ТЕМА 2. ПЛАНИРОВАНИЕ И РАЗВЕРТЫВАНИЕ КОРПОРАТИВНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

В предыдущей теме были рассмотрены общие вопросы, касающиеся построения корпоративных информационных систем. Независимо от классификации этих систем, в действительности они представляют собой большое количество компьютеров и других устройств, взаимодействующих друг с другом по компьютерной сети. На них должно быть установлено и настроено системное и прикладное программное обеспечение. В этом плане они отличаются от обычных компьютерных систем только масштабом и сложностью. В этой и нескольких последующих темах будут рассмотрены вопросы построения необходимой инфраструктуры для таких систем.

В данной теме рассматриваются следующие вопросы:

- управление IP-адресами в организации: DHCP, IPAM;
- построение разрешения имен на базе DNS в среде с несколькими доменами;
- служба каталогов Active Directory;
- логические компоненты Active Directory: разделы, схема, леса, домены, сайты, контейнеры.
- физические компоненты Active Directory: контролеры домена, глобальный каталог;
- инструменты администрирования Active Directory;
- управление пользователями и компьютерами;
- разделы схемы и каталога;
- доверие между доменами и лесами;
- основы служб федерации Active Directory.

Лекции – 3 часа, лабораторные занятия – 6 часа, самостоятельная работа – 10 часов.

Минимальный набор знаний:

DHCP: четыре фазы получения IP-адреса, обновление аренды IP-адреса, APIPA-адреса;

назначение и возможности IPAM (без подробностей);

DNS: виды зон DNS, серверы пересылки, делегирование;

Active Directory: разделы каталога, глобальный каталог, понятие домена, дерева, леса, сайта, организационного подразделения;

два вида доверия между лесами;

службы федерации (назначение и основные принципы).

2.1. Основные сетевые службы

2.1.1. Служба DHCP

Каждый узел сети должен иметь уникальный IP-адрес. В крупных сетях слишком сложно, даже практически невозможно использовать ручное назначение адреса. Для автоматического назначения адреса используется протокол Dynamic Host Configuration Protocol (DHCP).

Основные сведения о протоколе и службе DHCP приведены в пункте 5.2.6 учебника «Компьютерные сети» [1].

Напомню, что существует четыре фазы получения IP-адреса: Discover – Offer – Request – Acknowledge. Все эти пакеты посылаются широковещательно (ведь у узла сети еще нет адреса), а значит — могут быть заблокированы на маршрутизаторе.

Следовательно, если сеть состоит из многих локальных сетей, соединенных маршрутизаторами, то нужно обеспечить возможность получения адреса всеми узлами сети. Для этого можно:

1) разместить отдельный DHCP-сервер в каждой подсети;

2) использовать маршрутизаторы, которые поддерживают протокол RFC 1542;

3) использовать компонент DHCP Relay в службе RRAS.

Многие сетевые устройства, например, беспроводные точки доступа, имеют встроенный сервер DHCP.

Служба DHCP является критической службой сети: в случае ее недоступности узлы сети не смогут взаимодействовать друг с другом. С точки зрения пользователя, он не сможет получить доступ к файлам в сети, сетевым принтерам, электронной почте, Интернету и т. д.

Чтобы обеспечить отказоустойчивость, можно использовать следующие технологии:

1) установить сервер DHCP в отказоустойчивом кластере Windows;

2) настроить разделенные области адресов (при этом область адресов разделяется таким образом, что 80% диапазона используется для аренды адресов на первичном сервере DHCP отдельной подсети, чтобы отвечать на запросы клиентов, а оставшиеся 20% адресов аренды находятся на сервере DHCP удаленной подсети; эти адреса используются клиентами только тогда, когда локальный DHCP-сервер недоступен);

3) настроить отношение отказоустойчивости между двумя DHCP-серверами (начиная с Windows Server 2012).

Отношение отказоустойчивости между двумя DHCP-серверами можно настроить в двух режимах: балансировки нагрузки (load balancing) и горячего резервирования (hot standby). Балансировка нагрузки используется, когда все настроенные DHCP серверы обрабатывают клиентские запросы, при этом процент обрабатываемых запросов конкретным сервером настраивается дополнительно (Active-Active конфигурация). Горячее резервирование соответствует Active-Passive конфигурации. Необходимо будет указать, какой DHCP сервер будет обрабатывать клиентские запросы, второй в это время будет

находиться в резерве. Резервный сервер не занимается обслуживанием клиентских запросов, пока работает первый сервер. При этом он получает все обновления информации об аренде адресов от работающего сервера и сохраняет её в своей базе.

Отказоустойчивые DHCP серверы могут находиться в разных подсетях и даже в разных географических регионах.

Некоторого подобия отказоустойчивости можно достичь и с помощью автоматически настраиваемых альтернативных адресов. В окне настройки протокола IPv4 для сетевого интерфейса появляется закладка Альтернативная конфигурация (APIPA), если выбрана опция **Получить IP-адрес автоматически** (*рис. 1.1*). Если при этом альтернативная конфигурация не настроена, автоматически выбирается произвольный адрес в диапазоне 169.254.0.0–169.255.255.255. После проверки на уникальность выбранный адрес назначается сетевому интерфейсу в качестве временного. Компьютер продолжает периодически пытаться получить адрес от DHCP-сервера. Использование альтернативной конфигурации в масштабах всей сети невозможно по тем же причинам, что и использование статических адресов. К тому же, здесь недоступны все опции DHCP, а только основные параметры. Но альтернативная конфигурация может быть очень полезной для отдельных клиентских компьютеров, выполняющих критически важные функции и которые всегда должны быть полностью работоспособны.

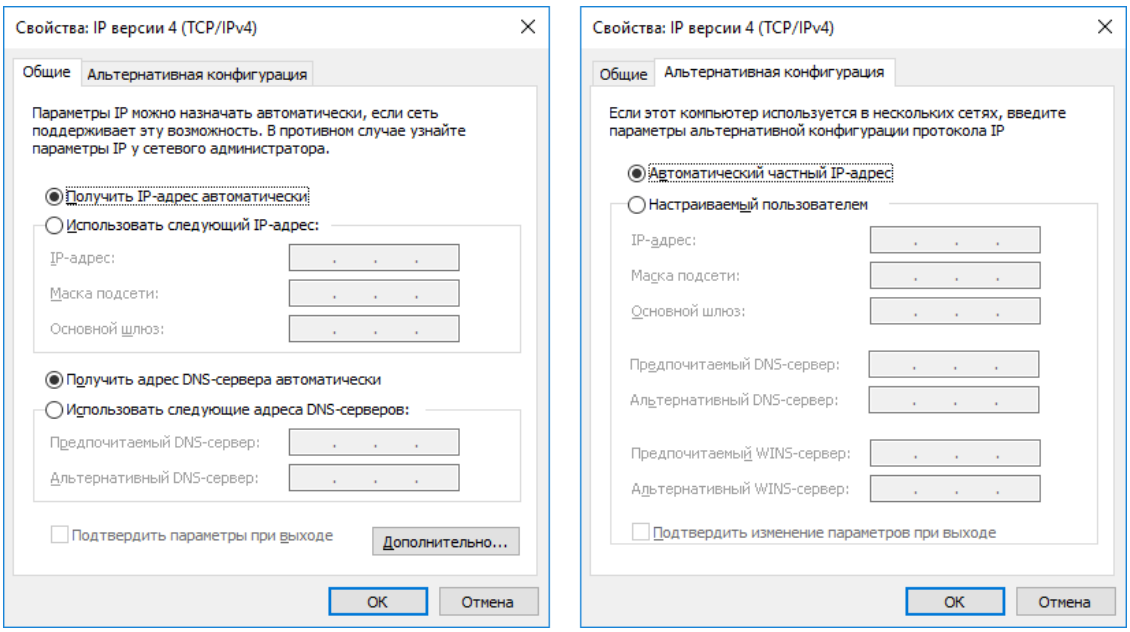

Рис. 1.1. Альтернативная конфигурация протокола IPv4

DHCP-сервер выдает IP-адрес на определенное время (по умолчанию в Windows Server срок аренды равен восьми суткам). По прошествии 50% срока аренды (то есть, через четыре дня) клиент DHCP начнет пытаться обновить срок аренды у того сервера, от которого он получил адрес. При этом используются только две последние фазы — Request и Acknowledge. В случае успешного обновления аренды срок действия IP-адреса будет продлен на следующие восемь дней. Если до конца срока аренды адрес не будет обновлен, клиент DHCP освобождает имеющийся адрес и начинает процесс получения сетевого адреса с самого

начала — пробует получить адрес от DHCP-сервера, затем пытается применить альтернативную конфигурацию.

Если изменения в сети происходят редко, срок аренды можно увеличить. Для сетей вроде конференц-зала срок аренды следует уменьшить до одного часа или даже меньше.

В крупных компьютерных сетях наверняка имеется множество отдельных DHCP-серверов, которые обслуживают различные диапазоны адресов. При этом могут возникать следующие проблемы:

- пересечение диапазонов адресов;
- отсутствие цельной картины использования IP-адресов в организации;
- сложности слежения за наличием доступных адресов в диапазонах;
- ручная настройка служб DHCP и DNS может привести к ошибочной конфигурации и конфликтам;
- отсутствие истории назначения IP-адресов.

Рассмотрим последний пункт подробнее. Если компьютер в сети каждый день и сервер DHCP работает непрерывно, IP-адрес компьютера, скорее всего, будет постоянным. Но если он долгое время был выключен или происходили неполадки на сервере DHCP, адрес наверняка изменится. В то же время иногда может возникнуть необходимость определить, какой компьютер имел определенный IP-адрес в определенное время и какой пользователь был тогда зарегистрирован на этом компьютере. Например, такая ситуация вполне может произойти при расследовании обстоятельств сетевой атаки или неправомерного доступа к ресурсам (большинство устройств защиты сети фиксирует лишь IP-адрес устройства).

Для автоматизации работы с IP-адресами применяют интегрированные системы управления пространством IP-адресов. В настоящее время такие системы переживают бурный рост, внедряются во всё большем количестве предприятий и становятся важной составляющей любой крупной ИТ-инфраструктуры.

Управление IP-адресами (IPAM) в Windows Server® 2012 — это встроенный набор инструментов для сквозного планирования, развертывания, администрирования и отслеживания инфраструктуры IP-адресов в многофункциональном пользовательском интерфейсе. IPAM автоматически определяет серверы инфраструктуры IP-адресов в вашей сети и позволяет управлять серверами из центрального интерфейса.

Компоненты IPAM позволяют делать следующее:

- управление адресным пространством;
- управление виртуальным адресным пространством;
- отслеживание нескольких серверов и управление ими;
- аудит сети;
- управление доступом на основе ролей.

Основное преимущество IPAM заключается в том, что он предоставляет единую консоль, в которой представлена информация о конфигурациях всех служб DNS и DHCP в лесу. С помощью этой консоли можно изменять настройки, например, как одной, так и нескольких зон DHCP, что не требует от системного

администратора написания дополнительных скриптов или ручной настройки каждого DHCP-сервера.

IPAM-сервер самостоятельно забирает информацию с DHCP-, DNS- и RRAS-серверов, а также с контроллеров домена и хранит ее в течение трех лет.

В рамках данного курса не предусматривается подробное изучение IPAM-сервера, достаточно общего представления о его назначении и возможностях.

Дополнительную информацию по установке и настройке DHCP-сервера в Windows Server можно найти по следующим ссылкам:

Установка и настройка DHCP Server на Windows Server 2012 R2
https://vmkh.net/ustanovka-i-nastroyka-dhcp-server-na-windows-server-2012-r2/

Windows Server 2012: делаем протокол DHCP высокодоступным
https://www.osp.ru/winitpro/2013/07/13036326/

Что такое IPAM?
https://technet.microsoft.com/ru-ru/library/jj878331(v=ws.11).aspx

Настройка службы IPAM шаг за шагом
https://habrahabr.ru/company/microsoft/blog/250653/

2.1.2. Служба DNS

2.1.2.1. Назначение службы DNS

Набор протоколов TCP/IP идентифицирует исходные и целевые компьютеры по их IP-адресам. Однако пользователи компьютеров намного лучше используют и запоминают имена, чем числа. Из-за этого администраторы обычно присваивают имена компьютерам. Затем администраторы связывают эти имена с IP-адресами компьютеров в системе разрешения имен, например, DNS. Эти имена находятся в формате имени хоста, например, dc1.contoso.com, который распознается DNS, или в формате имени NetBIOS, например, DC1, который распознается службой Windows Internet Name Service (WINS).

Имя хоста — это удобное для пользователя имя, связанное с IP-адресом компьютера, чтобы идентифицировать его как хост TCP/IP. Имя хоста может содержать до 255 символов и может содержать буквенные и цифровые символы, точки и дефисы.

Вы можете использовать имена хостов в различных формах. Двумя наиболее распространенными формами являются:

- Псевдоним (alias)
- Полное доменное имя (Fully Qualified Domain Name, FQDN)

Псевдоним — это одно имя, связанное с IP-адресом, например, mail. Вы можете комбинировать псевдоним с именем домена для создания полного доменного имени. Полное доменное имя структурировано для использования в Интернете и включает точки в качестве разделителей. Примером полного доменного имени является mail.contoso.com.

DNS — это служба, которая преобразует FQDN и другие имена узлов в IP-адреса. Все операционные системы Windows Server включают службу DNS-сервера.

Когда вы используете DNS, пользователи в вашей сети могут находить сетевые ресурсы, вводя удобные для пользователя имена (например, www.microsoft.com), которые затем компьютер преобразует в IP-адрес. Преимущество в том, что адреса IPv4 труднее запомнить (например, 131.107.0.32), в то время как имя домена обычно запоминается легче. Еще ярче эта проблема проявляется при работе с IPv6-адресами, например, 2001:db8:5176:e38c:18bf:3064:c5ac:3d98.

Кроме того, вы имена хостов редко изменяются, в то время как IP-адреса могут измениться вместе с изменением конфигурации компьютерной сети.

Для преобразования имен в IP-адреса сервер DNS использует базу данных имен и IP-адресов, хранящихся в файле или в доменных службах Active Directory. Клиентское программное обеспечение DNS выполняет запросы и обновляет базу данных DNS. Например, в организации пользователь, который пытается найти сервер печати, может использовать DNS-имя printserver.contoso.com, а клиентское программное обеспечение DNS определяет IP-адрес принтера, например, 172.16.23.55. Даже если IP-адрес принтера изменяется, FQDN-имя может оставаться неизменным.

2.1.2.2. Структура доменных имен

Доменные имена имеют иерархическую структуру. Эту структуру можно представить графически в виде перевернутого дерева (рис. 2.2).

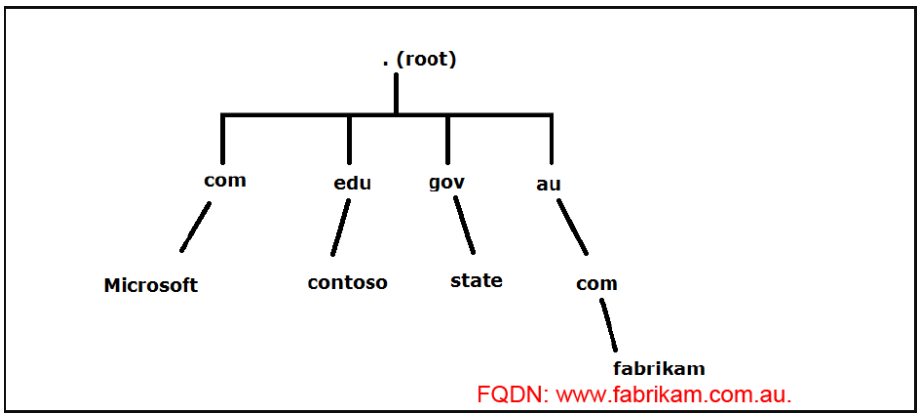

Рис. 2.2. Иерархия доменных имен

Интернет использует единое DNS-пространство имен с несколькими корневыми серверами. Чтобы участвовать в пространстве имен DNS в Интернете, доменное имя должно быть зарегистрировано в регистраторе DNS. Это гарантирует, что никакие две организации не попытаются использовать одно и то же доменное имя.

Если хостам, находящимся в Интернете, не нужно разрешать имена в вашем домене, вы можете создать домен, не регистрируя его. Самым простым способом обеспечения уникальности является создание поддомена в домене .local. Такой домен зарезервирован для внутреннего использования и недоступен из интернета.

Существует тринадцать серверов, которых хранят информацию о доменах верхнего уровня (Top Level Domain, TLD). Каждая страна имеет собственный домен верхнего уровня в соответствии со стандартом ISO 3166. Руководящие органы в этих странах могут дополнительно создавать домены второго уровня,

которые отражают тип организации, например, .com — коммерческие, .gov — правительственные, .org — некоммерческие. Например, Республика Беларусь имеет домен верхнего уровня .by. Следовательно, коммерческая компания в Беларуси может иметь полное доменное имя companyname.com.by, и на заре появления интернета такая практика была обязательна. Потом организации получили право регистрировать собственные домены второго уровня (например, belstu.by), а недавно появился кириллический домен верхнего уровня .БЕЛ. Организации в США традиционно не используют домен .us, а используют домены верхнего уровня .com, .org, .net, и т. д.

2.1.2.3. Зоны DNS

Зоной (zone) в DNS называется часть пространства имен DNS, за управление которой отвечает определенный сервер или группа серверов DNS. Это основной механизм для делегирования полномочий в DNS; он применяется для установки границ, в пределах которых определенный сервер может выполнять запросы. Любой сервер, который обслуживает какую-то определенную зону, считается авторитетным, или ответственным за эту зону; исключением являются зоны-заглушки, о которых будет рассказано ниже в разделе "Зоны-заглушки". На рис. 2.3 показано, как различные части пространства имен DNS могут делиться на зоны и обслуживаться разными серверами или группами серверов DNS.

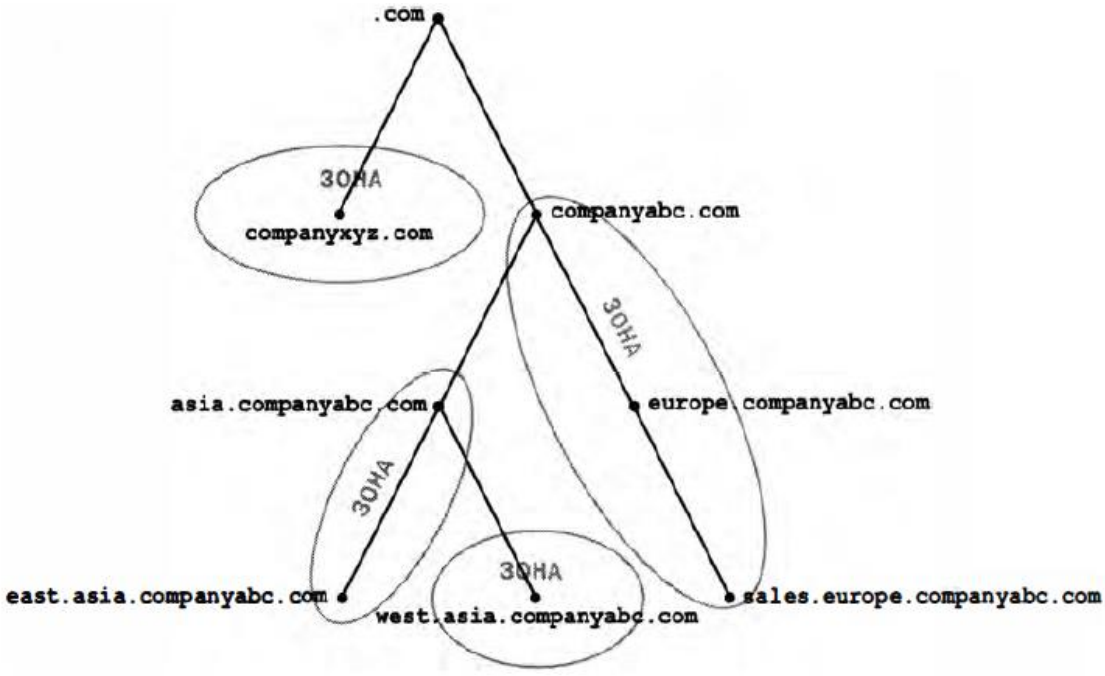

Рис. 2.3. Зоны DNS

Зоны прямого просмотра

Зоны прямого просмотра (forward lookup zone) выполняют преобразование имен в IP-адреса и предоставляют информацию о ресурсах. Например, если пользователь захочет обратиться к серверу srv.belstu.by и запросит его IP-адрес в зоне прямого просмотра, DNS-сервер возвратит ему значение 172.16.1.11 , то есть IP-адрес данного ресурса. Соответствующая запись в зоне может выглядеть следующим образом:

```
srv.belstu.by IN A 172.16.1.11
```

Зоны обратного просмотра

Зоны обратного просмотра (reverse lookup zone) выполняют операцию, прямо противоположную той, что выполняют зоны прямого просмотра — сопоставление IP-адресов с обычным именем. Как правило, зоны обратного просмотра содержат записи PTR, которые служат для указания на соответствующие имена в ответ на запросы обратного поиска. Обратите внимание, что в PTR-записях IP-адрес записывается в обратном порядке.

PTR-запись для ресурса из предыдущего примера может выглядеть так:

```
11.1.16.172.in-addr.arpa IN PTR srv.belstu.by.
```

Первичные зоны

В традиционной DNS (не интегрированной в Active Directory) какой-то один сервер выступает в роли эталонного DNS-сервера для зоны, и все изменения, вносимые в данную зону, выполняются именно на нем. Если зона является первичной, это означает, что все запрашиваемые для нее изменения должны проводиться на сервере, на котором находится эталонная копия этой зоны.

Вторичные зоны

Вторичные зоны (secondary zone) создаются для резервирования и разгрузки первичной зоны. Однако каждая копия базы данных DNS доступна только для чтения, поскольку все изменения в записи вносятся в первичной зоне. На одном сервере DNS могут размещаться несколько первичных и несколько вторичных зон.

Зоны-заглушки

Концепция зон-заглушек (stub zone) встречается только в DNS производства Microsoft. Это зона, которая не содержит никакой информации о членах домена и служит просто для перенаправления запросов к списку выделенных серверов имен для различных доменов. Поэтому в такой зоне могут находиться только записи типа NS, SOA и связанные записи. Связанные записи (glue record) — это записи типа A, которые используются в сочетании с конкретной записью NS для преобразования IP-адреса некоторого сервера имен. Сервер, содержащий зону-заглушку для какого-либо пространства имен, не является авторитетным для этой зоны.

Как показано на рис. 2.3, зона-заглушка служит заменителем той зоны, которая является авторитетной на другом сервере. Она позволяет серверу пере-направлять запросы в определенную зону в список серверов имен этой зоны.

ВАЖНО: Для функционирования зоны заглушки важно, чтобы на сервере с полнофункциональной зоной была разрешена передача зоны на сервер с зоной-заглушкой. Это не всегда возможно.

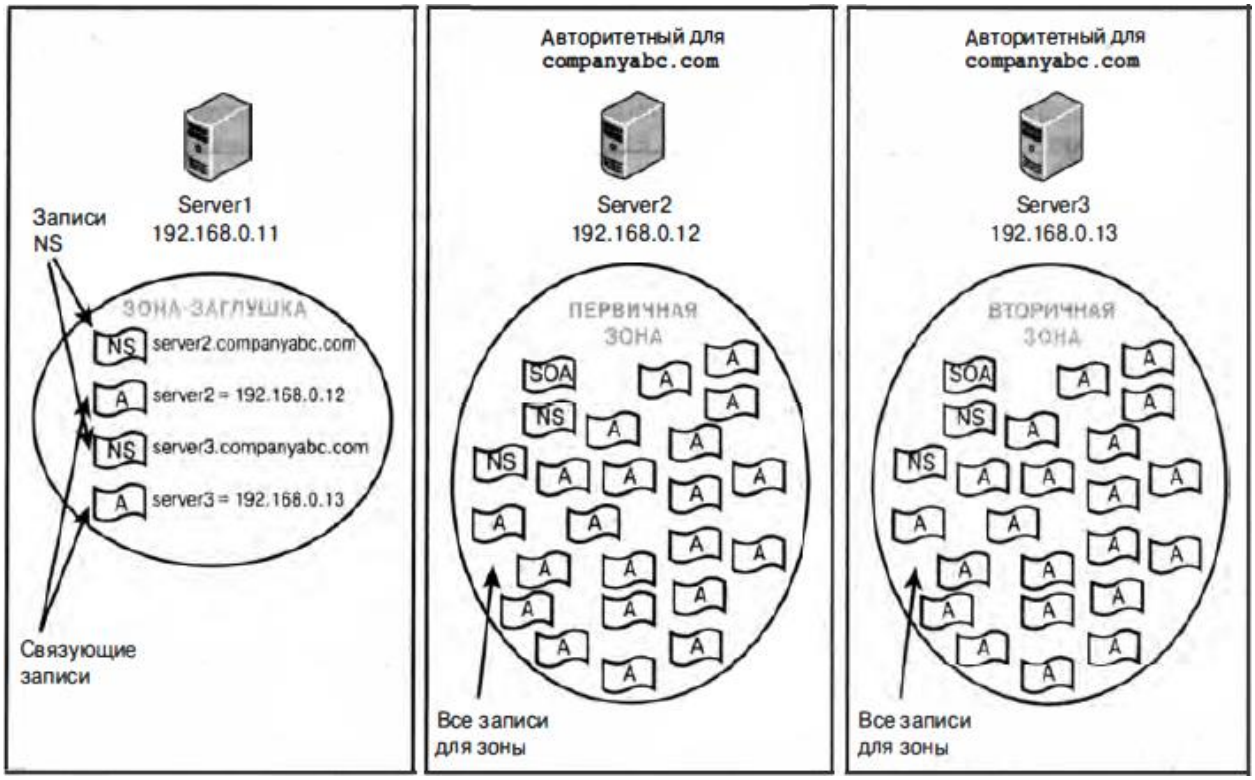

Рис. 2.3. Зоны-заглушки

Серверы пересылки

Ретрансляторами (forwarder), или серверами пересылки, называются серверы имен, которые отвечают за обработку всех итеративных запросов к серверу имен. То есть если сервер не может ответить на запрос от клиентского распознавателя, то серверы, имеющие ретрансляторы, просто передают этот запрос вышестоящему ретранслятору, который затем обработает эти итеративные запросы к корневым серверам Интернет-имен.

Ретрансляторы часто применяются в ситуациях, когда в организации для обработки всего связанного с преобразованием имен трафика используются DNS-серверы Интернет-провайдера. Например, все внутренние DNS-запросы по преобразованию имен обрабатываются внутренними серверами DNS, находящимися в среде Active Directory, а все исходящие DNS-запросы перенаправляются на отдельный сервер или непосредственно на сервер интернет-провайдера.

При условной переадресации запросы к конкретному домену или набору доменов посылаются специально определенному DNS-серверу пересылки. Обычно так делается для определения маршрутов трафика для внутреннего преобразования доменов. Например, в случае использования организацией пространств имен доменов companyabc.com и companyxyz.com можно указать, чтобы запросы между этими доменами отрабатывались на локальных DNS-серверах, а не пересылались в Интернет лишь для того, чтобы тут же возвратиться обратно для их внутреннего преобразования.

Просмотр корневых ссылок

По умолчанию инсталляция DNS включает в себя список серверов имен верхнего уровня, которые могут применяться для преобразования встречающихся в Интернете доменных имен — .com, . net , . by и т.д. Если серверу DNS не удается

удовлетворить запрос локально в своем кеше или в локальных зонах, он обращается к списку корневых ссылок (Root Hints), который указывает, с каких серверов нужно начинать итеративные запросы.

Файл этих ссылок должен регулярно обновляться, чтобы гарантировать актуальность всех перечисленных в нем серверов. Этот файл размещен в каталоге %systemroot%\system32\DNS\cache.dns и может обновляться из Интернета по адресу:

ftp://ftp.internic.net/domain/named.cache

2.1.2.4. Примеры сложных конфигураций DNS

Процесс установки и настройки одиночного сервера DNS в операционной системе Windows Server описан в пункте 5.3.1 учебника «Компьютерные сети» [1].

Здесь мы рассмотрим сценарии с несколькими серверами.

Во-первых, даже в самом простом случае с одним доменом и сайтом для обеспечения отказоустойчивости необходимо иметь не менее двух серверов DNS. При большом количестве клиентов для распределения нагрузки может потребоваться и большее количество серверов.

Примечание. Для распределения нагрузки необходимо так настроить клиентские компьютеры, чтобы только у определенной их части в настройках сетевого интерфейса первым был указан соответствующий DNS-сервер. При идентичной настройке всех клиентских компьютеров распределения нагрузки не будет.

Во-вторых, для разрешения внешних имен нужна связь с интернет. Соответственно, на межсетевом экране нужно создать исключения для каждого DNS-сервера внутренней сети. В целях безопасности обычно устанавливается дополнительный DNS-сервер, являющийся сервером пересылки для внутренних серверов, а на внешнем межсетевом экране разрешается доступ в интернет только для этого дополнительного сервера. Дополнительное преимущество этого решения — дополнительный сервер еще хранит общий кэш всех DNS-запросов организации, что увеличивает общую эффективность разрешения имен.

Стоит упомянуть, что в корпоративной сети целесообразнее использовать интегрированные с AD зоны, чем файловые. При этом синхронизация содержимого копий зон DNS выполняется автоматически в рамках общей репликации Active Directory. Но еще большее преимущество данного выбора — использование динамической регистрации компьютеров на сервере DNS, ведь при большом количестве компьютеров управление DNS-записями стало бы непосильной задачей для администратора сети.

Если лес Active Directory состоит из большого количества доменов (и деревьев), то серверы имен дочерних доменов обычно выполняют пересылку на корневые серверы имен своего дерева. В каждом родительском домене создается делегирование на дочерний домен.

Примечание. При использовании интегрированных в AD зон на каждом DNS-сервере существует зона _msdcs, которая служит для поиска других контроллеров домена этого леса.

До сих пор мы рассматривали лишь разрешение имен из внутренней сети предприятия. Здесь было все просто: внутренние запросы разрешаются своими внутренними серверами имен, внешние запросы пересылались на DNS-сервер в интернете с известным адресом. В крайнем случае можно воспользоваться корневыми ссылками и самостоятельно выполнить итеративный запрос. Осталось рассмотреть обратную задачу — как внешний клиент (например, из партнерской организации) сможет найти ресурсы в нашей сети (предполагается, что у него есть физический доступ к сети, например, с помощью VPN).

Когда проектировалась DNS, то предполагалось, что пространство DNS-имен является связным, то есть до любого узла сети можно последовательно дойти от корня. Но в действительности многие организации не интегрируют пространство имен своей внутренней сети в целях безопасности. Более того, иногда они используют при создании домена несуществующие суффиксы, например, .local. Такие домены в принципе недостижимы из интернета. Часто встречается так называемое расщепленное (split) пространство имен — одно и то же доменное имя ресурса используется внутри сети (разрешаемое во внутренний адрес, который хранится на внутренних серверах имен), и для внешних пользователей интернета (разрешаемое в реальный адрес интернет, которых хранится на серверах имен интернета). Например, почтовый сервер предприятия может иметь имя mail.belstu.by и разрешаться из интернета как 192.23.23.23, а из внутренней сети как 10.1.1.2. Расщепленные пространства имен реализуются легко: зона с одним и тем же именем создается и на внутренних серверах имен, и в интернете. Как правило, во внешней зоне будет очень небольшое количество ресурсов. Но в обоих этих случаях, чтобы внешние клиенты смогли найти внутренние ресурсы нашей сети, им нужно как-то сообщить IP-адреса DNS-серверов нашей организации.

Для разрешения имен из таких «закрытых» пространств имен нужно использовать условную пересылку или зоны-заглушки. На первый взгляд, эти технологии как бы похожи и служат для одного и того же, но между ними есть несколько принципиальных отличий.

Условная пересылка не требует административных разрешений в зоне, но требует ручного администрирования для поддержки актуальности информации о серверах имен, ответственных за целевую зону. Использование зон-заглушек автоматизирует актуализацию информации о серверах имен между зонами, но требует явного разрешения администратора целевой зоны на передачу зоны.

2.1.3. Служба аутентификации

В современных бизнес-средах людям обычно требуется доступ к нескольким системам и ресурсам. Они подключаются к ресурсам из внутренней или домашней сети, из Интернета, из корпоративных партнерских сетей, а также на нескольких и разных устройствах. В крупных предприятиях обычно имеется несколько репозиториев аутентификации.

Пользователи могут выполнять аутентификацию с помощью доменных служб Active Directory® (AD DS), а также с другими сторонними системами. Иногда разные отделы отдела информационных технологий (ИТ) поддерживают реестры

корпоративной аутентификации. В некоторых сценариях пользователи могут иметь учетные записи пользователей в каждом репозитории аутентификации.

Управление защитой доступа и информации (AIP — Access and Information Protection) упрощает работу пользователей онлайн-пользователей, оптимизируя административные усилия ИТ-отделов.

Решения AIP Management представляют собой набор технологий и продуктов, предназначенных для того, чтобы помочь организациям управлять идентификациями пользователей и связанными с ними привилегиями доступа, создавая один авторитетный источник аутентификации пользователей. Стоимость и административные усилия, необходимые для управления несколькими репозиториями, идентификаторами и политиками аутентификации, являются существенными. В крупных корпоративных средах, состоящих из различных систем, административные усилия могут быть существенными. Однако без хорошего решения AIP компании рискуют нарушениями безопасности, нарушениями нормативного соответствия, неэффективной производительностью сотрудников и неэффективной поддержкой пользователей или клиентов. Управление идентификациями пользователей и эффективный доступ к важной информации является главным приоритетом для большинства организаций сегодня.

Любое решение AIP, будь то развертывание в поддержку малого бизнеса или крупного предприятия, представляет собой баланс между безопасностью и доступностью. Задача ИТ-специалистов, которые разрабатывают и внедряют решение AIP, заключается в понимании баланса. В сущности, они должны внедрять систему, отвечающую требованиям бизнеса, без введения чрезмерных ограничений или неэффективности для пользователей. Чтобы понять баланс между безопасностью и доступностью, ИТ-специалист должен собрать и понять бизнес-причины для рассмотрения решения AIP.

Решения управления AIP помогают управлять различными идентификаторами, которые могут быть у пользователей. Многие организации борются с требованиями поддержания независимых справочников. Различные отделы внутри организации иногда поддерживают каталоги, что приводит к дополнительным проблемам управления. Это явление называется разрастанием каталогов.

В следующем списке перечислены функции решений управления AIP:

- Сохранение нескольких хранилищ личных данных в организации. Решения AIP помогают упростить обслуживание и администрирование нескольких хранилищ личных данных. Эти хранилища могут включать такие продукты, как:
    - AD DS;
    - облегченные службы каталогов Active Directory (AD LDS);
    - Lotus Notes;
    - Novell eDirectory;
    - Базы данных по персоналу (HR);
    - Приложения с поддержкой Active Directory;
    - Active Directory (AD) для Windows Azure ™

• Определение текущей и достоверной информации о личности. Решения AIP позволяют синхронизировать, поддерживать и обновлять идентификационную информацию в нескольких хранилищах идентификаторов. Авторитетная идентификация в этом контексте означает идентификацию атрибутов и источник этих атрибутов. Это будет действовать как доверенный источник информации, который затем может проверять синхронизированную информацию.

• Предоставление и деактивация учетных записей пользователей. Решения AIP могут автоматизировать процесс подготовки. Автоматизация обеспечивает целостность данных, целостность и повышенную безопасность по сравнению с ручными процессами. Предоставление и депровизирование — это процесс предоставления и удаления учетных записей пользователей и доступа к ресурсам предприятия.

• Аутентификация и авторизация пользователей. Решения AIP гарантируют, что пользователи аутентифицируют и авторизуют свои идентификаторы, используя информацию управления доступом, такую как ACL. Это определяет уровень доступа к определенным ресурсам, связанным с вашей личностью.

• Обеспечение совместной информации. Решения AIP помогают безопасно обмениваться конфиденциальной информацией в разрозненных сетях.

• Обеспечение взаимодействия между партнерами и поставщиками, а также между локальными и облачными решениями. С решениями AIP вы можете использовать доверительные отношения с доменами, доверительные отношения с лесами и федерацию для поставщиков, внешних партнеров и других подразделений для безопасного доступа к данным и ресурсам. Кроме того, вы можете расширить AD DS вашей организации с помощью облачных сервисов, таких как Microsoft Office 365, Microsoft SharePoint Online и Windows Azure AD. Используя службы федерации Active Directory (AD FS), интеграция и безопасная связь между локальными и облачными решениями намного проще.

• Обеспечение доступа и распространения конфиденциальных данных. С помощью решений AIP вы можете защитить конфиденциальную бизнес-информацию от несанкционированного доступа и распространения, даже если файл, содержащий информацию, скомпрометирован. Например, вы можете защитить презентацию Microsoft Office PowerPoint с помощью служб управления правами Active Directory (AD RMS), чтобы гарантировать, что только сотрудники имеют доступ к чтению презентации, даже если файл попадает в руки несанкционированного доступа. Вы можете защитить информацию на своем ноутбуке с помощью технологии шифрования диска BitLocker.

Windows Server 2012 и Windows Server 2012 R2 имеют несколько ролей сервера для управления AIP. Вы можете удовлетворить требования бизнеса, используя диспетчер сервера для установки и настройки этих ролей. Помимо включенных ролей Microsoft также предоставляет облачные сервисы для поддержки AIP-управления, такие как Windows Azure AD. Этот урок даст обзор этих ролей и технологий.

2.2. Служба каталогов Active Directory Domain Services

Доменные службы Active Directory® (AD DS) и связанные с ними службы образуют основу для корпоративных сетей, работающих под управлением операционных систем Windows®. База данных AD DS является центральным хранилищем всех объектов домена, таких как учетные записи пользователей, учетные записи компьютеров и группы. AD DS предоставляет иерархию поиска и способ применения настроек конфигурации и безопасности для объектов на предприятии. В этом пункте рассмотрим общую структуру AD DS и ее различные компоненты, таких как лес, домен и организационные подразделения (OU).

AD DS состоит из логических и физических компонентов. Вам нужно понять, как работают компоненты AD DS, чтобы вы могли эффективно управлять своей инфраструктурой. Кроме того, вы можете использовать многие другие параметры AD DS для выполнения таких действий, как установка, настройка и обновление приложений; управление инфраструктурой безопасности; включение удаленного доступа и DirectAccess; выдачи и управления цифровыми сертификатами.

Одной из наиболее используемых функций AD DS является групповая политика, которая позволяет настраивать централизованные политики, которые можно использовать для управления большинством объектов в AD DS. Понимание различных компонентов AD DS важно для успешного использования групповой политики.

2.2.1. Логические компоненты доменных служб Active Directory

Логические компоненты AD DS — это логические структуры, которые вы используете для реализации дизайна Active Directory, подходящего для организации. В таблице 3.1 описаны типы логических структур, содержащихся в базе данных Active Directory.

Таблица 3.1. Логические компоненты доменных служб Active Directory

Логический компонент	Описание
Раздел (Partition)	Это раздел базы данных AD DS. Хотя база данных — это единый файл с именем Ndts.dit, вы просматриваете его, управляете им и реплицируете его, как если бы он состоял из отдельных разделов или экземпляров. Они называются разделами, которые также называются контекстами именования (naming context).
Схема (Schema)	Это набор определений типов объектов и атрибутов, которые вы используете для создания объектов в AD DS
Домен (Domain)	Это логический, административный контейнер для пользователей и компьютеров.
Дерево доменов (Domain tree)	Это набор доменов, которые имеют общий корневой домен и непрерывное пространство доменных имен (DNS).
Лес (Forest)	Это набор доменов, которые имеют общую схему и конфигурацию AD DS.

Сайт (Site)	Это набор пользователей, групп и компьютеров, которые определяются их физическим расположением. Вы можете использовать сайты для планирования административных задач, таких как репликация изменений в базе данных AD DS.
Организационное подразделение (Organizational unit, OU)	Представляет собой контейнерный объект, который обеспечивает структуру для делегирования административных прав и для связывания объектов групповой политики (GPO).
Контейнер (Container)	Объект, который предоставляет иерархическую структуру для использования в AD DS. Объекты групповой политики не могут привязываться к контейнерам.

2.2.2. Физические компоненты доменных служб Active Directory

В таблице 3.2 описаны некоторые физические компоненты AD DS.

Таблица 3.2. Логические компоненты доменных служб Active Directory

Физический компонент	Описание
Контроллер домена (Domain controller)	Он содержит копию базы данных AD DS. Для большинства операций каждый контроллер домена может обрабатывать изменения и реплицировать изменения ко всем другим контроллерам домена в домене
Хранилище данных (Data store)	На каждом контроллере домена имеется база данных AD DS, которая использует технологию баз данных Microsoft Jet и хранит информацию о каталоге в файле Ntds.dit и связанных файлах журнала. Эти файлы по умолчанию хранятся в папке C:\Windows\NTDS.
Сервер глобального каталога (Global catalog server)	Это контроллер домена, в котором размещен глобальный каталог, который является частичной, доступной только для чтения копией всех объектов в лесу. Глобальный каталог ускоряет поиск объектов, которые могут храниться на контроллерах домена в другом домене в лесу.
Контроллер домена только для чтения (Read-only domain controller, RODC)	Это специальный вариант установки AD DS, при котором информация в каталоге доступна только для чтения. RODC часто используются в филиалах, где безопасность и поддержка ИТ менее развиты, чем в основных корпоративных центрах.

2.2.3. Что такое домен AD DS

Домен AD DS содержит пользователей, компьютеры, группы

Домен AD DS — это логический контейнер, используемый для управления пользователями, компьютерами, группами и другими объектами.

Все объекты домена хранятся в базе данных AD DS, копия которой хранится на каждом контроллере домена.

В базе данных AD DS существует множество типов объектов, включая учетные записи пользователей, учетные записи компьютеров и группы. В следующем списке кратко описаны эти три типа объектов:

- *Учетные записи пользователей*. Учетные записи пользователей содержат информацию, необходимую для аутентификации пользователя во время процесса входа и создания маркера защиты пользователя.
- *Учетные записи компьютеров*. Каждый подключенный к домену компьютер имеет учетную запись в AD DS. Учетные записи компьютеров используются для компьютеров, подключенных к домену, таким же образом, как учетные записи пользователей используются для пользователей.
- *Группы*. Группы используются для организации пользователей или компьютеров, чтобы упростить управление разрешениями и групповой политикой в домене.

Домен AD DS является границей репликации

Когда изменения происходят с любым объектом в домене, контроллер домена, в котором произошло изменение, реплицируется, что изменяется на все остальные контроллеры домена в домене. Если в лесу имеется несколько доменов, только подмножества изменений реплицируются в другие домены. AD DS использует модель репликации мультимастера, которая позволяет каждому контроллеру домена вносить изменения в объекты в домене. В одном домене может содержаться почти 2 миллиарда объектов.

Благодаря такой большой емкости большинство организаций могут развертывать только один домен и обеспечивать, чтобы все контроллеры домена содержали всю информацию о домене. Тем не менее, организации, которые имеют децентрализованные административные структуры или которые распределены по нескольким местоположениям, могут рассмотреть возможность внедрения нескольких доменов в том же лесу для удовлетворения административных потребностей своей среды.

Домен AD DS является административным центром

Домен содержит учетную запись администратора и группу «Администраторы домена». По умолчанию учетная запись администратора является членом группы «Администраторы домена» (Domain Admins), а группа «Администраторы домена» является членом каждой локальной группы «Администраторы» подключенных к домену компьютеров. Кроме того, по умолчанию члены группы «Администраторы домена» имеют полный контроль над каждым объектом домена. У учетной записи администратора в корневом домене леса также есть дополнительные права.

Домен AD DS обеспечивает аутентификацию

Всякий раз, когда компьютер, подключенный к домену, запускается или пользователь регистрируется на компьютере, подключенном к домену, AD DS аутентифицирует их. Аутентификация проверяет, что компьютер или пользователь имеют соответствующие учетные данные для учетной записи AD DS.

Домен AD DS обеспечивает авторизацию

Операционные системы Windows используют технологии авторизации и контроля доступа, позволяющие аутентифицированным пользователям получать доступ к ресурсам. Как правило, процесс авторизации выполняется локально на ресурсе.

В Windows Server 2012 был добавлен динамический контроль доступа (Dynamic Access Control, DAC), чтобы реализовать правила центрального доступа для контроля доступа к ресурсам. Правила центрального доступа не заменяют существующую технологию контроля доступа, а обеспечивают дополнительный уровень контроля.

2.2.4. Что такое организационные подразделения

Организационное подразделение (OU) — это контейнерный объект в домене, который можно использовать для консолидации пользователей, компьютеров, групп и других объектов. OU не следует путать с универсальными контейнерными объектами в AD DS. Основное различие между подразделениями и контейнерами — это возможности управления. Контейнеры имеют ограниченные возможности управления; например, вы не можете применять объект групповой политики непосредственно к контейнеру. Обычно вы используете контейнеры для системных объектов и в качестве местоположений по умолчанию для новых объектов. С OU вы имеете больше вариантов управления; вы можете напрямую связать объекты групповой политики, назначить менеджера OU и связать раздел COM + с OU.

Несмотря на отсутствие опции меню для создания новых контейнеров в консоли **Active Directory пользователи и компьютеры**, вы можете создавать новые подразделения в AD DS в любое время. Существует две причины создания подразделений:

- Группировать объекты вместе, чтобы упростить управление ими, применяя объекты групповой политики (GPO) для всей группы. Вы можете назначить объекты групповой политики для OU, и настройки применяются ко всем объектам в подразделении. Объекты групповой политики — это политики, которые администраторы создают для управления и настройки параметров для компьютеров и/или пользователей. Объекты групповой политики развертываются путем связывания их с подразделениями, доменами или сайтами.
- Делегировать административный контроль объектов внутри подразделения. Вы можете назначить разрешения управления для OU, тем самым делегируя управление этим подразделением пользователю или группе в AD DS в дополнение к группе администраторов.

Вы можете использовать OU для представления иерархических, логических структур внутри вашей организации. Например, вы можете создавать подразделения, которые представляют подразделения вашей организации, географические регионы вашей организации или комбинацию как ведомственных, так и географических регионов. Вы можете использовать подразделения для управления конфигурацией и использованием учетных записей пользователей, групп и компьютеров на основе вашей организационной модели.

В консоли Active Directory Users and Computers для OU используется другой значок. На рис.2.4 показано два OU: Domain Controllers и OU00.

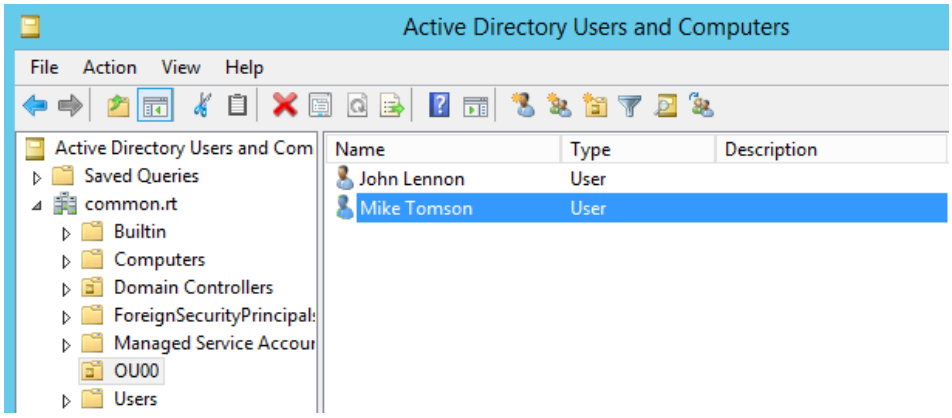

Рис. 2.4. OU и контейнеры в консоли Active Directory Users and Computers

Для обозначения объектов используется два вида записи: каноническая и полная.

В канонической записи OU и контейнеры не различаются, самый старший объект в иерархии располагается слева. Например, каноническое имя для объекта пользователя Mike Tomson будет следующим: `common.rt/OU00/Mike Tomson` (рис. 2.5).

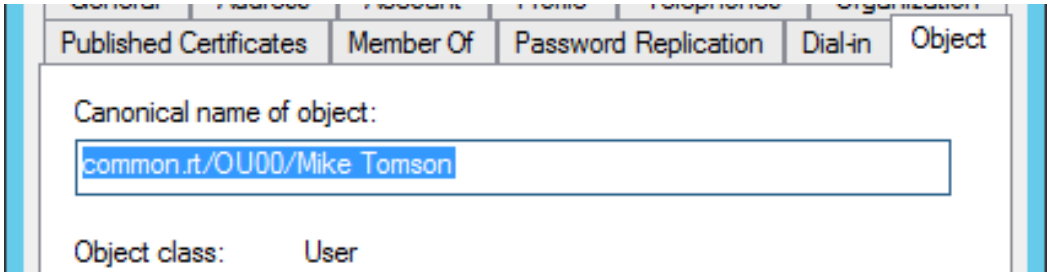

Рис. 2.5. Пример канонического имени объекта

В полной записи имени каждый компонент имени записывается отдельно, самый старший объект в иерархии при этом располагается справа. Для обозначения компонентов имени домена используется метка DC (Domain Component), для обозначения организационных подразделений — OU (Organizational Unit), для конечных элементов и обычных контейнеров — CN (Common Name). Полное имя для объекта из предыдущего примера будет `CN=Mike Tomson,OU=OU00,DC=common,DC=rt`(рис.2.6).

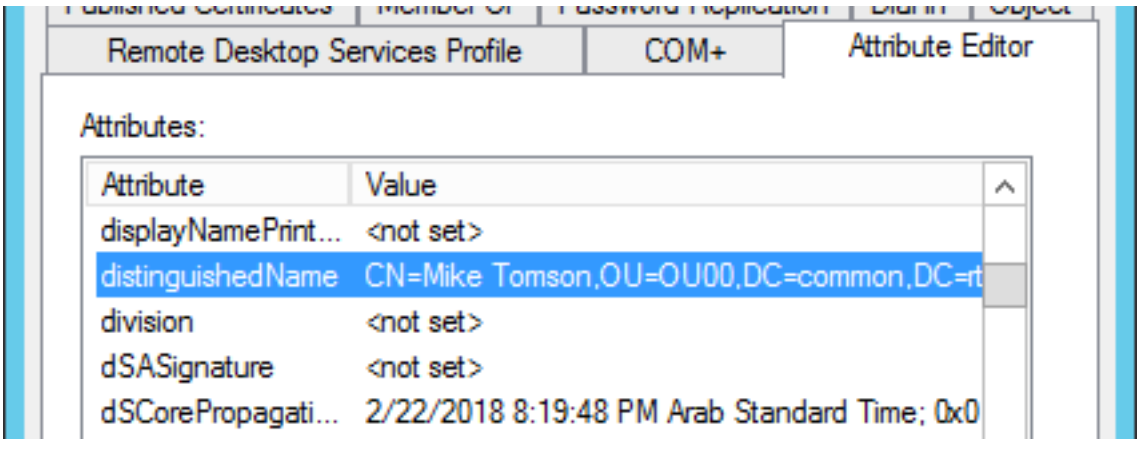

Рис. 2.6. Пример полного различаемого имени объекта

Дизайн иерархии

Конструкция иерархии OU диктуется административными потребностями организации. Дизайн может быть основан на географических, функциональных, ресурсных или пользовательских классификациях. Иерархия должна позволять администрировать ресурсы AD DS как можно эффективнее и с максимальной гибкостью. Например, если все компьютеры, используемые ИТ-администраторами, должны быть настроены определенным образом, вы можете сгруппировать все компьютеры в подразделении, а затем назначить объект групповой политики для управления этими компьютерами.

Вы также можете создавать подразделения в других подразделениях. Например, ваша организация может иметь несколько офисов, и каждый офис может иметь команду ИТ-администраторов, которые несут ответственность за управление учетными записями пользователей и компьютеров в своем офисе. Кроме того, каждый офис может иметь разные отделы с различными требованиями к конфигурации компьютера. В этой ситуации вы можете создать подразделение для каждого офиса, а затем в каждом из этих подразделений создать подразделение для ИТ-администраторов и подразделений для каждого из других отделов.

Несмотря на отсутствие технических ограничений на количество уровней в структуре вашего подразделения, чтобы обеспечить управляемость, ограничьте структуру своего подразделения до глубины не более 10 уровней. Большинство организаций используют пять уровней или меньше, чтобы упростить администрирование. Обратите внимание, что приложения с поддержкой Active Directory могут налагать ограничения на глубину OU в иерархии.

2.2.5. Что такое лес AD DS

Деревом доменов является коллекция из одного или нескольких доменов, которые разделяют непрерывное пространство имен. Лес — это коллекция из одного или нескольких деревьев доменов, которые имеют общую схему каталогов и глобальный каталог. Первый домен, созданный в лесу, называется корневым доменом леса. Корневой домен леса содержит несколько объектов, которые не существуют в других доменах в лесу. Поскольку эти объекты всегда создаются на первом созданном контроллере домена, лес может состоять всего из одного домена с одним контроллером домена или может состоять из нескольких деревьев с сотнями доменов. Следующие объекты существуют только в корневом домене леса:

- Роль мастера схемы. Это особая роль контроллера домена на уровне леса. В любом лесу есть только один хозяин схемы. Схему можно изменить только на контроллере домена, который владеет ролью мастера схемы.

- Роль хозяина именования доменов. Это также особая роль контроллера домена в масштабе всего леса. В любом лесу есть только один владелец именования доменов. Новые имена доменов могут быть добавлены в каталог только мастером именования доменов.

- Группа «Администраторы предприятия» (Enterprise Admins). По умолчанию группа «Администраторы предприятия» имеет учетную запись «Администратор» для корневого домена леса в качестве члена. Группа «Администраторы

предприятия» является членом локальной группы администраторов в каждом домене леса. Это позволяет членам группы «Администраторы предприятия» иметь полный контроль над правами администратора для каждого домена в лесу.

- Группа «Администраторы схемы». По умолчанию группа «Администраторы схемы» не имеет членов. Только члены группы Enterprise Admins или группа «Администраторы домена» (в корневом домене леса) могут добавлять членов в группу «Администраторы схемы». Только члены группы «Админы схемы» могут вносить изменения в схему.

Граница безопасности

Лес AD DS является границей безопасности. По умолчанию пользователи из-за пределов леса не могут получить доступ к каким-либо ресурсам внутри леса. Обычно организация создает только один лес, хотя вы можете создать несколько лесов, чтобы изолировать административные разрешения между различными частями организации.

По умолчанию все домены леса доверяют другим доменам в лесу автоматически. Это упрощает доступ к ресурсам, таким как общие файлы и веб-сайты для всех пользователей в лесу, независимо от домена, в котором находится учетная запись пользователя.

Граница репликации

Лес AD DS — это граница репликации для разделов конфигурации и схемы в базе данных AD DS. Это означает, что все контроллеры домена в лесу должны иметь одну и ту же схему. Поэтому организациям, которые хотят развернуть приложения с несовместимыми схемами, необходимо развернуть дополнительные леса.

Лес AD DS также является границей репликации для глобального каталога. Глобальный каталог позволяет находить объекты из любого домена в лесу. Глобальный каталог используется всякий раз, когда используются учетные данные аутентификации универсального имени участника (UPN) или когда адресные книги Microsoft Exchange Server используются для поиска пользователей.

2.2.6. Что такое схема AD DS

Схема AD DS — это компонент, который определяет все классы объектов и атрибуты, которые AD DS использует для хранения данных. Его иногда называют планом (blueprint) AD DS. Схема реплицируется среди всех контроллеров домена в лесу. Любые изменения, внесенные в схему, реплицируются на каждый контроллер домена в лесу от владельца главной схемы, который обычно является первым контроллером домена в лесу.

AD DS хранит и извлекает информацию для широкого спектра приложений и сервисов. Стандартизируя хранение данных, AD DS может извлекать, обновлять и реплицировать данные, обеспечивая при этом сохранение целостности данных.

Объекты

AD DS использует объекты как единицы хранения. Все типы объектов определены в схеме. Каждый раз, когда каталог обрабатывает данные, каталог

запрашивает схему для соответствующего определения объекта. Основываясь на определении объекта в схеме, каталог создает объект и сохраняет данные.

В определения объектов входят как типы данных, которые могут хранить объекты, так и синтаксис данных. Вы можете создавать только объекты, определенные схемой. Поскольку данные хранятся в жестко определенном формате, AD DS может хранить, извлекать и проверять данные, которыми он управляет, независимо от того, какое приложение его предоставляет.

Отношения между объектами, правилами, атрибутами и классами

В AD DS схема определяет следующее:

- Объекты, которые хранят данные в каталоге
- Правила, определяющие структуру объектов
- Структура и содержание самого каталога

Объекты схемы AD DS состоят из атрибутов, которые сгруппированы в классы. Каждый класс имеет правила, которые определяют, какие атрибуты требуются и которые являются необязательными. Например, пользовательский класс состоит из более чем 400 возможных атрибутов, включая **cn** (общий атрибут имени), **givenName**, **displayName**, **objectSID** и **manager**. Из этих атрибутов только атрибуты **cn** и **objectSID** являются обязательными. Атрибут **cn** определяется как строка Unicode длиной от 1 до 64 символов и реплицируемый в глобальный каталог.

Внесение изменений в схему

Только члены группы «Администраторы схемы» могут изменять схему AD DS. Вы не можете удалить что-либо из схемы AD DS; вы можете расширить схему AD DS только с помощью расширений схемы AD DS или путем изменения атрибутов существующих объектов. Например, при подготовке к установке Exchange Server 2013 вы должны применять расширения схемы Exchange Server 2013. Это расширение добавляет или изменяет более 200 классов и более 100 различных атрибутов.

Вы должны изменить схему только тогда, когда это необходимо, потому что схема определяет, как хранится информация, и любые изменения, внесенные в схему, влияют на каждый контроллер домена. Прежде чем вы измените схему, вы должны просмотреть изменения с помощью строго контролируемого процесса и реализовать их только после того, как вы проверили тестирование, чтобы гарантировать, что эти изменения не будут неблагоприятно влиять на остальную часть леса или на любые приложения, использующие AD DS.

Мастер схемы является одной из главных ролей операций, которые размещаются на одном контроллере домена в доменных службах Active Directory. Поскольку это единственный мастер, вы должны внести изменения в схему, настроив контроллер домена, который содержит мастер схемы.

2.2.7. Что такое контроллер домена

Контроллер домена — это сервер, который настроен для хранения копии базы данных каталога AD DS (Ntds.dit) и копии папки SYSVOL. Все контроллеры домена, кроме RODC, могут изменять данные в обоих ресурсах. Ntds.dit — это

сама база данных, а папка SYSVOL содержит все параметры шаблона и файлы для объектов групповой политики.

Контроллеры домена используют процесс репликации мультимастера; для большинства операций данные могут быть изменены на любом контроллере домена (естественно, за исключением RODC). Служба репликации AD DS затем синхронизирует изменения, внесенные в базу данных AD DS, на все остальные контроллеры домена в этом домене. В исходной версии Windows Server 2012 (RTM) вы можете использовать службу репликации файлов (FRS) или новую репликацию распределенной файловой системы (DFS) для репликации папок SYSVOL. В Windows Server 2012 R2 вы можете использовать только репликацию DFS.

Контроллеры домена содержат несколько других служб, связанных с Active Directory, включая службу проверки подлинности Kerberos, учетные записи пользователей и компьютеров для аутентификации входа; и Центр распределения ключей (KDC), который выдает билеты на выдачу билетов (TGT) на учетную запись, которая регистрируется в домене AD DS. При желании вы можете настроить контроллеры домена на размещение копии глобального каталога.

Все пользователи домена AD DS существуют в базе данных AD DS, и, если по какой-либо причине база данных недоступна по любой причине, все операции, зависящие от проверки подлинности на основе домена, потерпят неудачу. Как наилучшая практика, домен AD DS должен иметь как минимум два контроллера домена. Это делает базу данных AD DS более доступной и распределяет запросы на аутентификацию во время пиковой нагрузки (например, в начале рабочего дня).

При развертывании контроллера домена в филиале, где физическая безопасность менее оптимальна, вы можете использовать дополнительные меры для снижения влияния нарушения безопасности. Один из вариантов заключается в развертывании контроллера домена только для чтения.

RODC содержит копию базы данных AD DS только для чтения, и по умолчанию она не кэширует пароли пользователей. Вы можете настроить RODC для кэширования паролей для пользователей в филиале. Если RODC скомпрометирован, потенциальная потеря информации намного ниже, чем с полным контроллером домена для чтения/записи. Другой вариант — использовать шифрование диска Windows BitLocker® для шифрования жесткого диска контроллера домена. Если жесткий диск украден, шифрование BitLocker гарантирует, что злоумышленнику будет сложно получить от него какую-либо полезную информацию.

Примечание. BitLocker — это система шифрования дисков, доступная для операционных систем Windows Server и для некоторых клиентских версий операционной системы Windows. BitLocker надежно шифрует всю операционную систему, чтобы компьютер не запускался без предоставления закрытого ключа и (необязательно) передачи проверки целостности. Диск остается зашифрованным, даже если вы перенесите его на другой компьютер.

2.2.8. Что такое глобальный каталог

Глобальный каталог — это частичная, доступная только для чтения копия всех объектов в лесу. Это ускоряет поиск объектов, которые могут храниться на контроллерах домена в другом домене в лесу.

В пределах одного домена база данных AD DS на каждом контроллере домена содержит всю информацию о каждом объекте в этом домене, но только часть этой информации реплицируется на серверы глобальных каталогов в других доменах в лесу. В пределах данного домена запрос для объекта направляется на один из контроллеров домена в этом домене, но этот запрос не включает результаты об объектах в других доменах в лесу. Чтобы запрос включал результаты из других доменов в лесу, вы должны запросить контроллер домена, который является сервером глобального каталога. По умолчанию первый контроллер домена в корневом домене леса является единственным сервером глобального каталога. Чтобы улучшить поиск по доменам в лесу, вы должны настроить дополнительные контроллеры домена для хранения копии глобального каталога.

Глобальный каталог не содержит всех атрибутов для каждого объекта. Вместо этого глобальный каталог поддерживает подмножество атрибутов, которые, скорее всего, будут полезны при междоменном поиске. Эти атрибуты включают, например, **`givenName`**, **`displayName`**, and **`mail`**.

Существуют различные причины, по которым вы можете выполнять поиск по глобальному каталогу, а не к контроллеру домена, который не является глобальным каталогом. Например, когда сервер, на котором запущен Exchange Server, получает входящее сообщение электронной почты, ему необходимо выполнить поиск учетной записи получателя, чтобы он мог решить, куда перенаправить сообщение. Автоматически запрашивая глобальный каталог, сервер, на котором работает Exchange Server, может найти получателя в среде с несколькими доменами. В другом примере, когда пользователь регистрируется в домене с помощью своей учетной записи Active Directory, контроллер домена, который выполняет аутентификацию, должен связаться с глобальным каталогом, чтобы проверить членство в универсальных группах до того, как пользователь будет аутентифицирован.

В одном домене все контроллеры домена должны быть сконфигурированы для хранения копии глобального каталога; однако в среде с несколькими доменами мастер инфраструктуры не должен быть сервером глобального каталога, если все контроллеры домена в домене также не являются серверами глобального каталога. Решение о том, какие контроллеры домена должны быть настроены для хранения копии глобального каталога, зависит от трафика репликации и пропускной способности сети. Многие организации предпочитают делать каждый контроллер домена сервером глобального каталога.

2.2.9. Что такое раздел каталога

Физически, база данных Active Directory хранится в едином файле на жестком диске каждого контроллера домена и в качестве СУБД использует ESE (Extensible Storage Engine). Но логически она разделена на несколько логических разделов, каждый из которых хранит различные типы информации. Разделы Active

Directory называются контекстами именования (NC — naming contexts). Просмотреть их можно с помощью инструментов Ldp.exe или ADSI Edit.

Раздел домена каталога

В разделе домена происходит большая часть действий. Он содержит всю информацию домена о пользователях, группах, компьютерах и контактах: все, что можно просмотреть с помощью инструмента администрирования Active Directory Users And Computers (Пользователи и компьютеры Active Directory).

Раздел домена автоматически реплицируется на все контроллеры в домене. Информация, которая в нем содержится, требуется каждому контроллеру домена для подтверждения подлинности пользователей.

Раздел конфигурации каталога

Раздел конфигурации содержит информацию о конфигурации леса, например, информацию о сайтах, связях сайта и подключениях репликации. В нем хранят информацию многие прикладные программы. Например, приложение Exchange Server помещает свою конфигурационную информацию в раздел конфигурации каталога Active Directory, а не в свою собственную службу каталога.

Раздел конфигурации каталога имеет свои копии повсюду в пределах леса. Каждый контроллер домена содержит перезаписываемую копию раздела конфигурации, и изменения в этот раздел каталога могут быть внесены с любого контроллера домена в организации. Это означает, что конфигурационная информация реплицируется на все контроллеры домена. Когда репликация полностью синхронизирована, каждый контроллер домена в лесу будет иметь одну и ту же конфигурационную информацию.

Раздел схемы каталога

Раздел схемы содержит схему для всего леса. Как вы уже знаете, схема представляет собой набор правил о том, какие типы объектов можно создавать в Active Directory, а также правила для каждого типа объектов. Раздел схемы реплицируется на все контроллеры домена в лесу. Однако только один контроллер домена, хозяин схемы, хранит перезаписываемую копию раздела схемы каталога. Все изменения к схеме осуществляются на контроллере — хозяине схемы, а затем реплицируются на другие контроллеры домена.

Раздел глобального каталога

Раздел глобального каталога GC не является разделом в полном смысле. Он хранится в базе данных подобно другому разделу, но администраторы не могут вводить информацию в него напрямую. Раздел GC предназначен только для чтения на всех GC-серверах, он построен из содержимого баз данных домена. Каждый атрибут в схеме имеет булевое значение с именем isMemberOfPartialAttributeset. Если оно установлено на true (истина), атрибут копируется в каталог GC.

Разделы приложений каталога

Последний тип раздела в службе Active Directory Domain Services — это раздел приложений каталога. Только один тип раздела приложений каталога создается в Active Directory по умолчанию — это раздел, предназначенный для службы

сервера доменной системы имен (DNS — Domain Name System). При установке первой интегрированной (integrated) зоны Active Directory создаются прикладные разделы каталога ForestDnsZones и DomainDnsZones. Раздел приложений каталога может хранить любой тип объекта Active Directory, кроме участников безопасности. Кроме того, разделы приложений каталога создаются для управления процессом репликации данных, и ни один из объектов раздела приложений каталога не может реплицироваться в раздел GC.

Разделы приложений каталога используются для хранения специфической информации, связанной с приложениями. Выгода от их использования состоит в том, что имеется возможность управлять репликацией информации в раздел. Для слишком динамичной информации необходимо управлять репликами, чтобы ограничить количество трафика сети. При создании раздела приложений каталога вы можете указать, какие контроллеры домена будут получать реплику раздела. Контроллеры домена, которые получают реплику раздела приложений, могут находиться в любом домене или сайте леса.

2.2.10. Что такое сайт

Сайт AD представляет собой одну или несколько IP-подсетей, связанных между собой быстродействующими каналами связи (по умолчанию, более 500 кБ/с).

Приложения используют сайты, чтобы найти ближайшую (с точки зрения быстродействия) точку подключения к нужному ресурсу.

Основное применение сайтов — это управление репликацией изменений объектов в доменных службах Active Directory.

Также клиентские компьютеры используют сайты, когда им необходимо связаться с контроллером домена. Он начинается с поиска SRV-записей в DNS. Ответ на запрос DNS включает:

- Список контроллеров домена на том же сайте, что и клиент.
- Список контроллеров домена со следующего ближайшего сайта, который не включает RODC, если на этом же сайте нет контроллеров домена, а параметр групповой политики **`Try Next Closest Site`** включен.
- Случайный список доступных контроллеров домена в домене, если контроллер домена не найден в ближайшем сайте.

Также многие другие приложении ориентированы на работу с Active Directory и используют архитектуру ее сайтов для управления своим поведением. К таким приложениям относятся распределенная файловая система (Distributed File System — DFS) и центр управления конфигурацией системы (System Center Configuration Manager — SCCM) 2012. Поэтому важно полностью определить архитектуру сайтов Active Directory, включая подсети, которая должна отражать архитектуру глобальной сети организации.

Администраторы определяют сайты в AD DS, учитывая, какие участки сети имеют соединения с высокой пропускной способностью. Например, если филиал подключен к основному центру данных ненадежной связью WAN, вы должны определить филиал и центр обработки данных как отдельные сайты.

SRV-записи регистрируются в DNS службой Net Logon, которая выполняется на каждом контроллере домена. Если записи SRV неправильно введены в DNS, вы

можете заставить контроллер домена перерегистрировать эти записи, перезапустив службу Net Logon на этом контроллере домена. Этот процесс перерегистрирует только записи SRV; если вы хотите перерегистрировать информацию о записи хоста (A) в DNS, вы должны выполнить `ipconfig /registerdns` из командной строки, как и для любого другого компьютера.

Хотя процесс входа в систему представляется пользователю как одно событие, он фактически состоит из двух частей:

- Пользователь предоставляет учетные данные, обычно это имя учетной записи пользователя и пароль, которые проверяются в базе данных AD DS. Если имя учетной записи пользователя и пароль совпадают с информацией, которая хранится в базе данных AD DS, пользователь становится аутентифицированным пользователем и выдает TGT контроллером домена. На данный момент пользователь не имеет доступа к каким-либо ресурсам в сети.
- Вторичный процесс в фоновом режиме передает TGT контроллеру домена и запрашивает доступ к локальной машине. Контроллер домена выдает служебный билет пользователю, который затем может взаимодействовать с локальным компьютером. После этого пользователь регистрируется на локальном компьютере.

Когда пользователь пытается впоследствии подключиться к другому компьютеру в сети, вторичный процесс запускается снова, а TGT посылается на ближайший контроллер домена. Когда контроллер домена возвращает билет на обслуживание, пользователь может получить доступ к компьютеру в сети, который генерирует событие входа в систему на этом компьютере.

Примечание. Компьютер, подключенный к домену, также входит в систему AD DS при его запуске, о чем часто забывают. Вы не видите транзакцию, когда компьютер использует имя учетной записи компьютера и пароль для входа в AD DS. После аутентификации компьютер становится членом группы «Прошедшие проверку». Хотя событие входа в компьютер не имеет визуального подтверждения в графическом интерфейсе, оно записывается в журнал событий. Кроме того, если аудит включен, дополнительные события записываются в журнал безопасности в средстве просмотра событий.

Дополнительную информацию к пункту 2.2 вы можете найти на с. 291-325 главы 7 книги «Windows Server 2012 R2. Полное руководство. Том 1» [2].

2.3. Доверие между доменами и лесами

По умолчанию домен является границей доступа к ресурсам в организации. Имея соответствующие разрешения, любой участник безопасности (например, учетная запись пользователя или группы) может обращаться к любому общедоступному ресурсу в том же самом домене. Для получения доступа к ресурсам, которые находятся за пределами домена, используются доверительные отношения службы Active Directory. Доверительные отношения представляют собой опознавательную связь между двумя доменами, с помощью которой участники безопасности могут получать полномочия на доступ к ресурсам, расположенным на другом домене. Есть несколько типов доверительных отношений (рис. 2.7), включающих:

- транзитивные доверительные отношения;
- односторонние доверительные отношения;
- доверительные отношения леса;
- доверительные отношения области.

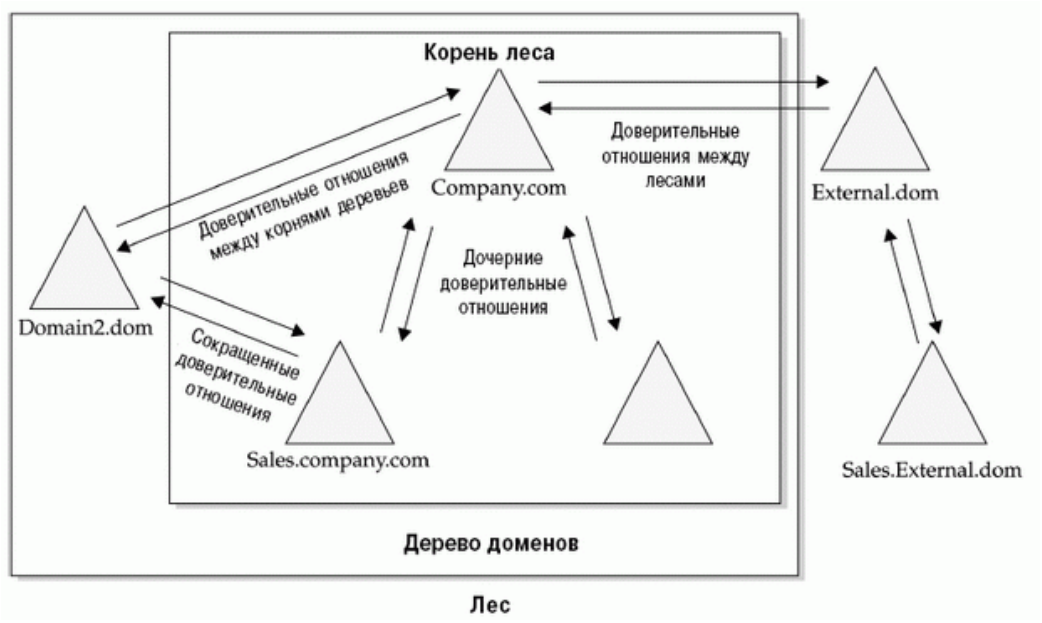

Рис.2.7. Различные типы доверительных отношений

Транзитивные доверительные отношения

Все домены дерева поддерживают транзитивные двухсторонние доверительные отношения с другими доменами в этом дереве. Через эти доверительные отношения любой пользователь из одного домена леса может обращаться к любому ресурсу в любом другом домене этого же леса (при наличии разрешения, естественно).

В пределах леса доверительные отношения устанавливаются или как родительско-дочерние доверительные отношения, или как доверительные отношения корня дерева (tree root).

Все доверительные отношения между доменами леса являются транзитивными. Это означает, что все домены в лесу доверяют друг другу.

Односторонние доверительные отношения

В дополнение к двухсторонним транзитивным доверительным отношениям, которые устанавливаются при создании нового дочернего домена, между доменами леса могут быть созданы односторонние доверительные отношения. Это делается для того, чтобы разрешить доступ к ресурсам между доменами, которые не состоят в прямых доверительных отношениях. Односторонние доверительные отношения также используются для оптимизации производительности работы между доменами, которые связаны транзитивными доверительными отношениями. Эти односторонние доверительные отношения называются укороченными доверительными отношениями (shortcut trusts). Укороченные доверительные отношения нужны в том случае, когда требуется частый доступ к ресурсам между доменами, которые удаленно связаны через дерево домена или лес.

Доверительные отношения леса

Доверительные отношения леса впервые появились в Windows Server 2003. Они представляют собой двухсторонние транзитивные доверительные отношения между двумя отдельными лесами. С помощью доверительных отношений леса участнику безопасности, принадлежащему одному лесу, можно давать доступ к ресурсам в любом домене совершенно другого леса. Кроме того, пользователи могут входить на любой домен обоих лесов, используя одно и то же имя UPN.

Доверительные отношения леса не являются транзитивными по отношению к другим лесам. Например, если Forest1 имеет доверительные отношения леса с Forest2, и Forest2 имеет доверительные отношения леса с Forest3, то Forest1 не имеет автоматических доверительных отношений леса с Forest3.

Доверительные отношения леса делают возможной только идентификацию между лесами, они не обеспечивают другие функциональные возможности. Например, каждый лес будет иметь уникальный каталог GC, схему и раздел конфигурации каталога. Информация между этими двумя лесами не копируется, доверительные отношения леса просто делают возможным назначение доступа к ресурсам между лесами.

В некоторых случаях вам потребуется установить доверительные отношения между всеми доменами одного леса и всеми доменами другого леса. Для этого вы можете устанавливать односторонние, не транзитивные доверительные отношения между индивидуальными доменами в двух отдельных лесах.

Доверительные отношения области

Последний тип доверительных отношений — это доверительные отношения области (RealmTrusts). Они устанавливаются между доменом или лесом Windows Server и не-Windows-реализацией области Kerberos v5. Защита Kerberos основана на открытом стандарте, имеются другие системы сетевой защиты, основанные на протоколе Kerberos. Доверительные отношения области можно создать между любыми Kerberos-областями, которые поддерживают стандарт Kerberos v5. Доверительные отношения области могут быть односторонними или двухсторонними, их можно также сконфигурировать как транзитивные и нетранзитивные.

Выборочная аутентификация

При создании доверительных отношений в диалоговом окне **Outgoing Trust Authentication Level** (Уровень аутентификации исходящего доверительного отношения) можно задать область действия этого доверительного отношения. Если выбрать **Domain-wide authentication** (Аутентификация в рамках домена), это позволит всем пользователям из второго домена выполнять доступ к ресурсам вашего домена. Если же выбрать **Selective Authentication** (Выборочная аутентификация), то потребуется явно указать пользователей из второго домена в свойствах компьютерного объекта AD, которые получат право проходить проверку на этом компьютере (это разрешение называется **Allow to authenticate**).

2.4. Основы служб федерации Active Directory

Windows Server 2012 и Windows Server 2012 R2 включают AD FS. AD FS — это технология, которая упрощает доступ, обеспечивает SSO и облегчает межорганизационное сотрудничество, позволяя отдельным или нескольким организациям обмениваться информацией безопасным образом, не требуя от пользователей активного управления несколькими идентификаторами. AD FS может расширять использование AD RMS, чтобы обеспечить аутентификацию с помощью взаимной организации с использованием AD DS, и может обеспечить упрощенный доступ к облачным службам.

Ниже приведены типичные сценарии развертывания AD FS:

- **Web SSO** (Single Sign-on, единый вход). Это поддерживает сценарии B2B, в которых партнеры в разных организациях могут обмениваться и совместно использовать информацию. Это наиболее известная реализация служб федерации.
- Единый вход для внутренних и веб-приложений на основе утверждений (claim) в одной организации. Вы можете реализовать это для обеспечения доступа SSO к нескольким бизнес-приложениям, для размещения нескольких пользователей, работающих за пределами офиса, или для управления проверкой подлинности при слиянии или поглощении организаций.
- **Федерация с облачными службами**. Это обеспечивает SSO доступ к облачным платформам, таким как Windows Azure, и к онлайн-сервисам, таким как Office 365, который содержит Microsoft Exchange Online, SharePoint Online и другие программные службы. Облачные сервисы становятся все более распространенными, и AD FS позволяет пользователям получать доступ к нескольким платформам с помощью единого набора учетных данных. Эта возможность поддерживается как для облачных сервисов Microsoft, так и для не-Microsoft.

В зависимости от конкретной реализации будут существовать разные требования. Типичные моменты, которые следует учитывать или знать, заключаются в следующем:

- AD FS требует, чтобы хранилище учетных записей, например, AD DS, выполняло аутентификацию пользователей;
- AD FS поддерживает веб-приложения, такие как приложения на основе токенов и заявок, которые работают в системах на базе Windows;
- AD FS позволяет организациям совместно использовать ресурсы, поддерживая отдельные стратегии управления учетными записями, возможность обмениваться контактами и информацией о занятости в Outlook 2010 или новее и возможность использовать службы отчетов Microsoft SQL Server (SSRS) для отправки внешним клиентам;
- AD FS поддерживает следующие типы утверждений, используемых для целей авторизации в приложении:
  - идентификационные утверждения, такие как имя участника-пользователя, адрес электронной почты и общее имя;

▪ групповые утверждения;

▪ пользовательские утверждения.

Типичными бизнес-причинами для внедрения AD FS могут быть:

• предоставление внешним клиентам или клиентам доступа к сайтам SharePoint;

• возможность использования общих портов, таких как 443 (HTTPS);

• возможность обмениваться контактами и информацией о занятости в Outlook 2010 или новее;

• возможность использования SSRS для отчета внешним пользователям.

Для многих организаций SharePoint хранит проектные документы для сотрудников. Если бизнес-партнер хочет безопасно получить доступ к этим документам, AD FS - это решение, которое позволяет партнеру сделать это.

В Windows Server 2012 AD FS также предоставляет некоторые дополнительные функции, такие как:

• интеграция со сценариями динамического контроля доступом;

• улучшенный процесс установки с помощью диспетчера сервера;

• дополнительные инструменты интерфейса командной строки Windows PowerShell;

• Workplace Join, появившееся в Windows Server 2012 R2;

• Многофакторная аутентификация, появившаяся в Windows Server 2012 R2;

• Многофакторное управление доступом, которое появилось к Windows Server 2012 R2.

Ключевые компоненты и термины AD FS

• **Партнер учетной записи (account partner).** Партнер учетной записи — это организация, выдающая маркеры безопасности, которые используются учетными записями пользователей для доступа к ресурсам, находящимися в среде партнера ресурса. Партнер учетной записи отвечает за хранение и аутентификацию учетных записей пользователей, создание утверждения пользователя и упаковку утверждений в маркеры безопасности, применяемые партнером ресурса во время аутентификации для своих приложений и служб. Партнеры учетных записей работают совместно в рамках доверительного отношения федерации, чтобы предоставить возможность доступа SSO к нужным ресурсам.

• **База данных конфигурации AD FS (AD FS configuration database).** База данных конфигурации AD FS используется для хранения всех конфигурационных данных, которые представляют одиночный экземпляр AD FS или службу федерации. База данных конфигурации AD FS предусмотрена для каждой отдельной фермы серверов федерации. Службы AD FS предоставляют возможность хранения данных во внутренней базе данных Windows (Windows Intemal Database — WID) или в базе данных Microsoft SQL Server. Имейте в виду, что в одном экземпляре AD FS можно запускать либо WID, либо SQL, но не то и другое вместе. Вы должны обдумать, какая топология базы данных будет лучше работать в вашем развертывании. SQL отличается высокой масштабируемостью,

тогда как WID ограничивается пятью серверами WID на ферму серверов федерации.

• **Хранилище атрибутов (attribute store).** Хранилище атрибутов лучше всего определить как базу данных или службу каталогов, которая содержит атрибуты, описывающие клиентов. Эти атрибуты можно применять для выдачи утверждений от клиентов. Службы AD FS поддерживают несколько разных возможностей для хранилища атрибутов. В качестве хранилища атрибутов главным образом используются Active Directory и SQL Server. Можно построить и работать со специальными хранилищами атрибутов, но при этом требуется дополнительное конфигурирование вроде создания специальной строки подключения.

• **Утверждение (claim).** Утверждение — это заявление, которое один субъект делает о себе или о другом объекте. Например, заявление может касаться имени, адреса электронной почты, группы, полномочия или возможности. Утверждения выдаются и потребляются между партнерами учетных записей и ресурсов для предоставления учетным записям пользователей доступа SSO, обеспечивая свободное перемещение между организациями или службами. Такие утверждения применяются для целей входной аутентификации и авторизации в приложении, совместно используемом поставщиком и потребителем. Утверждения идентифицируют для учетной записи пользователя группу атрибутов, таких как имя или роль этого пользователя. Партнер учетной записи упаковывает утверждения в маркеры безопасности и затем отправляет эти маркеры партнеру ресурса, который запрашивает аутентификацию пользователя в приложениях и службах, размещенных партнером ресурса.

• **Метаданные федерации (federation metadata).** Метаданные федерации можно охарактеризовать как формат данных, который используется для передачи данных конфигурации между проверяющей стороной и поставщиком утверждений. Метаданные федерации могут применяться для создания доверительного отношения между поставщиком утверждений и проверяющей стороной. Доверительные отношения федерации требуются учетным записям пользователей для безопасного перемещения между организациями, приложениями и службами.

• **Сервер федерации (federation server).** Сервер федерации — это сервер, который был построен и сконфигурирован для службы роли AD FS. Сервер федерации выступает как часть службы федерации, которая используется для перенаправления запросов аутентификации и размещения службы маркеров безопасности для учетных записей пользователей между доверенными организациями и службами. Работа сервера федерации заключается в создании и выдаче маркеров безопасности, применяемых учетными записям и пользователей для аутентификации внутри служб федерации.

• **Ферма серверов федерации (federation server farm).** Когда вы кластеризуете множество серверов федерации, чтобы они действовали как единственная служба федерации в одной сети с балансировкой нагрузки, такой кластер серверов называется фермой серверов федерации. Эта ферма может состоять из многих устройств, таких как серверы федерации, прокси и веб-агенты AD FS.

• **Прокси-сервер федерации (federation server proxy).** Прокси-сервер федерации — это сервер федерации, который вынесен за пределы корпоративной сети, чтобы предоставлять промежуточную службу прокси между открыто недоступной корпоративной сетью, защищенной брандмауэром, и клиентами из Интернета. Для того чтобы разрешить удаленный доступ к облачной службе, например, со смартфона, домашнего компьютера либо Интернет-киоска, понадобится развернуть прокси-сервер федерации, который будет действовать в качестве посредника между Интернетом и корпоративной сетью.

• **Балансировщик сетевой нагрузки (network load balancer — NLB).** При наличии нескольких серверов федерации, функционирующих вместе внутри фермы таких серверов, существует требование AD FS по балансировке нагрузки между серверами с использованием какого-нибудь вида балансировщика сетевой нагрузки. Балансировщиком NLB может быть фрагмент программного обеспечения, такой как встроенная в Windows Server функциональность NLB. Добавление этого очень важного фрагмента дает огромные преимущества. В дополнение к балансировке нагрузки в среде AD FS наличие множества серверов федерации с балансировщиком NLB между ними обеспечит для инфраструктуры AD FS устойчивость к отказам и высокую готовность.

• **Проверяющая сторона (relying party).** Проверяющая сторона — это любая организация, приложение или служба, потребляющая утверждения, которые выдаются партнером учетной записи. Хороши м примером проверяющей стороны является партнерская организация или облачная служба, подобная Office 365.

• **Доверительное отношение для проверяющей стороны (relying party trust).** Доверительное отношение для проверяющей сторон ы создается между двумя службами федерации. Будучи очень похожим на доверительное отношение леса Active Directory, доверительное отношение для проверяющей стороны создает безопасный туннель, который предоставляет учетным записям пользователей возможность защищенным образом проходить аутентификацию в приложениях и службах между сущностями. Обратите внимание, что доверительные отношения леса Active Directory и доверительные отношения федерации работают независимо друг от друга.

• **Партнер ресурса (resource partner).** Партнер ресурса — это другая организационная часть доверительного отношения федерации с партнером учетной записи. Работа партнера ресурса заключается в размещении приложений и служб, к которым пользователи партнера учетной записи хотят получать доступ с применением технологи и SSO. Партнер ресурса просматривает маркеры безопасности, отправленные партнером учетной записи, и решает, предоставлять ли учетной записи пользователя доступ к свои м приложениям и службам.

Сертификаты AD FS

Сертификаты являются фундаментальными строительными блоками, позволяющими AD FS функционировать должным образом. Каждый клиент, который нуждается в возможностях SSO, должен иметь и быть способным

принимать эти сертификаты безопасности. Сертификаты создаются и выдаются IIS и AD FS, чтобы поддерживать доверительные отношения. Эти сертификаты можно использовать для защищенного взаимодействия со всеми объектами внутри среды AD FS. Без таких доверенных сертификатов реализовать AD FS в качестве решения SSO не удастся. Ниже перечислены требования к серверу федерации.

• **Сертификат для подписи маркера (token-signing certificate).** Сертификат для подписи маркера — это защищенный сертификат X.509, который используется сервером федерации для цифровой подписи маркеров безопасности, создаваемых и распространяемых по инфраструктуре AD FS. Вы обязан ы применять сертификат для подписи маркера на сервере федерации для AD FS, чтобы данный сервер нормально функционировал. Именно этот сертификат из обсуждаемых здесь четырех службы AD FS фактически используют для подписания маркеров. Сертификатов для подписи маркера может быть несколько. На самом деле рекомендуется и меть их множество, причем с повторяющимся циклом, чтобы в случае, если активный сертификат устаревает или подвергается компрометации, в запасе окажется резервный сертификат.

• **Сертификат для шифрования маркера (token-decryption certificate).** Сертификат для шифрования маркера применяется вместе с сертификатом для подписи маркера. Когда партнер учетной записи выдает маркер безопасности для учетной записи пользователя, чтобы он мог получить доступ к приложению или службе на стороне партнера ресурса, сервер федерации в среде партнера ресурса должен иметь возможность расшифровать этот маркер безопасности и удостовериться в том, что он не был изменен или подделан.

• **Сертификат уровня защищенных сокетов (Secure Sockets Layer certificate).** Сертификат Secure Sockets Layer (SSL) предназначен для использования с трафиком между прокси-серверами федерации и клиентами из Интернета. Для того чтобы веб-служба или клиент безопасно взаимодействовали с прокси-сервером федерации, клиент должен иметь возможность принятия сертификата SSL, выданного прокси-сервером.

• **Сертификат для взаимодействия со службами (service communication certificate).** Сертификат для взаимодействия со службами предлагает ту же самую функциональность, что и сертификат SSL, но с дополнительным преимуществом. Дополнительно к защите трафика между веб-клиентами и прокси-серверами федерации этот сертификат защищает коммуникации между клиентами и приложениями Windows Communication Foundation (WCF). Поскольку на базе инфраструктуры WCF построено довольно много веб-служб и клиентских приложений для веб-служб, по умолчанию этот сертификат применяется сервером федерации для сертификата SSL в lIS.

2.5. Обзор FIM 2010 R2

Управление идентификацией может быть затруднено для организаций, которые имеют несколько реализованных служб каталогов и пользователей со учетными записями в нескольких каталогах. Пользователям необходимо запомнить несколько наборов учетных данных, а администраторы тратят дополнительное время на управление учетными записями пользователей в этих системах.

Помимо централизованной системы идентификации, компаниям может потребоваться более безопасная аутентификация. Общим способом повышения подлинности является использование смарт-карт, но для их внедрения у вас должно быть надежное решение для управления смарт-картами.

Продукт Microsoft FIM решает эти проблемы. FIM напрямую связан с некоторыми ролями AIP, такими, как AD DS для аутентификации и AD CS для цифровых сертификатов и смарт-карт. В этом курсе приводится лишь обзор основных функциональных возможностей FIM.

Microsoft выпустила FIM для решения проблем, возникающих из-за наличия нескольких идентификаторов в разных системах внутри одной компании и предоставления решения для управления смарт-картами.

FIM имеет два основных компонента:

- управление идентификацией;
- протокол управления сертификатами

Вы можете установить эти два компонента независимо друг от друга, но в некоторых сценариях, таких как управление жизненным циклом идентификации, они могут работать вместе.

Компонент управления идентификацией FIM обращается к нескольким проблемам управления идентификационными данными, устанавливая общую идентификацию внутри одной организации. Он обеспечивает полное управление жизненным циклом идентификационных данных с момента создания учетной записи до момента ее удаления. FIM упрощает управление жизненным циклом идентификации посредством автоматических рабочих процессов и бизнес-правил и предлагает интеграцию с гетерогенными или не-Microsoft-платформами.

FIM может автоматизировать идентификацию и создание групп на основе бизнес-политики посредством рабочих процессов. Он также предоставляет функциональный и простой в использовании инструмент самообслуживания для конечных пользователей, который восстанавливает свои пароли.

Для компаний, которые хотят внедрить или уже используют аутентификацию по смарт-картам, компонент управления сертификатами FIM обеспечивает надежное управление смарт-картами в дополнение к сертификатам в целом.

FIM централизованно управляет процессом предоставления смарт-карт, что снижает затраты, обычно связанные с развертыванием многофакторной аутентификации. Кроме того, он полностью управляет управлением смарт-картами и всеми задачами, связанными с управлением смарт-картами, такими как аннулирование, приостановка, восстановление, обновление, копирование и замена смарт-карт.

Организации, у которых есть несколько каталогов идентификаторов, должны гарантировать, что все эти каталоги содержат одну и ту же информацию. Если информация изменяется в одном каталоге, она должна синхронизироваться в других каталогах, чтобы общий идентификатор оставался согласованным. Одной из основных особенностей FIM является синхронизация идентичности. Основная цель этой технологии — поддерживать синхронизацию информации по нескольким системам. Например, если компания имеет как AD DS, так и сторонний каталог, любое изменение атрибутов пользователя в AD DS, такое как имя, пароль или другая информация, может синхронизироваться с сторонним каталогом или наоборот. Точно так же, когда новый пользователь создается в AD DS, FIM может автоматически вводить новую учетную запись пользователя в сторонний каталог, а затем поддерживать учетные записи как общую идентификационную информацию.

FIM предоставляет несколько методов и технологий для управления идентификацией. Наиболее важными являются предоставление пользователей, управление пользователями и управление группами.

Чтобы установить синхронизацию каталогов, задействовано несколько компонентов FIM, в том числе:

- **Подключенный источник данных.** Этот компонент обеспечивает расширяемость для разработки дополнительных разъемов. В большинстве обычных хранилищ идентификаторов есть встроенные разъемы. Связанный источник данных предоставляет данные FIM с помощью агента управления.

- **Metaverse (метабаза).** Этот компонент представляет собой хранилище данных, которое содержит агрегированную идентификационную информацию из нескольких подключенных источников данных. Metaverse обеспечивает единое глобальное интегрированное представление данных идентификации, которое выполняется в пространствах соединителей. Агенты управления выталкивают и извлекают информацию из метаподразделения.

- **Коннектор**. Этот компонент является местоположением, в котором хранится информация из разных источников, например, база данных HR и система электронной почты. Он помогает поддерживать и синхронизировать данные в нескольких каталогах или хранилищах данных. Пространство коннектора может определять изменение в подключенном источнике данных. Это помогает сменить входящие изменения. Коннекторное пространство принимает данные от агента управления.

- **Агент управления.** Этот компонент связывает определенные связанные источники данных с FIM. Агент управления отвечает за перемещение данных между подключенным источником данных и FIM.

> *Примечание: Последняя версия этого продукта называется Microsoft Identity Manager 2016, доступен в составе подписки Azure AD Premium P1 и P2.*

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная:

1. Урбанович, П. П. Компьютерные сети: учеб. пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. — Минск: БГТУ, 2011. — 399 с. — 119 экз.

2. Windows Server 2012 R2. Полное руководство. Том 1: установка и конфигурирование сервера, сети, DNS, Active Directory и общего доступа к данным и принтерам. / М. Минаси, К. Грин, К.Бус, Р. Батлер и др. : — М.: Вильямс, 2015. — 960 с. — Электр. версия

3. Windows Server 2012 R2. Полное руководство. Том 2: дистанционное администрирование, установка среды с несколькими доменами, виртуализация, мониторинг и обслуживание сервера. / М. Минаси, К. Грин, К.Бус, Р. Батлер и др.: — М.: Вильямс, 2015. — 960 с. — Электр. версия

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб.: Питер, 2016. – 992 с. — Электр. версия

5. Олейник, П. П. Корпоративные информационные системы: Учебник для вузов. Стандарт третьего поколения. – СПб.: Питер, 2012. – 176 с.: ил. — Электр. версия

6. Станек, У. Р. Windows PowerShell 2.0. Справочник администратора / У. Р. Станек. — М.: Издательство «Русская редакция»; СПб.: БХВ-Петербург, 2010. — 416 с. — Электр. версия

Дополнительная:

7. Линн, С. Администрирование Windows Server 2012 / С. Линн. – СПб.: Питер, 2014. – 304 с. — 1 экз.