ГБПОУ Республики Марий Эл «МРМТ»

Допущен к защите
Зам. Директора по УМР
_____И.Ю.Бурханова
«___»_____2022 г.

ДИПЛОМНАЯ РАБОТА

ПОСТРОЕНИЕ ДОМЕНА MICROSOFT НА CORE - СЕРВЕРАХ

Рецензент
_____ В.С. Целищев

Разработчик
Студент группы КС-41
_____ Д.И. Кузьмин

Нормоконтроль
_____Е.В. Матвеева

Руководитель
_____А.М. Глозштейн

Оценка Экзаменационной комиссии по защите_____

Председатель ГЭК_____/В.Г. Тужаров /

Йошкар-Ола 2022

Государственное бюджетное профессиональное образовательное учреждение
Республики Марий Эл «Марийский радиомеханический техникум»

«УТВЕРЖДАЮ»
Зам. директора по УМР
_____ Бурханова И.Ю.
«__» _____2022 г.

ЗАДАНИЕ НА ВЫПОЛНЕНИЕ ДИПЛОМНОЙ РАБОТЫ

Студента группы *КС-41* специальности *09.02.06*

Сетевое и системное администрирование
(код, наименование специальности)
Кузьмин Дмитрий Иванович

(Фамилия, Имя, Отчество)

Тема дипломной работы *Построение домена Microsoft на Core - серверах*

Исходные данные _____

Содержание дипломной работы:
Введение _____

Теоретический раздел *Рассмотрение Windows Server Core и его возможностей*
Аналитический раздел *Анализ Active Directory и его построения*

Исследовательский раздел *Установка AD, настройка протоколов и служб*

Заключение _____

Список использованных источников _____

Дата выдачи задания «____» _____ 2022 г.
Дата сдачи законченной работы «____»_____ 2022 г

_____
Руководитель дипломной работы (подпись)
Преподаватель МРМТ Глозштейн Александр Моисеевич

(должность, место работы, ФИО)

Задание рассмотрено на заседании цикловой комиссии _____
_____протокол № ___ от «___» _____ 20___г.

Председатель ЦК _____ (Муравьева Е.А.)

(подпись, ФИО)

Задание принял к исполнению _____(Кузьмин Д.И.)

(дата, подпись, ФИО)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Структура доменов (Active Directory) является неотъемлемой частью сети компаний, организаций и учебных заведений. Актуальность исследования построения домена на Windows Server Core определяется безопасностью сервера контролера домена и автоматизации этого процесса.

В ходе дипломной работы будет изучено построение домена Microsoft на Core – серверах. Объектом исследования в большей степени будет оболочка Windows PowerShell, поскольку при помощи нее устанавливается и настраивается Active Directory, как и необходимые службы и протоколы.

Поскольку целью работы является не только построение, а также автоматизация и оптимизация построения домена Microsoft, в ходе работы будут изучены командленты и сценарии PowerShell, что позволит сократить время компаниям, организациям и учебным предприятиям при создании или настройке домена Microsoft.

Построение домена на Microsoft Core – серверах является наименее ресурсоемким процессом, быстрым и безопасным. Поэтому большинство продвинутых системных администраторов выбирают именно этот способ создания доменной зоны.

В дипломной работе будет создана небольшая сеть, эмулированная в программе VMware, внутри которой будет создан домен Microsoft на сервере Windows Server Standard (Core) 2019, где будут рассмотрены установка и настройка: Active Directory, Sconfig, сервера DNS, сервера DHCP, групповых политик.

1 Теоретический раздел

1.1 Windows Server Core

Server Core - один из множества вариантов установки для Windows Server. Такой вариант ОС Windows Server содержит меньше компонентов. Поскольку такие компоненты, как встроенный веб-браузер, есть возможность установки без графического интерфейса, Server Core GUI менее уязвим для вредоносных программ, чем вариант установки Server with Desktop Experience.

Поскольку для него не требуются все компоненты версии, включающей графический интерфейс, он требует меньше ресурсов. Server Core можно установить с установочного носителя Windows Server 2019 или развернуть различными способами из файла install.wim, расположенного на установочном носителе.

После завершения установки Server Core в системе и входа в систему в первый раз вы сможете немного неожиданно. Основное различие между вариантами установки «сервер с возможностями рабочего стола» и «ядро сервера» состоит в том, что Server Core не включает следующие пакеты оболочки GUI:

- Microsoft-Windows-Server-Shell-Package;
- Microsoft-Windows-Server-Gui-руководства-Package;
- Microsoft-Windows-Server-гип-RSAT-Package;
- Microsoft-Windows-Кортана-PAL-Desktop-Package.

Иными словами, в архитектуре Server Core нет рабочего стола. При поддержке функций, необходимых для поддержки традиционных бизнес-приложений и рабочих нагрузок на основе ролей, серверное ядро не имеет традиционного интерфейса рабочего стола. вместо этого серверное ядро предназначено для удаленного управления с помощью командной строки,

PowerShell или средства графического пользовательского интерфейса (например, RSAT или Windows центра администрирования).

В дополнение к отсутствию пользовательского интерфейса ядро сервера также отличается от сервера с возможностями рабочего стола следующим образом.

– Server Core не имеет специальных средств;

– отсутствует OOBE (встроенное взаимодействие) для настройки ядра сервера;

– отсутствует поддержка звука [3, 7, 11].

Различия вариантов установки предоставлены на таблице 1.

Таблица 1 – Возможности версий Windows Server Core и Windows Server with Desktop Experience

Программа	Windows Server Core	Windows Server with Desktop Experience
1	2	3
Командная строка	доступен	доступен
Windows PowerShell и Microsoft .NET	доступен	доступен
Perfmon.exe	недоступно	доступен
WinDbg (графический пользовательский интерфейс)	Поддерживается	Поддерживается
Resmon.exe	недоступно	доступен
Regedit	доступен	доступен
Fsutil.exe	доступен	доступен
Disksnapshot.exe	недоступно	доступен
Diskpart.exe	доступен	доступен
Diskmgmt. msc	недоступно	доступен
Devmgmt. msc	недоступно	доступен
Диспетчер серверов	недоступно	доступен
Mmc.exe	недоступно	доступен
Файл eventvwr	недоступно	доступен
Wevtutil (запросы событий)	доступен	доступен
Services.msc	недоступно	доступен
Панель управления	недоступно	доступен

Продолжение таблицы 1

1	2	3
Центр обновления Windows (графический пользовательский интерфейс)	недоступно	доступен
Проводник	недоступно	доступен
Панель задач	недоступно	доступен
Уведомления на панели задач	недоступно	доступен
Панели Диспетчер задач	доступен	доступен
Internet Explorer или пограничная	недоступно	доступен
Встроенная система справки	недоступно	доступен
оболочка Windows 10	недоступно	доступен
Проигрыватель Windows Media	недоступно	доступен
PowerShell	доступен	доступен
Интегрированная среда сценариев PowerShell	недоступно	доступен
Редактор IME для PowerShell	доступен	доступен
Mstsc.exe	недоступно	доступен
Службы удаленных рабочих столов	доступен	доступен
В диспетчере Hyper-V	недоступно	доступен
Программы	недоступно	доступен

1.2 Active Directory

Службы Active Directory (AD) - решение от компании Microsoft позволяющее объединить различные объекты сети (компьютеры, сервера, принтера, различные сервисы) в единую систему. В данном случае AD выступают в роли каталога (базы данных), в котором хранится информация о пользователях, ПК, серверах, сетевых и периферийных устройствах.

Для реализации данного решения, необходим специальный сервер - контроллер домена. Именно он будет выполнять функции аутентификации пользователей и устройств в сети, а также выступать в качестве хранилища базы данных. При попытке использовать любой из объектов (ПК, сервер, принтер) сети, выполняется обращение к контроллеру домена, который либо.

С помощью Active Directory можно поделить компьютеры на различные рабочие группы (организационные подразделения). Это существенно упрощает использование инфраструктуры в двух случаях:

- изменение существующих настроек группы. Поскольку настройки хранятся в единой базе данных, при их модификации, они будут применены для всех компьютеров, относящихся к этой группе;
- добавление нового пользователя. Он автоматически получает установленные для его группы настройки, что существенно ускоряет создание новой учетной записи.

В зависимости от пользователя (учетной записи, которая используется) и его группы можно ввести ограничение на использование функционала операционной системы. Например, вы можете ограничить установку приложений всем кроме администраторов.

Службы Active Directory существенно увеличивают защиту корпоративной сети. Так, все данные (учетные записи) хранятся на контроллерах доступа, которые защищены от внешнего доступа. Кроме того, для аутентификации в AD используется протокол Kerberos (протокол для взаимной аутентификации клиента и сервера перед установкой соединения, в нем учтена перехвата и модификации пакетов, что повышает его надежность), который значительно безопаснее аналога в рабочих группах.

С помощью AD достаточно легко реализуется технология Distributed File System (DFS), которая используется для управления файлами. Фактически, это распределенная сеть для хранения файлов - физически они располагаются на нескольких серверах, но логически находятся в одном месте.

Это удобная функция, позволяющая масштабировать существующую инфраструктуру, добавляя новые сервера, а не заменяя ими старые.

Службы Active Directory позволяют организовать все оборудование и сервисы в единую систему. Например, присутствует поддержка стандарта LDAP (протокол для доступа к службе каталогов X.500), который позволяет

работать с почтовыми и прокси серверами (Exchange Server и ISA Server соответственно). Поддерживаются не только продукты Microsoft, но и сторонние решения:

- IP-телефония;
- 1С;
- шлюз удаленных рабочих столов (Remote Desktop Gateway).

Стоит отметить, возможность интеграции с Windows Server используя протокол RADIUS. Благодаря которому можно использовать VPN подключение для работы вне офиса.

Active Directory является центральным узлом инфраструктуры предприятия, поэтому в случае его отказа все ПК и сервера будут недоступны. Поэтому можно выделить несколько основных пунктов, позволяющих обеспечить бесперебойное круглосуточное функционирование системы.

Вся база данных хранится на контроллере доменов Active Directory, поэтому при его отказе, вся система будет недоступна. Для обеспечения отказоустойчивости следует развернуть 1 или более дублирующих контроллеров доменов и настроить автоматическую репликацию всех изменений. В данном случае, при выходе из строя одного из контроллеров работоспособность сети не нарушается, ведь оставшиеся продолжают работать.

Надежная система резервного копирования позволяет быстро восстановить работоспособность сервера. При использовании одного контроллера доменов резервное копирование не позволяет избежать простоя, но значительно снижает временные затраты на восстановление сервера.

Служба каталогов Active Directory – является сердцем ИТ-инфраструктуры предприятия. В случае её отказа вся сеть, все сервера, работа всех пользователей будут парализованы. Никто не сможет войти в компьютер, получить доступ к своим документам и приложениям. Поэтому служба каталогов должна быть тщательно спроектирована и развёрнута, с

учётом всех возможных нюансов. Например, структура сайтов должна строиться на основе физической топологии сети и пропускной способности каналов между филиалами или офисами компании, так как от этого напрямую зависит скорость входа пользователей в систему, а также репликация между контроллерами домена [3, 6].

1.3 PowerShell

PowerShell позволяет взаимодействовать с операционной системой, используя преимущества инструментов, доступных из командной строки, и используя возможности программирования сценариев для автоматизации рутинной работы.

При использовании Windows Server Core оболочка позволяет работать с Active Directory (AD), в частности настройки контроллера домена (Active Directory). Windows PowerShell позволяет:

- менять настройки операционной системы;
- управлять службами и процессами;
- настраивать роли и компоненты сервера;
- устанавливать программное обеспечение;
- управлять установленным ПО через специальные интерфейсы;
- встраивать исполняемые компоненты в сторонние программы;
- создавать сценарии для автоматизации задач администрирования;
- работать с файловой системой, реестром Windows, хранилищем сертификатов и т.д.

Команды, исполняемые в Windows PowerShell, могут быть в форме командлетов, которые являются специализированными классами .NET, созданными с целью предоставления функциональности в PowerShell в виде сценариев PowerShell (.ps1) или являются обычными исполняемыми файлами. Если команда является исполняемым файлом, то PowerShell запускает её в отдельном процессе; если это команда, то он исполняется

внутри процесса PowerShell. PowerShell предоставляет интерфейс командной строки, в котором можно вводить команды и отображать выводимые ими данные в текстовом виде. Этот пользовательский интерфейс, базирующийся на стандартном механизме консоли Windows, предоставляет настраиваемый механизм автозавершения команд, но не обладает возможностью подсветки синтаксиса, хотя при желании её можно обеспечить. В PowerShell также можно создавать псевдонимы (alias) для командлетов, которые при вызове преобразуются в оригинальные команды. Кроме того, поддерживаются позиционные и именованные параметры для командлетов. При выполнении командлета работа по привязке значений аргументов к параметрам выполняется самим PowerShell, но при вызове внешних исполняемых файлов аргументы передаются им для самостоятельного разбора.

Другое понятие, используемое в PowerShell, — это конвейер (pipeline). Подобно конвейерам в UNIX, они предназначены для объединения нескольких команд путём передачи выходных данных одной команды во входные данные второй команды, используя оператор « | ». Но, в отличие от аналога в UNIX, конвейер PowerShell является полностью объектным, то есть данные между командлетами передаются в виде полноценных объектов соответствующих типов, а не как поток байтов. Когда данные передаются как объекты, содержащиеся в них элементы сохраняют свою структуру и типы между командлетами, без необходимости использования какой-либо сериализации или посимвольного разбора данных. Объект также может содержать некоторые функции, предназначенные для работы с данными. Они также становятся доступными для получающего их командлета. Вывод последнего командлета в конвейере PowerShell автоматически передаёт на командлет Write-Host, который создаёт текстовое представление объектов и содержащихся в них данных и выводит его на экран.

Так как все объекты PowerShell являются объектами «.NET», они содержат метод «.ToString()», возвращающий текстовое представление данных объекта. PowerShell использует этот метод для преобразования

объекта в текст. Кроме того, он позволяет указать правила форматирования, так что текстовое представление объектов может быть настроено. Однако с целью поддержания совместимости, если в конвейере используется внешний исполняемый файл, то он получает текстовый поток, представляющий объект, и не интегрируется с системой типов PowerShell.

Расширенная система типов (Extended Type System) PowerShell базируется на системе типов «.NET», но реализует некоторые дополнения. Например, она позволяет создавать различные представления объектов, отображая лишь некоторые из их свойств и методов, а также применять специальное форматирование и механизмы сортировки. Эти представления привязываются к оригинальным объектам с помощью конфигурационных файлов в формате XML.

Командлеты (cmdlets) — это специализированные команды PowerShell, которые реализуют различную функциональность. Это встроенные в PowerShell команды. Командлеты именуются по правилу Глагол-Существительное, например, Get-ChildItem, благодаря чему их предназначение понятно из названия. Командлеты выводят результаты в виде объектов или их коллекций. Дополнительно командлеты могут получать входные данные в такой же форме и, соответственно, использоваться как получатели в конвейере. Хотя PowerShell позволяет передавать по конвейеру массивы и другие коллекции, командлеты всегда обрабатывают объекты поочередно. Для коллекции объектов обработчик командлета вызывается для каждого объекта в коллекции по очереди [4, 5 , 11].

1.4 Sconfig

SConfig — это удобное средство, которое особенно полезно при настройке или устранении неполадок с одним сервером. Однако это не единственный способ настройки параметров и может оказаться не эффективным в большом масштабе.

В утилите SConfig настраиваются:

- присоединение к домену или рабочей группе;
- обновления Windows Server;
- удаленный доступ;
- настройки сети;
- времени и даты;
- выход;
- перезагрузка и выключение устройства;
- установка графического интерфейса (до версии Windows Server Core 2012 включительно).

Вызывается утилита при помощи командной строки терминала – Sconfig. Пример показан на рисунке 1.

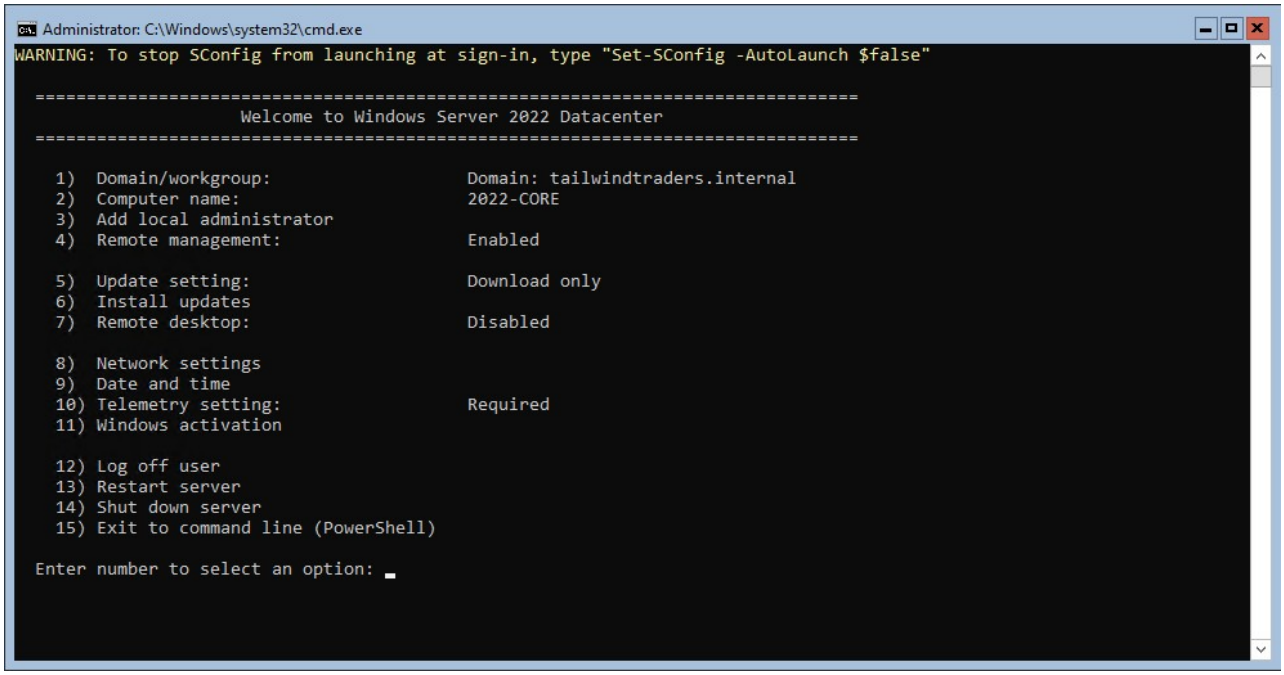

Рисунок 1 – Утилита Sconfig

1.5 DNS

Протокол DNS (Domain Name Service) – предназначен для преобразования IP – адреса в имя из символов и обратно.

Домен (domain — область) — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости): вначале корневой домен (не имеющий идентификатора), ниже идут домены первого уровня (доменные зоны), затем — домены второго уровня, третьего и т.д.

Ключевыми понятиями DNS являются:

- Поддомен (subdomain) — подчинённый домен. Теоретически деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. На практике больше трёх уровней встречается крайне редко. Ресурсная запись — единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определенному Доменному имени, узлу в дереве имен), тип и поле данных, формат и содержание которого зависит от типа.
- Зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен, а чаще — одновременно на нескольких серверах. Целью выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации (делегирование).
- Делегирование — операция передачи ответственности за часть дерева доменных имен другому лицу или организации. За счет делегирования в DNS обеспечивается распределенность администрирования и хранения. Технически делегирование выражается в выделении этой части дерева в отдельную зону, и размещении этой зоны на DNS-сервере, управляемом этим лицом или организацией.

– DNS-сервер — специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется;

– DNS-клиент — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента;

– Авторитетность — признак размещения зоны на DNS-сервере. Ответы DNS сервера могут быть двух типов: авторитетные (когда сервер заявляет, что сам отвечает за зону) и неавторитетные (англ. Non-authoritative), когда сервер обрабатывает запрос, и возвращает ответ других серверов. В некоторых случаях вместо передачи запроса дальше DNS-сервер может вернуть уже известное ему (по запросам ранее) значение (режим кеширования).

– DNS-запрос (DNS query) — запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным.

– для присоединения к домену, нужно поставить IP – адрес контроллера домена, в поле DNS [2, 3, 6].

1.6 DHCP

DHCP - это клиент-серверный протокол динамической конфигурации хоста (Dynamic Host Configuration Protocol), с помощью которого в ИТ-инфраструктуре сетевые параметры каждого нового устройства прописываются автоматически. Использование DHCP существенно упрощает работу системных администраторов в случаях расширения сети. DHCP доступен как для IPv4 (DHCPv4), так и для IPv6 (DHCPv6).

DHCP-сервер представляет собой фоновый процесс, использующий в качестве транспорта UDP-порт 67 и ожидающий запросы от клиентов, которые хотят подключиться к сети. Применение технологии DHCP-сервера дает возможность прописывать на каждом клиенте:

– IP-адрес;

– маску сети или подсети - адресацию сети или узла в пределах IP-адреса;

– шлюз - компонент, который создает соединение между двумя системами;

– адрес DNS-сервера, который отвечает на запросы о разрешении имен в Интернете;

– время (NTP) - сервис синхронизации внутреннего времени компьютера.

Существует три режима работы DHCP-сервера:

– Ручное назначение, при котором IP, указанные в конфигурации хоста, назначаются фиксированным MAC-идентификатором, при этом аппаратный адрес отдельного сетевого адаптера будет уникальным для каждого устройства. IP в данном случае назначаются на постоянной основе, но дополнительные клиенты в сеть подключены быть уже не могут.

– Динамическое назначение, при котором сервер определяет в своих записях, как надолго IP-адрес может быть предоставлен клиенту. Установленное администратором время называется «временем аренды». По истечении срока аренды сервер DHCP возвращает адрес в пул, где он может быть перераспределен по мере необходимости.

– Автоматическое назначение, при котором протокол динамической конфигурации хоста назначает определенный диапазон IP-адресов. Как только адреса «завязываются» друг на друга, они остаются связанными на бесконечное время. Недостатком этого способа является то, что новые клиенты не получат IP, если область полностью назначена.

Присвоение IP-адреса проводится через DHCP-сервер в несколько этапов:

– Discover (поиск сервера). Когда клиент загружается (или хочет присоединиться к сети), он запускает процесс с широковещательным (broadcast) сообщением DHCPDISCOVER со своим собственным MAC-адресом для обнаружения доступных серверов DHCPv4. Поскольку у клиента

нет способа узнать подсеть, к которой он принадлежит, у сообщения DHCPDISCOVER адресом назначения IPv4-адреса будет 255.255.255.255. А поскольку у клиента еще нет настроенного адреса IPv4, то исходными IPv4-адресом будет 0.0.0.0. Сообщение DHCPDISCOVER обнаруживает серверы DHCPv4 в сети. Поскольку у клиента не имеется IPv4 информации при загрузке, он использует для связи с сервером широковещательные адреса 2 и 3 уровня.

– Offer (предложение сервера). Когда DHCPv4-сервер получает сообщение DHCPDISCOVER, он резервирует доступный IPv4-адрес для аренды или постоянного присвоения клиенту. Сервер также создает запись ARP, состоящую из MAC-адреса клиента и предоставленного IPv4-адреса. DHCP-сервер отправляет связанное сообщение DHCPOFFER запрашивающему клиенту, как одноадресную передачу (unicast), используя MAC-адрес сервера в качестве исходного адреса и MAC-адрес клиента в качестве адреса доставки.

– Request (запрос). Когда клиент получает DHCPOFFER с сервера, он отправляет обратно сообщение DHCPREQUEST. Это сообщение используется как для получения IP-адреса, так и для продления его аренды. Когда DHCPREQUEST используется для получения аренды, оно служит уведомлением о принятии выбранных и предложенных конкретным сервером параметров, и оповещением об отклонении предложений от других серверов. Многие корпоративные сети используют несколько DHCP серверов, и сообщение DHCPREQUEST отправляется в виде широковещательной передачи, чтобы информировать все серверы о принятом предложении.

– Acknowledge (подтверждение). При получении сообщения DHCPREQUEST сервер проверяет информацию об аренде с помощью ICMP-запроса на этот адрес, чтобы убедиться, что он уже не используется, и создает новую ARP запись для аренды клиента, а затем отвечает одноадресным DHCPACK-сообщением. Это сообщение является дубликатом DHCPOFFER, за исключением изменения поля типа сообщения. Когда

клиент получает сообщение DHCPACK, он регистрирует информацию и выполняет поиск ARP для назначенного адреса. Если ответа на ARP нет, клиент знает, что адрес IPv4 действителен и начинает использовать его как свой собственный.

Использование DHCP-серверов позволяет автоматически создавать конфигурацию для новых пользователей и встраивать в ИТ-инфраструктуру практически любые устройства, подключаемые к сети - компьютеры, коммутаторы, смартфоны. При этом динамическое назначение IP-адресов снижает вероятность того, что два устройства будут иметь один и тот же IP-адрес (что бывает достаточно часто при использовании статических IP-адресов, назначенных вручную).

Поскольку каждое из этих устройств получает IP-адрес автоматически, устройства могут свободно перемещаться из одной сети в другую (при условии, что все они настроены с помощью DHCP), что очень удобно для мобильных устройств.

Однако, помимо преимуществ, у использования серверов DHCP есть определенные недостатки. Так, динамические IP-адреса не должны использоваться для стационарных устройств (принтеров и файловых серверов), требующих постоянного доступа. Для таких устройств следует назначать статические IP-адреса [2, 3].

1.7 Групповые политики

Групповая политика — важный элемент любой среды Microsoft Active Directory (AD). Её основная цель — дать ИТ-администраторам возможность централизованно управлять пользователями и компьютерами в домене. Групповая политика, в свою очередь, состоит из набора политик, называемых объектами групповой политики (GPO).

Во многих компаниях, как правило, применяется деление на отделы: отдел кадров, бухгалтерия, юристы, отдел системного администрирования.

Предположим, что каждому отделу необходим собственный минимальный набор программного обеспечения, а рабочие станции должны быть настроены для конкретных нужд и под конкретные задачи. Благодаря групповым политикам появляется возможность создать настройки для конкретных групп пользователей в домене. При помощи Active Directory GPO администратор может устанавливать и управлять стандартизированными наборами настроек, конкретно для бухгалтерии или отдела кадров.

Выделяют два компонента групповых политик - клиентский и серверный, т.е. формируется структура «клиент-сервер»:

– Серверный компонент представляет оснастка MMC (Microsoft Management Console), предназначенная для настройки групповой политики. MMC можно использовать для создания политик, а также для контроля и управления административными шаблонами, настройками безопасности (установка ПО, скрипты и т.п.). Обобщенное название «возможностей» называется расширением. Каждое расширение может иметь дочернее расширение, которое разрешает добавление новых или удаление старых компонентов, а также их обновление.

– Клиентский компонент получает и применяет настройки групповой политики. Клиентские расширения являются компонентами, запускаемыми на клиентской ОС, которые отвечают за интерпретацию и обработку объектов групповой политики.

Для администрирования GPO используют оснастки MMC - Group Policy Management Console (GPMC) и Group Policy Management Editor.

Сценарии использования Active Directory GPO:

– централизованная настройка пакета программ Microsoft Office;

– централизованная настройка управлением питанием компьютеров;

– настройка веб-браузеров и принтеров;

– установка и обновление ПО;

– применение определенных правил в зависимости от местоположения пользователя;

– централизованные настройки безопасности;

– перенаправление каталогов в пределах домена;

– настройка прав доступа к приложениям и системным программам.

Административные шаблоны облегчают доступ к реестровым параметрам политики, которые иногда требуется конфигурировать.

Набор административных шаблонов по умолчанию для пользователей и компьютеров конфигурируется в консоли Групповая политика (Group Policy). Административные шаблоны можно добавлять и удалять. Любые изменения в политиках, совершаемые через административные шаблоны, сохраняются в реестре. Конфигурации компьютеров сохраняются в разделе HKEY_ LOCAL_MAC HINE, а конфигурации пользователей - в HKEY_CURRENT_USER.

Настроенные шаблоны позволяют просмотреть узел Административные шаблоны (Administrative Templates) консоли Групповая политика (Group Policy). Он содержит политики, конфигурируемые для локальных систем, ОП, доменов и сайтов. Наборы шаблонов в узлах Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration) различаются. Добавлять дополнительные шаблоны, содержащие новые политики, можно вручную, а также при настройке новых компонентов Windows. Пользовательский интерфейс для узла Административные шаблоны (Administrative Templates) настраивается в файлах с расширением .adm. Эти текстовые файлы в формате ASCII разрешается редактировать или создавать в любом текстовом редакторе. При конфигурации политик в узле Административные шаблоны (Administrative Templates) параметры сохраняются в файлах Registry.pol. Для разделов реестра HKEY_LQCAL_MACHINE и HKEY_CURRENT_USER применяются отдельные файлы Registry.pol.

Чтобы узнать, какие политики административных шаблонов доступны, достаточно просмотреть узлы Административные шаблоны (Administrative Templates) в консоли Групповая политика (Group Policy). Политики находятся в одном из трех состояний:

– не задана (Not Configured) — политика не используется, и ее параметры не сохранены в реестре;

– включена (Enabled) — политика активно выполняется, и ее параметры сохраняются в реестре;

– отключена (Disabled) — политика отключена и не выполняется, если не замещена. Этот параметр сохраняется в реестре [3, 11].

2 Аналитический раздел

2.1 Понятия Active Directory

Active Directory нужен для облегчения работы в сети, большинство действий не нужно повторять, поскольку все структурировано в самом домене.

Единая точка аутентификации в рабочей группе на каждом компьютере или сервере придётся вручную добавлять полный список пользователей, которым требуется сетевой доступ. Если вдруг один из сотрудников захочет сменить свой пароль, то его нужно будет поменять на всех компьютерах и серверах. Хорошо, если сеть состоит из 10 компьютеров, но если их больше? При использовании домена Active Directory все учётные записи пользователей хранятся в одной базе данных, и все компьютеры обращаются к ней за авторизацией. Все пользователи домена включаются в соответствующие группы, например, «Бухгалтерия», «Финансовый отдел». Достаточно один раз задать разрешения для тех или иных групп, и все пользователи получат соответствующий доступ к документам и приложениям. Если в компанию приходит новый сотрудник, для него создаётся учётная запись, которая включается в соответствующую группу, – сотрудник получает доступ ко всем ресурсам сети, к которым ему должен быть разрешён доступ. Если сотрудник увольняется, то достаточно заблокировать – и он сразу потеряет доступ ко всем ресурсам (компьютерам, документам, приложениям);

Единая точка управления политиками в рабочей группе все компьютеры равноправны. Ни один из компьютеров не может управлять другим, невозможно проконтролировать соблюдение единых политик, правил безопасности. При использовании единого каталога Active Directory, все пользователи и компьютеры иерархически распределяются по

организационным подразделениям, к каждому из которых применяются единые групповые политики. Политики позволяют задать единые настройки и параметры безопасности для группы компьютеров и пользователей. При добавлении в домен нового компьютера или пользователя, он автоматически получает настройки, соответствующие принятым корпоративным стандартам. При помощи политик можно централизованно назначить пользователям сетевые принтеры, установить необходимые приложения, задать параметры безопасности браузера, настроить приложения Microsoft Office.

Повышенный уровень информационной безопасности использование служб Active Directory значительно повышает уровень безопасности сети. Во-первых – это единое и защищённое хранилище учётных записей. В доменной среде все пароли доменных пользователях хранятся на выделенных серверах контроллерах домена, которые, как правило, защищены от внешнего доступа. Во-вторых, при использовании доменной среды для аутентификации используется протокол Kerberos, который значительно безопаснее, чем NTLM, использующийся в рабочих группах.

Интеграция с корпоративными приложениями и оборудованием большим преимуществом служб Active Directory является соответствие стандарту LDAP, который поддерживается другими системами, например, почтовыми серверами (Exchange Server), прокси-серверами (ISA Server, TMG). Причем это не обязательно только продукты Microsoft. Преимущество такой интеграции заключается в том, что пользователю не требуется помнить большое количество логинов и паролей для доступа к тому или иному приложению, во всех приложениях пользователь имеет одни и те же учётные данные – его аутентификация происходит в едином каталоге Active Directory. Windows Server для интеграции с Active Directory предоставляет протокол RADIUS, который поддерживается большим количеством сетевого оборудования. Таким образом, можно, например, обеспечить

аутентификацию доменных пользователей при подключении по VPN извне, использование Wi-Fi точек доступа в компании.

Единое хранилище конфигурации приложений некоторые приложения хранят свою конфигурацию в Active Directory, например, Exchange Server. Развёртывание службы каталогов Active Directory является обязательным условием для работы этих приложений. Хранение конфигурации приложений в службе каталогов является выгодным с точки зрения гибкости и надёжности. Например, в случае полного отказа сервера Exchange, вся его конфигурация останется нетронутой. Для восстановления работоспособности корпоративной почты, достаточно будет переустановить Exchange Server в режиме восстановления.

Службы Active Directory являются сердцем ИТ-инфраструктуры предприятия. В случае отказа вся сеть, все сервера, работа всех пользователей будут парализованы. Никто не сможет войти в компьютер, получить доступ к своим документам и приложениям. Поэтому служба каталогов должна быть тщательно спроектирована и развёрнута, с учётом всех возможных нюансов, например, пропускной способности каналов между филиалами или офисами компании (от этого напрямую зависит скорость входа пользователей в систему, а также обмен данными между контроллерами домена) [1, 3, 10].

2.2 Возможности графического управления Windows Server Core

Не смотря на консольное управление Windows Server Core, в ней есть графические оснастки, например:

- Notepad.exe - приложение блокнот;
- MSInfo32.exe - просмотр сведений о системе, программных и аппаратных ресурсах;

– Regedit.exe и Regedt32.exe - редактирование реестра;

– TimeDate.cpl - панель управления временем и датой;

– Intl.cpl - панель управления региональными настройками;

– Iscsicpl.exe - панель управления «Свойства: инициатор iSCSI», для возможности подключаться к общему хранилищу через iSCSI.

Так же в версиях Windows Server Core до 2012 года включительно есть возможность включения графического интерфейса (GUI), посредством PowerShell, где необходимо вписать: «Install-WindowsFeature Server-Gui-Mgmt-Infra -Restart» для установки минимального графического интерфеса, чтобы была возможность запускать такие оснастки, как например Server Manager. Для полного графического интерфейса нужно написать: «Install-WindowsFeature Server-Gui-Mgmt-Infra, Server-Gui-Shell –Restart».

Так же есть возможность удаленного администрирования домена с использованием графической оболочки, нужно установить инструменты администрирования «RSAT: средства служб сертификации Active Directory». В сборке они заранее не установлены, а установка происходит только при наличии интернета. Так – же можно скачать инструменты администрирования с официального сайта Microsoft.

Для предусмотренной системой установки инструментов в ОС Windows 10 нужно зайти в: параметры Windows – Приложения – Дополнительные возможности – добавить компаненты.

Нужно выбрать инструмент «Средства удаленного администрирования сервера: средства доменных служб Active Directory и служб облегченного доступа к каталогам».

Для управления AD, нужно зайти на компьютер из домена, под именем и паролем администратора домена. Затем нужно зайти в: «панель управления – Система и безопасность – Администрирование». Открывается папка с инструментами администрирования [8, 9].

2.3 Проектирование домена

В рамках данной дипломной работы, будет установлен домен, на основе Microsoft Windows Server Core, после чего проведется основная настройка: установка инструментов администрирования домена, пользователей, групп, протокола DCHP, протокола DNS.

Эти действия будут реализованы посредством программы VMware Workstation Pro, которая эмулирует операционные системы и локальные сети. Так – же будут использованы образы операционных систем: Microsoft Windows Server 2019 Standard, Microsoft Windows 10 (2 виртуальные машины –пользовательский и для администрирования).

Схема структуры виртуальных машин, где: WINGUI – Windows Server 2019 Standard, DESKTOP01 – Windows 10 (пользовательский), DESKTOP02 – Windows 10 (пользовательский) [1, 2]. Схема показана на рисунке 2.

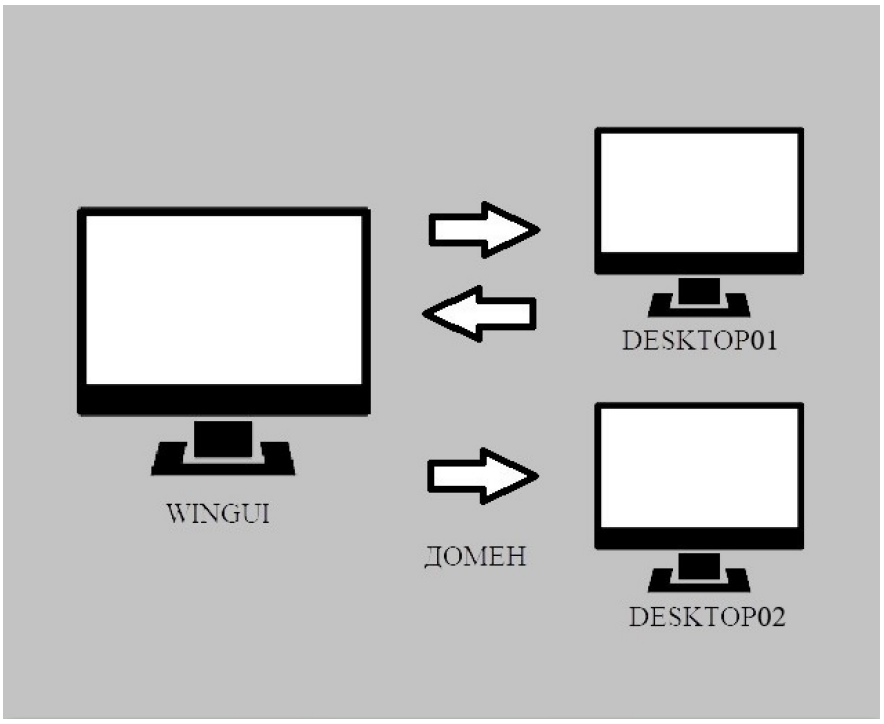

Рисунок 2 – Схема виртуальных машин

3 Исследовательский раздел

3.1 Первоначальная настройка Windows Server Core

Первоначальная установка Windows Server Core происходит при помощи утилиты «Sconfig».

В командную строку (CMD) вводится команда «sconfig» для вызова утилиты Sconfig. Для успешного построения домена нужно, чтобы сервер имел доступ к пользовательским компьютерам. В случае данной дипломной работы в одной сети. Основные настройки: для изменения сети нужно выбрать настройки сети, введя команду - «8». Для присоединения к домену – «1». Изменить имя устройства «2».

Разбор настроек сети. Сначала идет выбор интерфейса. Затем можно установить ip – адрес (статический или динамический), но на сервере лучше ставить статический, адрес dns, шлюз, как показано на рисунке 3.

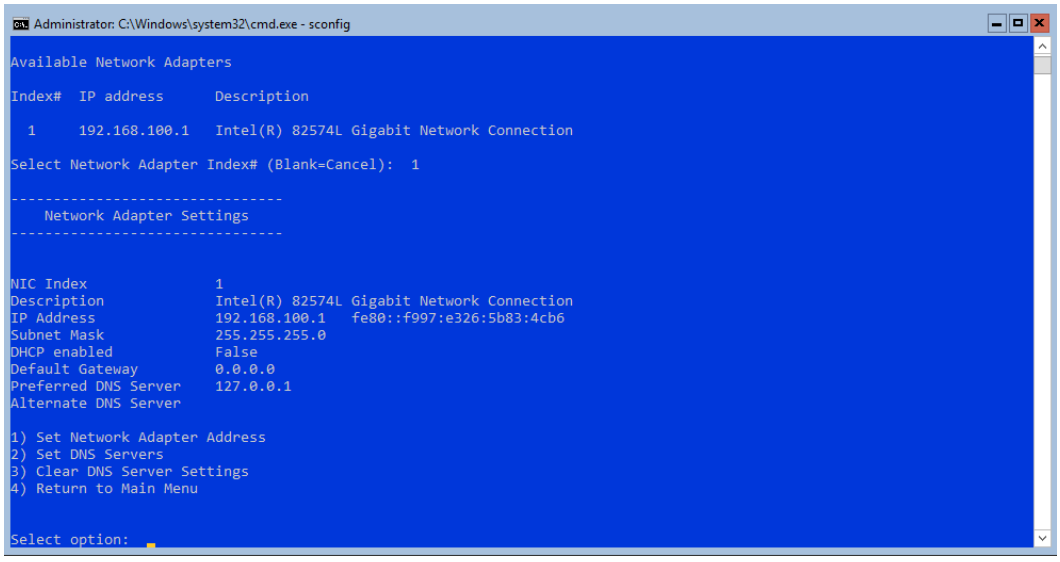

Рисунок 3 – Настройки сети в утилите Sconfig

Для выхода из настроек сети ввод команды «4». Для выхода из утилиты нужно ввести команду – «15».

3.2 Установка Active Directory с помощью PowerShell

Поскольку у версии Windows Server Core нет рабочего стола, то установка и настройка AD происходит при помощи оболочки PowerShell.

Для установки сначала нужно зайти в PowerShell при помощи командной строки: «powershell».

Сначала нужно создать репозиторий для утилиты «dcpromo». Заходим в корневую папку с помощью «cd..». Далее создаем там репозиторий для текстового файла создания AD. С помощью команды «New-Item –ItemType Directory –Path [диск]:[\название папки]». Теперь можно войти в эту папку при помощи команды «Set-Location .[\путь]». Пример показан на рисунке 4.

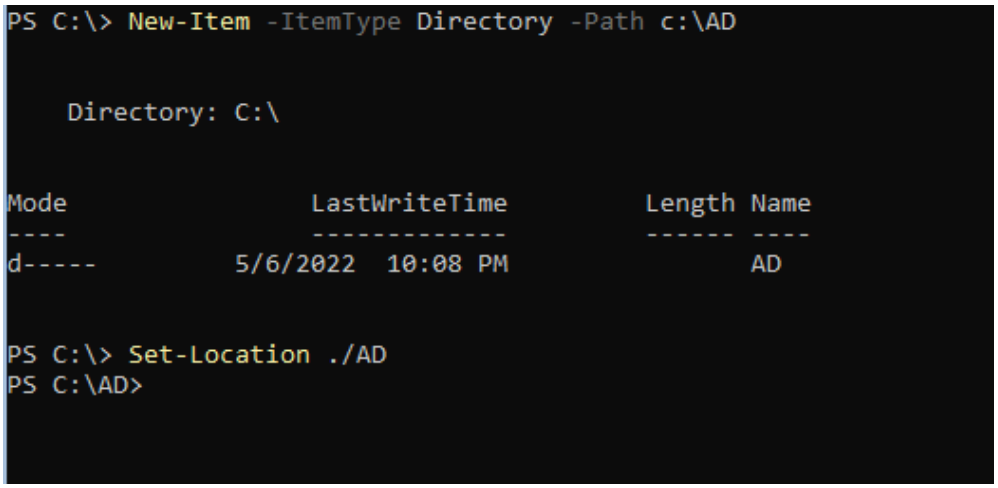

Рисунок 4 – Создание репозитория

Теперь нужно создать файл txt. Для этого нужно использовать команду- «start notepad.exe». Далее нужно заполнить ее инструкциями для установки AD, как показано на рисунке 5.

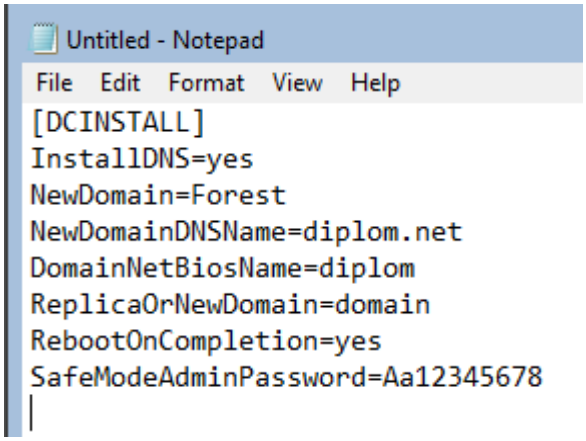

Рисунок 5 – Содержимое текстового файла для утилиты dcpromo

Означают эти инструкции следующее:

- [DCINSTALL] – заголовок для установки;
- InstallDNS=yes – установить DNS;
- NewDomain=Forest – тип установки, в этом случае Forest;
- NewDomainDNSName=Diplom.net – DNS имя домена;
- DomainNetBiosName=diplom – NetBios DNS имя домена;
- ReplicaOrNewDomain=domain – новый домен или реплика;
- RebootOnComletion=yes – перезагрузка после установки;
- SafeModeAdminPassword=[пароль домена] – пароль режима восстановления домена.

Теперь нужно сохранить этот файл в созданный для этого ранее путь.

Если пароль для администратора не установлен, то нужно его назначить. Делается это при помощи команды: «net user administrator *». Где «administrator» - имя пользователя администратора домена.

И последний шаг – установка Active Directory. Для установки нужно ввести следующую команду: «dcpromo.exe /unattend:.\[путь файла]». Где dcpromo.exe – это утилита для установки, /unattend – установку без необходимости пользователя. Если установка выполнена успешна, то покажется уведомление о успешной установке. Показано на рисунке 6.

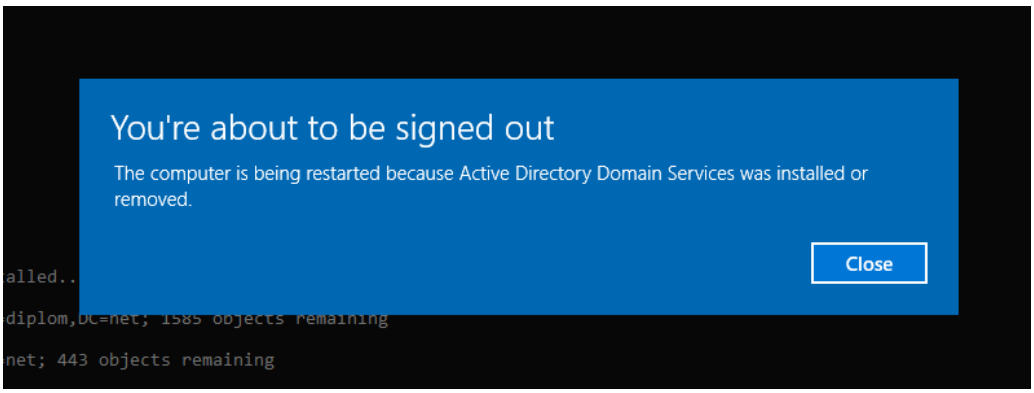

Рисунок 6 – Успешная установка Active Directory

После установки компьютер перезагрузится и войдет в уже созданный домен.

3.3 Добавление пользователей и групп

Для добавления пользователей и групп можно использовать как PowerShell, так и обычную оснастку CMD.

Для создания группы используется командная строка: «New-ADGroup [Имя группы]». Пример показан на рисунке 7.

```
PS C:\Users\WinGUI> New-ADGroup "Marketing"

cmdlet New-ADGroup at command pipeline position 1
Supply values for the following parameters:
GroupScope: 1
PS C:\Users\WinGUI> New-ADGroup "Sales"

cmdlet New-ADGroup at command pipeline position 1
Supply values for the following parameters:
GroupScope: 1
PS C:\Users\WinGUI> New-ADGroup "Booking"

cmdlet New-ADGroup at command pipeline position 1
Supply values for the following parameters:
GroupScope: 1
PS C:\Users\WinGUI> New-ADGroup "IT"

cmdlet New-ADGroup at command pipeline position 1
Supply values for the following parameters:
GroupScope: 1
PS C:\Users\WinGUI>
```

Рисунок 7 – Создание групп

Для создания пользователей используется команда: «New-ADUser –Enabled $true –AccountPassword (ConvertTo-SecureString –String [пароль] –AsPlainText -Force)». Пример показан на рисунке 8.

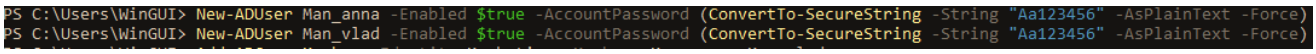

Рисунок 8 – Создание пользователей

Для добавления пользователей в группу используется команда: «Add-ADGroupMember –Identity [Название группы] –Members [Имя пользователя], [Имя пользователя]». Пример показан на рисунке 9.

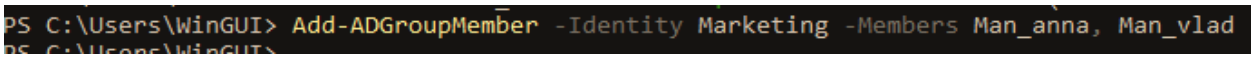

Рисунок 9 – Добавления пользователей в группу.

Для проверки пользователей, входящих в группу, используется команда:

«Get-ADGroupMember [Название группы] –Recursive | ft name». Пример показан на рисунке 10.

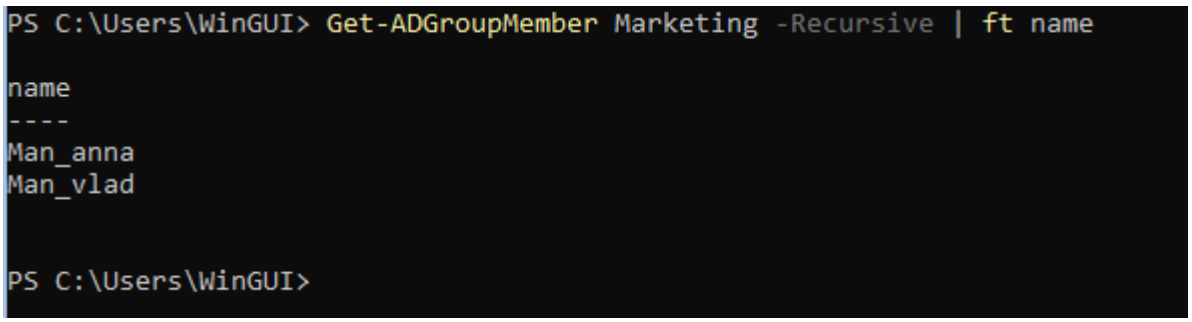

Рисунок 10 – Пользователи группы

Для автоматизации процесса создания пользователей и добавления их в группы, есть возможность создания PowerShell сценария, который получает список пользователей из CSV-файла, создает учетную запись с заготовленными параметрами (запретить смену пароля пользователем; срок действия пароля не ограничен; не изменять пароль при первом входе в систему), после чего добавляет пользователя в заранее определённую группу.

Для начала нужно создать скрипт:

```
Import-Module ActiveDirectory
$UserList = Import-Csv users.csv | ForEach-Object -Process {
$Login = $_.Name[0] + “.” + $_.Surname
$Displayname = $_.Name + “ “ + $_.Surname
$Domain = "diplom.net"
$UPN = $Login + "@" + $Domain
New-ADUser -SamAccountName $Login `
-Surname $_.Surname -DisplayName $Displayname -Name $Displayname `
-Department $_.Department -Title $_.Title -Enabled $true `
-UserPrincipalName $UPN `
-AccountPassword (ConvertTo-SecureString $_.Password -AsPlainText -force) `
-ChangePasswordAtLogon $false -CannotChangePassword `
$True -PasswordNeverExpires $True
$Identity = $_.Department
Add-AdGroupMember -Identity $Identity -Members $Login
}
```

Теперь нужно создать файл CSV с пользователями, в примере он называется «users.csv», можно сделать с помощью Excel, или блокнота:

```
Name,Password,Surname,Department
Dmitriy,Qq123456,Vlasov,Management
Vlad,Ll123456,Simonov,Management
Ksenia,Oo123456,Smirnoff,Booking
```

Anna,Pp123456,Anisimoff,Booking

Oleg,Ss123456,Kuznetzoff,Sales

Vitaly,Dd123456,Laptzhuk,Sales

Konstantin,Aa123456,Sergeev,Sales

Anton,Bb123456,Vladimirovitch,Sales

Peter,Kk123456,Romanov,IT

Vasily,Mm123456,Botshev,IT

После чего открыть скрипт. Если ошибок не возникло, то после выполнения, все пользователи будут созданы, и помещены в группы, как показано на рисунке 11.

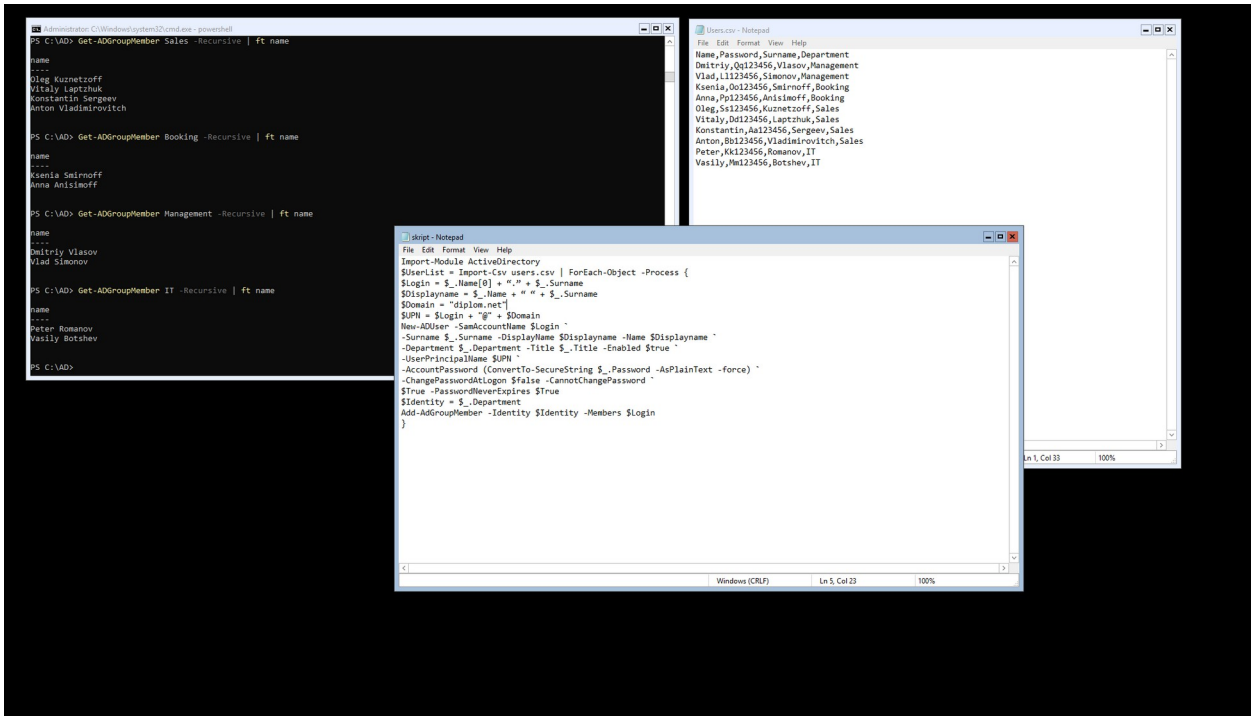

Рисунок 11 - Итог успешного создания и запуска скрипта

3.4 Настройка DHCP

Dynamic Host Configuration Protocol (DHCP) возможно настроить как через PowerShell на сервере, так и дистанционно с компьютера через утилиту Администрирование – DHCP.

Для начала нужно установить функцию DHCP сервера на Windows Server Core. Делается это через PowerShell – В командной строке нужно прописать: «Install-WindowsFeature DHCP – IncludeManagementTools». Для проверки установки можно ввести команду «Get-WindowsFeature –Name *DHCP* Where Installed», как на рисунке 12.

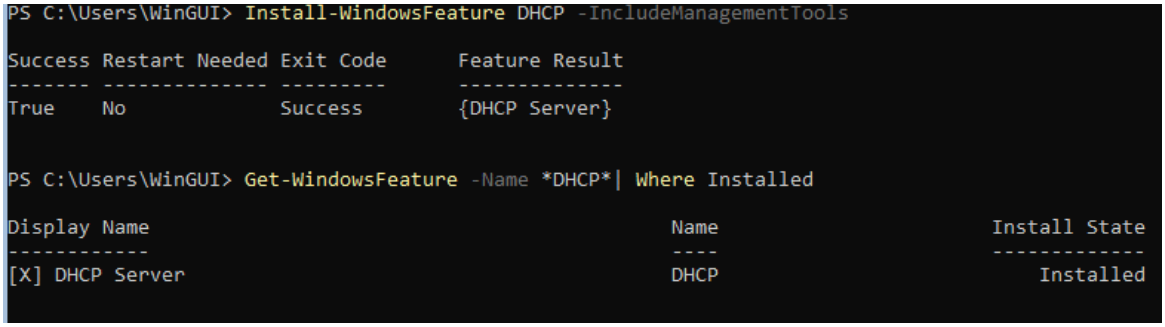

Рисунок 12 – Установка службы DHCP

Сначала добавляются пользователи DHCP и администраторы DHCP групп безопасности на сервере, при помощи команды: «Add-DHCPServerSecuritryGroup – ComputerName [Имя Сервера]»

Затем указывается DNS – сервер, который будет использоваться для регистрации DNS - записей клиента, при помощи команды: «Set-DHCPServerDnsCredential –ComputerName [Имя сервера]»

Следующим шагом определяется область пула ip – адресов, которые DHCP – сервер будет раздавать клиентам. Делается это при помощи команды: «Add-DhcpServerV4Scope –Name dhcp –StartRange 192.168.100.101 –EndRange 192.168.100.254 –SubnetMask 255.255.255.0 –Description ‘DHCP’ – State Active», где:

- StartRange – первый адрес пула;
- EndRange – последний адрес пула;

– SubnetMask – маска сети.

Далее устанавливаются параметры шлюза по умолчанию и DNS – сервера при помощи команды: «Set-DHCPServerV4OptionValue –ScopeID 192.168.100.0 –DnsServer 192.168.100.1 –DnsDomain diplom.net –Router 192.168.100.1», где:

– DnsServer – IP адрес DNS – сервера;

– DnsDomain – адрес DNS – сервера;

– Router – шлюз.

Проверить работу DHCP сервера можно при помощи команды: «Get-DhcpServerv4Scope». Пример показан на рисунке 13.

```
PS C:\Users\WinGUI> Get-DhcpServerv4Scope

ScopeId         SubnetMask      Name            State    StartRange      EndRange        LeaseDuration
-------         ----------      ----            -----    ----------      --------        -------------
192.168.100.0   255.255.255.0   dchp            Active   192.168.100.101 192.168.100.254 8.00:00:00
```

Рисунок 13 – DHCP зона

3.5 Настройка сервера DNS

Domain Name System (DNS) сервер возможно настроить как через PowerShell на сервере, так и дистанционно с компьютера через утилиту Администрирование – DNS.

Для начала нужно установить функцию DNS сервера на Windows Server Core. Делается это через PowerShell – В командной строке нужно прописать: «Install-WindowsFeature DNS – IncludeManagementTools», как показано на рисунке 14.

```
PS C:\Users\WinGUI> Install-WindowsFeature -Name DNS -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}
```

Рисунок 14 – Установка DNS сервера

Теперь можно добавить первичную зону DNS интегрированную с доменом названной именем diplom.local: «add-DnsServerPrimaryZone –Name diplom.local –ReplicationScope “Forest” -Passthru».

Далее создать обратную зону (Lockup Zone): «Add-DnsServerPrimaryZone –NetworkId “192.168.100.0/24” -ReplicationScope Domain». Пример показан на рисунке 15.

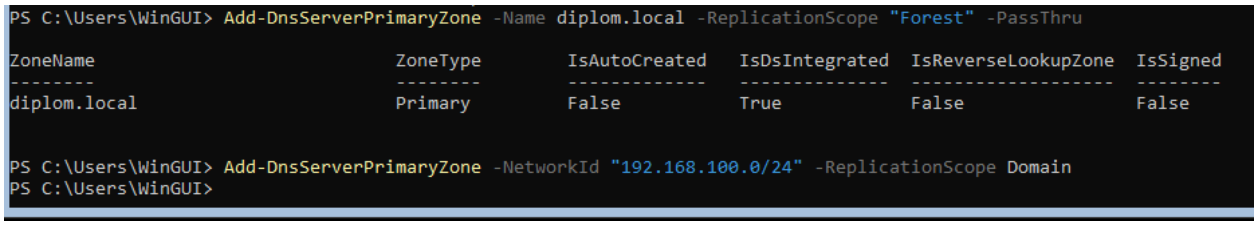

Рисунок 15 – Запись основной и обратной зоны DNS

Теперь можно задать узлам записи типа «A», делается это при помощи команды: «Add-DnsServerResourceRecordA -Name computer01 -IPv4Address 192.168.100.101 -ZoneName diplom.local –CreatePtr». Где командлет – «CreatePtr» создает запись обратной зоны PTR. Можно проверить установку командой: «Get-DnsServerResourceRecord -ZoneName diplom.local -RRType A».

Для автоматизации процесса можно создать небольшой сценарий:

Import-CSV "C:\AD\DNSA.csv" | %{

Add-DNSServerResourceRecordA -ZoneName diplom.local -Name $_."HostName" -IPv4Address $_."IPAddress" -createPtr

}

Где в кавычках указывается путь к CSV файлу, на котором находятся узлы:

HostName, IPaddress

computer02,192.168.100.102

computer03,192.168.100.103

computer04,192.168.100.104

computer05,192.168.100.105

computer06,192.168.100.106

computer07,192.168.100.107

computer08,192.168.100.108

computer09,192.168.100.109

В случае успеха можно проверить выполнение командой: «Get-DnsServerResourceRecord -ZoneName diplom.local -RRType A», как показано на рисунке 16.

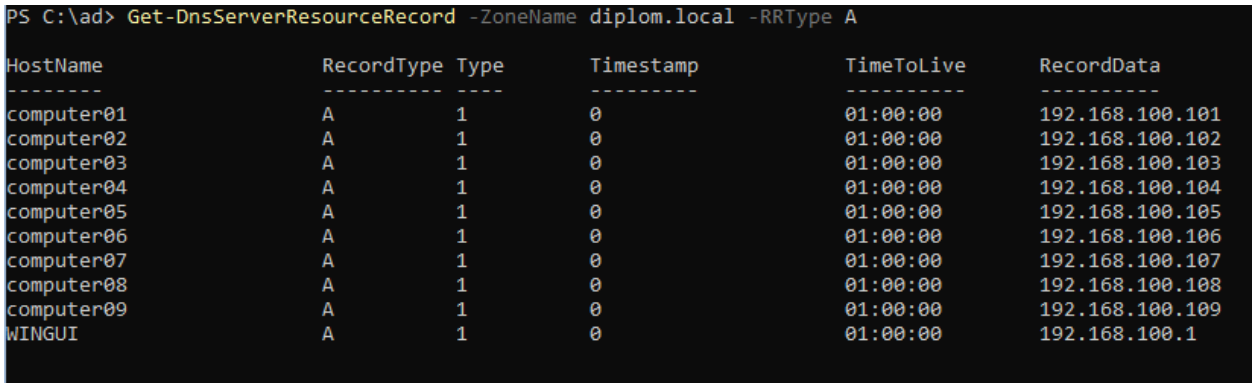

Рисунок 16 – Записи типа «A»

3.6 Настройка групповой политики

С помощью PowerShell модуля GroupPolicy возможно:

- создать или удалить GPO;
- привязать, отвязать GPO от OU;
- создать резервную копию или восстановить политику;
- задать разрешения на GPO, настроить наследование.

В отличии от версии групповой политики на Windows Server с графическим интерфейсов, изменение прав GPO на Core серверах возможны только через PowerShell, в котором доступны только параметры реестра. Ниже будут приведены примеры таких прав.

Для начала нужно установить групповые политика на сервер, делается это командой PowerShell: «Install-WindowsFeatur GPMC -IncludeManagementTools», как показано на рисунке 17.

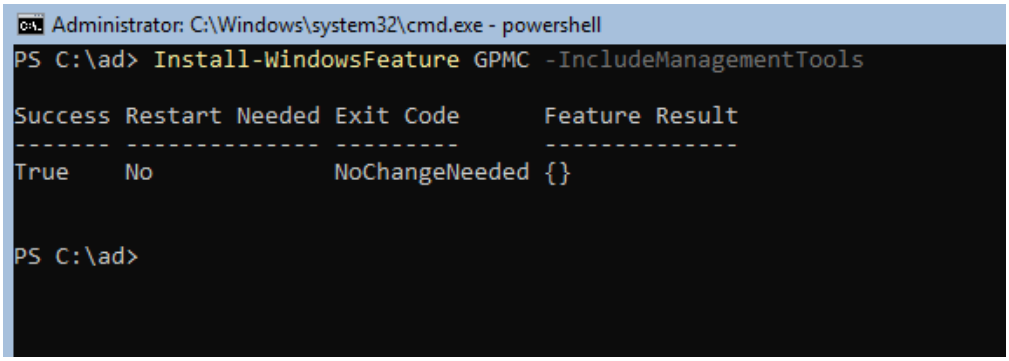

Рисунок 17 – Установка GPO

Теперь можно создать политику, используя команду: «New-GPO -name Drivers».

Для отключения автоматического обновления Wnidows используется команда: «Get-GPO -name drivers | Remove-GPRegistryValue -key HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows -ValueName 'WindowsUpdate'», где «–key» -это путь реестра, «ValueName» -строка реестра, «Value» -значение строки. Пример показан на рисунке 18.

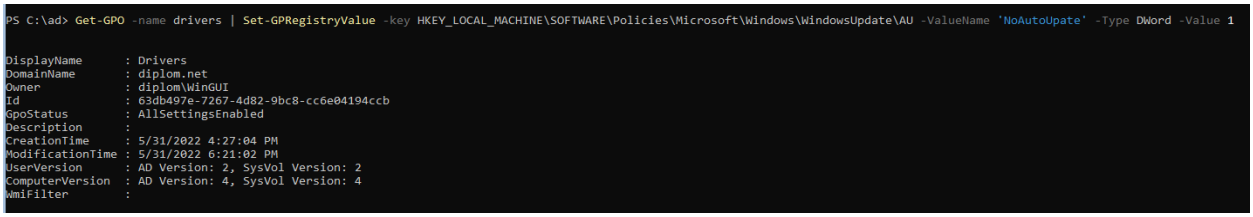

Рисунок 18 – Изменения параметров реестра через GPO

Для автоматического обновления драйверов используется командная строка: «Get-GPO -name drivers | Set-GPRegistryValue -key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\DriverSearching -ValueName 'SearchOrderConfig' -Type DWord -Value 0», где «–key» -это путь реестра, «ValueName» - строка реестра, «Value» -значение.

Для автоматического выхода из пользователя. По истечению 300 секунд бездействия используется команда: «Get-GPO -name drivers | Set-GPRegistryValue -key HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop -ValueName 'ScreenSaveTimeOut' -Type DWord -Value 300»

Для отключения USB – портов используется команда: «-name drivers | Set-GPRegistryValue –key HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\USBSTOR -ValueName 'start' -Type DWord -Value 4».

Чтобы применить установленные правила на домен, необходимо выполнить команду: «Get-GPO drivers | New-GPLink -Target "dc=diplom,dc=net"», где «"dc=diplom,dc=net"» - доменная зона применения, как показано на рисунке 19.

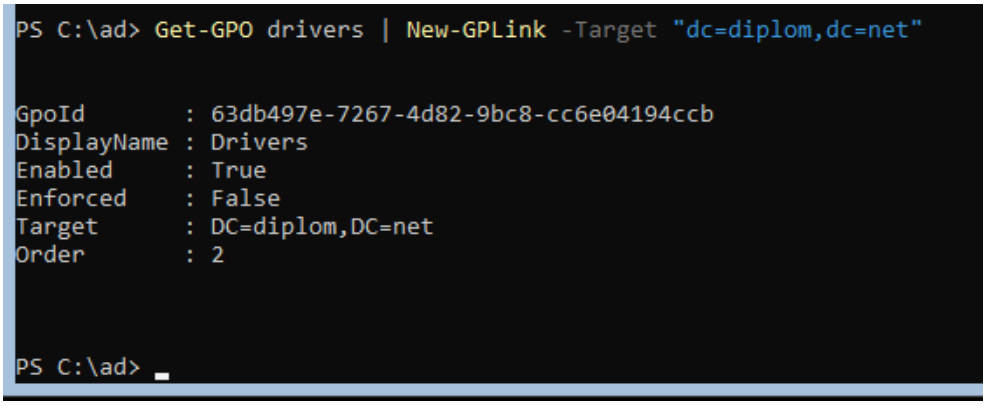

Рисунок 19 – Применение групповой политики на домен

Для остановки правил на домен, используется команда: «Get-GPO drivers | Remove-GPLink -Target "dc=diplom,dc=net"».

Для обновления групповых политик (без перезагрузки пользовательских пк), применяется команда: «gpupdate /force».

Для создания резервной копии политики, применяется команда: «Backup-GPO -Name drivers -Path C:\gpo_backup\», для восстановления используется команда: «Restore-GPO -name drivers -path C:\gpo_backup\». Пример показан на рисунке 20.

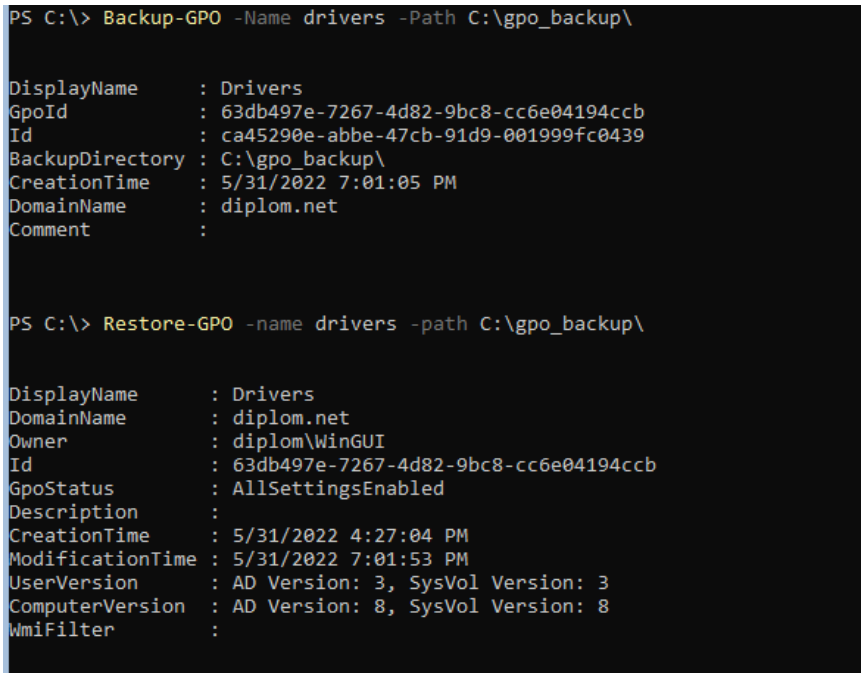

Рисунок 20 – Резервное копирование групповых политик

ЗАКЛЮЧЕНИЕ

Анализ построения домена Microsoft на Core – серверах позволяет утверждать, что домен можно не только построить без графической оснастки, а также автоматизировать этот процесс, путем скриптов и командлентов PowerShell, которые позволяют: создавать пользователей и добавлять их в группы из заранее заготовленного списка, раздачу DNS имен узлам сети.

Были изучены настройки: сервера DHCP, сервера DNS, групповой политики оснасткой PowerShell.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Проектирование сетевой инфраструктуры. Организация, принципы построения и функционирования компьютерных сетей. Лабораторные работы. Учебное пособие. / Тенгайкин Е. – 2-е изд. – М.: Лань, 2021. - 108 с. (учебное пособие). – ISBN - 978-5-8114-7216-1. – Текст: непосредственный.

2. Компьютерные сети. Принципы, технологии, протоколы: учебник для ВУЗов / В. Олифер, Н. Олифер – 4-е изд. – СПб.: Питер, 2010. – 943 с. (учебное пособие). – ISBN - 978-5-498-07389-7. – Текст: непосредственный.

3. Мак-Кейб, Джон. Введение в WindowsServer 2016 / Джон Мак-Кейб – Редмонд: издательство MicrosoftPress, 2016. – 168 с. – ISBN - 978-0-7356-9774-4 – Текст: непосредственный.

4. Попов, А.В. Введение в WindowsPowerShell / А.В. Попов – СПб.: БХВ-Петербург, 2009. – 464 с. - ISBN - 978-5-9775-0283-2 – Текст: непосредственный.

5. Lee, Thomas. Windows Server 2016 Automation with PowerShell Cookbook / Thomas Lee – Birmingham: Packt Publishing Ltd., 2017. – P. 627 – ISBN – 9781787122048 - Текст: непосредственный.

6. Станек, УильямР. Windows Server 2012. Справочник администратора / Уильям Р. Станек – СПб.: БХВ-Петербург, 2014. – 688 с – ISBN - 978-5-9775-0940-4 - Текст: непосредственный.

7. Официальная документация Microsoft [Сайт] – URL: https://docs.microsoft.com/ru-ru/ (дата обращения: 20.05.2022) – Текст: электронный.

8. Гид по технологиям цифровой трансформации - OSP [Сайт] – URL: https://www.osp.ru/ (дата обращения: 22.05.2022) – Текст: электронный.

9. Гид для системного администратора «Заметки сис.Админа» [Сайт] – URL: https://sonikelf.ru/ (дата обращения: 21.05.2022) – Текст: электронный.

10. Сообщество IT- специалистов [Сайт] – URL: https://habr.com/ (дата обращения: 24.05.2022) – Текст: электронный.

11. WinItPro – Windows Для системных администраторов [Сайт] – URL: https://winitpro.ru/ (дата обращения: 27.05.2022) – Текст: электронный.

Дипломная работа выполнена мной самостоятельно. Использованные в работе материалы и концепции из опубликованной научной литературы и других источников имеют ссылки на них.

Отпечатано в _____экземпляре(ах).

Библиография_____ наименований.

«_____» _____20 ___ г.

_____ _____

Ф.И.О.