методическое пособие

Ижевск
2019

УДК 004.451
ББК 32.972.11
Д 95

Рекомендовано к изданию Учебно-методическим советом УдГУ

Рецензенты: к.ф.-м.н., доцент, В. И. Родионов
к.ф.-м.н., М. А. Клочков

Дюгуров Д. В.
Д 95 Операционные системы: учебно-методическое пособие. – Ижевск: Изд-во «Удмуртский университет», 2019. – 110 с.

ISBN

Настоящее учебно-методическое пособие посвящено настройке и использованию базовых сервисов серверных операционных систем на примере Microsoft Windows Server 2016 Standard Edition.

Пособие предназначено студентам, обучающимся по направлениям подготовки/специальностям «Прикладная информатика», «Фундаментальная информатика и информационные технологии», «Информатика и вычислительная техника», «Информационные системы и технологи», «Информационная безопасность», «Судебная экспертиза» и др., изучающим курс «Операционные системы» и другие смежные дисциплины.

ISBN

УДК 004.451
ББК 32.972.11

Содержание

Предисловие

В настоящем пособии последовательно рассмотрены следующие аспекты:

1. Служба каталогов Active Directory: базовый и дополнительный контроллеры домена, участники безопасности, простые групповые политики.
2. DNS: виды серверов и зон, записи ресурсов механизмы разрешения запросов, .поиск и устранение неполадок.
3. DHCP: авторизация в домене, создание областей, обеспечение отказоустойчивости, поиск и устранение неисправностей.
4. Файловый сервер: создание общих папок, настройка разрешений, задание квот, использование файловых экранов.
5. Сервер печати: управление принтерам, настройка разрешений, использование пулов и приоритетов.
6. Web-сервер: создание статических сайтов, эмуляция подключения к интернету.
7. Сервер удаленного доступа: маршрутизация сетей, общие сведения об адресации.

Основу пособия составляет лекционный материал, изложенный блочно-модульно, рассчитанный на студентов бакалавриата и магистратуры, изучающих курс «Операционные системы».

Лекционный материал подкреплен лабораторными работами. Все работы связаны между собой. В результате выполнения всех лабораторных работ у студента должна получиться действующая модель корпоративной сети, в которой настроены и функционируют все названные выше технологии. Лабораторные работы имеют аннотации и требования к выполнению.

Также в настоящее пособие включены инструкции

по выполнению упражнений из лабораторных работ. Инструкции структурированы так, чтобы сложилось целостное представление о выполняемой работе (в инструкциях отсутствует деление действий на упражнения, напротив, рекомендации даны именно по настройке всех технологий в рамках конкретной модели корпоративной сети).

§1. Обзор семейства систем Windows Server 2016. Консоли управления

Windows Server 2016 – 64-х разрядная операционная система, которую выпускают в 2-х различных редакциях:

- Windows Server 2016 Standard Edition;
- Windows Server 2016 Datacenter Edition.

Отличаются редакции количеством одновременно поддерживаемых ядер процессора, а также объемом поддерживаемой оперативной памяти. Следует отметить, что при организации корпоративных вычислительных сетей наиболее часто используется Standard Edition. Это объясняется тем, что при одинаковом функционале обеих редакций, его лицензии дешевле.

Каждая из редакций может быть установлена в двух вариантах: Graphic User Interface (GUI) и Core. В первом случае система предусматривает использование «классического» рабочего стола и графических оснасток управления, а во втором случае графический интерфейс отсутствует, при этом управление системой возможно из командной строки или удаленно.

Следует отметить, что существует еще одна редакция этой операционной системы, так называемый Nano Server. В нем используется сокращенное ядро и его рассмотрение выходит за рамки настоящего курса.

В дальнейшем будем предполагать, что мы рассматриваем Windows Server 2016 Standard Edition + GUI (Desktop Experience).

Установка этой ОС не отличается от установок других продуктов Microsoft, за исключением того, что после завершения установки, можно (и нужно) настроить роли сервера с помощью специального инструмента – Server Manager. С помощью этой утилиты можно, например, настроить следующие роли:

1. файловый сервер (обеспечивает доступ к общим ресурсам и управляет дисковыми квотами и файловыми экранами, системе DFSи т.д.);
2. сервер печати (обеспечивает централизованное управление печатающими устройствами и их драйверами);
3. почтовый сервер (устанавливает протоколы входящих и исходящих сообщений);
4. сервер терминалов (позволяет удаленным клиентам обращаться к дисковому пространству внутренней сети особым образом, имитируя ситуацию нахождения ресурсов внутренней сети на дисках удаленного клиента);
5. DNS-сервер (использоваться для разрешения имен в доменах AD);
6. DHCP-сервер (используется для динамического назначения IP-адресов клиентских компьютерам);
7. контроллер домена AD (предоставляет службу каталогов клиентам сети, создает новый контроллер домена);
8. сервер удаленного доступа (обеспечивает подключение удаленных клиентов к внутренней сети с помощью маршрутизации/VPN/Direct Access);
9. Web-сервер (IIS) (предоставляет службы для развертывания Web-сервера);
10. Сервер сертификации (позволяет развернуть на предприятии систему открытых ключей – PKI).

Отметим, сто существует еще достаточное количество других серверных ролей.

Windows Server 2016 поддерживает два варианта службы каталогов: рабочую группу и домен. Домен наиболее предпочтителен, т.к. имеет общий для всех членов каталог ресурсов – Active Directory (AD).

Компьютеры же в рабочей группе имеют собственные базы безопасности и ресурсов. AD – не просто база данных, это совокупность средств безопасности, протоколов, общих ресурсов, сценариев, групповых политик, учетных данных пользователей и пр. Каждый контроллер домена хранит копию (реплику) AD. Изменение AD на одном из контроллеров домена влечет их дальнейшее реплицирование на все остальные контроллеры. AD не существует без домена, а домен не существует без AD.

Несколько доменов с общим корнем образуют дерево, а несколько доменов с разными корнями могут образовывать лес. Образуют ли домены деревья и леса, зависит от отношений доверия между ними и настроек репликации.

Чтобы добавить роль контроллера домена нужно использовать Server Manager. В рабочей области этой утилиты нужно выбрать пункт меню Manage, далее перейти в раздел добавления ролей и выбрать из списка Active Directory Domain Service.

Вместе с ролью контроллера домена установятся роли DNS и файлового сервера. После установки будут доступны различные управляющие оснастки, важнейшие из них: Active Directory – Users and Computers, Active Directory – Domains and Trusts, Active Directory – Sites and Services, DNS.

AD состоит из объектов. У каждого объекта есть атрибуты и свойства. Создавать и изменять объекты в AD можно с помощью оснастки Active Directory – Users and Computers, а также с помощью утилит командной строки *net*, *ds*, массы командлетов powershell, и других. Объектов в AD может быть десятки тысяч. Для удобства управления объектами со схожими свойствами внутри

домена существуют особые контейнеры – организационные подразделения или юниты (OU). Также с OU можно связывать групповые политики (кроме юнитов, созданных в домене по умолчанию).

У каждого объекта в AD, к которому требуется доступ, есть список управления доступом (ACL). ACL сравнивается с маркерами доступа, и при наличии совпадений пользователям или службам доступ разрешается или запрещается. С помощью ACL и OU можно назначать разрешения на доступ к объектам и настраивать полномочия различных пользователей.

Управлять OU удобно с помощью групповых политик – списков параметров, затрагивающих все возможные настройки системы. Используя объекты групповой политики (GPO) можно изменить уровень безопасности, установить программное обеспечение, настроить вид рабочего стола на любом множестве компьютеров, входящих в домен.

Управляющие элементы (оснастки) собраны в Windows Server 2016 в меню Tools в Server Manager. Этим удобно пользоваться – все в одном месте. Но есть одно «но» – Server Manager использует дополнительные элементы безопасности, которые не всегда положительно отражаются на работоспособности оснасток, входящих в его состав.

Универсальным графическим инструментом управления в Windows Server 2016 являются мультимедиа-консоли (MMC) – родительское приложение для одной или нескольких оснасток. Можно создавать свои консоли, добавляя те или иные оснастки в корень консоли. Каждая консоль состоит из дерева оснасток и рабочей области, в которой отображаются свойства оснастки.

Оснастки бывают двух типов: изолированные (создаются разработчиками административных систем, к таковым относятся все предустановленные оснастки) и оснастки расширения (предназначены для работы совместно с изолированными оснастками, некоторые оснастки могут быть как изолированными, так и оснастками расширения). Собственные консоли можно сохранять в авторском или пользовательском режиме. Консоли, сохраненные в авторском режиме, могут редактировать только их создатели. Существуют три типа пользовательского режима:

- полный доступ (функционал оснастки полностью доступен другим пользователям);
- ограниченный доступ, несколько окон (пользователи в праве просматривать все открытые в оснастке окна, но не в праве открывать новые);
- ограниченный доступ, одно окно (пользователи просматривают только верхнее открытое в консоли окно, и не в праве перемещаться по дереву оснасток).

Для создания собственной консоли необходимо выполнить команду *mmc*, добавить необходимые оснастки, и сохранить консоль в одном из режимов. Файлы консоли имеют расширение .msc.

Большинство оснасток имеют динамический фокус, т.е. с их помощью можно управлять настройками не только локального, но и удаленного компьютера. Фокус оснастки изменяется либо при старте консоли, либо в ее свойствах.

Для совместного использования ресурсов и удаленного управления сервером можно также использовать программу Подключение к удаленному рабочему столу, входящую в стандартный комплект

Windows Server 2016 Для работы с этой программой необходимо обладать административными полномочиями или быть членом группы Пользователи удаленного рабочего стола, также необходимо, чтобы на сервере, к которому производится удаленное подключение, оно было разрешено. Также не надо забывать, что данная программа поддерживает только два одновременных подключения к серверу. Если удаленно необходимо подключаться к контроллеру домена еще кому-то кроме администратора сети, необходимо дополнительно настраивать групповую политику.

§2. Управление учетными записями пользователей. Введение в групповые политики

Объект пользователя в AD состоит из имени пользователя, пароля, идентификатора безопасности (SID), профиля пользователя. Создавать объекты пользователей можно в консоли Active Directory – Users and Computers или в командной строке с помощью команды *dsadd user*, а также с помощью командлета powershell – *NewADUser*.

При создании объекта пользователя через консоль необходимо заполнить ряд обязательных полей:

- полное имя (на его основе генерируются обычное имя (cn), различающееся имя (dn), собственно имя и отображаемое имя (displayname);
- имя входа пользователя (представляет собой имя_пользователя@имя_домена);
- имя входа пользователя (пред-Windows 2000), используется для входа в домен с клиентов под управлением ранних версий Windows;

- пароль (пароль должен отвечает требованиям сложности, установленным групповой политикой).

Также можно задать некоторые свойства пользователей: требовать смену пароля при следующем входе в систему, запретить смену пароля пользователем, снять ограничение срока действия пароля или отключить учетную запись. В ряде случаев, настройки свойств объекта пользователя могут противоречить настройкам политики безопасности, действующей в системе. Настройки объекта пользователя приоритетнее настроек политики безопасности.

После создания объекта пользователя можно настроить его остальные свойства, среди которых путь к профилю пользователя, членство в группах, личные данные пользователя и прочее (свойств огромное количество, ведь AD – разветвленная база данных, позволяющая хранить о своих объектах множество информации, и не только хранить, но и при необходимости делать выборки, сортировки и т.д.).

Также можно настроить список компьютеров, с которых пользователь может входить в сеть, время входа пользователя в систему, использование смарт-карт и срок действия самой учетной записи. Из консоли Active Directory – Users and Computers можно управлять несколькими объектами пользователей одновременно. Для этого их достаточно выделить в рабочей области оснастки. Перемещать несколько объектов пользователей, копировать и удалять их можно без ограничений. Но далеко не все свойства учетных записей доступны для совместного редактирования (*одновременно можно изменять* путь к профилю пользователя, сценарий входа в систему, домашнюю

папку, должность, практически все свойства адреса, срок действия учетных записей и некоторые другие свойства). Все операции с объектами пользователей, доступные в графической консоли, можно осуществлять из командной строки.

Для создания объектов пользователей можно использовать так называемые шаблоны – заранее созданные объекты пользователей, копируемые при необходимости создания конкретных объектов. При копировании шаблона копируются не все свойства, настроенные в шаблоне. *Свойства копируются в следующем порядке*: на вкладках Общие: телефоны, входящие звонки, среда, сеансы, удаленное управление, профиль служб терминалов; COM+ - свойства не копируются; на вкладке Адрес копируются все свойства кроме Улица; на вкладке Учетная запись копируются все свойства кроме Имя входа; на вкладке Организация копируются все свойства кроме Должность; свойства на вкладках Профиль и Член групп копируются полностью.

В случае если нужно создать очень много однотипных объектов в AD (в том числе и объекто в пользователей) можно импортировать их из специально созданного текстового файла формата .csv, текстовые записи в котором соответствуют свойствам создаваемых объектов. Для импорта объектов в AD из файла .csv может быть использована утилита *csvde* или, гораздо более часто, командлет powershell *ImportCSV* в пакетном режиме с командлетом *New-ADUser*. Эта команда также может экспортировать объекты из AD в файлы .csv.

Также для управления объектами в AD можно использовать команды семейства ds: *dsadd* – добавляет объекты в каталог; *dsget* – отображает свойства объектов каталога; *dsmod* – изменяет свойства объекта; *dsmove* –

перемещает объект в каталоге; *dsrm* – удаляет объект из каталога; *dsquery* – выбирает объекты из каталога по заданным признакам.

Разница команд *dsquery* и *dsget* в том, что с помощью *dsget* можно просмотреть свойства заданного объекта, а *dsquery* выбирает из каталога объекты с заданными свойствами. Все команды семейства ds поддерживают пакетный режим, т.е. результаты выполнения одной команды могут быть поданы на вход другой команде в качестве параметров (например, с помощью команды *dsrm* можно удалить объекты, которые были выбраны командой *dsquery*).

Преимущество использования командной строки два – контроль над ситуацией и скорость работы. Также несомненным плюсом является встроенная справка. Для вызова справки можно использовать ключ */?* после каждой команды или ее части. При этом на экран будет выведено подробное описание ключей команды с примерами их использования. Возможности справки в powershell еще шире: в редакторе PowerShell ISE есть встроенная контекстная подсказка (после ввода нескольких букв можно выбрать из списка походящий по названию командлет или ключ).

Каждый пользователь имеет свой профиль – набор файлов и папок, содержащих элементы рабочего стола. Профиль включает в себя ярлыки на рабочем столе и в панели инструментов; документы рабочего стола и домашней папки пользователя (если нет перенаправления папок, то это папка Documents); избранное в IE; сертификаты; настройки Microsoft Office; настройки папки Сетевое окружение; параметры рабочего стола. Профили пользователей могут быть локальными и перемещаемыми.

Локальные профили пользователей хранятся в папке %Systemdrive%\Users\%Username%. При первом входе пользователя в систему в указанную папку копируется содержимое папки %Systemdrive%\Users\Default. Для каждого пользователя локальные профили уникальны. Дополнять локальные профили пользователей можно с помощью внесения изменений в профиль с именем All Users. Но для этого необходимо быть членом группы Администраторы. При использовании локального профиля, в случае если пользователь входит в систему с другого компьютера, настройки и свойства его профиля не перемещаются, а система создает новый локальный профиль.

Перемещаемые профили хранятся на сервере, и при входе пользователя в систему с разных компьютеров они копируются на эти компьютеры с сервера, поэтому пользователь всегда использует привычные настройки. Для использования перемещаемых профилей необходимо скопировать файлы профиля на сервер (в любую доступную общую папку), а в свойствах учетной записи пользователя указать путь к этой папке (необходимо также позаботиться, чтобы пользователь имел необходимые права на чтение, изменение файлов из этой папки). Перемещаемые профили выгружаются обратно на сервер при выходе пользователя из системы, поэтому не влияют на общее свободное дисковое пространство того или иного компьютера. Но при этом скорость загрузки системы (время копирования файлов профиля с сервера) снижается только в первый раз, т.к. Windows Server 2016 загружает и выгружает профиль не полностью, а синхронизирует его (загружает и выгружает только изменения), в связи с этим затрагиваются дисковые квоты, установленные для данного пользователя на том

компьютере, с которого он входит в сеть.

В случае если одному или нескольким пользователям необходимо настроить одинаковые параметры профиля, можно воспользоваться так называемым преднастроенным профилем. Для этого надо создать новую учетную запись и настроить необходимые свойства для нее. А потом просто скопировать профиль этой записи в профиль нужных пользователей. Это справедливо для локальных и перемещаемых профилей.

В ряде случаев необходимо сделать так, чтобы пользователи не могли изменять свойства профиля. Существуют два варианта решения этой задачи:

1. использование групповых политик для настройки свойств системы (пользователи не смогут вносить никаких изменений, даже временных);
2. использование обязательного профиля (во время текущей сессии пользователи могут изменять настройки профиля, например, создать ярлык на рабочем столе, но при перезагрузке компьютера все произведенные изменения пользователем будут удалены).

Чтобы сделать профиль пользователя обязательным, необходимо в корневом каталоге профиля найти файл *ntuser.dat.* и сменить расширение этого файла на *.man.*

При управлении объектами пользователей необходимо выполнять ряд требований безопасности, в частности, настраивать *политику паролей, политику блокировки учетных записей и политику аудита*.

Групповые политики применяются на уровне домена в целом и на уровне локального компьютера. Локальные политики приоритетнее доменных. Редактировать указанные выше политики на уровне

домена можно в консоли Group Policy Object Manager.

Далее рассмотрим важные параметры в Default Domain Policy. С помощью политики паролей *(Password Policy)* можно настроить следующие свойства:

- *требовать неповторяемость паролей* (сохраняется список ранее использованных паролей и пользователю не разрешается менять пароль на пароль из этого списка, максимально может храниться 24 старых пароля);
- *максимальный срок действия пароля* (определяет временной интервал, по истечении которого пользователь должен сменить пароль, значение по умолчанию 42 дня);
- м*инимальный срок действия пароля* (задает временной промежуток, который должен пройти между сменами паролей);
- *минимальная длина пароля* (по умолчанию 7 символов);
- *пароль должен отвечать требованиям сложности* (при включении этого параметра пароль должен содержать не менее 6 символов, при чем символы должны быть четырех разных типов – заглавные и строчные буквы, цифры и специальные символы).

Политика блокировка учетной записи позволяет временно заблокировать учетную запись при некотором количестве неудачных входов в систему с реквизитами этой учетной записи. Одноименная политика безопасности содержит 3 параметра:

- *пороговое значение блокировки* (количество неудачных попыток входов в систему, после которых учетная запись блокируется. Значение от 0 до 999, если значение равно 0,

учетные записи никогда не блокируются);

- *блокировка учетной записи на* (задает период времени, по истечении которого учетная запись будет разблокирована автоматически. Значения измеряются в минутах и берутся из диапазона от 0 до 99999. Если выбран 0, то учетную запись может разблокировать только администратор);
- *сброс счетчика блокировки через* (задает количество минут, которое должно пройти после последней неудачной попытки входа в систему, чтобы счетчик блокировки был сброшен до 0. Значения берутся из диапазона от 1 до 55555, причем значение должно быть меньше *Порогового значения блокировки*).

В корпоративной сети необходимо отслеживать события, связанные с учетными записями, для этого необходимо сконфигурировать политики аудита. Политика аудита также содержат три параметра, связанных с учетными записями:

- *аудит событий входа в систему* (регистрирует все события, связанные с аутентификацией на контроллере домена);
- *аудит управления учетными записями* (включает запись событий, связанных с созданием, удалением и изменением групп, учетных записей пользователей и компьютеров и событий смены пароля);
- *аудит входа в систему* (генерируется на локальных компьютерах для локальных учетных записей).

Вход в систему под учетной записью отличается от общего входа. При входе пользователя на рабочую

станцию с реквизитами доменной учетной записи эта станция регистрирует событие входа, а контроллер домена – событие входа учетной записи. Когда пользователь подключается к общей папке на сетевом сервере, тот регистрирует событие входа, а контроллер домена – событие входа учетной записи. События входа в систему учетных записей необходимо проверять на всех контроллерах домена, а событие входа в систему необходимо проверять на всех компьютерах.

Интервал обновления групповой политик в домене по умолчанию не превышает 15 минут. Обновление групповой политики можно инициировать вручную, выполнив команду *gpupdate /force* вначале на контроллере (контроллерах) домена, а затем – не клиентских компьютерах.

Просматривать данные аудита можно в журналах безопасности с помощью утилиты Event Viewer.

§3. Управление учетными записями групп и компьютеров

В активном каталоге есть контейнеры, которые содержат учетные записи пользователей и компьютеров – группы. Существуют два типа групп:

1. группы безопасности (используются для назначения прав доступа к ресурсам);
2. группы распространения (используются для рассылки электронной почты).

Группы безопасности могут использоваться в качестве групп распространения, но не наоборот.

По областям действия различают три вида групп:

1. локальные доменные;
2. глобальные;

3. универсальные.

Локальная доменная группа может объединять учетные записи пользователей и компьютеров из разных доменов, и используется для назначения прав доступа к ресурсам в том домене, в котором создана группа.

Глобальная группа объединяет учетные записи пользователей и компьютеров домена, в котором создана группа, и используется для назначения прав на ресурсы, находящиеся в других доменах.

Универсальная группа может содержать учетные записи из разных доменов и предоставлять права доступа к ресурсам разных доменов.

Глобальные группы могут быть членами локальных доменных групп и содержать в себе другие глобальные группы, локальные доменные и универсальные группы. Локальные доменные группы могут содержать в себе локальные доменные группы из того же домена. Универсальные группы могут содержать в себе другие универсальные группы, глобальные группы и локальные доменные.

Также существуют локальные группы. Они используются для совместимости с доменами на базе Windows NT и не используются на контроллерах домена. Область действия группы также называется ее скопом (scope). Локальные доменные и глобальные группы можно преобразовать в универсальные, если первоначально группы не входили в состав других групп с той же областью действия.

Также в Windows Server 2016 существует ряд специальных групп. Их нельзя удалить или изменить их состав, но для них можно задавать разрешение на доступ к ресурсам. В эти группы, например, попадают пользователи и компьютеры в зависимости от способа

входа в сеть. Примеры таких групп: *Все, Сеть, Анонимный вход, Прошедшие проверку, Удаленный доступ* и пр. Это так называемы группы с ограниченным членством (Restricted Groups). Все же администраторы могут вмешиваться в управление такими группами, используя одноименный раздел групповой политики.

Создавать группы и изменять их состав можно в консоли Active Directory – Users and Computers, и с помощью утилит семейства ds и net, а также с помощью командлетов powershell New-ADGruop +Add-ADGroupMember.

Поскольку группы могут быть вложенными друг в друга, иногда бывает сложно сказать, к каким именно группам принадлежит тот или иной пользователь (информации на вкладке Член групп свойства пользователя недостаточно, т.к. принадлежность к группам с ограниченным членством там не учитывается). Для решения этой проблемы можно использовать команду *dsget*. Изменять состав групп можно, добавляя или удаляя из них учетные записи групп, компьютеров и других пользователей.

Если необходимо создать множество групп (любых других объектов безопасности) одновременно, можно использовать команду *dsadd* в пакетном режиме или утилиту *LDIFDE.exe*. Утилита *LDIFDE* реализует процедуру обмена данными с активным каталогом по протоколу LDAP. Подробную справку о ключах данной команды можно найти в справочной системе Windows, а список ключей можно получить, выполнив команду *ldifde /?* Ключ /? можно использовать для получения справки о параметрах любой команды командной строки.

Создавать учетные записи компьютеров можно также, как и учетные записи пользователей. Учетная

запись компьютера также содержит имя, пароль и SID (идентификатор безопасности). Помимо прочего, для создания учетных записей компьютеров можно воспользоваться командой netdom. В любом случае необходимо быть членом группы Администраторы или Операторы учета на контроллере домена. Для того чтобы компьютер стал членом домена, недостаточно просто создать для него учетную запись в AD, компьютер необходимо присоединить к домену. Для этого необходимо зайти в раздел *Control Panel → System → Computer Name.* Затем необходимо выбрать одноименный параметр и ввести полное DNS-имя домена. Если клиентскому компьютеру удастся связаться с DNS-сервером и найти работающий контроллер домена (используется srv-локатор _ldap), то появится приглашение о присоединении с просьбой ввести имя пользователя и пароль, у которого есть привилегии пристыковывать компьютеры к домену. Если в домене учетная запись для присоединяемого компьютера была создана заранее, то она будет использоваться и в дальнейшем. Если же запись для нового компьютера не была создана, она будет создана автоматически в контейнере (OU) *Computers*.

Нужно помнить, что к контейнеру *Computers* нельзя привязывать групповые политики, поэтому учетные записи компьютеров необходимо перемещать из этого юнита в другие. Также для присоединения компьютера к домену можно использовать команду *netdom join* или *djoin,* а если нужно присоединить к домену новый сервер, то очень удобно пользоваться утилитой *sconfig*.

Присоединять компьютер к домену могут члены любой группы, которым это прямо разрешено (соответствующее разрешение можно настроить при

создании учетной записи компьютера). Перемещать объект компьютера внутри каталога без ограничений могут члены группы Администраторы, а члены группы Операторы учета могут перемещать объекты компьютеров везде, за исключением организационного подразделения *Domain Controllers*.

Учетная запись компьютера имеет некоторые свойства, которые не настраиваются при ее создании (например, информация об операционной системе). Эти свойства становятся доступными после присоединения компьютера к домену.

Для поиска объектов в AD (в том числе учетных записей компьютеров) удобно использовать фильтрацию в консоли Active Directory – Users and Computers. Причем в случае учетных записей компьютеров к найденным объектам можно подключиться прямо из консоли управлять некоторыми их свойствами (например, просматривать журналы безопасности и редактировать локальные учетные записи пользователей и групп).

Неполадки с учетными записей компьютеров возникают крайне редко. Признаками таких неполадок являются: невозможность связаться с контроллером домена при старте системы из-за отсутствия учетной записи компьютера; сообщение об ошибках в журнале событий или возможное предположение системы об ошибке паролей. Устранить все эти неполадки можно, действуя в следующем порядке: если учетная запись компьютера есть в AD, то ее нужно переустановить; если записи нет – ее нужно создать; если проблемный компьютер является членом домена, его нужно сделать членом рабочей группы, а потом снова присоединить к домену. Применять правила можно в произвольном порядке, кроме последнего (присоединять компьютер к

домену нужно всегда в последнюю очередь).

Удалять, отключать и переустанавливать учетные записи компьютеров можно с помощью команд семейства *ds, netdom*, командлетов powershell и в консоли Active Directory – Users and Computers (как и любые другие объекты). При отключении учетная запись остается членом групп (настроенные разрешения и политики сохраняют свое действие). При удалении учетной записи компьютера (или учетной записи пользователя) все настроенные разрешения перестают действовать, поэтому при создании учетной записи с таким же именем вновь придется восстанавливать ее членство в группах заново.

§4. Управление данными: File server, Web-server (IIS)

Традиционно создать общую папку на локальном компьютере можно, используя *Проводник (File Explorer).*

В Windows Server 2016, как и в других операционных системах Microsoft, существуют стандартные общие папки: корень каждого жесткого диска и системный каталог. Они не отображаются в обозревателе, но к ним всегда можно обратиться по UNC-пути, дополнив его значком $ (\\<имя_сервера>\c$). Подключаться к таким папкам могут только администраторы.

Для управления общими папами в Windows Server 2016 существует специальная роль – File server. На контроллере домена она устанавливается по умолчанию, а на рядовом сервере ее нужно добавить. Чтобы добавить роль файлового сервера нужно использовать Server Manager. В рабочей области этой утилиты нужно выбрать пункт меню Manage, далее перейти в раздел добавления

ролей и выбрать из списка File Server. В базовом варианте установятся службы, позволяющие создавать общие папки. Для управления квотами и файловыми экранами потребуется дополнитешльно установить File Server Resource Manager. Также функционал файлового сервера можно расширить, установив другие дополнительные возможности, например, среду DFS – элемент управления распределенной файловой системой, позволяющей организовать файловую репликацию.

После установки в списке функций сервера в утилите Server Manager будет доступна вкладка File Server. Именно с ее помощью можно создавать общие папки.

К общим папкам, созданным с помощью консоли File Server, может подключаться любой пользователь в зависимости от настроенных разрешений. С помощью указанной консоли также можно управлять свойствами общих папок: количеством одновременных подключений, сетевым именем, доступностью файлов в автономном режиме, разрешением для общего ресурса, разрешениями NTFS и пр. Также можно опубликовать общий ресурс в AD (после этого папку можно будет искать в AD, как и любой объект).

Разрешений доступа к общим ресурсам три:

1. *Чтение* (пользователь может просматривать список папок, содержимое и атрибуты файлов, просматривать подпапки внутри родительской папки и запускать программы внутри папки);
2. *Изменение* (пользователь может создавать файлы, папки, редактировать их, изменять атрибуты файлов, удалять файлы и папки внутри родительской папки и выполнять все действия, установленные разрешением *Чтение*);

3. *Полный доступ* (в дополнение к правам разрешения *Изменение* пользователи могут изменять разрешение файлов и становиться их владельцами).

Для конкретного пользователя разрешения доступа к общему ресурсу определяются прямой суммой разрешений, назначенных его учетной записи, и всем группам, членом которых он является. Причем, явный запрет приоритетнее явного разрешения.

Система разрешений доступа к общему ресурсу недостаточно гибкая и надежная. Поэтому данные, к которым необходимо предоставить общий доступ, рекомендуется размещать на томах NTFS, т.к. эта файловая система предоставляет собственные инструменты для защиты файлов и папок. С помощью разрешений NTFS можно не только ужесточить доступ к общему ресурсу, но и настроить его весьма гибко.

Разрешения NTFS настраиваются на вкладке *Безопасность (Security)* свойств общего ресурса. Если общий ресурс расположен на томе NTFS, а вкладка *Безопасность* не отображается, то необходимо снять флажок напротив параметра Использовать простой общий доступ в консоли Свойства папки в *Панели управления*. На вкладке *Безопасность* формируется ACL для общего ресурса. После авторизации пользователя в системе для учетной записи последнего создается Маркер доступа. В дальнейшем Маркеры доступа сравниваются с ACL-объектов и пользователь получает те или иные права на доступ. Добавлять, удалять и изменять разрешения можно для любых участников безопасности (в т.ч. для компьютеров независимо от пользователей и в зависимости от входа пользователя в сеть). Для этого достаточно проставить галочки разрешения или запрета

того или иного права на вкладке *Безопасность*.

Разрешения на вкладке *Безопасность* в первом окне упорядочены по шаблону, а во втором перечислены в списке. Шаблоны – это совокупность разрешений из списка.

В Windows Server 2016 поддерживается система наследования разрешений, которая означает, что разрешения, назначенные родительской папке, наследуются всеми ее дочерними объектами. Унаследованные разрешения отображаются в виде серых флажков. Разрешения, назначенные явно, помечаются черными флажками. При желании этот порядок можно изменить: унаследованные разрешения можно прямо заменить явными или полностью отменить наследование для папки, сняв соответствующий флажок. При этом унаследованные разрешения можно скопировать (они просто станут явными) или удалить (ACL дочерних объектов не будет содержать разрешений, назначенных родительской папке).

Восстановить наследование можно либо со стороны дочернего ресурса (сохранятся явно назначенные разрешения для дочернего ресурса и скопируются разрешения родительской папки), либо со стороны родительской папки (явные разрешения, назначенные дочерним ресурсам, будут удалены и скопируются разрешения родительской папки).

Для того чтобы определить список разрешений для каждого конкретного участника безопасности можно воспользоваться вкладкой Действующие разрешения. Действующие разрешения определяются по следующим правилам: разрешения файлов приоритетнее разрешений папок; разрешения, позволяющие доступ, суммируются; разрешения, запрещающие доступ, приоритетнее

позволяющих; явные разрешения приоритетнее унаследованных. У данного инструмента есть одна слабая сторона – при определении действующих разрешений система не учитывает разрешения, назначенные группа с ограниченным членством.

По умолчанию разрешения для файлов и папок могут изменять *Администраторы* и создатели объектов (члены группы *Создатель-Владелец*). Создатели объектов всегда получают доступ к ACL-объекта, поэтому если необходимо запретить создателю доступ к объекту, администратору необходимо перехватить владение и только потом ограничить доступ пользователя, создавшего объект. Также становиться владельцами объектов могут пользователи или группы, если им предоставлено разрешение NTFS *Смена владельца* (администраторы могут передавать право владения, привилегия *Восстановление файлов и каталогов* включает возможность перехвата владения объектом).

Общие ресурсы можно организовать не только в виде общих папок, но и с помощью технологий FTP и Web. Для управления этими объектами в Windows Server 2016 предусмотрен ароль Web-server (IIS), которая не утсанавливается оп умолчанию. Добавить ее можно с помощью матера добавления ролей сервера через Server Manager→Manage→
Add Roles and Features (аналогично рассмотренным ранее ролям).

После установки IIS создается стандартный Web-узел и становится доступной консоль *Internet Information Services Manager*. Данная служба представляет собой все необходимое для организации собственного Web или FTP-сервера (поддержу FTP нужно устанавливать дополнительно при использовании мастера установки

роли Web-server).

Для создания собственных Web и FTP-узлов необходимо использовать специальные мастера, доступные в консоли *IIS Manager*, позволяющие настроить имена узлов, их размещение, порты, страницы по умолчанию и пр. также с помощью *IIS Manager* можно создавать виртуальные каталоги. IIS 10.0 имеет систему защиты файлов, состоящую из проверки подлинности, использования NTFS-разрешений и использования IIS-разрешения. Средствами Web подлинность проверяется в следующих вариантах: анонимная проверка (пользователи не вводят реквизитов), обычная проверка (используются реквизиты учетной записи пользователя, передаваемые открытым текстом), краткая проверка (данные пользователя шифруются), расширенная краткая проверка (взаимодействует с AD, а в остальном – то, что краткая), встроенная проверка Windows (имя пользователя и пароль хэшируются перед передачей по сети), проверка по сертификату (использует SSL, возможна если на компьютере установлены и настроены Службы сертификации). При использовании FTP доступны анонимная и обычная проверки подлинности.

На ресурсы IIS можно назначать собственные разрешения, распространяющиеся на все пользователи и группы: Чтение, Запись, Доступ к тексту сценария, Обзор каталогов. Также можно настраивать разрешения на выполнение сценариев и приложений: Нет, Только сценарии, Сценарии и исполняемые файлы.

На вкладке *Дополнительные параметры безопасности* свойств общего ресурса можно настроить параметры аудита ресурса. Параметры аудита наследуются. Аудиту подлежат успешные и неудачные попытки доступа учетной записи пользователя или

компьютера к ресурсу с использованием каждого из назначенных разрешений. Аудит необходимо включить через политику безопасности и только потом настроить его параметры в свойствах общего объекта. Анализировать события в журналах аудита можно с помощью оснастки *Просмотр событий,* изучив журнал *Безопасность*.

§5. Управление принтерами

Существуют два типа принтеров: *локальные* (подключенные к какому-либо порту сервера печати) и *сетевые* (подключенные к сети, а не к физическому порту). Оба типа принтеров представлены в операционной системе как логические принтеры (содержат драйвера, параметры принтера, параметры печати и прочие свойства).

Можно по разному управлять сетевыми принтерами: установить логические принтеры на каждом сетевом узле и связать их напрямую с сетевым принтером, и централизованно – установить логический принтер на сервере печати с подключенным физическим принтером, а на сетевых узлах установить клиенты печати, подключенные к логическому принтеру сервера. Второй способ выгоднее, т.к. используется одна очередь печати, все контролируют состояние принтера, выполнять административные задачи проще.

В Windows Server 2016 для установки принтера можно использовать Control Panel. При этом необходимо указать тип принтера, выбрать для него порт (или создать новый), установить драйвер принтера, а для сетевого принтера указать еще UNC-имя.

В случае если в сети есть клиенты под управлением

различных операционных систем, то вполне возможно, что для каждой из них необходим собственный драйвер принтера. Для удобства клиентов драйверы принтера для различных ОС можно установить на сервере печати. При этом клиенты смогут получить их автоматически.

Для того чтобы настроить логический принтер на клиенте, можно также использовать Мастер установки принтеров с включенной опцией *Сетевой принтер, подключенный к другому компьютеру*. В случае если сетевой принтер опубликован в качестве общего ресурса в AD, то для подключения клиента достаточно найти этот принтер в каталоге, а потом запустить Мастер установки принтеров.

В случае если принтер является общим, можно настроить разрешения на его использование для учетных записей пользователей и групп (по аналогии с общими папками и файлами). Для этого в свойствах принтера необходимо выбрать вкладку Безопасность. ACL-принтера может содержать 3 разрешения:

- печать (позволяет пользователям отправлять документы на принтер);
- управление принтерами (позволяет пользователям изменять параметры и конфигурацию принтера, включая разрешения и права разрешения *Управление документами*);
- управление документами (позволяет управлять заданиями для печати и очередью принтера и права разрешения *Печать*).

Есть специальные группа безопасности Операторы печати. Членам этой группы по умолчанию назначается разрешение *управлениями принтерами*.

При необходимости можно настроить расписание

работы принтера. В случае если заданы часы работы принтера, пользователи с соответствующими разрешениями смогут направлять на принтер задания в любое время, но распечатываться они будут строго в соответствии с графиком.

В больших сетях целесообразно использовать несколько принтеров, объединенных в пул – один логический принтер, обслуживающий несколько физических. В этом случае задание из очереди печати логического принтера направляются на первое свободное физическое устройство. Пул принтеров настраивается на вкладке Порты свойств логического принтера. Желательно объединять в пулы принтеры одной марки и модели, т.к. драйвер, используемый пулом, должен подходить для всех физических устройств.

Иногда удобно использовать конфигурацию, обратную пулу – использовать несколько логических принтеров, подключенных к одному физическому. Это целесообразно делать, если в сети мало принтеров, а пользователи печатают различные типы документов в большом количестве. Тогда для каждого из выбранных логических принтеров можно задать приоритет (число от 1 до 99). Чем выше приоритет принтера, тем раньше выполнятся задачи из его очереди.

В случае если сервер печати управляется Windows Server 2016, при добавлении на него нового логического принтера, последний автоматически публикуется в AD. Все логические принтеры опрашиваются каждые восемь часов. Если подключиться не удается к ним два раза подряд, объект принтеров удаляется из активного каталога.

В Windows Server 2016 реализован протокол IPP, с помощью которого можно осуществлять печать через

Интернет и настраивать свойства принтера с помощью любого браузера. Для того, чтобы эти функции были включены, на сервере необходимо установить службы IIS. После установки для принтеров будет создан специальный виртуальный каталог, к которому можно обращаться с помощью браузера. Введя в поле *Адрес* следующее http://<имя_сервера_печати>/printers.

Если один из принтеров сломался можно перенаправить задания из его очереди на другой принтер. Для этого в свойствах логического принтера (связанного с неисправным физическим устройством) необходимо выбрать другой порт (обслуживаемый исправным устройством).

Вообще, для мониторинга принтеров можно использовать оснастки Системный монитор и Журналы и оповещения производительности. Наиболее важные счетчики таковы: *Печатаемых байт в секунду* (низкие значения говорят о неравномерности нагрузки на принтеры), *Ошибок заданий* (большие показания свидетельствуют о неправильной конфигурации порта), *Всего напечатано страниц* (накопительный счетчик, полезен для контроля за состоянием картриджа). Также события очереди печати можно просматривать с помощью консоли Просмотр событий. По умолчанию регистрируются события, связанные с созданием, удалением и изменением свойств принтера.

Как и для общих папок и файлов для принтеров можно настроить аудит, с помощью которого в журналы будут записываться события успешных и неудачных попыток использования стандартных разрешений, используемых участниками безопасности. Для этого необходимо средствами групповой политики включить *Аудит доступа к объектам*, а в свойствах логического

принтера выбрать тип регистрируемых событий.

Неполадки печати устраняются следующим образом: определить область сбоя (если клиент не может печатать из одного приложения, но может из других, значит неправильно работает приложение, а не принтер; если пользователь может печатать с помощью других принтеров, то неправильно установлен логический принтер; если пользователь вообще не может отправлять задания на печать, а другие пользователи не испытывают проблем, значит виноват компьютер пользователя); проверить доступность сервера печати; проверить исправность принтера; проверить IP-конфигурацию принтера и проверить запущены ли *Службы сервера печати*.

§6. Управление оборудованием и драйверами

Устройства и драйверы для них делятся на две категории: с поддержкой PnP и без. Для большинства PnP-устройств драйвер есть на в комплекте Windows Server 2016. При установке нового устройства система автоматически находит для него драйвер и выделяет для него ресурсы (запросы на прерывание IRQ и каналы прямого доступа к памяти DNA). В случае если системе не удается найти подходящий драйвер, она запросит его у пользователя, а устройство в консоли Диспетчер устройств будет помечено восклицательным знаком в желтом треугольнике. Если системе вообще не удается определить тип устройства, тогда запрос на драйвер не выдается, а устройство помечается знаком вопроса в желтом треугольнике как неизвестное.

Для обновления конфигурации устройств служит оснастка Диспетчер устройств. Ее можно использовать в

двух видах: с *деревом устройств* и с *деревом ресурсов для устройств* (настраивать ресурсы вручную не рекомендуется). Оснастку Диспетчер устройств для редактирования конфигурации можно использовать только на локальном компьютере, на удаленном компьютере она работает в режиме только для чтения. Для получения подробной сводки об устройствах и драйверах, можно использовать утилиту командной строки *DriverQuery*.

Администраторы компьютера могут устанавливать любые устройства и драйверы. Обычные пользователи могут устанавливать драйвера в следующих случаях: драйвер имеет цифровую подпись, файлы драйвера уже есть на компьютере и для дальнейшей установки не требуется дополнительного вмешательства пользователя, причем необходимо соблюдение всех трех условий одновременно (эти условия, как правило, справедливы для принтеров, USB-устройств и для шины IEE1394).

Начиная с Windows 2000 драйвера для устройств имеют цифровую подпись, которая показывает, что файл не был изменен в процессе использования. Некоторые драйвера могут не иметь цифровой подписи. В случае если драйвер не подписан, можно настроить три варианта действия системы: *Пропускать* (устанавливать драйвер, даже если нет подписи. Доступен только для администратора), *Предупреждать* (спрашивать у пользователя – устанавливать ли драйвер), *Блокировать* (не устанавливает драйвера без цифровой подписи).

В оснастке Диспетчер устройств можно обновлять драйвера для выбранного устройства (например, если производитель выпустил новую версию). В случае если после установки нового драйвера в работе устройства возникли проблемы, то можно вернуться к предыдущей

версии драйвера, нажав на кнопку *Откатить*. Также драйвера для устройств можно удалять (если это PnP-устройство, удаление драйвера повлечет удаление самого устройства, если драйвер устройства был добавлен вручную, оно останется в системе, но без сконфигурованного драйвера). В случае если у устройства есть дополнительные свойства, с помощью которых можно осуществлять его настройку, доступ к ним будет осуществляться с такими же правами, что и к Диспетчеру задач. Ограничить доступ к таким настройкам также можно с помощью групповой политики.

При возникновении неполадок в работе устройств можно использовать следующие средства: *возврат предыдущей версии драйвера* (если система загружается), *загрузка последней удачной конфигурации* (сработает в случае если неполадка случилась до последнего удачного входа в систему), *безопасный режим* (загружается минимальный набор драйверов и подсистем; после загрузки можно отключить в Диспетчере устройств), *консоль восстановления* (применяется в случае если все вышеперечисленное не дает эффекта, позволяет управлять устройствами и драйверами из командной строки, но необходимо знать имя устройства или файл драйвера). При возникновении ошибок устройств в Диспетчере устройств отображаются коды состояний, позволяющие определить тип ошибки. Описание кодов можно найти в справочной системе Windows.

§7. Управление дисковой памятью

Физический диск – устройство для хранения данных (жесткий диск). Логический том – единица дисковой памяти, подлежащая настройке и управлению. Может

объединять пространство нескольких физических дисков. Один физический диск может быть «разбит» на несколько логических томов. *Логические диски* и *логические тома* – синонимы. Как правило, логические диски обозначают одной буквой латинского алфавита. При необходимости пространство логического диска можно смонтировать к папке файловой системы, расположенной на другом диске. Это позволяет расширить объем нужных папок и снимает ограничение на количество логических дисков, обозначаемых одной буквой.

Отказоустойчивость – способность системы продолжать работу при сбое одной из ее частей. Отказоустойчивость дисковой системы обеспечивают два типа логических томов: *зеркальный* (RAID-1) и *чередующийся с четностью* (RAID-5). В отказоустойчивых дисковых системах используется не менее двух дисков, продолжить работу нельзя в случае, если в системе сломалось более одного диска. При создании отказоустойчивых систем не рекомендуется использовать диски, подключенные к разным шинам.

Системы RAID-5, реализованные программно, могут сильно снизить производительность системы, поэтому по возможности рекомендуется приобретать аппаратные RAID-5 – массивы. При планировании дисковой системы следует разделять данные между логическими томами по их типам. Данные системы нужно хранить на одном диске, приложения на другом, а данные пользователя на третьем. При этом отказоустойчивость обеспечивают для тома с системными файлами, а для остальных данных ограничиваются процедурами резервного копирования.

Физический диск может быть разделен на *базовые (простые) логические диски* и *динамические диски*.

Базовые диски разбивают на *разделы* (партиции), каждый из которых представляет собой единицу хранения. Базовый диск может содержать до четырех разделов (четыре основных или три основных и один дополнительный). Информация о расположении и размере каждого из разделов хранится на диске в таблице разделов главной загрузочной записи (MBR). Основной раздел может быть активным, если он используется для запуска операционной системы. Каждому основному разделу соответствует один логический том на базовом диске. Дополнительный раздел не форматируется и ему не назначается буква диска. Его делят на логические диски. В предыдущих версиях Windows дополнительные разделы использовали потому что система видела только два раздела: один основной и один дополнительный, который можно было разбить на несколько логических томов. Начиная с Windows NT, такого ограничения нет и дополнительный раздел используется в случае если один физический диск требуется разбить более чем на четыре логических диска.

Динамические диски отличаются от базовых тем, что на них можно настроить неограниченное количество томов, информация о которых хранится в базе данных службы *Диспетчер логических дисков*. Если на компьютере настроено несколько динамических дисков, их можно компоновать в следующие структуры:

- *простой том* (аналог раздела на базовом диске. Его можно расширять, добавляя нераспределенное пространство того же диска),
- *составной том* (содержит пространство нескольких физических дисков – до 32, данные записываются последовательно,

занимая пространство с первого диска, не обеспечивают отказоустойчивости, т.к. если хотя бы один диск выйдет из строя, теряются все данные),

- *чередующийся (полосатый) том* (обозначается как RAID-0, объединяет пространство нескольких жестких дисков, но данные записываются параллельно на все жесткие диски, время записи очень велико, но скорость чтения достаточно высокая. Если из строя выходит один диск, теряются все данные тома. Для восстановления чередующегося тома необходимо иметь резервные копии всего тома в целом. При выходе из строя какого-либо из дисков тома, необходимо удалить том, восстановить диск и заново создать том),
- *зеркальный том* (RAID-1, состоит из двух одинаковых копий простого тома, каждая из которых находится на отдельном жестком диске. Если один из дисков вышел из строя, система продолжает работу. В случае если на зеркальном томе присутствуют ошибки ввода – вывода, необходимо проверить состояние кабелей и выполнить команду *Реактивировать том* в консоли Управление дисками. При более серьезных ошибках необходимо либо *Разбить зеркало* – копии данных останутся на обоих дисках, либо *Удалить зеркало* – копии данных останутся на одном диске, а на втором будет нераспределенное пространство),
- *том RAID-5* (объединяет пространство трех и более дисков, данные равномерно

записываются на все физические диски и чередуются с информацией о контрольной сумме, называемой четностью. Если один из дисков выходит из строя, потерянную информацию можно восстановить, используя оставшиеся данные и информацию о контрольной сумме).

На практике полезно использовать зеркала для системных томов, RAID-5 – тома, для томов с приложениями и базами данных и полосатые тома для данных пользователей. В сочетании со стратегией резервного копирования такая конфигурация обеспечит наилучшую производительность и необходимую отказоустойчивость.

Динамические диски не поддерживаются на портативных компьютерах и для съемных носителей. Динамические диски не дают преимуществ, в случае если на компьютере установлен только один физический диск. По умолчанию в Windows Server 2016 все диски являются базовыми, т.к. это промышленный стандарт и к базовым дискам можно обращаться из любой операционной системы.

Для управления дисками используют одноименную оснастку из консоли Computer Management или утилиту *diskpart*. С помощью этой оснастки можно управлять дисками не только на локальном, но и на удаленном компьютере. Она взаимодействует с дисками не напрямую, а использует *Службу администрирования диспетчера логических дисков*.

Настройка дисков включает в себя следующие действия:

- *установка диска* (диск необходимо подключить к шине компьютера и подать на него питание, а

в оснастке Управление дисками выбрать команду *Повторить сканирование дисков*),

- *инициализация дисков* (чтобы с диском можно было работать его нужно инициализировать, выбрав в оснастке Управления дисками одноименную команду),
- *создание разделов и логических томов* (можно перевести базовый диск в динамический, указать размеры разделов на данном диске и создать их с помощью мастера),
- *форматирование томов* (поддерживаются три файловые системы FAT, FAT32 и NTFS. Использовать первые две файловые системы необходимо только в случаях если на компьютере установлена более ранняя вервия Windows в качестве второй системы или в сети есть клиенты под управлением таких ОС),
- *назначение букв дискам или монтирование томов к пустым папкам* (монтировать можно только к папкам, расположенным на локальных томах NTFS, а монтируемый том может быть отформатирован с использованием любой файловой системы. Назначать дискам можно любые латинские буквы кроме уже занятых. Нельзя изменить букву тома, который является системным или загрузочным).

В случае если в системе используются динамические диски, а на физическом диске есть неразмеченное пространство, динамические диски можно расширять. Расширять можно тома NTFS, не являющиеся системными и загрузочными.

Диски с одного компьютера можно переносить на другой. Для этого необходимо сделать следующее:

- проверить работоспособность диска на родительском компьютере (в консоли Управление дисками диск должен быть помечен значком *Исправен*);
- удалить диск на родительском компьютере;
- отключить физический диск;
- подключить диск к новому компьютеру (если он не обнаружен автоматически, *пересканировать диски* в консоли Управление дисками);
- следовать инструкциям Мастера нового оборудования;
- в консоли Управление дисками выбрать любой диск с пометкой *Чужой* и выполнить команду *Импорт чужих дисков*.

При импорте необходимо учитывать: если переносимый диск содержит тома, распространяющийся на другие физические диски, необходимо переносить их все вместе; переносить с нескольких дисков на один нужно последовательно. При переносе буквы диска могут измениться.

Базовые диски можно преобразовывать в динамические. При преобразовании разделы становятся простыми томами, а данные не теряются. Если базовые диски содержат несколько операционных систем, после преобразования такого диска в динамический доступной останется система, используемая в момент преобразования.

Динамические диски можно преобразовывать в базовые, но при этом теряются все данные на диске, а разделы придется создавать заново.

Для управления дисками также можно использовать команды *CHKDSK* (ищет ошибки на диске) и *CONVERT*

(преобразует файловые системы). Также полезно выполнять *Дефрагментацию диска*. Смысл дефрагментации в том, что большие файлы начинают занимать соседние кластеры (по умолчанию в файловой системе NTFS кластер равен 4Кб). Для полной дефрагментации требуется, чтобы на томе было свободно не менее 15% его объема.

§8. Мониторинг системы

Системная служба *Журнал событий* запускается по умолчанию и регистрирует события в трех журналах (в зависимости от роли сервера журналов может быть больше):

- Приложение (содержит информацию об изменении конфигурации системы);
- Система (содержит данные о системных событиях);
- Безопасность (содержит записи о событиях входа в систему и о доступе к ресурсам).

Для поиска определенных событий в файлах журналов можно использовать фильтры по типам события источнику события и прочим параметрам. Также можно настраивать максимальный размер файла журналов и задавать поведение системы при достижении файлом журнала максимально заданного размера: *Затирать старые события по необходимости* (события всегда перезаписываются); *Затирать события старее n-дней* (перезаписываются события, дата создания которых раньше установленной); *Не затирать события* (файлы журнала очищаются вручную, а до этого события перестают регистрироваться).

Чтобы не потерять информацию из файлов

журналов необходимо либо ежедневно их архивировать, либо с помощью политики безопасности заставлять компьютер перезагружаться, если события не могут быть записаны в системные журналы.

Контролировать производительность системы можно с помощью одноименной консоли, в которой можно анализировать данные множества счетчиков. Данная консоль может собирать данные на локальном или удаленном компьютере. Также можно задавать интервалы снятия показаний счетчиков. Счетчики можно добавлять и удалять. Счетчики упорядочены по типам объектов, для контроля за которыми они применяются, видам и экземплярам. Экземпляров счетчика может быть несколько, например, если один и тот же счетчик следит за производительностью разных жестких дисков. Также можно использовать сводные счетчики, тогда значение его экземпляра равно не порядковому номеру, а «_Total». При использовании оснастки Журналы и оповещения производительности можно просматривать данные счетчиков параллельно с их записей в журнал и при превышении пороговых значений счетчиков направлять соответствующее сообщение администратору по электронной почте.

Не зависимо от стратегии выбора счетчиков необходимо сначала сформировать так называемую базовую линию (Base Line): записать показания выбранных счетчиков при нормальной работе компьютера. Эти показания в дальнейшем станут эталоном в сравнении с текущими показаниями счетчиков при мониторинге.

Существуют два метода выбора счетчиков: в зависимости от роли сервера и анализ базовых подсистем компьютера. В любом случае желательно контролировать

совокупности счетчиков, относящихся к работе памяти, процессора, дисковой подсистемы и сетевых интерфейсов.

Полезной утилитой является программа Диспетчер задач. С ее помощью можно узнать о том, какие процессы и приложения запущены на компьютере, от имени каких пользователей осуществляются те или иные операции, получить информацию о некоторых счетчиках, связанных с памятью и сетью, и просмотреть список пользователей, использующих компьютер удаленно. Запущенные приложения и процессы можно прерывать и запускать вновь, пользователей, вошедших в систему, можно принудительно отключать.

В Windows Server 2016, как и ранее, реализована технология *Инструментарий управления Windows (WMI).* Это специализированный интерфейс на основе базы данных, в котором собираются сведения о различных компонентах системы. В зависимости от этого администратор может ими управлять. На основе технологии WMI созданы оснастки *Сведения о системе*, *Свойства системы*, *Службы* и пр. Использовать технологию WMI можно из командной строки с помощью утилиты *WMIC*. С помощью данной утилиты можно управлять локальным компьютером, составлять административные сценарии или удаленно управлять одним или несколькими компьютерами.

§9. Основные сведения об инфраструктуре сети и создание сетей на основе стандартных компонентов Windows

Инфраструктура сети – совокупность определенных компонентов, обеспечивающих связь, управление, безопасность и другие свойства сети. Синонимом физической инфраструктуры является термин «топология» - фактическое расположение сетевых узлов и соединительных элементов сети (кабелей, маршрутизаторов, компьютеров, серверов и пр.). Также к ней относятся транспортные технологии: 802.11x, Ethernet и другие. Логическая инфраструктура – множество программных элементов, используемых для связи управления и безопасности сети. Например, система доменных имен (DNS), сетевые протоколы (UDP), сетевые службы и прочие.

В серверных продуктах Microsoft сетевыми подключениями называют логические интерфейсы между программными и аппаратными средствами (связующий элемент между «железом» и программным кодом). Все сетевые подключения, настроенные на компьютере отображаются в окне Сетевые подключения. Сетевые подключения поддерживают различные *протоколы*, службы и клиентов. *Сетевые протоколы* – это языки взаимодействия компьютеров в сети (стандартизированные методы передачи информации от одного узла к другому). В сетях Windows для соединения компьютеров используются только те протоколы, которые установлены на локальном компьютере. По умолчанию устанавливается только протокол TCP/IP, все остальные протоколы нужно устанавливать вручную. *Сетевые службы* – это подпрограммы, предоставляющие определенные функции узлам или протоколам в сети.

Сетевые клиенты – это подпрограммы, позволяющие компьютеру подключаться к уже организованным сетям. Список доступных для установки сетевых служб, протоколов и клиентов можно увидеть в свойствах сетевого подключения.

Адресация – это система назначения и использования компьютерами сетевых адресов, позволяющая объединять их друг с другом. Тип адресации зависит от используемого протокола и внутренних правил организации. Адреса можно настраивать вручную, распределять в сети с помощью DHCP – сервера или операционная система назначит их автоматически.

С точки зрения пользователя к компьютеру или ресурсу удобно обращаться не по цифровому адресу, а по значащему имени. В большинстве сетей используется технология разрешения имен – это преобразование значащего имени в адрес (прямое преобразование) или преобразование цифрового адреса в значащее имя (обратное преобразование). В операционных системах Windows используются две системы разрешения имен: NetBIOS и DNS.

Количество компьютеров в мире гораздо больше числа возможных сетевых адресов, поэтому сетевые адреса, используемые во внутренних сетях различных организаций, часто совпадают. Внешние сетевые адреса уникальны и используются для взаимодействия в Интернете. Система NAT – это программа преобразования сетевых адресов, позволяющая внутренним компьютерам сети с частными адресами, взаимодействовать с Интернетом. Использование NAT подразумевает внесение изменений в систему частных адресов. ICS (общие подключения к Интернету) – простейшая реализация NAT в Windows системах.

Для конфигурирования подключений в ОС Windows Server 2016 необходимо запустить утилиту Network and Sharing Center из Control Panel, в которой отображаются сетевые адаптеры, установленные на данном компьютере. Сами по себе подключения связи компьютеров не обеспечивают: к ним необходимо «привязать» протоколы, клиенты и, в ряде случаев, службы.

По умолчанию к каждому сетевому подключению привязывается протоколы TCP/IPv4-v6, Клиент для сетей Microsoft. Для привязки других протоколов и сетевых служб в свойствах сетевого подключения на вкладке Общие нужно нажать кнопку Установить. Дополнительными параметрами конфигурирования (вкладка Дополнительно свойств сетевого подключения) являются приоритет сетевых подключений (компьютер связывается по сети с использованием установленных подключений идя по списку сверху вниз), порядок привязки служб к каждому из подключений, порядок служб доступа. Порядок служб доступа связан сразу со всеми подключениями.

Свойства протокола TCP/IP можно просмотреть, щелкнув по нему кнопкой правой мыши в окне свойства сетевого подключения и выбрав в выпадающем меню команду Свойства. По умолчанию считается, что новый компьютер подключается к сети из одного сегмента и в ней нет DHCP-сервера. Это значит, что сетевой адрес (ip-адрес) должен быть присвоен компьютеру автоматически. Для этого существует система APIPA, назначающая компьютеру адрес из диапазона 169.254.0.1 – 169.254.255.254. Система APIPA используется в случае если, на компьютере не применяется альтернативная конфигурация.

Команда *ipconfig /all* позволяет получить полную

информацию об ip-конфигурации компьютера, в т.ч. и об использовании системы APIPA. Если компьютеру назначен адрес из указанного диапазона, а в строке Автонастройка включена стоит Да, значит APIPA работает. Компьютер с таким адресом «видит» только компьютеры с APIPA-адресами до первого маршрутизатора, т.к. в этом случае не задаются адреса основного шлюза, DNS-сервера. Если в данном сегменте сети появляется DHCP-сервер, адрес APIPA заменяется адресом, полученным от DHCP. Если нужно, чтобы компьютеры взаимодействовали со всеми внутренними и внешними ресурсами в отсутствии DHCP, необходимо настроить альтернативную конфигурацию. APIPA отключается либо при использовании DHCP-сервера либо при задании IP-адреса вручную, либо через системный реестр. Можно отключить автоматическую адресацию либо на одном сетевом адаптере, либо сразу на всех. Чтобы отключить APIPA на одном адаптере нужно в редакторе реестра *regedit* в разделе *HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<код адаптера>* добавить параметр *IPAutoconfigurationEnabled* типа REG_DWORD со значением 0. Чтобы отключить APIPA на всех адаптерах можно так: нужно в редакторе реестра *regedit* в разделе *HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters* добавьте параметр *IPAutoconfigurationEnabled* типа REG_DWORD со значением 0. В обоих случаях, для того чтобы изменения вступили в силу необходимо перезагрузить компьютер.

В крупных сетях APIPA адреса не применяются, поэтому если сетевой адрес компьютера попадает в диапазон адресов APIPA – это явный признак ошибки. В этом случае необходимо проверить состояние сетевого

кабеля, адрес и доступность шлюза по умолчанию и выполнить две команды *ipconfig /release* + *ipconfig /renew* (при наличии в сети DHCP) или назначить компьютеру статический ip-адрес.

Если проблема не решена необходимо продолжить проверку исправности оборудования: кабелей, концентраторов, коммутаторов. Зачастую достаточно удалить пыль с разъемов, переставить сетевую карту в другой слот или заменить кабель заведомо рабочим. Также не нужно забывать о методе последовательных отключений. Если компьютеру присваивается адрес из одних нолей, нужно проверить, не отключен ли APIPA в реестре или запросить новый адрес у DHCP. В случае если компьютеру не удается получить APIPA-адрес нужно также проверить, не используется ли альтернативная конфигурация. В любом случае не нужно забывать, что система APIPA – временная мера, пригодная для небольших или тестовых сетей.

§10. Адресация в Windows

TCP/IP- это набор протоколов, лежащих в основе связи в сетях Windows и Интернете. Стек протоколов TCP/IP состоит из четырех уровней: *сетевого интерфейса, межсетевого, транспортного и прикладного*.

Уровень сетевого интерфейса определяет тип передачи электрических импульсов и методы взаимодействия с физическими устройствами. К стандартам этого уровня относятся: Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI) X.25, Frame Relay, RS-232 и V.35.

Межсетевой уровень обеспечивает упаковку

данных, присвоение им адреса и перенаправление в нужную точку сети. На этом уровне используются протоколы: *IP* (обеспечивает маршрутизацию пакетов между узлами согласно их адресам, не исправляет ошибки очередности, потери или дублирования пакетов), *ARP* (служит для нахождения в каждом из сегментов сети физических компьютеров, которым предназначаются IP-пакеты, информация сопоставления IP и MAC адреса компьютера хранится в локальном кэше ARP, для просмотра которого служит команда *ARP –a*, а для очистки – команда *ARP –d*), *ICMP* (обеспечивает функционирование команды *ping* и обмен информации об ошибках между узлами маршрутизации).

Транспортный уровень – это этап передачи информации, на котором определяются стандарты передачи данных. На этом уровне работают протоколы TCP (группирует в пакеты принятые с прикладного уровня данные, нумерует их и ставит в очередь на доставку по конкретному адресу. Поскольку каждое приложение-адресат прослушивает собственный TCP-порт на предмет входящих сообщений, на одном узле можно использовать различные TCP-сервисы. Гарантирует очередность и доставку пакетов) и UDP (сервис без установления соединения, обеспечивающий лишь доставку узлу сети без контроля очередности и отложенных пакетов. Его используют большинство сетевых сервисов, т.к. он работает быстрее TCP).

Прикладной уровень. На этом этапе данные конечного пользователя обрабатываются, упаковываются и пересылаются на порты транспортного уровня. На этом уровне функционируют протоколы: HTTP, FTP, DNS, POP3, SMTP и другие.

В стеке протоколов TCP.IPv4 адреса разделяются на

общие и частные. Общие адреса используются для компьютеров, непосредственно видимых из Интернета, а частные адреса никогда в Интернете не используются. Диапазоны частных адресов: 10.0.0.0-10.255.255.254; 172.16.0.0-172.31.255.254; 192.168.0.0-192.168.255.254. IP-адреса назначаются либо вручную (для важных сетевых узлов), либо динамически (DHCP), либо автоматически (APIPA). IP-адрес представимы в разных формах. Первая форма – десятично-точечная нотация: четыре числа из диапазона 0-255, разделенных точкой. В компьютере применяется двоичная нотация. В ней числа представляют четыре 8-битных значения, составляющих 32-битный адрес. В любой нотации каждое из четырех чисел называется октетом (потому что это 8 бит). В адресах биты и октеты считаются слева направо. Для перевода IP-адреса из одной нотации в другую достаточно знать соотношение между десятичной и двоичной системами счисления.

Часто между узлом-отправителем и узлом-адресатом в сети много маршрутизаторов, поэтому при доставке пакета необязательно сразу иметь четкий маршрут его доставки. Достаточно знать адрес подсети на каждом следующем шаге пересылки. Для этого IP-адрес разделяют на две части: идентификатор сети (первая слева направо часть IP-адреса) и идентификатор узла (вторя слева направо часть IP-адреса).

Правила назначения идентификаторов сетей и узлов:

1. идентификатор узла должен быть уникален в пределах локальной подсети (до ближайшего маршрутизатора);
2. нельзя присваивать всем битам идентификаторов сети и узлов значение

единица – такие адреса используются для широковещания;

3. нельзя присваивать всем битам идентификаторов сети и узлов значение ноль – с таких адресов не отправляются пакеты.

IP-адреса подразделяются на классы в зависимости от того сколько октетов используется для идентификаторов сети (от этого также зависит количество узлов в сети): класс A (идентификатор сети – первый октет, его десятичное значение 1-126), класс B (идентификатор сети – первые два октета, десятичные значения первого октета 128-191), класс C (идентификатор сети – первые три октета, десятичные значения первого октета 192-223), класс D (значения первого октета: 224-239), класс E (значение первого октета: 240-254). Для адресации используются адреса классов A, B и C. Класс D зарезервирован для многоадресной рассылки, класс E – для экспериментального использования. Для определения принадлежности конкретного IP-адреса к той или иной подсети используется так называемая маска подсети: IP-адрес, представляющий собой последовательность битов со значением единица на местах идентификатора сети и битов со значением ноль на местах идентификатора узла (например, маска подсети для IP-адресов класса B – 11111111 11111111 00000000 00000000). Часто для обозначения маски подсети используют количество единиц в ней и записывают его через дробь после IP-адреса, например, адрес класса C – 192.168.0.1 будет иметь маску 24 и это записывается 192.168.0.1/24 (нотация с префиксом).

Связь между узлами разных сетей осуществляют маршрутизаторы – устройства с несколькими

интерфейсами (сетевыми картами), подключенными к разным подсетям. Процесс пересылки пакетов с одного интерфейса на маршрутизаторе на другой называется маршрутизацией, а сетевой адрес внутреннего интерфейса называется основным шлюзом. В случае если на компьютере не указан основной шлюз, он не может отправлять данные в другую подсеть (дальше первого маршрутизатора).

Подсетью называется логическая сеть, определяемая маской подсети. Механизм разбиения на подсети заключается в процессе установки в единицу дополнительных битов маски подсети. При этом компьютеры с IP-адресами из одного класса, но с разными масками, смогут посылать пакеты только тем компьютерам, у которых маски подсетей будут совпадать. Для связи с другими компьютерами будет необходим, например, коммутатор. С помощью разбиения на подсети можно решить задачи соответствия физической и логической инфраструктур сети, сократить нагрузку на сеть за счет уменьшения широковещания и адекватно использовать адресное пространство. Для определения количества узлов в подсети необходимо возвести 2 в степень, равную количеству битов в идентификаторе узла, и вычесть 2 (убираем адреса из одних нолей и единиц). Для определения количества доступных в адресном пространстве подсетей надо возвести 2 в степень, равную количеству бит в идентификаторе подсети (количество бит в идентификаторе подсети равно нулю, если вы используете стандартные маски).

Десятично-точечная форма маски подсети позволяет легко определить диапазон IP-адресов в каждой подсети: нужно вычесть из 256 значение в соответствующем октете маске. Например, в сети класса С адресом

205.200.70.0 и маской подсети 255.255.255.168 вычитание 168 из 256 даст 88. таким образом каждый диапазон начинается после каждого 68-го адреса: 205.200.70.0-205.200.70.87, 205.200.70.88-205.200.70.175 и т.д. Компьютеры из разных диапазонов могут соединяться друг с другом через маршрутизатор. Обратным к процессу создания подсетей является процесс создания надсетей (в стандартных масках подсети единицы справа налево заменяют нулями) это позволяет более эффективно использовать конечное адресное пространство. Например, в сеть нужно объединить 2000 узлов, это слишком много для сети класса С, где возможно всего 254 узла. Сеть класса В может иметь 65534 узла, но таких сетей возможно 16383 и количество свободных быстро сокращается, провайдерам нет смысла давать клиенту адрес класса В, если он будет использовать всего 2000 клиентов. В таком случае выдается адрес класса С, а маска подсети уменьшается с 24 до 21. безусловно, на практике встречаются гораздо более сложные задачи маршрутизации, например, разбиение на подсети самих подсетей или разбиение сети на подсети разных размеров. Для этого существует технология VLSM (маски подсети переменной длины). О ней вы можете узнать в справочной системе Windows.

При установке операционной системы протокол TCP/IP настроен на автоматическое получение адреса, как в общем случае, так и в альтернативной конфигурации. Настройки протокола можно изменить, выбрав свойства сетевого подключения, а потом выбрав свойства протоколы TCP/IP. При отсутствии в сети DHCP-сервера можно вручную задать IP-адрес компьютера, маску подсети, основной шлюз, адреса DNS-серверов и прочие.

Для внесения изменений в настройки TCP/IP

необходимо обладать привилегиями учетной записи Администратор.

§11. Мониторинг и устранение неполадок TCP/IP

Одной из частей мониторинга работы сети является анализ сетевого трафика, который осуществляется с помощью того или иного анализатора протоколов. В Windows Server 2016 есть специальная утилита *Сетевой монитор*, позволяющая: перехватывать кадры прямо из сети; отображать и фильтровать перехваченные кадры, а в полной версии еще и редактировать перехваченные кадры и перехватывать кадры с удаленного компьютера. В данном определении термины «кадр» и «пакет» являются синонимами, хотя с технической точки зрения между ними есть разница – кадр содержит информацию не только о протоколах межсетевого, но и транспортного уровней, а пакет несет информацию только о протоколах межсетевого уровня. Однако анализаторы протоколов корректно работают только в сетях, где нет коммутаторов. При наличии коммутаторов в сети *Сетевой монитор* способен перехватить пакет в сегменте до ближайшего коммутатора. *Сетевой монитор* не устанавливается по умолчанию и добавляется с установочного диска с помощью утилиты *Установка и удаление программ*. При установке *Сетевого монитора* устанавливается также *драйвер Сетевого монитора*. Драйвер можно установить и отдельно. Это целесообразно сделать на клиентских компьютерах. Для установки драйвера *Сетевого монитора* необходимы привилегии учетной записи Администратор.

При запуске административной части *Сетевого монитора* можно начать запись входящих или

исходящих из локального компьютера потоков данных. Данные разбиваются на кадры, которые содержат следующую информацию: адрес компьютера-отправителя, адрес компьютера-приемника, заголовочная информация всех протоколов, использованных при пересылке данных, собственно данные. Сетевой монитор копирует все кадры в буфер, объем которого ограничен объемом памяти компьютера.

Во время и по окончании записи данных можно просматривать и анализировать разнообразную статистику как, то: показания счетчиков работоспособности сети, информацию об узлах, использующих широковещание и пр. Также можно просмотреть детальную информацию о кадрах в порядке их поступления. Кадры нумеруются, начиная с единицы, записывается время записи кадра, аппаратные адреса компьютеров отправителя и приемника, запись о протоколе самого высокого уровня, который удалось распознать и пр. Протоколы, используемые при передаче кадра, указаны сверху вниз (от самого низкого до самого высокого уровня).

В случае если при передаче кадра используются протоколы, не входящие в стандартный набор TCP/IP, порядок ссылки на них определяется в соответствии с моделью OSI, содержащей не 4, а 7 уровней. Уровню *Сетевого интерфейса* соответствуют физический и канальный уровни. *Межсетевому* уровню соответствует сетевой уровень. *Транспортный* уровень остается без изменений, а до *прикладного* уровня выделяют сеансовый и презентационный уровни (например, протокол NBT считается интерфейсом сеансового уровня, а протокол SMB – протоколом презентационного уровня).

Чтение и анализ содержимого кадров называется

разбором и выполняется специальными модулями «парсерами». Сетевой монитор содержит более 20 парсеров в форме DLL-файлов. Можно добавлять собственные парсеры для анализа специфических протоколов, для этого специальную DLL-библиотеку нужно записать в папку Windows\System32\Netmon\Parsers. Кроме этого нужно добавить информацию о новом парсере и протоколе в файл Parser.ini, находящийся в папке Windows\System 32\Netmon.

Устранять неполадки IP-конфигурации на неисправном компьютере нужно начинать с команды *ipconfig /all*, дающей информацию об адресах компьютера на всех активных сетевых интерфейсах.

Также для диагностики сети может применяться утилита *Netdiag*. Netdiag выполняет проверки локального компьютера и отображает их результаты, в которых и следует искать сообщения об ошибках. В случае если неполадку на локальной машине устранить не получилось, «узкое место» продолжают искать дальше в сети с помощью команд *ping, pathping* и *tracert. Ping* служит для проверки связи на уровне IP, а *pathping* обнаруживает потерю пакетов на маршрутизаторе со многими переходами. Команду *ping* применяют в следующем порядке: проверяют адрес замыкания на себя, проверяют адрес локального компьютера, проверяют доступность основного шлюза, проверяют доступность удаленного узла за основным шлюзом. На четвертом этапе можно воспользоваться командой *pathping* или *tracert.* Отличие последних в том, что *pathping* позволяет точно установить, где потерялся пакет, а *tracert* выделяет маршрутизаторы, на которых произошли какие-либо ошибки. В случае если первые два этапа применения

команды *ping* были успешными, а третий этап – неудачным, следует проверить корректность информации в кэше ARP.

На компьютере и сетевом шлюзе нужно выполнить команду *arp –a*, затем на обеих машинах выполнить команду *ipconfig \all* и посмотреть соответствие фактических и кэшированных MAC-адресов. В случае ошибок нужно удалить неправильные записи из кэша командой *arp –d* и создать новые записи командой *arp –s*. Если ошибки кэша не выявлены, а узлы не могут обмениваться информацией, следует проверить исправность физических устройств: кабелей, маршрутизаторов и сетевых карт.

§12. Разрешение имен в Windows Server 2016

Для разрешения имен в сетях на базе Windows Server 2016 используются два механизма: DNS и NetBIOS. DNS имеет приоритет перед NetBIOS (DNS более масштабируема, безопасна и совместима с Интернетом, используется в подавляющем большинстве случаев при организации сети, NetBIOS применяется в качестве вспомогательного механизма для быстрой организации связи компьютеров внутри одного сегмента сети). В отличие от NetBIOS пространство имен DNS выстроено в иерархию, основанную на полных доменных именах (FQDN). NetBIOS-имя должно быть уникальным в пределах всей сети, DNS-имя – в пределах домена. При установке операционной системы компьютеру необходимо присвоить имя. По умолчанию это имя считается DNS-именем, а его первые15 символов – NetBIOS-именем.

Методы разрешения имен в DNS и NetBIOS также

различны. DNS использует два метода: поиск имени в кэше *DNS-клиента* (имена кэшируются при более ранних запросах или загружаются из файла Hosts, находящегося в папке Windows\System32\Drivers\etc) и запрос DNS-сервера (в случае, если в корпоративной сети используется проксирование, то в первую очередь запрашивается реализация DNS-сервера на прокси, также нужно учесть, что браузеры сторонних празработчиков имеют собственный механизм разрешения dns-запросов). NetBIOS использует 4 метода: поиск имени в кэше NetBIOS-имен, запрос WINS-сервера, широковещательные запросы в сегменте, поиск имени в файле LMhosts из той же самой папки, что и в прошлый раз.

В ряде случаев использование той или иной системы разрешения имен обязательно. DNS обязательно при построении сети на основе доменов, для выхода в Интернет или иную внешнюю сеть. NetBIOS обязательна в сети на основе доменов Windows NT или рабочих групп, а также при использовании в сети старых приложений, использующих протокол NetBT, а также для любителей функции *Мое сетевое окружение*.

Однако в Windows Server 2016 NetBIOS включена по умолчанию. Возможность широковещания в сети сильно подрывает безопасность последней, т.к. NetBIOS хранит информацию обо всех сетевых ресурсах сегмента и предоставляет ее любому в ответ на широковещательный запрос без идентификации опрашивающего. Поэтому в сетях, где нет нужды во взаимодействии с системами младше Windows 2000, механизм NetBIOS должен быть отключен. Чтобы отключить NetBIOS необходимо в свойствах TCP/IP, привязанного к сетевому подключению, открыть

свойства WINS-сервера и установить галочку напротив параметра *Отключить NetBIOS через TCP/IP*.

Система DNS представляет собой древовидную структуру с одним корнем, имеющим не ограниченное число поддоменов, в свою очередь каждый из поддоменов может иметь неограниченное число дочерних поддоменов. Верхним корневым доменом является пустая строка «». Этот домен имеет, например, поддомен первого уровня «.ru», который в свою очередь имеет массу поддоменов второго уровня, например «yandex.ru». Каждый компьютер в системе DNS идентифицируется при помощи FQDN, однозначно определяющего положение компьютера по отношению к корневому домену. Буквально FQDN состоит из записанных слева направо через точку имени компьютера и имен всех доменов и поддоменов вплоть до корневого. FQDN всегда заканчивается завершающей точкой, как бы отделяющей значащее имя от корневого домена – пустой строки. Также существуют домены с обратными именами – это специальные домены, использующиеся для преобразования IP-адресов в имена компьютеров (обратного просмотра). Их имена принадлежат домену in-addr.arpa.

Организации, не пользующиеся Интернетом вправе организовывать частные пространства DNS-имен, задавать там иерархию и конкретные имена доменов и поддоменов администраторы вольны сами. Таким образом, внутри своей организации легко можно организовать домен Microsoft.com. Для правильного функционирования DNS необходимо настроить DNS-серверы, зоны, записи ресурсов и распознаватели.

DNS-сервер – это компьютер с запущенной службой *DNS-сервера*, поддерживающий базу данных имен и

обрабатывающий запросы на их разрешение от *DNS-клиента*. При размещении зоны на DNS-сервере он является полномочным для этой зоны, если выполняет роль основного или дополнительного DNS-сервера. Полномочные сервера используют только записи ресурсов, а не информацию из кэша. DNS-серверы могут быть полномочными и для нескольких уровней доменной иерархии.

Зона DNS – это единая часть пространства имен, обслуживаемая полномочным сервером. Сервер может обслуживать несколько зон, а зона может содержать несколько доменов. Файлы зон содержат записи ресурсов, для которых сервер является полномочным. Это, как правило, текстовые файлы, а на контроллерах доменов - это часть базы данных Active Directory.

Записи ресурсов – это информация, используемая для ответов на запросы DNS-клиентов. Буквально это тип и имя сетевого узла и сопоставленный ему IP-адрес.

Распознаватель DNS – это служба, использующая протокол DNS для запросов информации у DNS-сервера. Windows Server 2016 – это служба DNS-клиент.

Существует несколько способов разрешения DNS-запросов. *Первый способ* - клиент обращается к DNS-серверу, который сам разрешает запрос, используя собственную базу данных записей ресурсов (DNS-клиент направляет запрос предпочтительному серверу, указанному в настройках TCP/IP. Получив запрос, сервер проверяет записи локальных зон, а потом собственный кэш. Если нужная информация найдена, то она пересылается клиенту, а если нет – сервер выполняет *рекурсию* или клиент выполняет *итеративные запросы*). Или клиент просто обращается к своему кэшу без обращения к серверу (в кэш попадают все записи из

файла hosts при включении компьютера или при изменении файла hosts, также в кэш попадают ответы, полученные на предыдущие DNS-запросы). *Второй* – рекурсия (этот метод используется по умолчанию): DNS-сервер от имени клиента обращается к другим DNS-серверам. Получив от них ответ, DNS-сервер пересылает его клиенту. *Третий способ* – итерация (используется на DNS-сервере, если запрещена рекурсия): *DNS-клиент* для разрешения запроса сам обращается к дополнительным DNS-серверам, направляя им дополнительные запросы.

Корректное разрешение имен Интернета обеспечивается существованием так называемых корневых ссылок. Это список записей ресурсов, содержащих адреса полномочных серверов в корне доменного дерева глобальной DNS. Файл корневых ссылок Cache.dns находится в папке Windows\System32\DNS. Его содержимое загружается в память сервера при старте системы. На корневом DNS-сервере наличие корневых ссылок не допускается. На таких серверах файл с корневыми ссылками удаляется автоматически.

DNS-сервер направляет клиентам ответы разных типов: *полномочный ответ* (ответ с записью ресурса с удостоверением, что он получен от полномочного сервера), *положительный ответ* (ответ с записью ресурса), *ответ-ссылка* (ответ означает, что DNS-сервер не может разрешить запрос и на нем запрещена рекурсия. Полученную ссылку DNS-клиент использует для следующего итеративного запроса), *отрицательный ответ* (либо сообщение полномочного сервера о том, что запрашиваемое имя не существует в указанном пространстве DNS либо сообщение об отсутствии указанного в запросе типа записи ресурса).

Ответ на запрос распознаватель передает клиенту и копирует его в кэш. DNS-клиент и DNS-сервер поддерживают собственные кэши. Кэш DNS-клиента формируется на основе файла Hosts и ранее сделанных запросов. Кэш DNS-сервера формируется на основе только ранее сделанных запросов. Записи в кэше DNS-сервера по умолчанию хранятся один час. Однако это время можно корректировать. Очищать кэши сервера и клиента можно принудительно из командной строки. Для очистки кэша DNS-клиента используется команда *ipconfig /flushdns*, а для очистки кэша DNS-сервера используется команда *dnscmd /clearcache*.

§13. Развертывание DNS-сервера и настройка DNS-клиента

На всех компьютерах под управлением операционных систем Windows (начиная с 2000) служба *DNS-клиент* устанавливается и запускается по умолчанию, а службу DNS-сервера необходимо устанавливать вручную с помощью добавления новой роли используя Server Manager→Add Roles and Features→DNS. Следует отметить, что при установке роли контроллера домена роль DNS-сервера будет установлена автоматически.

На DNS-серверах можно настраивать два вида зон: *прямого* (для разрешения FQDN-имен в IP-адреса) и *обратного просмотра* (для разрешения IP-адресов в FQDN-имена). Также зоны бывают трех типов: *основная зона* (хранит базовые данные для всех доменов в зоне), *дополнительная* (резервная копия основной зоны или других дополнительных зон), *зона-заглушка* (содержит только записи ресурсов полномочных DNS-серверов

главной зоны).

В зависимости от типа зоны DNS-сервера также различаются на типы. *Основной сервер* создается при добавлении на него основной зоны. Новым зонам всегда назначается такой тип. Основные зоны могут быть стандартными (размещаются только на одном сервере) или интегрированными с AD (являются частью базы данных активного каталога, реплицируются на все контроллеры доменов, одновременно являющихся DNS-серверами, а значит обеспечивают отказоустойчивость и защищенность). Дополнительные серверы необходимо развертывать в сильно сегментированных сетях, чтобы сократить маршрут запроса от DNS-клиента к серверу. Вообще рекомендуется, чтобы одну зону обслуживали два DNS-сервера.

Дополнительный DNS-сервер получает информацию от главного сервера, которым может быть основной сервер или другой дополнительный. Таким образом, количество дополнительных серверов, обслуживающих одну и ту же зону ограничено лишь практической потребностью.

Серверы зон-заглушек используются для поддержания в родительской зоне свежего списка серверов имен дочерней зоны.

Существуют DNS-сервера, на которых зоны вообще не размещаются. Однако на них кэшируется информация, полученная при запросах на разрешение имен. Такие сервера называются *серверами кэширования*. Применение таких серверов целесообразно при связи через медленные каналы и в сетях, не подключенных к Интернету. Содержимое кэша можно просмотреть в консоли DNS, причем в расширенном варианте. Очистить кэш DNS-сервера можно либо с помощью одноименной команды в

консоли или, выполнив команду dnscmd /clearcache, или перезапустить службу DNS-сервера.

Вновь созданная зона содержит только две записи ресурсов: SOA – начальная запись зоны и NS – запись сервера имен (указатель на DNS-сервер, полномочный для этой зоны). Для того чтобы зона начала работать, ее необходимо заполнить другими записями ресурсов, часть из которых создается автоматически, а часть вручную, в консоли DNS. Можно также непосредственно редактировать файлы зон, которые представляют собой упорядоченные текстовые записи, в которые можно вставлять комментарии и пустые строки, но лучше избегать подобного вмешательства.

Существуют пять наиболее часто используемых типов записей ресурсов, создаваемых вручную: адрес узла (A), каноническое имя (CNAME), почтовый обменник (MX), указатель (PTR), локатор службы (SRV). Запись ресурса узла A – хранит информацию о соответствии доменных имен и IP-адресов имен. Добавляются в зону либо вручную, либо DHCP (если компьютер в сети доступен в сети по IP-адресу и не доступен по имени, это значит в DNS отсутствует корректная запись узла A для этого компьютера (можно попробовать решить проблему командой *ipconfig /registerdns*). Запись ресурса CNAME позволяет ссылаться на узел сети более чем по одному имени. Имена серверов (ftp, www) могут регистрироваться как записи ресурса CNAME. Они сопоставляют имя узла сети, определенного для данной службы, обычной записи ресурса A, на котором размещается данная служба. Также записи ресурса CNAME используются, если необходимо переименовать существующий узел A без временно прекращения доступа к нему по старому имени, а также для

развертывания группы резервных серверов. Запись ресурса почтового обменника MX используется почтовыми программами для поиска почтового сервера данной зоны. Эти записи сопоставляют доменное имя, указанное в адресе электронной почты, записи ресурса A, где размещается почтовый сервер. Запись ресурса указателя PTR используется исключительно в зонах обратного просмотра для разрешения IP-адреса в FQDN-имя. Обратные просмотры выполняются в зонах, корень которых расположен в домене in-addr.arpa. Записи PTR добавляются в зоны также как записи ресурса A. Запись ресурса локатора службы SRV определяет местоположение конкретных служб в домене. С помощью них в сети ищут нужные сервера приложений.

Настройка клиента DNS подразумевает выполнение трех обязательных и трех дополнительных процедур. Обязательные процедуры:

1. *задание DNS-имени компьютера* (крайнее левое слово до первой точки в FQDN. Его длина не должна превышать 63 байта и может содержать только прописные и строчные английские буквы, цифры и дефисы. Имя компьютера можно изменить на вкладке Имя компьютера окна Свойства системы);
2. *определение основного суффикса DNS* (он совпадает с именем домена, которому принадлежит компьютер, изменить значение основного суффикса DNS можно также на вкладке Имя компьютера окна Свойства системы. Кроме основного суффикса DNS компьютеру с несколькими сетевыми адаптерами можно присваивать разные DNS-суффиксы подключений. В зависимости от IP-

адреса, присвоенному сетевому адаптеру на вкладке DNS свойств протокола TCP/IP можно указать DNS суффикс для данного подключения. Однако не нужно забывать, что объединение имени компьютера с DNS-суффиксом должно давать FQDN компьютера, совпадающее с записью узла A в зоне DNS. Для компьютеров, соединенных разными подсетями в зоне DNS может быть сконфигурировано количество записей ресурса A, равное количеству подсетей плюс один, но должна быть сконфигурирована хотя бы одна запись ресурса A);

3. *определение списка DNS-серверов* (в свойствах протокола TCP/IP каждого клиента необходимо указать IP-адрес DNS-сервера. Можно указать список с любым количеством DNS-серверов. Клиент начнет обращаться к ним на разрешение имен по списку сверху вниз).

Дополнительные действия:

1. *определение списка поиска суффиксов DNS* (если имя в запросе является неполным, например, yandex вместо yandex.ru, служба DNS-клиент может дополнить его суффиксом из указанного списка на вкладке DNS Свойств протокола TCP/IP. Суффиксы добавляются по списку сверху вниз. Если в этом списке ничего не указано, включается механизм автоматического дописывания суффиксов: сначала дописывается основной DNS-суффикс локального компьютера, если запрос разрешить не удалось, то дописывается DNS-

суффикс подключения, присвоенный сетевому адаптеру, если и в этот раз попытка неудачная, то дописывается родительский суффикс основного суффикса DNS);

2. *задание для каждого сетевого адаптера DNS-суффикса подключения* (обсуждалось ранее);
3. *настройка порядка динамического обновления DNS* (DNS-сервера под управлением Windows Server 2016 способны принимать динамические обновления записей ресурсов A и PTR. Обновления могут выполняться либо клиентом DNS, либо DHCP-сервером. Динамические обновления возможны, только если основной DNS-суффикс клиента совпадает с именем зоны, расположенной на основном DNS-сервере. Чтобы настроить DNS-клиент на выполнение динамических обновлений, необходимо на вкладке DNS свойств протокола TCP/IP, нужно поставить флажок напротив параметра Зарегистрировать адрес этого подключения в DNS. Клиенты со статическим IP-адресом могут обновлять записи ресурсов A и PTR, а клиенты, получающие адреса у DHCP-сервера могут обновлять только записи ресурсов A.)

Настройка DNS-сервера производится с помощью консоли DNS. Окно свойств DNS-сервера содержит восемь вкладок, с помощью которых можно управлять сервером. Вкладка *Интерфейсы* указывает, на каком из IP-адресов (сетевых контроллеров) многоадресного DNS-сервера будут обслуживаться DNS-запросы. По умолчанию обслуживает все IP-адреса. Вкладка *Пересылка* позволяет перенаправлять DNS-запросы на

другие DNS-сервера (сервера пересылки). На этой вкладке также могут быть указаны доменные имена и IP-адреса, запросы на разрешение которых необходимо пересылать другим серверам. Пересылка будет активирована только в том случае, если DNS-сервер самостоятельно не может разрешить поступивший запрос. Пересылку выгодно использовать в сильно сегментированной сети для уменьшения внешнего трафика от провайдера при разрешении имен Интернета. В этом случае имена Интернета будет разрешать один DNS-сервер, которому DNS-сервера других сегментов сети будут пересылать запросы клиентов. При выполнении запросов на сервере пересылки появится информация в кэше, которая будет использоваться в дальнейшем, что сократит внешний трафик, используемый для разрешения имен. В случае если в сети используется брандмауэр, также выгодно использовать сервер пересылки, расположенный за ним. В этом случае на брандмауэре открывается только один порт, а не несколько (для каждого из DNS-серверов сегментов сети), что улучшает безопасность.

Вкладка *Дополнительно* позволяет включать и отключать различные функции DNS-сервера. Например, функция *Отключить рекурсию*- DNS-сервер при невозможности разрешить запрос клиента направляет ему ссылки на другие DNS-сервера для итеративных запросов. Если в сети есть UNIX-сервера, необходимо активировать функцию *Дополнительные функции BIND*. Функция *Включить расстановку по адресу* возвращает в ответ на запрос клиента тот адрес многоадресного компьютера, который находится в подсети клиента. Активная функция *Ошибка*, если данные при загрузке зоны повреждены, запрещает DNS-серверу загружать

зоны с ошибками в базе данных. Функция *Включить циклическое обслуживание* выполняет ротацию IP-адресов многоадресного компьютера при ответе клиенту. Это простейший способ балансировки нагрузки сети. Расстановка по адресу приоритетнее циклического обслуживания. Функция *Безопасный кэш* позволяет размещать в кэше DNS-сервера только записи с именами, соответствующими запрошенному домену. Также на этой вкладке можно выбирать методы проверки имен в запросах, разрешать автоматическое удаление устаревших записей и выбирать источник загрузки данных зоны при старте системы. Данные зоны могут загружаться из файла, из реестра или из AD-реестра одновременно.

Вкладка *Корневые ссылки* содержит информацию о корневых DNS-серверах Интернета. Вкладка *Ведение отладки* определяет порядок ведения отладки DNS-сервера. Вкладка *Журнал событий* определяет, какие события регистрируются в журнале DNS. На вкладке *Наблюдение* можно выполнить два простых теста DNS: *запрос локального DNS-сервера* (попытка ответить на запросы прямого и обратного разрешения собственного имени), *рекурсивный запрос корневого DNS-сервера* (опрос серверов, указанных на вкладке корневые ссылки). Эти тесты можно выполнять вручную или автоматически по графику. В случае если DNS-сервер одновременно является контроллером домена, то доступна еще и вкладка *Безопасность*, на которой определены пользователи и группы, имеющие полномочия администрировать DNS-сервер.

Важным элементов конфигурирования DNS-сервера является настройка зон и его свойств. Свойства зоны доступны из консоли DNS. Окно свойств зоны содержит

пять или шесть вкладок в зависимости от того является ли DNS-сервер контроллером домена или нет. Так можно временно приостановить разрешение имен зоны, сменить ее тип, интегрировать зону с AD и выбрать вариант динамического обновления информации зоны. Если есть возможность интегрировать зону с AD, необходимо это сделать, т.к. в этом случае информация из базы данных DNS реплицируется вместе с базой AD, что резко повышает отказоустойчивость и уменьшает количество административного вмешательства. Зоны, интегрированные с Active Directory, можно изменить тип репликации. Можно реплицировать зону на все DNS-серверы в пределах леса или в пределах домена, либо на все контроллеры домена в домене, либо на все контроллеры домена, указанные в области видимости каталога приложений. Чем больше охват серверов репликации, тем выше отказоустойчивость и нагрузка на сеть. Раздел каталогов приложений – это раздел каталога, реплицируемый на указанное множество контроллеров домена под управлением Windows Server 2016. Для каждого домена в AD существуют два встроенных каталога приложений: DomainDNSZones и ForestDNSZones. Первые два варианта репликации фактически означают третий с использованием соответствующих встроенных разделов каталогов. Можно создавать свои разделы каталогов с помощью специальных команд. Windows 2000 Server не поддерживает разделы каталогов приложений, поэтому если в сети есть такая операционная система, то базу данных DNS надо реплицировать на все контроллеры домена в домене.

Существуют три варианта динамического обновления зон DNS, интегрированных в AD: *Никакие*

(обновления записей производятся вручную), *Небезопасные и безопасные* (информация записей ресурса изменяется без аутентификации владельца), *Только безопасные* (возможны только в зонах, интегрированных с AD). Запись имеет право обновить только владелец – ранее создавший ее компьютер, прошедший аутентификации по протоколу Kerberos. Это может вызвать проблему, в случае если первоначально запись ресурса была создана DHCP-сервером, а потом клиент пытается обновить ее самостоятельно. В этом случае обновление не произойдет. Для предотвращения такой ситуации DHCP-сервера рекомендуется сделать членами группы *DNSUpdateProxy*. Члены этой группы не сохраняют информации о владельцах записей ресурсов DNS. В любом случае DHCP-клиент направляет запрос на динамическое обновление записей ресурса DNS-серверу в следующих случаях: изменение IP-адреса на любом сетевом интерфейсе локального компьютера; изменение параметров аренды IP-адреса на любом из сетевых интерфейсов локального компьютера; выполнение команды *ipconfig* с ключом */registerdns*; выключение компьютера DNS-клиента; повышение роли сервера до контроллера домена.

Записи ресурсов в базе данных зоны могут устаревать. Это применимо только к динамически созданным записям. В случае если заданы временные *интервалы блокирования* (период времени, в течение которого отклоняются запросы на обновление записей ресурсов) и *интервалы обновления* (начало времени очистки) записи, не обновленные во время интервала обновления, удаляются из базы данных DNS. По умолчанию интервалы блокирования и обновления равны семи дням. Это значит, что очистка зоны по умолчанию

начнется через 14 дней.

Вкладка Начальная запись зоны (SOA) окна свойств зоны содержит номер редакции файла зоны (увеличивается на единицу при каждом изменении зоны), имя основного сервера зоны, значение интервала изменения зоны, значение интервала повтора, время нахождения информации в кэше и временной интервал, в течение которого DNS-сервер отвечает на запросы клиентов, не имея контакта с основным сервером зоны. Эти параметры связаны между собой следующим образом. По истечении интервала обновления основному DNS-серверу направляется запрос на обновления файла зоны. Если серийный номер зоны на основном сервере больше, инициируется передача зоны. Если передача не удалась, по истечении интервала повтора дополнительный DNS-сервер пытается инициировать передачу снова.

На вкладке Серверы имен можно настраивать имена полномочных серверов в данной зоне. Запись ресурса NS первого основного сервера зоны создается автоматически. На вкладке WINS указываются имена WINS-серверов, используемых для широковещательного разрешения имен. Для уменьшения сетевого трафика можно ограничить передачу зон кругом определенных серверов.

Для основных зон передача на дополнительные серверы запрещена Изменить эти настройки можно на вкладке *Передача зон*.

Передача зоны происходит при любом из трех событий: по *окончании периода обновления записи ресурса SOA основной зоны, при загрузке дополнительного сервера, при изменении конфигурации основного сервера, настроенного на уведомление*

дополнительных DNS-серверов об обновлении зоны.

Часто в сегментированных сетях возникает необходимость передать часть полномочий по управлению частью пространства имен DNS другому администратору или серверу. Для этого применяется механизм делегирования зон. Зоны необходимо делегировать, если: *управление филиалом компании осуществляется обособленно; необходимо распределить нагрузку базы данных DNS среди многих серверов имен*; *необходимо, чтобы структура имен совпадала с физической структурой сети*. Для успешного делегирования необходимо, чтобы родительская зона содержала обе записи ресурсов A и NS, указывающие на полномочный сервер вновь делегированного домена.

До делегирования создают домен, делегируемый серверу, на котором будет размещаться делегированная зона. Затем на DNS-сервере, обслуживающем родительскую зону выполняют Мастер делегирования, вводят имя делегируемого поддомена и имя полномочного в новой зоне сервера имен. Вновь созданный узел в консоли DNS уже содержит запись делегирования (NS), а связывающая запись (A) записывается в базу данных, но в консоли не отображается.

В делегированных зонах необходимо отслеживать сервера имен, поэтому в родительских зонах часто применяют зоны-заглушки. В зонах-заглушках информация о серверах имен обновляется регулярно автоматически. Также зоны-заглушки применяют для упрощения процесса разрешения имен между доменами, т.к. не нужно искать в пространстве DNS общий родительский сервер. Зона-заглушка содержит записи ресурсов SOA, NS и связывающие записи A

полномочных DNS-серверов зоны.

Информация в зоне-заглушке обновляется тремя способами: *перезагрузка из локальной базы DNS-сервера*; *передача с главного сервера* (в зависимости от серийного номера SOA), *перезагрузка с главного сервера* (вне зависимости от серийного номера SOA). Таким образом, зоны-заглушки обязательно разворачиваются в родительских доменах при делегировании и подменяют дополнительные зоны, когда необходима DNS-связь между различными доменами, но избыточность данных основной зоны не нужна.

§14. Мониторинг и устранение неполадок DNS

Для устранения неполадок в DNS чаще всего используют утилиту *Nslookup*, *журнал событий DNS* и *журнал DNS*.

Nslookup – команда, позволяющая направлять тестовые запросы на DNS-сервер и получать подробные ответы в окне командной строки. Существуют два режима использования Nslookup: *неинтерактивный режим* (простые запросы) и *интерактивный режим* (последовательность команд и запросов). В режиме простых запросов Nslookup определяет IP-адрес узла по его имени. В интерактивном режиме Nslookup принимает команды на выполнение различных операций. В этом режиме есть команда *Set*, позволяющая настраивать параметры и изменять порядок обработки запросов. Также можно менять режим утилиты с обычного на отладочный. По умолчанию Nslookup возвращает только записи ресурсов типа A. Для запросов данных других типов необходимо использовать команду *Set type*. Ответ на первый запрос об удаленном имени всегда

полномочней. Также Nslookup может имитировать зонную передачу, что позволяет увидеть все узлы удаленного домена. Зонные передачи могут блокироваться на уровне DNS-сервера. Таким образом, эта операция возможна лишь с авторизованных адресов или сетей.

Журнал событий DNS регистрирует ошибки DNS-сервера. Этот журнал можно просмотреть в консоли DNS. По умолчанию в этом журнале регистрируются все события. Однако, в окне свойств журнала можно выбрать тип регистрируемых событий, а для их упорядоченного отображения можно использовать фильтр. Помимо журнала событий на DNS-серверах ведется отдельный журнал DNS. Для начала записи в этот журнал необходимо активировать функцию *Запись пакетов в журнал для отладки* и выбрать типы пакетов в зависимости от их направления движения, содержания используемого транспортного протокола и пр.

Чтобы просматривать *журнал событий DNS* и *журнал DNS* необходимо быть членом хотя бы одной из групп: Администраторы, Пользователи журналов производительности или Пользователи системного монитора.

Устранять ошибки репликации данных DNS в зонах, интегрированных с AD, помогает утилита *Replication Monitor*. Эта утилита устанавливается дополнительно и запускается командой *replmon*. С помощью этой утилиты можно задать репликацию трех, относящихся к DNS, разделов AD (описание дается для зоны DNS с именем Domain.local): DC=domain, DC=local – содержит объекты, относящиеся к локальному домену. Для хранения данных зоны DNS в разделе домена в качестве области репликации зоны задайте параметр *На все контроллеры*

домена в домене AD;
DC=DomainDNSZones, DC=domain, DC=local – чтобы данные зоны DNS хранились в этом разделе задайте в области репликации зоны параметр *На все DNS серверы в домене AD*; DC=ForestDNSZones, DC=domain, DC=local – чтобы данные зоны DNS хранились в этом разделе задайте в области репликации зоны параметр На все DNS серверы в лесу AD.

Для того чтобы узнать раздел AD, который используется для хранения зоны DNS, используется команда *DNScmd /zoneinfo*. Если данные зоны устарели, с помощью Replication Monitor можно инициировать принудительную передачу данных зоны. Также Replication Monitor можно настроить на отправку писем администратору в случае возникновения ошибок репликации.

Производительность DNS-сервера (как и любых других систем) контролируют с помощью утилиты Системный монитор и ряда счетчиков. Всего существует 62 счетчика, относящихся к производительности DNS, в т.ч.: счетчики общей статистики; счетчики TCP и UDP; счетчики использования памяти; счетчики рекурсивного поиска, счетчики зонных передач. Наиболее часто используемыми являются следующие счетчики: *кэш-память* (объем системной памяти, используемый для кэширования*); получено динамических обновлений* (позволяет узнать пытаются ли DNS-клиенты обновить свои адреса); *отклонено динамических обновлений* (сравнение этого счетчика с предыдущим помогает понять испытывают ли клиенты проблемы с изменением адреса и пытаются ли злоумышленники заменить сетевые адреса своими); *записано в базу данных динамических обновлений* (количество клиентов, успешно обновивших

свои адреса, используется вместе с предыдущими двумя счетчиками для полноты картины); *получено безопасных обновлений*; *ошибок безопасных обновлений* (счетчики, похожие на два предыдущих, но используемые для зон, интегрированных с AD*); общее число полученных запросов; общее число полученных запросов в секунду; отправлено всего ответов и отправлено ответов в секунду* (четыре последних счетчика дают общую картину работы DNS-сервера в сети с высокой нагрузкой); *неудачных передач зоны; успешных передач зоны; получено запросов на передачу зоны* (сравнение этих трех счетчиков дает общую картину передач зон).

§15. Конфигурирование DHCP-серверов и клиентов

DHCP-сервер является необходимым атрибутом сколько-нибудь больших сетей, т.к. использование данного протокола упрощает администрирование сети и позволяет избежать ошибок адресации. Добавление роли DHCP производится точно также как и DNS-сервера (Server Manager→Add Roles and Features→DHCP).

Серверу, на который устанавливается служба DHCP, необходимо присвоить статический IP-адрес из того же диапазона, из которого он предоставляет адреса клиентов. В случае если в домене используется AD, DHCP-сервер до начала работы должен быть авторизован. Авторизация осуществляется из консоли DHCP-сервера. Неавторизованные DHCP-серверы называются ложными. В случае если в домене появляется авторизованный DHCP, ложный сервер автоматически отключается.

Как и на DNS-сервере необходима настройка зон, так и на DHCP-сервере необходима настройка областей –

совокупностей IP-адресов определенного диапазона, которые DHCP-сервер будет присваивать клиентам. Кроме IP-адресов в областях можно определить любые другие настройки TCP/IP для клиентов. Процесс передачи IP-адреса клиенту называется арендой. Продолжительность аренды по умолчанию 8 дней, после этого клиент обязан обновить аренду. Также аренда обновляется при перезапуске клиента, при перезапуске DHCP-сервера, а также при выполнении команды *ipconfig /renew*.

Области на DHCP-сервере создаются с помощью Мастера, позволяющего настроить следующие параметры:

- *имя области*;
- *диапазон адресов* – набор последовательных адресов, составляющих подсеть, в которую устанавливается DHCP. Однако из этого диапазона необходимо исключить уже используемые в нем статические IP-адреса (например, для самого DHCP, контроллера домена, DNS-сервера и пр.). В свойствах области указываются начальный и конечный адреса желаемого диапазона. В случае если сеть уже сконфигурирована полностью, для выделения компьютеров со статическими IP-адресами задают *Диапазон исключений*. Если же сеть еще не сформирована, то начальный адрес диапазона увеличивают на двадцать, тем самым, резервируя двадцать первых IP-адресов для важных серверов;
- *диапазоны исключения* – множество IP-адресов из диапазона области, которые никогда не должны предоставляться в аренду. Адреса

области, предоставляемые в аренду, составляют так называемый пул адресов;

- *срок действия аренды адреса*;
- *IP-адрес основного шлюза*;
- *имя домена и список DNS-серверов*.

Активировать область можно сразу после завершения мастера. Параметры уровня резервирования обладают наивысшим приоритетом, а параметры области приоритетнее параметров сервера. В качестве дополнительных параметров доступно более 60 стандартных настроек. Использовать область можно только после ее активации.

В крупных сетях необходимо позаботиться об отказоустойчивости системы DHCP. Для этого в подсетях рекомендуется устанавливать два DHCP-сервера (если один недоступен – работает другой). В случаях, если оба сервера работают для балансировки сетевой нагрузки рекомендуется использовать правило 80/20 – один из серверов настраивается на обслуживание первых 80% адресного пула, а второй дает в аренду оставшиеся 20%. Для настройки этого правила на обоих серверах задается один и тот же диапазон адресов. В диапазон исключений на первом сервере попадают последние 20% адресного пула, а в диапазон исключений второго сервера – первые 80% адресного пула. При сбое одного из серверов на втором убирают диапазон исключений.

Для обеспечения отказоустойчивости (а равно, для балансировки нагрузки на DHCP-сервера) можно использовать и «способ для ленивых» - DHCP-failover. Для этого в свойствах области нужно выбрать одноименнуюлпцию, а затем указать второй авторизованный в домене DHCP-сервер. После этого система автоматически настроит использование правила

80/20 (только по умолчанию это будет правило 50/50) и будет в автоматическом режиме следить за работоспособностью и доступностью обоих DHCP-серверов.

Важным объектам в сети (сетевым принтерам, серверам с важными ролями) необходимо назначать постоянные адреса. Но зачастую конфигурировать их вручную нет возможности, поэтому в DHCP существует механизм резервирования – постоянной аренды адреса. Для резервирования необходимо знать MAC-адрес сетевого узла и в консоли DHCP связать его с IP-адресом из адресного пула. Также необходимо помнить, что исключение приоритетнее резервирования.

Чтобы настроить клиентский компьютер на получение IP-адреса от DHCP-сервера необходимо на выбранном сетевом интерфейсе в настройках TCP/IP выбрать параметр Получить IP-адрес автоматически. Если необходимо чтобы клиент получал автоматически еще и параметры DNS необходимо также установить флажок напротив параметра Получите адрес DNS-сервера автоматически. Если до этого клиент имел статический IP-адрес, то изменения вступят немедленно. Если в сети использовалась технология APIPA и не использовалась *Общие подключения к Интернету (ICS)* необходимо выполнить команду *ipconfig /renew* или перезагрузить клиентский компьютер. Если в сети использовалась технология ICS необходимо сначала удалить все ICS подключения и только затем установить в сети DHCP-сервер. Технология ICS на базовом уровне сама по себе реализует службы DNS и DHCP. Таким образом, ICS клиентам уже назначаются динамические адреса. Поэтому рекомендуется после удаления ICS-подключения назначить клиентским компьютерам

статические IP-адреса, а потом развернуть систему DHCP.

Для управления DHCP разработана специальная консоль, ряд утилит командной строки и консоль Службы. С помощью *консоли DHCP* можно запускать, останавливать, приостанавливать, возобновлять и перезапускать DHCP-сервер. Эти же службы доступны в консоли Службы, а в командной строке они реализованы с помощью команды Net Start|Stop|…DHCP-сервер.

Для управления DHCP-сервером из всех возможных инструментов необходимо быть членом группы Администраторы или группы Администраторы DHCP.

IP-адреса посылаются клиентам при помощи широковещания. Маршрутизаторы по умолчанию не пропускают широковещательные пакеты, поэтому если в подсети нет DHCP-сервера, клиенты не получат от него настройки TCP/IP. Если развертывать дополнительный DHCP-сервер в каждой подсети накладно, то эту проблему решают с помощью *Агента ретрансляции DHCP*, перехватывающего широковещательные DHCP-сообщения и доставляющего их DHCP-серверу. Агенты ретрансляции перед пересылкой сообщения DHCP-серверу вписывают в него собственный адрес, таким образом, давая DHCP-серверу указания из какой подсети предоставлять адреса.

Часто в крупных сетях диапазоны IP-адресов, предназначенные для аренды, в разных логических подсетях объединяют в единый объект администрирования – *суперобласть*. Суперобсласти используются в двух случаях:

1. если число клиентских компьютеров в подсети превышает емкость начального адресного пространства;

2. если в одном физическом сегменте сети сконфигурированы два или более DHCP-сервера, предоставляющих клиентам IP-адреса из разных диапазонов. В этом случае создание суперобласти на всех серверах имитирует ситуацию балансировки нагрузки с использованием нескольких DHCP-серверов.

При необходимости изменения адресации в подсетях недостаточно просто изменить диапазон в используемой области, необходимо сначала создать новую область, обновить клиенты, выполнив на них последовательно команды *ipconfig /release* и *ipconfig /renew*. После этого старую область можно деактивировать и удалить.

Часто в сетях возникает потребность предоставлять клиентским компьютерам конфигурацию в зависимости от выполняемых ими функций. Для этого в DHCP реализованы так называемые классы параметров:

- *классы поставщиков* – для назначения параметров клиентам, для которых определен конкретный тип поставщика;
- *классы пользователей* – для назначения параметров клиентам, которым необходимы одинаковые параметры настройки DHCP.

Для создания класса компьютеров необходимо сначала определить его на DHCP-сервере, назначив ему идентификатор и набор параметров. Затем на нужных клиентских компьютерах выполнить команду *ipconfig /setclassid*.

DHCP-сервер автоматически обновляет записи ресурсов PTR на DNS-серверах для DHCP-клиентов. Однако можно настроить DHCP-сервер и на обновление записей ресурсов A. Эта функция настраивается на

вкладке DNS свойств DHCP-сервера. DHCP-сервер может обновлять записи ресурсов в DNS по запросу DHCP-клиента или без такового при каждом событии, связанном с адресом. Также можно настроить DHCP-сервер на удаление записей ресурсов A и PTR при истечении срока аренды. В случае если система DNS интегрирована в AD, DHCP-сервера рекомендуется добавлять в группу безопасности *DNSUpdateProxy* для предотвращения проблем с владельцем записи ресурса. Такое решение ухудшает безопасность сети, т.к. любые имена DNS, зарегистрированные DHCP-сервером являются небезопасными. Если DHCP-сервер член группы *DNSUpdateProxy* устанавливается на контроллере домена, то в этом случае все записи ресурсов A, SRV и CNAME, зарегистрированные в DNS этим DHCP-сервером, являются небезопасными. Поэтому совмещать роли контроллера домена и DHCP-сервера крайне не рекомендуется.

Для восстановления DHCP-сервера после сбоя или для его переноса на другой сервер необходимо архивировать базу данных DHCP. DHCP-сервер может архивироваться автоматически и вручную. Автоматические копии используются для восстановления поврежденных баз данных DHCP, а для восстановления вручную пригодны копии только заархивированные вручную. Существуют данные, которые не сохраняются ни при каком способе архивирования. Например, реквизиты динамического обновления в DNS. При переносе DHCP-сервера с одного сервера на другой нужно заархивировать базу данных DHCP, а затем восстановить на новом месте. Эту операцию можно выполнить из консоли DHCP. Для исправления ошибок в базе данных DHCP и ее одновременного сжатия для

экономии пространства используется утилита *Jetpack*. Нужно пользоваться ею, если размер базы DHCP превышает 30 Мбайт и при появлении сообщений об ошибках базы данных DHCP.

§16. Мониторинг и устранение неполадок DHCP

Для мониторинга DHCP-сервера предусмотрен еженедельно обновляемый журнал аудита, представляющий собой текстовые файлы с именами дней недели. Местоположение этих файлов можно найти, а также произвести их включение и отключение в окне свойств DHCP-сервера. Максимальный размер файла журнала 1 Мбайт, а если на диске осталось менее 20 Мбайт свободного пространства, то ведение файла журнала прекращается. Файлы журнала представляют собой совокупность текстовых однострочных записей, состоящих из кода записанного события и его описания.

Если клиенты не могут подключиться к ресурсам сети, это может быть сигналом об отказе DHCP-сервера. В этом случае необходимо на клиентских компьютерах выполнить команду *ipconfig /all* и если в листинге этой команды фигурирует строка *IP-адрес автонастройки*, нужно заглянуть в журнал DHCP-сервера и искать в нем ошибку с кодом 56 (ошибка авторизации). Также в сети могут возникать конфликты адресов, в случае если часть клиентов используют статические IP-адреса, а другую часть обслуживает DHCP-сервер с некорректно настроенной областью. Также такая ситуация возможна если в сети есть два конкурирующих DHCP-сервера. В этих случаях необходимо проверить диапазоны адресных пулов на этих DHCP-серверах, найти конкурирующие DHCP-сервера с помощью утилиты DHCPloc.exe

(устанавливается дополнительно), удалить конкурирующий сервер и обновить аренду адресов клиентами.

Если конфликт DHCP-адреса обнаружен на единственном клиенте, можно попробовать решить проблему нажатием кнопки *Исправить* в окне состояния подключения. При этом в пакетном режиме выполняться следующие команды*: ipconfig /renew, arp –d* (сброс кэша arp); *nbtstat –r* (сброс кэша NetBIOS*); ipconfig /flushdns*; *nbtstat –rr* (перерегистрация клиента на WINS-сервера); *ipconfig /registerdns* (перерегистрация клиентов в DNS). Если это не устраняет неполадку, значит, повреждена связь с DHCP-сервером на физическом уровне или в подсети отсутствует агент ретрансляции DHCP.

Иногда клиенты DHCP-сервера могут получать от него IP-адреса из некорректных областей. Это происходит в двух случаях: если DHCP-сервер обслуживает много областей и их диапазоны перекрываются или агенту ретрансляции DHCP из подсети клиента назначен неправильный адрес.

Для проверки работоспособности DHCP-сервера выполняют следующие операции:

- проверяют адрес самого DHCP-сервера;
- проверяют привязки подключений DHCP-сервера;
- проверяют авторизацию DHCP в AD (авторизованные сервера помечаются направленной вверх зеленой стрелкой, а неавторизованные – направленной вниз красной стрелкой).

Далее проверяют конфигурацию области: проверяют активизирована ли она (помечается также как авторизованные и неавторизованные серверы).

Проверяют диапазоны области, проверяют наличие свободных адресов в диапазоне. Проверяют исключения, затем проверяют резервирование. Проверяют перекрывание исключений и резервированных адресов.

Если в базе данных DHCP обнаруживаются противоречия, необходимо выполнить согласование областей. Эту операцию проводят из консоли DHCP, при этом адреса, вызывающие сомнения либо возвращаются первоначальным клиентам, либо для них задается временное резервирование. В любом случае при ошибках работы DHCP-сервера полезно изучить журнал *Система* в утилите *Просмотр событий*, в которой могут содержаться подробные описания системных ошибок DHCP. При обнаружении в этом журнале ошибок базы данных JET, связанных с DHCP-сервером, рекомендуется воспользоваться утилитой *JetPack*. Если это не помогло, можно восстановить базу данных DHCP-сервера из консоли DHCP или выполнив следующую команду: *netsh dhcpserver set databaserestoreflag 1*.

Лабораторная работа №1
Подготовка рабочего места

В этой работе будут созданы пять виртуальных машин: четыре – под управлением Microsoft Windows Server 2016 Standard Edition, одна – под управлением Microsoft Windows 10 Enterprise.

Также будут созданы элементы сетевой инфраструктуры – виртуальные свитчи. Виртуальные машины будут объединены в сеть, состоящую из двух сегментов – корпоративного и внешнего.

Для выполнения работы необходимо:

1. Сервер, обеспечивающий средства виртуализации, со следующими характеристиками:
    - не менее 12 Гб свободной оперативной памяти;
    - не менее 200 Гб свободного дискового пространства на твердотельном накопителе;
    - не менее 4 выделенных ядер процессора с тактовой частотой не менее 3 ГГц;
    - сетевой интерфейс с пропускной способностью не менее 100 Мбит/с.
2. Среда виртуализации VMWare ESXi 5.5 или новее.
3. Клиентский компьютер для подключения к серверу виртуализации с установленным VMWare Workstation Pro 12.0 или новее.
4. Дистрибутив Microsoft Windows Server 2016 Standard Edition (US).
5. Дистрибутив Microsoft Windows 10 Enterprise (US).

Упражнение 1. Реализация схемы сети на сервере виртуализации. Установка ОС

1. Необходимо реализовать схему, представленную на рисунке 1.

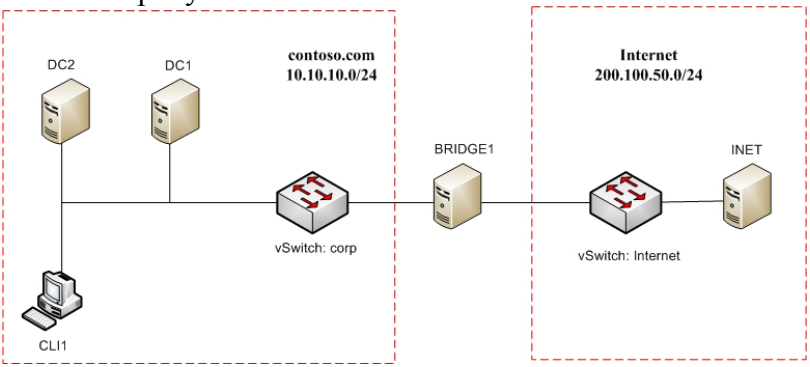


Рис.1. Схема сети, используемой для выполнения лабораторных работ.

2. В VMWare Esxi создать два виртуальных коммутатора *corp* и *Internet* с одноимнными подключенными порт-группами.
3. В хранилище VMWare Esxi загрузить дистрибутивы Microsoft Windows Server 2016 Standard Edition и Microsoft Windows 10 Enterprise.
4. Создать виртуальную машину DC1:
    - использовать одно ядро процессора;
    - использовать 2 Гб оперативной памяти;
    - создать новый жесткий диск (SATA) объемом в 20 Гб.
    - сетевую карту подключить к виртуальному коммутатору *corp*;
    - установить операционную систему Microsoft Windows Server 2016 Standard Edition Desktop Experience (GUI).

5. Повторить шаг 4 для создания виртуальных машин DC2, BRIDGE1, INET и CLI1 с учетом следующих условий:
    - При создании виртуальной машины DC2 добавить четыре дополнительных жестких диска объемом 5 ГБ каждый.
    - При создании виртуальной машины BRIDGE1 добавить еще один сетевой интерфейс и подключить его к виртуальному коммутатору Internet.
    - При создании виртуальной машины INET подключить ее сетевой интерфейс к виртуальному коммутатору Internet.
    - При создании виртуальной машины CLI1 использовать дистрибутив Microsoft Windows 10 Enterprise.

NB !Не используйте локализованные операционные системы!

6. На всех виртуальных машинах после завершения установки операционной системы установить *Гостевые дополнения VMWare*.
7. На всех виртуальных машинах после завершения установки гостевых дополнений выполнить команду *sysprep* (c:\windows\system32\sysprep) с включенной опцией Generalize (выбрать вариант *shutdown* по завершении установки).
8. Сделать снимки всех созданных виртуальных машин.

Лабораторная работа №2
Настройка DC1

В этой работе будет создан учебный корпоративный домен contoso.com с некоторыми элементами инфраструктуры – организационными подразделениями, учетными записями пользователей и групп.

Также будут установлены и настроены такие серверные роли как DNS, DHCP и Web-сервер.

Для выполнения работы необходимо:

Выполненная в полном объеме лабораторная работа №1. Дистрибутив Microsoft Office. Файл для импорта пользователей users.xlsx.

Упражнение 1. Установка роли контроллера домена на DC1

- переименуйте компьютер в DC1;
- настройте сетевое подключение: ip-адрес – 10.10.10.1, маска – 255.255.255.0, основной шлюз – 10.10.10.250, DNS – 127.0.0.1 (10.10.10.2);
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- сделайте сервер первым контроллером домена contoso.com.

Упражнение 2. Настройка DNS на DC1

- настройте необходимые зоны прямого и обратного просмотра;
- обеспечьте возможность передачи всех зон на DC2 в будущем;

- создайте вручную все необходимые записи типа A и PTR для серверов домена и корпоративного web-сайта (www.contoso.com).

Упражнение 3. Создание доменной инфраструктуры на DC1

- в домене cotoso.com создайте подразделения: Experts, Competitors, Managers, Visitors и IT;
- в соответствующих подразделениях создайте доменные группы: Experts, Competitors, Managers, Visitors, IT;
- установить на DC1 Microsoft Office;
- создайте пользователей, используя прилагаемый excel-файл (вся имеющаяся в файле информация о пользователях должна быть внесена в Active Directory); поместите пользователей в соответствующие подразделения и группы; все созданные учетные записи должны быть включены и доступны;
- в качестве имени входа в домен каждый пользователь должен использовать свою фамилию и именz (например, Abbot Blackwell – BlackwellAbbot@pest.com).

Упражнение 4. Создание консоли управления на DC1

1. В командной строке выполните команду *mmc*.
2. Добавьте в консоль оснастки Active Directory – Users and Computers и DNS.
3. Сохраните консоль на рабочем столе.

Упражнение 5. Настройка DHCP на DC1

- установите роль DHCP-сервера;

- авторизуйте DHCP от имени доменного администратора;
- настройте новую IPv4 область – в качестве диапазона выдаваемых адресов используйте 10.10.10.100 – 10.10.10.200;
- настройте дополнительные свойства области (адреса DNS-серверов – 10.10.10.1 + 10.10.10.2 и основного шлюза – 10.10.10.250).

Упражнение 6. Настройка групповых политик на DC1

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
- члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
- разрешите членам группы Domain Users локальный вход на контроллер домена.

Упражнение 7. Настройка Web-сервера на DC1

- создайте папку *c:\site*;
- создайте файл *c:\site\index.htm* на основе текстового файла с содержанием “Hi! It`s my first site!”;
- установите роль Web-server, используйте компоненты, предлагаемые системой к установке по умолчанию;
- остановите Default web site;
- создайте сайт с домашней папкой *c:\site*, с привязкой *http://www.contoso.com* на стандартном порту (80);
- убедитесь в работоспособности созданного сайта.

Лабораторная работа №3
Настройка DC2

В этой работе созданный ранее домен будет дополнен вторым контроллером, не выполняющим функции глобального каталога.

Также будет настроен дисковый массив по технологии RAID-5. На созданном томе будут организованы общие папки, настрены файловые квоты и экраны.

В конце работы в домен будут добавлены простые групповые политики.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №1 и №2.

Упражнение 1. Установка роли контроллера домена на DC2

- переименуйте компьютер в DC2;
- настройте сетевое подключение: ip-адрес – 10.10.10.2, маска – 255.255.255.0, основной шлюз – 10.10.10.250, DNS – 10.10.10.1 + 10.10.10.2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- сделайте сервер дополнительным контроллером домена contoso.com;
- контроллер домена на DC2 не должен выполнять функцию глобального каталога.

Упражнение 2. Настройка DNS на DC1

- загрузите все зоны прямого и обратного просмотра с DC1;
- обеспечьте возможность передачи всех зон на DC1 в будущем;
- настройте во всех зонах безопасные и небезопасные динамические обновления;
- проверьте список корневых ссылок Интернета.

Упражнение 3. Настройка DHCP на DC2

- установите роль DHCP-сервера;
- авторизуйте DHCP от имени доменного администратора;
- настройте failover: mode – Load balancer (80/20), partner server – DC1, state switchover – 10 min.

Упражнение 4. Настройка групповых политик на DC2

- запретите использование «спящего режима» на всех клиентских компьютерах домена.

Упражнение 5. Управление дисками и общими папками

- с помощью дополнительных жестких дисков создайте RAID-5 том, назначьте ему букву D:\;
- установите дополнительную опцию File Server Resource Manager в службе File Server;
- создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу d:\shares\departments;
- обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\ (через групповую политику);

- установите максимальный размер в 1Gb для каждой папки каждого подразделения;
- запретите хранение в созданных общих папках файлов с расширениями .cmd и .exe; учтите, что файлы остальных типов пользователи вправе хранить.

Лабораторная работа №4
Настройка BRIDGE1

В этой работе будет создан учебный корпоративный маршрутизатор, способный передавать трафик между двумя сетями.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №1 и №2.

Упражнение 1. Базовая настройка BRIDGE1. Установка роли сервера удаленного доступа

- переименуйте компьютер в BRIDGE1;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к коммутатору Internet, используйте адрес 200.100.50.2/24 + dns 200.100.50.1; для сетевого адреса, подключенного к коммутатору corp, используйте адрес 10.10.10.250/24 + dns 10.10.10.1+10.10.10.2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену contoso.com.

NB !Теперь BRIDGE1 является членом домена contoso.com, значит возможно входить в BRIDGE1 локально, а возможно входить в домен. Для входа в домен с BRIDGE1 используйте имя учетной записи в формате имя_пользователя@имя_домена, в нашем случае *Администратор@contoso.com*. Всегда входите исключительно в домен!

Упражнение 2. Настройка маршрутизации на BRIDGE1

- установите роль Remote Access;
- в качестве опций выберите Routing + Direct Access;
- запустите оснастку Routing and Remote Access Manager и настройте на сервере маршрутизацию пакетов между внутренней и внешней сетью.

Лабораторная работа №5
Настройка эмуляции подключения к Интернету

В этой работе будет создана «заглушка», позволяющая операционным системам внутри учебного домена использовать «подключение к Интернету».

Это не только интересная лабораторная задача, также наличие подобного эмулятора необходимо для настройки и отладки удаленных подключений, например, по технологии Direct Access.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №1.

Упражнение 1. Базовая настройка INET

- переименуйте компьютер в INET;
- задайте настройки сети: адрес – 200.100.50.1, маска 255.255.255.0, dns 127.0.0.1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- не присоединяйте компьютер к какому-либо домену.

Упражнение 2. Настройка DNS на INET

- установите роль DNS-сервера;
- создайте зоны прямого просмотра msftncsi.com и msftconnecttest.com;
- создайте зоны обратного просмотра 200.100.50. и 131.107.255.;
- создайте необходимые записи типа A в соответствующих зонах прямого (dns.msftncsi.com – 131.107.255.255; www.msftconnecttest.com – 200.100.50.1) и соответствующие им PTR в зонах обратного просмотра.

Упражнение 3. Настройка Web-server на INET

- создайте папку *c:\site*;
- создайте файл *c:\site\connecttest.txt* с содержимым “Microsoft Connect Test”;
- установите роль Web-server, используйте компоненты, предлагаемые системой к установке по умолчанию;
- создайте новый web-сайт с привязкой http://www.msftconnecttest.com на стандартом порту (80), в качестве домашней папки укажите *c:\site*.

Упражнение 4. Настройка DHCP на INET

- установите роль DHCP-сервера;
- авторизуйте DHCP от имени локального администратора INET;
- настройте новую IPv4 область – в качестве диапазона выдаваемых адресов используйте 200.100.50.100 – 20.100.50.200;
- настройте дополнительные свойства области (адрес DNS-сервера – 200.100.50.1 и основного шлюза – 200.100.50.1).

NB !Упражнение №4 выполнять не обязательно. Его результат понадобится, если, например, подключить компьютер CLI1 в виртуальный коммутатор Internet для непосредственной проверки работоспособности эмуляции!

Лабораторная работа №6
Настройка CLI1

В этой работе будет настроен и введен в домен клиентский компьютер, с помощью которого можно наглядно убедиться в работоспособности всех ранее сделанных настроек.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №1 – №5.

Упражнение 1. Базовая настройка CLI1

- переименуйте компьютер в CLI1;
- обеспечьте работоспособность протокола ICMP (для использования команды ping);
- присоедините компьютер к домену contoso.com.

Упражнение 2. Проверка настроенных технологий

- войдите в систему как доменный администратор;
- выполните команду *ipconfig /all*, убедитесь, что сетевая настройка получена по протоколу DHCP;
- временно отключите DHCP-сервер, выдавший адрес для CLI1, на CLI1 выполните команды *ipconfig /release* + *ipconfig /renew*, убедитесь, что DHCP-failover работает;
- на CLI1 выполните команду *nslookup www.contoso.com*, убедитесь в работоспособности DNS в домене;
- на CLI1 выполните команду *ping 200.100.50.2*, убедитесь в работоспособности маршрутизации на BRIDGE1;
- на CLI1 откройте оснастку Computer management→Local Users and Groups, убедитесь в том, что группа contoso\IT является членом группы Administrators;
- выберите какого-нибудь пользователя, члена группы Experts (при необходимости уточните реквизиты для входа в свойствах учетной записи пользователя на DC1 в оснастке Active Directory – Users and Computers), и войдите в домен на CLI1 с реквизитами выбранного пользователя – убедитесь в отсутствии приветственной анимации, в недоступности «спящего режима», а также в

наличии корпоративной общей папки в Проводнике;

- попробуйте сохранить файл с расширением .exe в корпоративной общей папке – убедитесь в работоспособности файлового экрана;
- откройте Internet Explorer – убедитесь в работоспособности сайта www.contoso.com.

Инструкции
для выполнения лабораторных работ

INET

Назначаем компьютеру имя INET (через System), НЕ присваиваем компьютеру DNS суффикс, переименовываем рабочую группу в INETGROUP, не перезагружаемся. Назначаем IP-адрес без шлюза 200.100.50.1/24, отключаем QoS, в качестве DNS сервера указываем адрес замыкания на себя (127.0.0.1). НЕ присоединяем сервер ни к одному из доменов, оставляем его в рабочей группе.

Отключаем firewall командой: *netsh advfirewall set allprofiles state off*, перезагружаемся.

С помощью Server Manager устанавливаем стандартными мастерами роли: DHCP, DNS, Web-server.

Открываем оснастку DNS. Создаём на нем основные зоны прямого просмотра: msftncsi.com, msftconnecttest.com и разрешаем в них любые динамические обновления. Создаём зоны обратного просмотра 200.100.50. и 131.107.255. разрешаем в них любые динамические обновления.

Создаём необходимые записи типа A (dns.msftncsi.com 131.107.255.255; www.msftconnecttest.com 200.100.50.1) и соответствующие им PTR.

Открываем оснастку DHCP. Создаём новую область (scope), называем её Internet (pool: 200.100.50.100-200/24; dg: 200.100.50.1; dns: 200.100.50.1). Активируем скоп.

На диске C:\ создать папку Site, в ней создать текстовый файл connecttest.txt с текстом Microsoft Connect Test.

В оснастке IIS создать web-сайт с привязкой к имени www.msftconnecttest.com, в качестве домашней папки указать папку C:\Site. В IE ввести адрес www.msftconnecttest.com/connecttest.txt – должен отобразиться текст. После этого компьютер CLI1 (если его переместить в свит Internet) должен получить адрес по DHCP и показывать, что у него имеется подключение к Интернету (для проверки надо залогиниться, стартовый экран не всегда верно показывает состояние сети).

DC1

Назначаем адрес 10.10.10.1/24, шлюз 10.10.10.250, dns – 127.0.0.1, 10.10.10.2 Переименовываем комп в DC1, отключаем firewall. Устанавливаем AD DS, DNS, DHCP, WEB-server, File server + resource manager (стандартные мастера). Повышаем до контроллера домена. Снова отключаем фаер.

В DNS создаем зону обратного просмотра: 10.10.10. – разрешаем любые обновления и передачу на любой сервер. Для зоны прямого просмотра contoso.com назначаем такие же настройки и создаем в ней записи узлов типа A для: DC2 – 10.10.10.2, BRIDGE1 – 10.10.10.250, www.contoso.com – 10.10.10.1.

Завершить настройку DHCP. В оснастке DHCP создать зону contoso с параметрами из задания, в качестве DG указать 10.10.10.250, dns указать два адреса – dc1 и dc2.

В оснастке AD U&C создать все OU (снимать галочку о защите от удаления) и группы по заданию. Группы создаваем сразу в OU, чтоб пользаки не валялись в корне домена.

В доменной дефолтной GPO (Computer -> Policies -

> Windows -> Security -> Account -> Password) поменять параметры сложности и длины пароля – уменьшить до 3 + Запретить анимацию (Computer Configuration → Policies → Administrative Template → System → Logon → Show first sign-in animation→ Disabled) + делаем локальных админов (Computer Configuration→ Policies → Security Settings → Restricted Groups → Add Group – IT – This group is a member of – Administrators).

В приложенной экселькe поменять названия столбцов – укоротить (новые названия столбцов записать на бумажку), сохранить с коротким именем в корень диска C:\ в формате .csv. Для импорта юзеров использовать скрипт типа:

- *Import-Csv C:\Users.csv | ForEach-Object {*
- *New-ADUser -EmployeeNumber $_.Number -GivenName = $_.FN -Surname = $_.LN*
- *-OfficePhone = $_.Phone -StreetAddress = $_.Street -PostalCode = $_.ZIP*
- *-City = $_.City -Country = “RU” -UserPrincipalName = ($_.logon+”@skills39.net”)*
- *-SamAccountName = $_.Logon -Name = ($_.FirstName+” “+$_.LastName+” “+$_.Number)*
- *-Path = (“ou=”+$_.Dept+”, dc=russia, dc=net”) -Enabled = $True*
- *-AccountPassword = (ConvertTo-SecureString $_.Password –AsPlainText -Force*
-
- *$grs = $_.Group.split(“;”)*
- *Foreach ($gr in $grs) {*
- *Add-ADGroupMember –Identity $gr –Members $_.Logon (Name должен совпадать и уникальным)*
- *}*
- *}*

В скрипте обязательно должно быть два командлета New-AdUser и ADD-ADGroupMember.

Создаем папку c:\site с файликом index.htm. В оснастке IIS добавляем новый сайт: имя – site, папка – c:\site, привязка http→на все IP→www.contoso.com, порт 80.

DC2

Отключаем фаер. Через *sconfig* настраиваем имя, назначаем адрес 10.10.10.2/24, шлюз 10.10.10.250, dns – 10.10.10.1 и 10.10.10.2, вводим в домен. Отключаем фаер.

На DC1 в Server Manager добавляем DC2 для удаленного управления. Устанавливаем AD DS, DNS, DHCP, File server + resource manager (стандартные мастера).

С помощью оснастки (mmc) Computer Management настраиваем RAID-5 с буквой D (оснастка не динамическая, поэтому после каждого действия переключаемся на локальный комп и обратно на DC2).

Через Server Manager повышаем до контроллера домена (снимаем галочку Global Catalog).

Через Server Manager авторизуем DHCP. В оснастке DHCP на DC1 настраиваем failover (это свойство области).

В оснастке DNS на DC1 подключаемся к DC2 и разрешаем все обновления и передачи зон во всех имеющихся зонах.

Далее создаем шары. Надо удалять стандартные разрешения для Domain Users, но это можно в мастере (вообще в мастере сразу отключаем наследование + копируем унаследованное + не трогаем пользователей system и creator/owner !).

С DC1 создать на DC2 (через \\dc2\d$) папки d:\shares\competitors (experts, managers). С помощью File and Storage Services на DC1 создать общие папки из

указанных каталогов. Разрешения: Competitors (для каждой папки своя группа) – Write; соответственно. При создании шары сразу установить квоту в 1 GB для каждой папки.

На DC2 в оснастке GPO редактируем Default Domain Policy: User Configuration Preferences → Windows Settings→ Drive Map → New → Mapped drive →Create, \\dc2\experts→ G:\, show. Повторяем для Managers и Competitors. Использовать таргетинг для соответствующих групп.

На DC2 запустить File Server Resource Manager. Отредактировать шаблон Block Executable Files (удалить все расширения, кроме .cmd и .exe). Применить шаблон к папке d:\shares\.

BRIDGE1

На BRIDGE1 меняем имя, настраиваем адреса (сеть contoso без шлюза с указанием dns-серверов, сеть Internet – с dns-сервером и шлюзом INET). Вводим в домен. В настройках firewall включаем все правила для всех профилей, касающиеся ICMP.

Устанавливаем роль Remote Access. Запустить оснастку Routing and Remote Access. Запустить мастер настройки службы маршрутизации, выбрать параметр маршрутизации сетей.

Через sconfig разрешить пинг (4 -> 3).

CLIENT-M

Меняем имя на CLIENT-M, вводим в домен. В свойствах firewall включаем все правила во всех входящих и исходящих, касающиеся ICMP.

На DC1 в Default Domain Policy изменить следующие параметры: Computer -> Policies -> AdmTempl -> System -> Power Management -> Active power plan + High perfomance; + Sleep settings -> Все параметры со словами sleep и hybernate включить и сделать равными нулю.

Проверяем все настойки, следуя инструкциям в последнем упражнении.

Литература

1. *Томас О. Холме Д.* Управление и поддержка Microsoft Windows Server 2016. – М: Русская редакция, 2017. 420 с.
2. *Дюгуров Д.В.* Управление контроллером домена. Упражнения и задачи. – Ижевск: УдГУ, 2012. 102 с.
3. Дюгуров Д.В. Сетевая адресация, разрешение имен, маршрутизация. Упражнения и задачи. – Ижевск: УдГУ, 2014. 94 с.
4. *Кондратьев В.К.* Операционные системы и оболочки – М.: Евразийский открытый институт, Московский государственный университет экономики, статистики и информатики, 2007. 172 с.
   URL: http://www.iprbookshop.ru/10730.html. – ЭБС «IPRbooks».
8. Промышленные АСУ и контроллеры // Ежемесячный журнал.
9. Информатика и системы управления // Ежемесячный журнал.

Учебное издание

Дюгуров Денис Владимирович

Операционные системы

Учебно-методическое пособие

Авторская редакция

Компьютерный набор и верстка Д. В. Дюгуров

Подписано в печать. Формат 60×84 1/16.
Усл. печ. л. 5,6. Уч-изд. л. 2,8.
Тираж 50 экз. Заказ № 2140.

Издательство «Удмуртский университет»
426034, Ижевск, ул. Университетская, 1, корп. 4
Тел./факс: +7(3412) 500-295 E-mail: editorial@udsu.ru

Типография ФГБОУ ВО
«Удмуртский государственный университет»
426034, Ижевск, Университетская,1, корп. 2.
Тел. 68-57-18