УДК 004

АНАЛИЗ ВОЗМОЖНОСТЕЙ ACTIVE DIRECTORY ПРИ ПОСТРОЕНИИ СЕТИ С КЛИЕНТ-СЕРВЕРНОЙ АРХИТЕКТУРОЙ

Кряжева Е. В.,

к.псих.н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Мишкина Е.М.,

магистрант,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация.

В статье рассмотрена проблема проектирования и дальнейшей реализации сети организации с клиент-серверной архитектурой. Описывается система Active Directory, которая является реализацией службы каталогов и работает на операционной системе (ОС) Windows Server. Представлена логическая структура Active Directory и проанализированы ее компоненты. Рассмотрена физическая структура Active Directory и понятие сайта Windows Server. В конце представлены выводы по проделанной работе.

Ключевые слова: Active Directory, каталог, домен, Windows Server, сайт, лес, дерево, физическая структура, контроллер домена.

ANALYZING THE CAPABILITIES OF ACTIVE DIRECTORY WHEN BUILDING A NETWORK WITH A CLIENT-SERVER ARCHITECTURE

Kryazheva E. V.,

Candidate of Psychological Sciences, Associate Professor,

Kaluga State University named after K.E. Tsiolkovsky,

Kaluga, Russia

Mishkina E.M.,
Undergraduate,
Kaluga State University named after K.E. Tsiolkovsky,
Kaluga, Russia

Annotation.
The article discusses the problem of designing and further implementing an organization's network with a client-server architecture. Describes Active Directory, which is an implementation of a directory service and runs on the Windows Server operating system (OS). The logical structure of Active Directory is presented and its components are analyzed. Discusses the physical structure of Active Directory and the concept of a Windows Server site. At the end, conclusions on the work done are presented.
Keywords: Active Directory, directory, domain, Windows Server, site, forest, tree, physical structure, domain controller.

Каждая современная компания нуждается в безопасной организации работы всей её IT-инфраструктуры. Эту проблему решает система Active Directory. Она помогает объединить все ресурсы предприятия, такие как пользователи, компьютеры, принтеры, группы пользователей, и организовать их централизованное управление. Также в возможности Active Directory входит отслеживание и журналирование любого процесса, проходящего на рабочей машине, контроль доступа для пользователей домена организации, удаленная настройка оборудования и многое другое [10, 13].

Active Directory (AD) – это реализация службы каталогов, которую разработала корпорация Microsoft. Работает на операционных системах семейства Windows Server. Сервис позволяет представить инфраструктуру организации как набор управляемых объектов, что является его главной особенностью.

Каталог – это определенная структура, в которой хранятся сведения о всех объектах в сети. Это понятие является ключевым в Active Directory, поскольку с помощью него организовывается доступ авторизованным пользователям к информации в этой сети. Сам каталог реализуется через физическую структуру, состоящую из базы данных, которая хранится на всех контроллерах леса доменов.

Все управление за сервисами и каталогами в Windows Server организовывается при помощи системы System Center Configuration Manager [6]. Сами доменные службы хранятся в службе Active Directory. Именно она предоставляет такие виды функций в локальной сети, как управление группами и пользователями, организация их аутентификации, получение доступа к ресурсам организации и так далее. Администрирование на основе групповых политик облегчает управление сетью, организовывает ее безопасность – гораздо удобнее исправлять ошибки и инциденты в сети удаленно и на одной машине, чем локально выполнять такие же задачи на каждом оборудовании в разных точках большой инфраструктуры [3]. Службы каталогов Active Directory соответствуют стандарту LDAP.

LDAP – (Lightweight Directory Access Protocol) стандартный протокол прикладного уровня, организовывающий быстрый доступ к каталогам, а также позволяет производить такие операции, как добавление, удаление и изменения, аутентификации, поиска, сравнения записей [8].

Администраторы используют Active Directory для хранения и организации объектов в сети (таких как пользователи, компьютеры, устройства и т.д.) в защищенную иерархическую структуру, известную как логическая структура. Ее основой является такие понятия, как лес и домен. Сама логическая структура Active Directory представляет собой организацию всех пользователей, компьютеров и других физических ресурсов [9]. В нее входят следующие определения:

Лес – это группа доменов (он может быть один), связанных двусторонними транзитивными доверительными отношениями. Их объединяет общая схема и конфигурация каталогов, а также общий глобальный каталог. Леса содержат домены. Если лесов в организации несколько, существует возможность построить доверительные отношения между ними, что позволяет получить доступ к объектам из «дружественного» леса (forest trust).

Домен – группа объектов, которые могут совместно использовать одинаковую базу данных каталога. Каждое имя домена должно быть уникальным.

Объект – ресурс домена. Он хранит в себе набор атрибутов. Объекты, описывающие одинаковые атрибуты, объединяются в классы. Каждый объект, защищается списками управления доступом (ACL).

Дерево – иерархия доменов. Домен, который был создан первым, является корневым. Такой домен уже образует дерево. Последующие домены называются дочерними и образуют общую схему и пространство имен [1].

Организационные единицы (OU) – предоставляют возможность объединения различных групп объектов, например, пользователей, для организации удобного администрирования сети.

Домены могут быть структурированы в виде леса, чтобы обеспечить автономность данных и сервисов (но не изоляцию) и оптимизировать репликацию в заданной области. Так как логическая структура позволяет контролировать доступ к данным, значит существует возможность использовать логическую структуру для разделения данных таким образом, чтобы можно было контролировать доступ к ним, управляя доступом к различным разделам [2].

Физическая структура состоит всего из двух компонентов: сайты и контроллеры домена.

Контроллер домена – сервер, работающий на ОС Windows Server, который хранит параметры учетных записей доменных пользователей каталога Active Directory, параметры политик для домена, а также параметры безопасности [4].

Контроллеры домена хранят полную копию раздела домена, которым они управляют. При этом, в домене может существовать любое количество контроллеров домена, что может положительно сказаться на его отказоустойчивости (при организации настройки репликации).

Формируя физическую структуру сети, администратор должен самостоятельно создать новые сайты и задать для них границы, создав объекты, ассоциированные с имеющимися подсетями. В процессе создания нового контроллера, на основании выделенного ему IP-адреса, служба каталога автоматически отнесет его к соответствующему сайту.

Для контроллера домена существует возможность добавить роль, после которой данный контроллер домена будет являться сервером глобального каталога. Этот сервер позволяет сервисам и пользователям находить объекты в дереве доменов, а также проходить аутентификацию в любой части леса. Active Directory позволяет назначить нескольким контроллерам домена роль сервера глобального каталога.

В физической структуре Active Directory существует понятие сайта. Сайтом Windows Server является группа из одного или нескольких контроллеров домена, связанных сетевым соединением скоростью от 1 Мбит/с и находящихся в одной IP-подсети. Поэтому границы сайта принято приравнивать к границам локальной сети.

Сайты важны для распределения трафика репликации в базу данных Active Directory. В зависимости от сайта, в котором находится контроллер домена, информация об изменении может передаваться различно. Так, если контроллеры домена находятся в отличных сайтах, трафик будет передан в сжатом виде и по определенному расписанию. Внутри сайта же репликация производится без вышеописанных ограничений, автоматически.

Организация репликации необходима для работы всех контроллеров домена в сети Active Directory. Репликация между двумя контроллерами домена и выполняется на основе уведомлений, а именно при появлении изменений на

одном контроллере, отправляется уведомление другим контроллерам в приделах сайта. Далее партнеры по репликации производят запрос на изменения, после запускается процесс репликации. Если репликация осуществляется внутри сайта, то изменения передаются по мере необходимости, так как имеется скоростное соединение между контроллерами домена. Такой вид репликации называется внутрисайтовой (intrasite replication).

Существует также возможность реплицировать информацию по менее скоростным каналам. Для этого необходимо создать дополнительные сайты и установить связь между ними. Вид передачи трафика по такому принципу имеет название межсайтовой репликации (intersite replication).

В Active Directory процесс поиска домен-контроллера происходит при помощи DNS. DNS – система доменных имен, необходимая для соотнесения IP-адресов объектов в сети и символьных имен в распределенной базе данных, которые более удобны для восприятия [5]. Эта служба состоит из базы имен, причем каждое имя является уникальным.

В момент аутентификации пользователя клиент инициирует DNS-локатор, задействуя службу NetLogon и сервиса RPC (Remote Procedure Call). В качестве исходных данных в NetLogon запросе передаются несколько параметров: имя компьютера, название домена, сайт. Далее в ответ на запрос DNS сервер отправляет запрошенный список серверов, который рассортирован по приоритету и весу. Клиент, приняв этот ответ, посылает следующий запрос – CLDAP (Lightweight Directory Access Protocol), по каждому из указанных сервером адресу. Процесс разрешения имен происходит, когда сервис или пользователь ищет устройство по его имени (по имени хоста). Служба разрешения имен ищет соответствующий адрес в базе данных или других источниках информации. После этого IP-маршрутизация определяет путь, по которому данные должны быть отправлены к нужному узлу в сети.

Для разрешения имен используются два вида файлов – HOSTS и LMHOSTS, а также службы DNS и WINS (Windows Internet Naming Service).

Служба WINS с помощью базы данных сверяет IP-адреса и NetBIOS-имена. В современных конфигурациях данная служба не используется и условно считается устаревшей. Все DNS – домены организованы в иерархическую структуру: от корневого домена следуют домены верхнего уровня, далее домены второго уровня, третьего, а в конце располагаются имена хостов.

Корневой домен имеет имя длинной в один символ – точка.

Домены верхнего уровня регулируются организацией IAB (Internet Activities Board). Примеры имен доменов верхнего уровня: com (для коммерческих организаций), edu (образовательные учреждения), net (сетевые сервисы, провайдеры), ru (двухбуквенный код России) и т.д. [12].

Домены второго уровня регистрируются различными организациями. После этапа регистрации имени передаются и права на управление пространством имен (namespace) в рамках зарегистрированного домена. Такое пространство имен организация в дальнейшем может поделить на поддомены (домены третьего уровня). При редактировании пространства имен важно, чтобы все схожие компоненты были уникально идентифицированы. FQDN (fully qualified domain name) – полное доменное имя хоста в иерархии DNS. Оно отражает местоположение узла в домене.

Пространство имен разделяется не только на домены, но и на определенные зоны. Эти зоны представлены в системе DNS в виде баз данных с записями ресурсов (resource records), в которых находятся сопоставления IP-адреса и службы (хоста) [8]. Они хранятся как минимум на одном сервере имен в конкретной зоне. Для повышения отказоустойчивости и балансировки нагрузки часто используется несколько серверов имен в одной зоне. Это позволяет обеспечить непрерывность работы сервисов DNS и эффективное распределение запросов между серверами.

В Windows Server существует несколько видов зон:

1) Интегрированная зона Active Directory (Active Directory Integrated Zone).

2) Основная зона (Primary Zone).
3) Дополнительная (вторичная) зона (Secondary Zone).
4) Зона обратного просмотра (Reverse Lookup Zone).

DNS работает по умолчанию по протоколу UDP (User Datagram Protocol), а именно по 53 порту [7, 11]. Однако, если размер посылаемого пакета превысит 512 байт, что является пределом для UDP отклика, клиент получит обрезанный отклик и заново пошлет такой же запрос, но уже по протоколу TCP (Transmission Control Protocol). Этот протокол сможет гарантированно передать больший объем данных до адресата. Все доступные контроллеры домена отвечают на пришедший от клиента запрос, сообщая тем самым о своей работоспособности. В конце, когда обнаружился DC, устройство клиента устанавливает соединение с ним по протоколу LDAP, но уже для получения доступа к AD. Важным фактом также является, что служба NetLogon сохраняет в кэш информации о местонахождении контроллера домена клиенту на устройство, чтобы при каждом моменте аутентификации не запрашивать по DNS данные у контроллеров домена.

Таким образом, Active Directory является удобным инструментом для перехода информационной системы организации с одноранговой на клиент-серверную архитектуру на основе служб активного каталога Active Directory.

Использование Active Directory предоставляет возможность централизованного управления сетью, улучшает ее безопасность за счет возможности использования аутенфикации и авторизации пользователей, удобен в управлении. К недостаткам Active Directory можно отнести то, что его использование возможно только для системы на Windows. Если необходимо управлять компьютерами Linux или Mac, им потребуются клиенты LDAP (облегченный протокол доступа к каталогам) вместо активного каталога.

Библиографический список:

1. Active Directory Schema Technical Reference // Microsoft. Learn : [сайт]. — URL https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-server-2003/cc759402(v=ws.10) (дата обращения: 16.12.2023).

2. Active Directory Structure and Storage Technologies // Microsoft. Learn : [сайт]. — URL https://learn.microsoft.com/ru-ru/previous-versions/windows/it-pro/windows-server-2003/cc759186(v=ws.10) (дата обращения: 12.12.2023).

3. Айвенс, К. Администрирование Microsoft Windows Server 2003 : учебное пособие / К. Айвенс. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 486 с. — ISBN 978-5-4497-0853-3. // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101986.html (дата обращения: 11.12.2023).

4. Безопасность в Windows Server 2008 // КОМПЬЮТЕР.Пресс: [сайт]. — URL: https://www.securitylab.ru/contest/393073.php (дата обращения: 16.12.2023).

5. Берлин, А. Н. Основные протоколы интернет : учебное пособие / А. Н. Берлин. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 601 с. — ISBN 978-5-4497-0337-8. // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/89452.html (дата обращения: 20.12.2023).

6. Власов, Ю. В. Администрирование сетей на платформе MS Windows Server : учебное пособие / Ю. В. Власов, Т. И. Рицкова. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 622 с. — ISBN 978-5-4497-0649-2. // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/97536.html (дата обращения: 08.12.2023).

7. Гаврилов, А.В. Системы управления телекоммуникационных систем информационно-вычислительных сетей. Стандарты, модели, протоколы : учебное пособие / А.В. Гаврилов, Е.Л. Кон, В.И. Фрейман. — Пермь : Пермский государственный технический университет, 2005. — 102 с. — ISBN 5-88151-492-0. // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/105412.html (дата обращения: 11.01.2024).

8. Коробко, И. Active Directory–теория построения / И. Коробко // Системный администратор, 2004. – №. 1. – С. 90-94.

9. Ларина, Т.Б. Администрирование сетей. Логическая организация и конфигурирование : учебное пособие / Т.Б. Ларина — Москва : Российский университет транспорта (МИИТ), 2017. — 172 с. // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/116019.html (дата обращения: 12.12.2023).

10. Мониторинг событий безопасности в Windows Server 2008 // SecurityLab.ru by Positive Technologies : [сайт]. — URL https://www.securitylab.ru/contest/393073.php (дата обращения: 05.12.2023).

11. Олифер, В.Г. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. — СПб : Питер, 2001. — 672 с. — ISBN 5-8046-0133-4.

12. Рожкова, М. А. Доменные споры: избранные аспекты / М. А. Рожкова, Д. В. Афанасьев // Право в сфере Интернета, 2018. – С. 224-245.

13. Чижиков, Д. В. Методология внедрения Microsoft Active Directory : учебное пособие / Д. В. Чижиков. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2024. — 199 с. — ISBN 978-5-4497-2409-0. // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/133947.html (дата обращения: 05.12.2023).

Оригинальность 80%