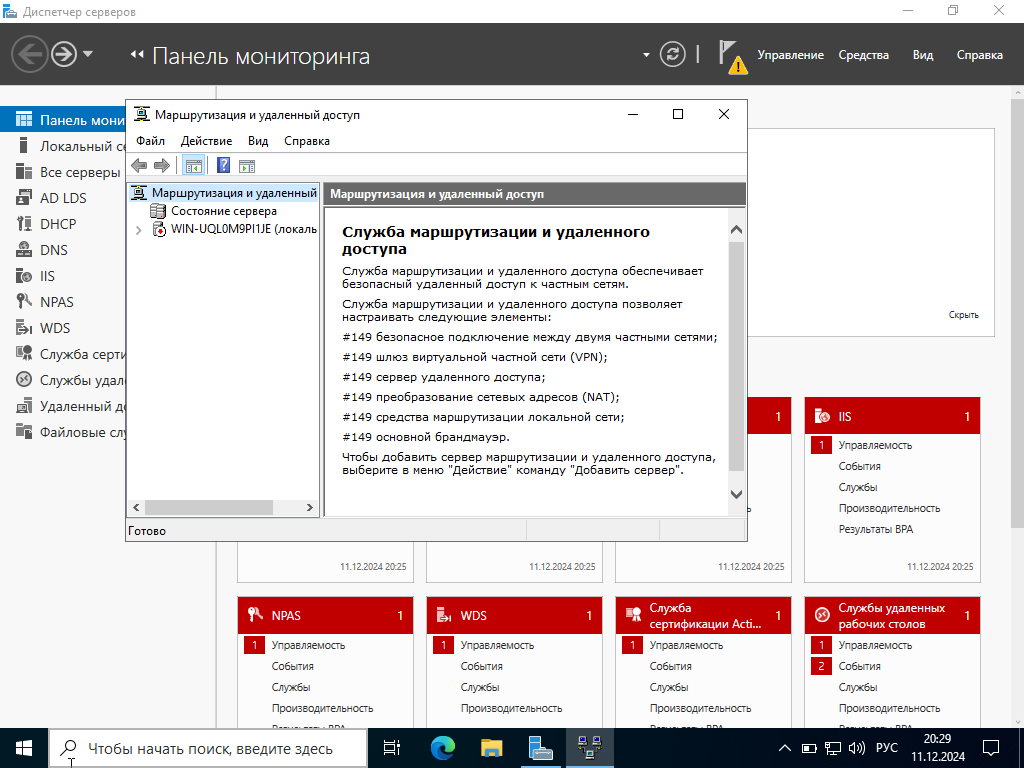
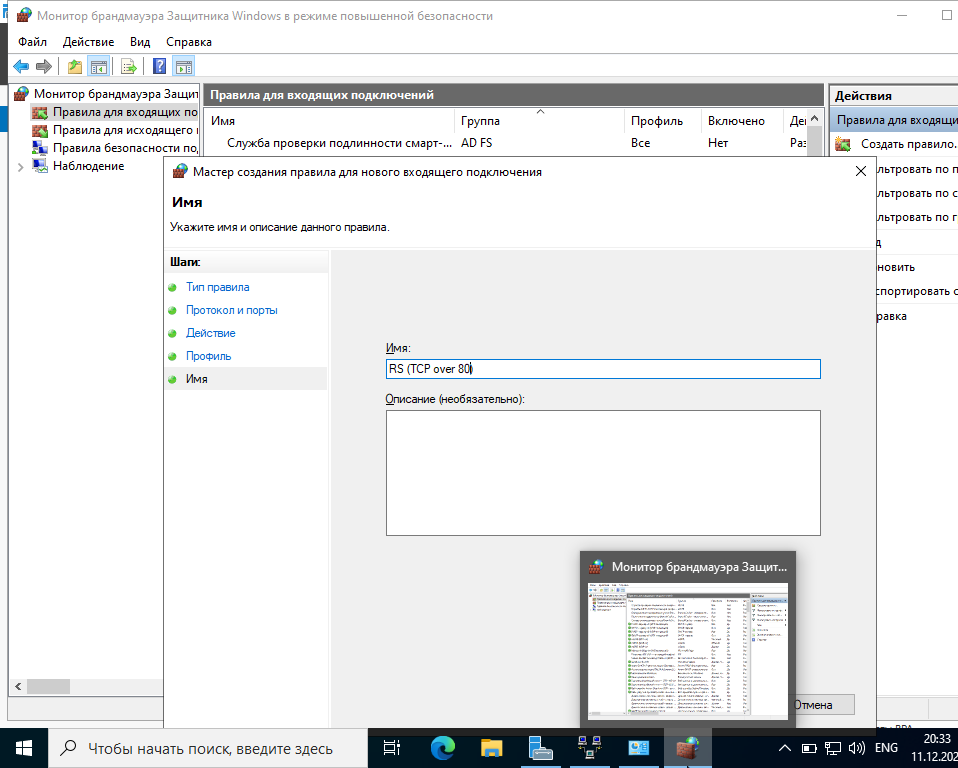
Загайнов Иван, 307 группа, Лабораторный практикум №3. Базовые средства администрирования Microsoft Windows Server 2012. Администрирование сетей передачи данных. Сетевые службы и протоколы.

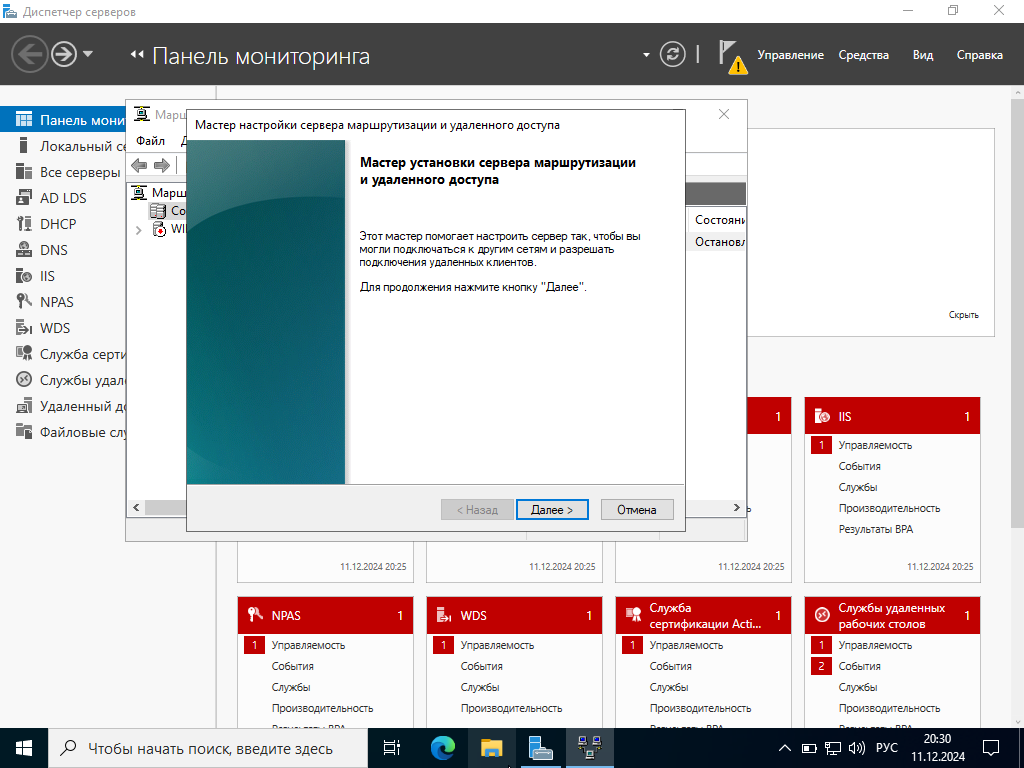


Добавлена роль Службы маршрутизации и удаленного

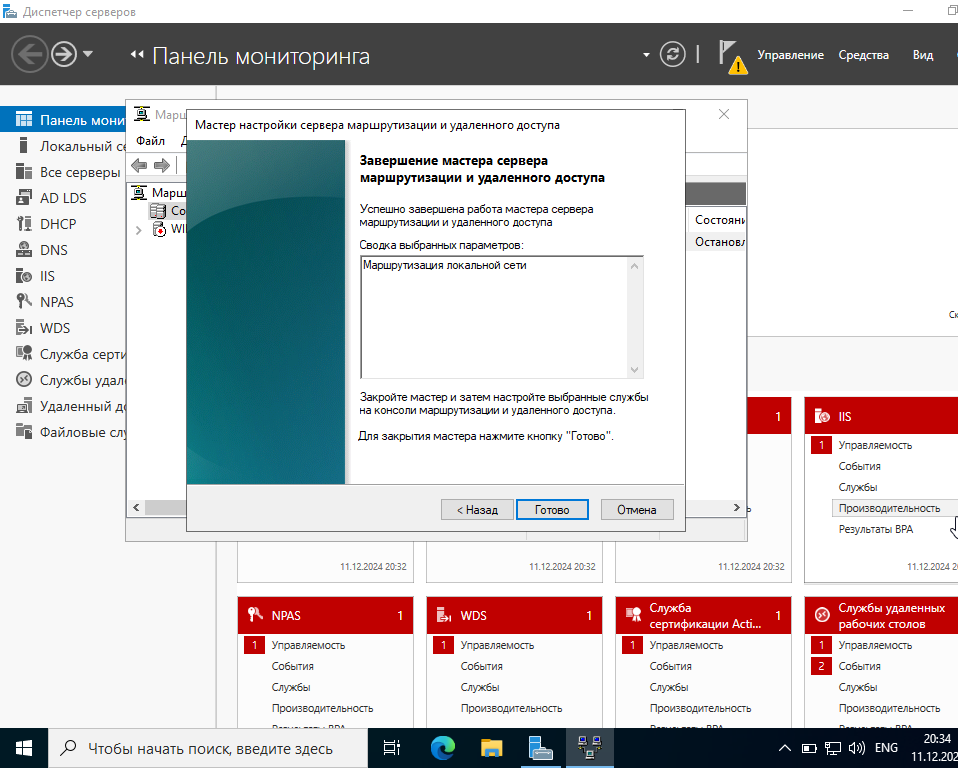
В составных компонентах добавлены Маршрутизация DirectAccess и VPN (RAS)



Открытие локального порта (80)

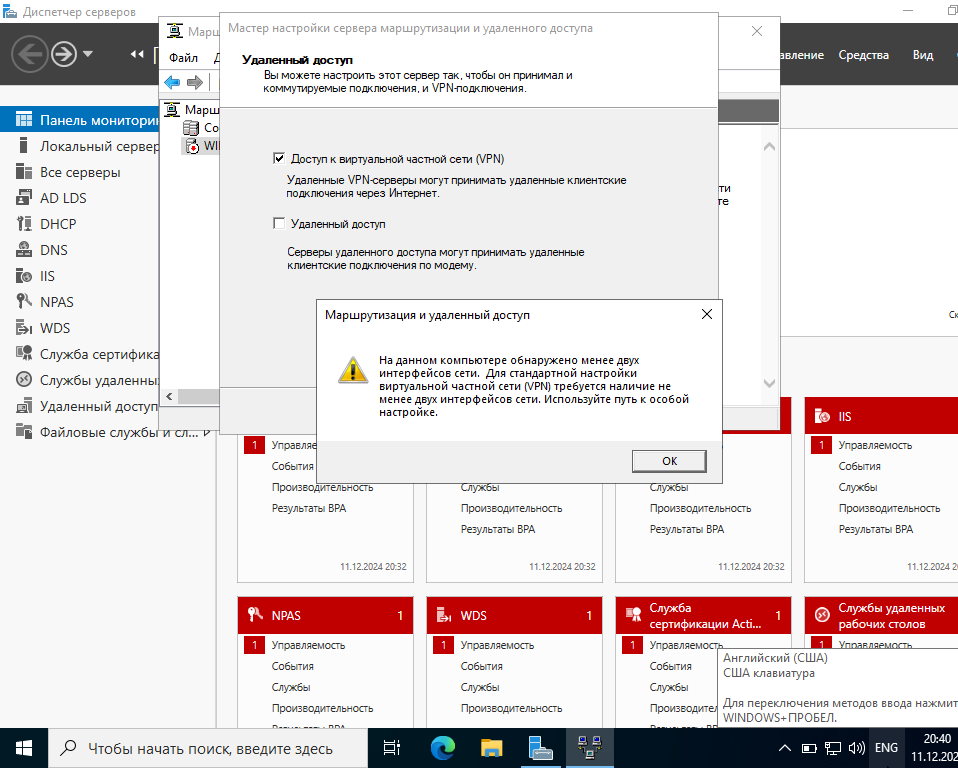


Настройка и включение маршрутизации



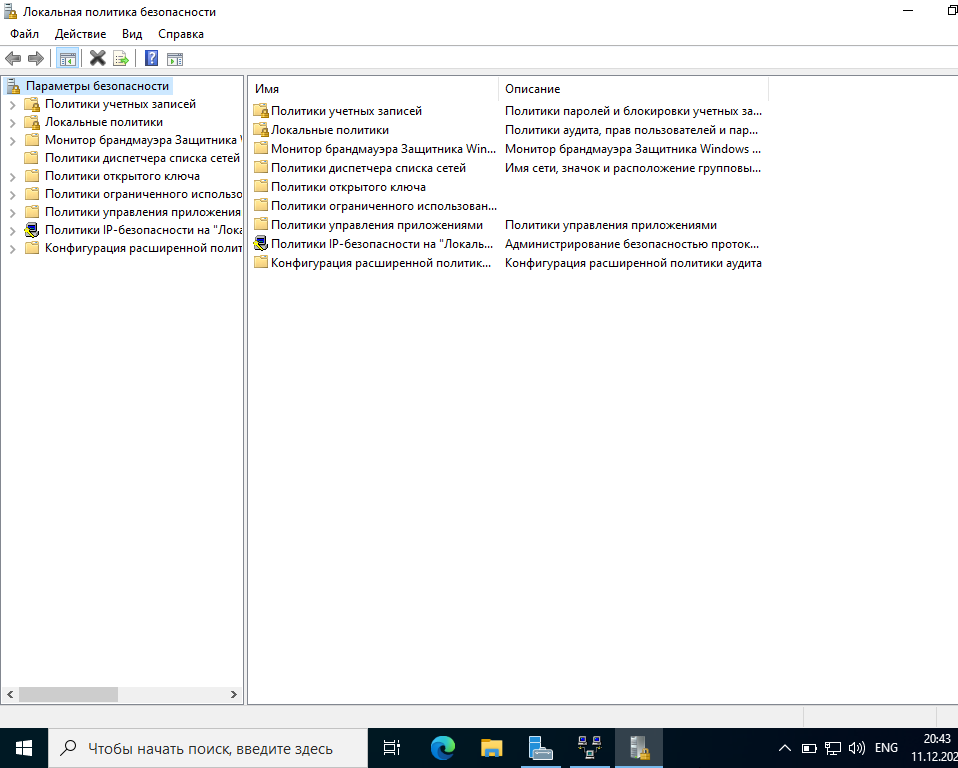
Настройка включена.

Настройка средств удаленного доступа в Microsoft RRAS.

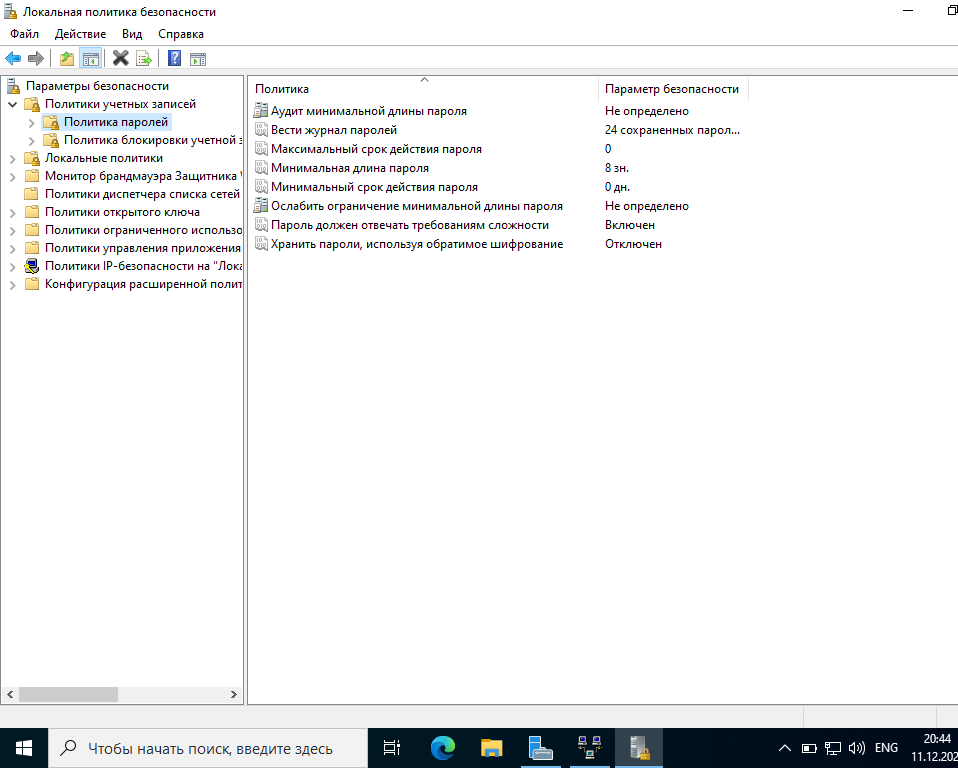


Настроить дальше не могу, т.к. в виртуальной машине один сетевой интерфейс и тот не рабочий.

Настройка параметров политики безопасности на Windows Server 2022

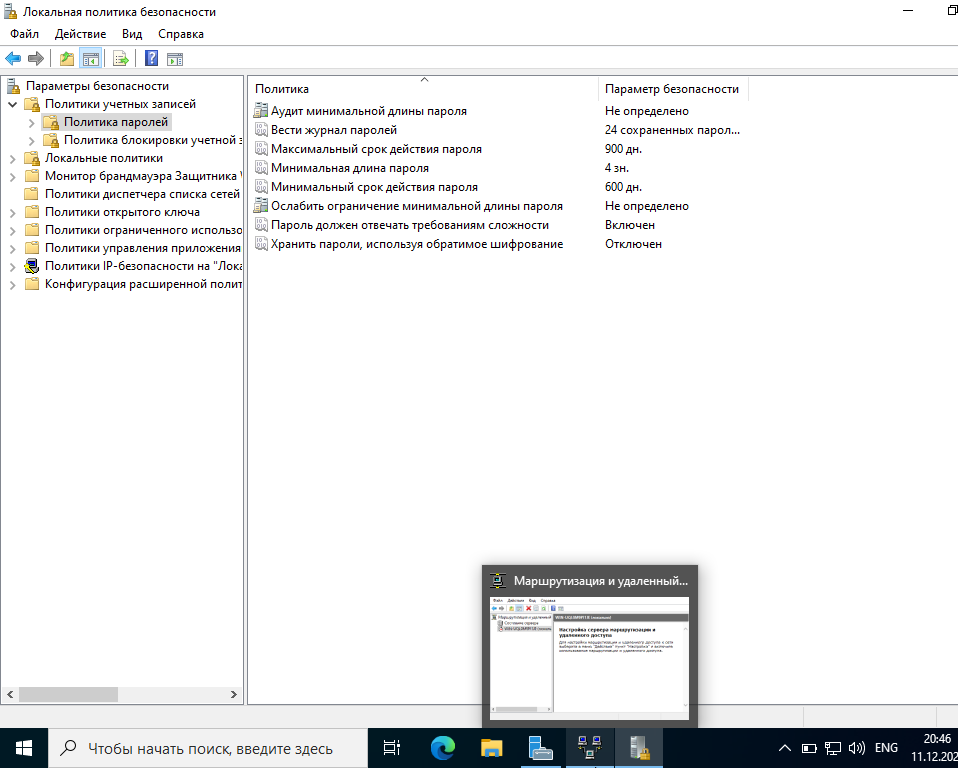


Открываем локальную политику безопасности.



В ней можно задать требования к паролю, срок его действия и т.п.

Стандартный пароль 8 символов, минимальный и максимальный срок действия не заданы.



Настройка политики паролей:

* Перейдите в Политики учетных записей > Политика паролей.
* Здесь можно настроить:
  + Минимальная длина пароля.
  + Требования к сложности пароля.
  + Максимальный срок действия пароля.
  + История паролей.

Настройка политики блокировки учетной записи:

* Перейдите в Политики учетных записей > Политика блокировки учетной записи.
* Настройте параметры, например:
  + Порог блокировки учетной записи (количество неудачных попыток входа).
  + Сброс счетчика блокировки через (время сброса).
  + Продолжительность блокировки учетной записи (на сколько времени учетная запись будет заблокирована).

Настройка прав пользователей:

* Перейдите в Локальные политики > Назначение прав пользователя.
* Здесь можно настроить права для пользователей или групп, например:
  + Локальный вход или Удаленный вход.
  + Запрещенные пользователи для входа на сервер.

Настройка аудита безопасности:

* Перейдите в Конфигурация расширенной политики аудита.
* Настройте параметры для различных типов аудита:
  + Аудит входа/выхода.
  + Аудит доступа к объектам.
  + Аудит изменения политик и другие.

Настройка политик безопасности через групповую политику (для домена):

* Если сервер является членом домена, откройте Консоль управления групповыми политиками (GPMC).
* Создайте или отредактируйте политику безопасности в рамках домена.
* Настройте параметры политики безопасности, такие как:
  + Аудит, пароли, блокировка учетных записей.
  + Примените эти настройки ко всем компьютерам в домене.

Применение политик безопасности:

* После настройки политик безопасности в Локальной политике безопасности или Групповой политике выполните команду gpupdate /force для принудительного применения новых политик или перезагрузите сервер.

Рекомендации:

* Мониторинг и аудит: Включите аудит событий безопасности, чтобы отслеживать попытки несанкционированного доступа и изменения в системе.
* Тестирование настроек: После настройки VPN, маршрутизации и политики безопасности протестируйте их на тестовых устройствах.
* Обновления и безопасность: Убедитесь, что сервер регулярно получает обновления безопасности.

Дополнительные особенности Windows Server 2022:

* Поддержка более новых протоколов: Windows Server 2022 поддерживает улучшенные версии VPN-протоколов, такие как TLS 1.3 и улучшенную поддержку HTTP/3.
* Улучшения в безопасности: Включение защиты от атак на уровне ядра с помощью Secured-core server (для более высокообеспеченных серверов).
* Система управления виртуальными машинами и улучшенная работа с Hyper-V и Kubernetes.