????????? Active Directory

??? 0: ??????? ??????? ?? ?????? (????? ??????)

Вам нужно решить два вопроса, чтобы мы могли двигаться дальше:

1. **Имя домена:** Как договорились, используем поддомен реального сайта.
   - Например, если ваш сайт mysite.ru, то внутренний домен назовем **ad.mysite.ru** (или corp.mysite.ru).
2. **IP-адресация:** Какой у вас диапазон сети?
   - Например, 192.168.1.xxx или 10.0.0.xxx?
   - Совет: Под серверы лучше выделить диапазон в начале или в конце (например, с .10 по .20), исключив их из раздачи DHCP на роутере.

??? 1: ????????? ?????? ?? (??????? DC1)

Зайдите в первую машину.

1. **Имя компьютера (Hostname):**
   - Нажмите Win + X -> Система -> Переименовать этот ПК.
   - Дайте понятное имя. Стандарт: **SRV-DC01** (Server - Domain Controller 01).
   - Перезагрузитесь.
2. **Сетевые настройки (Static IP):**
   - Зайдите в настройки адаптера (ncpa.cpl).
   - Установите **Статический IP**.
   - Пример (подставьте свои данные):
     - **IP:** 10.177.178.254 (или любой свободный)
     - **Mask:** 255.255.255.0
     - **Gateway:** 10.177.178.1 (ваш роутер)
     - **DNS:** Пока оставьте 8.8.8.8 (чтобы скачать обновления), перед поднятием роли мы поменяем его на 127.0.0.1.
3. **Обновления:**
   - Запустите Windows Update и поставьте все обновления. Это важно сделать ДО поднятия контроллера домена.

??? 2: ????????? ?????? ?? (??????? DC2)

Зайдите во вторую машину.

1. **Имя компьютера:**
   - Переименуйте в **SRV-DC02**.
   - Перезагрузитесь.
2. **Сетевые настройки:**
   - Установите **Статический IP**.
   - Пример:
     - **IP:** 10.177.178.253 (следующий свободный)
     - **Mask:** 255.255.255.0
     - **Gateway:** 10.177.178.1
     - **DNS:** 8.8.8.8 (тоже пока внешний для обновлений).
3. **Обновления:**
   - Аналогично, обновите систему.

Начинаем работу с первого сервера **SRV-DC01**. Второй сервер (SRV-DC02) пока не трогаем, он ждет своей очереди.

??? 3: ?????????? DNS ?? SRV-DC01

Перед установкой роли AD, сервер должен «смотреть на себя», чтобы корректно создать DNS-зоны.

1. Зайдите в настройки сетевого адаптера на **SRV-DC01**.
2. В свойствах IPv4 измените **Предпочтительный DNS-сервер (Preferred DNS)** на: 127.0.0.1
   - *Почему: Мы сейчас сделаем этот сервер DNS-сервером. Он должен спрашивать сам себя.*
3. Нажмите OK.

??? 4: ????????? ???? AD DS

1. Откройте **Server Manager** (Диспетчер серверов).
2. В центре нажмите **Add roles and features** (Добавить роли и компоненты).
3. Жмите Next до раздела **Server Roles** (Роли сервера).
4. Поставьте галочку напротив **Active Directory Domain Services**.
   - *Выскочит окно с предложением добавить компоненты — жмите **Add Features**.*
5. Жмите Next до конца и затем **Install**.
6. Ждите окончания установки (полоска заполнится, но перезагрузки пока не будет).

??? 5: ????????? ?? ??????????? ?????? (???????? ????)

Это самый важный момент.

1. В Server Manager сверху, возле флага уведомлений (желтый треугольник), нажмите на флаг.
2. Нажмите ссылку **Promote this server to a domain controller** (Повысить роль этого сервера...).
3. Откроется мастер настройки.

Вкладка Deployment Configuration:

- Выберите пункт: **Add a new forest** (Добавить новый лес).
- Root domain name: **ad.mysite.ru**
- Жмите Next.

Вкладка Domain Controller Options:

- Functional Level (Уровень леса и домена): Оставьте максимальный (Windows Server 2016 — это нормально, Microsoft не меняла название уровня функциональности).
- Галочки **DNS Server** и **Global Catalog (GC)** должны стоять.
- **DSRM Password:** Придумайте и запишите сложный пароль.
  - ***Важно:*** *Этот пароль нужен для восстановления AD, если всё сломается. Это* ***НЕ*** *пароль администратора, это отдельный пароль. Запишите его в блокнот.*
- Жмите Next.

Вкладка DNS Options:

- Появится предупреждение «A delegation for this DNS server cannot be created...».
- **Игнорируйте.** Это нормально, так как родительская зона (mysite.ru) находится в интернете, и мы не имеем к ней прямого доступа отсюда.
- Жмите Next.

Вкладка Additional Options (NetBIOS):

- Мастер предложит NetBIOS имя. Скорее всего, он предложит **AD** (берет первую часть от ad.mysite.ru).
- Рекомендация: Имя AD слишком общее. Я рекомендую изменить его на **MYSITE**.
  - Тогда вход в систему будет выглядеть как MYSITE\Ivanov, а не AD\Ivanov. Это понятнее пользователям.
- Жмите Next.

Вкладка Paths:

- Оставьте всё по умолчанию (C:\Windows\NTDS и т.д.).
- Жмите Next.

Вкладка Review Options:

- Проверьте, всё ли верно. Жмите Next.

Вкладка Prerequisites Check:

- Система проверит сервер. Должно появиться зеленая галочка "All prerequisite checks passed successfully".
- Могут быть желтые восклицательные знаки (про криптографию NT 4.0 или DNS delegation) — это нормально.
- Жмите **Install**.
- **Внимание:** Логин теперь должен быть **MYSITE\Administrator** (или AD\Administrator, если вы оставили NetBIOS AD). Пароль тот же, что был у локального админа.

Супер. Лес создан. Теперь у нас есть «Голова».

Но сейчас система уязвима: если SRV-DC01 перезагружается или ломается, никто не войдет в сеть.
Поэтому сейчас мы поднимаем **второй контроллер домена (SRV-DC02)**.

Переходим на вторую виртуальную машину — **SRV-DC02**.

??? 6: ????????? DNS ?? SRV-DC02 (????????)

Чтобы второй сервер увидел первый и смог скачать настройки домена, он должен использовать первый сервер как DNS.

1. На **SRV-DC02** откройте сетевые настройки (ncpa.cpl).
2. Свойства IPv4 -> Измените DNS:
   - **Предпочтительный DNS (Preferred):** 10.177.178.254 (IP первого сервера SRV-DC01).
   - **Альтернативный:** Оставьте пустым пока.
3. Нажмите OK.

Проверка связи:
Откройте командную строку (CMD) и напишите:
ping ad.mysite.ru
Должен пойти обмен пакетами с IP 10.177.178.254. Если пинг идет — всё отлично. Если пишет "не удалось обнаружить узел" — проверяйте настройки DNS или фаервол.

??? 7: ????????? ????

Точно так же, как на первом сервере:

1. **Server Manager** -> **Add roles and features**.
2. Выбираем роль **Active Directory Domain Services**.
3. Жмем **Install** и ждем окончания.

??? 8: ????????? ???? (Promote)

1. Нажимаем на желтый треугольник -> **Promote this server to a domain controller**.
2. **Вкладка Deployment Configuration:**
   - ВЫБИРАЕМ ПЕРВЫЙ ПУНКТ: **Add a domain controller to an existing domain** (Добавить контроллер в существующий домен).
   - В поле **Domain** напишите: `ad.mysite.ru` (если не заполнилось само).
   - Внизу раздел **Credentials** (Учетные данные). Нажмите кнопку **Change...**.
   - Введите логин/пароль администратора домена, который вы создали на первом сервере:
     - User: `MYSITE\Administrator` (или просто `Administrator`, он сам подставит домен).
     - Password: Ваш пароль.
   - Жмите Next.
3. **Вкладка Domain Controller Options:**
   - Галочки **DNS Server** и **Global Catalog (GC)** должны стоять.
   - Введите пароль DSRM (для восстановления) — такой же, как на первом, чтобы не путаться.
   - Жмите Next.
4. **Вкладка DNS Options:** Пропускаем (Next).
5. **Вкладка Additional Options:**
   - **Replicate from:** Выберите `SRV-DC01.ad.mysite.ru` (или Any domain controller). Лучше выбрать явно первый сервер.
   - Жмите Next.
6. **Paths:** Оставляем как есть. Next.
7. **Prerequisites Check:** Ждем зеленую галочку. Жмем **Install**.

Сервер перезагрузится.

??? 9: ????????? ????????? DNS (????????? ?????)

Когда **SRV-DC02** перезагрузится и вы войдете в систему (уже под доменным админом `MYSITE\Administrator`), нам нужно настроить «перекрестное опыление» DNS, чтобы серверы страховали друг друга. Это Best Practice.

1. Зайдите на **SRV-DC01**:
   - Сетевые настройки -> IPv4.
   - Preferred DNS: `127.0.0.1`

- Alternate DNS: `10.177.178.253` (Указываем на второй сервер).

2. Зайдите на **SRV-DC02**:
   - Сетевые настройки -> IPv4.
   - Preferred DNS: `10.177.178.254` (Указываем на первый сервер).
   - Alternate DNS: `127.0.0.1` (Указываем на себя как запасной вариант).

Теперь нужно сделать так, чтобы домен «дышал» (синхронизировал время) и видел внешний мир (интернет), а затем построим правильный скелет организации.

??? 10: ????????? DNS Forwarders (????? ??????? ????????)

Сейчас ваши серверы знают только о себе. Если спросить у них `google.com`, они не ответят. Нужно настроить пересылку запросов.

Сделайте это **на обоих серверах** (сначала SRV-DC01, потом SRV-DC02), чтобы настройки были идентичны:

1. Нажмите `Win + R`, введите **`dnsmgmt.msc`** (Диспетчер DNS).
2. В дереве слева кликните правой кнопкой мыши по имени вашего сервера -> **Properties** (Свойства).
3. Вкладка **Forwarders** (Серверы пересылки).
4. Нажмите **Edit...**.
5. Добавьте туда надежные внешние DNS. Например:
   - `77.88.8.8` (Yandex)
   - `8.8.8.8` (Google)
6. Нажмите OK, затем еще раз OK.

Проверка: Откройте командную строку (CMD) и введите

```
powershell Resolve-DnsName google.com
```

Если вам вернулся IP-адрес гугла — всё настроено верно.

??? 11: ????????? ??????? (NTP) — ???????? ??? ??

Виртуальные машины очень любят «убегать» по времени. Если время уйдет на 5 минут, никто не сможет войти в домен (Kerberos заблокирует вход).

Настроим **SRV-DC01** (так как он сейчас главный — PDC Emulator) как источник точного времени для всей сети.

1. На **SRV-DC01** запустите командную строку (CMD) или PowerShell **от имени администратора**.
2. Выполните следующие команды по очереди (можно копировать):

```
w32tm /config /manualpeerlist:"0.ru.pool.ntp.org 1.ru.pool.ntp.org" /syncfromflags:manual
/reliable:yes /update
```

(Эта команда говорит: бери время из интернета и скажи всем в сети, что твоему времени можно верить).

1. Перезапустите службу времени:

```
net stop w32time && net start w32time
```

1. Принудительная синхронизация:

```
w32tm /resync
```

На втором сервере (DC02) это делать **не надо**. Он сам по умолчанию будет тянуть время с DC01.

??? 12: ???????? ?????????? ????????? (OU)

Наводим порядок в иерархии.

1. Нажмите Win + R, введите **dsa.msc**. Откроется оснастка **«Пользователи и компьютеры Active Directory»** (Active Directory Users and Computers).
2. В верхнем меню нажмите **Вид** (View) -> **Дополнительные компоненты** (Advanced Features).
   - Это нужно, чтобы видеть системные вкладки.
3. Нажмите правой кнопкой мыши (ПКМ) по вашему домену ad.mysite.ru -> **Создать** (New) -> **Подразделение** (Organizational Unit).
4. Назовите его **MYSITE_Corp**.
   - Убедитесь, что стоит галочка **«Защитить контейнер от случайного удаления»** (Protect container from accidental deletion).
   - Нажмите OK.

Теперь внутри MYSITE_Corp создайте структуру папок (ПКМ по MYSITE_Corp -> Создать -> Подразделение):

1. Создайте подразделение **_Admins** (для админов).
2. Создайте подразделение **Groups** (для групп).
3. Создайте подразделение **HeadOffice** (Головной офис).
4. Внутри папки **HeadOffice** создайте еще две:
   - **Users** (Пользователи)
   - **Computers** (Компьютеры)

??? 13: ???????? ?????? ?????-??????

Работаем в папке MYSITE_Corp -> _Admins.

1. ПКМ по пустому месту -> **Создать** (New) -> **Пользователь** (User).
2. **Поля:**
   - **Имя** (First name): Ваше имя (например, Ivan).
   - **Имя входа пользователя** (User logon name): Рекомендую **adm.ivanov**.
   - Нажмите **Далее** (Next).
3. **Пароль:**
   - Придумайте сложный пароль.
   - Поставьте галочку **«Срок действия пароля не ограничен»** (Password never expires).
   - Снимите галочку «Требовать смены пароля при следующем входе» (User must change password at next logon).
   - Нажмите **Далее** (Next) -> **Готово** (Finish).
4. **Выдача прав:**
   - Нажмите ПКМ по созданному пользователю adm.ivanov -> **Свойства** (Properties).
   - Вкладка **Член групп** (Member Of).
   - Нажмите **Добавить** (Add).
   - В поле ввода пишите русские названия групп (можно по очереди):
     - **Администраторы домена** (Domain Admins) -> нажмите **Проверить имена** (Check Names) -> OK.
     - **Администраторы предприятия** (Enterprise Admins) -> Проверить имена -> OK.
     - **Администраторы схемы** (Schema Admins) -> Проверить имена -> OK.
   - Нажмите OK, чтобы сохранить.

Теперь у вас есть полные права.

Сейчас мы сделаем следующее:

1. Создадим общую папку на сервере.
2. Настроим **Групповую Политику (GPO)**, чтобы у всех сотрудников автоматически появлялся **Сетевой Диск Z:**.

3. Подготовим и введем тестовый компьютер в домен, чтобы убедиться, что всё сработало.

??? 14: ???????? ????? ????? (File Share)

Чтобы подключать диск, нужно чтобы было что подключать. Создадим папку на **SRV-DC01**.

1. Откройте Проводник (File Explorer) -> Диск C.
2. Создайте папку **CompanyData**.
3. Нажмите по ней ПКМ -> **Свойства** (Properties) -> вкладка **Доступ** (Sharing).
4. Нажмите **Расширенная настройка** (Advanced Sharing).
5. Поставьте галочку **Открыть общий доступ** (Share this folder).
6. Имя общего ресурса оставьте CompanyData.
7. Нажмите **Разрешения** (Permissions).
   - Сейчас там стоит Все (Everyone) — Чтение.
   - Для теста поставьте галочку **Полный доступ** (Full Control) -> OK -> OK.
   - (В продакшене права настраиваются тоньше, через вкладку Безопасность/Security, но для теста нам хватит).
8. Нажмите Закрыть (Close).

Теперь путь к папке: \\SRV-DC01\CompanyData.

??? 15: ???????? ????????? ???????? (GPO) ??? ????? Z

Теперь скажем домену: "Каждому, кто входит в систему, подключай эту папку как диск Z".

1. На **SRV-DC01** нажмите Win + R -> введите **gpmc.msc** (Управление групповой политикой / Group Policy Management).
2. Раскройте дерево: Forest: ad.misyte.ru -> Domains -> ad.mysite.ru -> **MYSITE_Corp**.
   - Мы будем привязывать политику сюда, чтобы она работала на всех внутри вашей компании.
3. ПКМ по папке MYSITE_Corp -> **Создать объект GPO в этом домене и связать его...** (Create a GPO in this domain, and Link it here...).
4. Назовите политику: **GPO_Drive_Maps**. Нажмите OK.
5. Теперь политика появилась в списке справа. Нажмите по ней ПКМ -> **Изменить** (Edit).
   - Откроется редактор политик.

Настройка внутри редактора:

1. Идем по пути:
   Конфигурация пользователя (User Configuration) -> **Настройка** (Preferences) -> **Конфигурация Windows** (Windows Settings) -> **Сопоставления дисков** (Drive Maps).
2. ПКМ по пустому месту справа -> **Создать** (New) -> **Сопоставленный диск** (Mapped Drive).
3. **Вкладка Общие (General):**
   - **Действие** (Action): Выберите **Обновить** (Update). (Это самый надежный вариант).
   - **Расположение** (Location): `\\SRV-DC01\CompanyData`
   - **Восстановить подключение** (Reconnect): Поставьте галочку.
   - **Метка** (Label as): Напишите `Общая папка`.
   - **Буква диска** (Drive Letter): Выберите **Z:**.
4. Нажмите OK.

Закройте редактор политик. GPO готова и уже привязана.

??? 16: ???? ??????? ? ?????

Теперь переходим на нашу машину (Windows 10/11).

1. Настройка DNS (Пока руками. По правильному нужно на `SRV-DC01` развернуть DHCP сервер. Но пока мы этого не делали и DHCP у нас идет от Роутера):

1. Параметры сети -> Ethernet -> Свойства IP версии 4.
2. **IP-адрес:** Оставьте автоматический (от Роутера).
3. **DNS-серверы:**
   - Предпочтительный: `10.177.178.254` (Ваш DC1).
   - Альтернативный: `10.177.178.253` (Ваш DC2).
4. Нажмите OK.

Проверка: Откройте командную строку на клиенте и введите `ping ad.misyte.ru`. Если пинг идет — вы видите контроллер.

2. Вступление в домен:

1. Откройте «Этот компьютер» -> Свойства -> **Дополнительные параметры системы** (или просто поиск: "Присоединение к домену").
2. Нажмите **Изменить...** (Change...) на вкладке Имя компьютера.
3. Переключите точку на **Домен** (Domain).
4. Введите: **ad.jinnvl.ru**.
5. Нажмите OK.
6. Спросит логин/пароль. Введите данные вашего супер-адмена:
   - Логин: `adm.ivanov` (или `MYSITE\adm.ivanov`)
   - Пароль: Ваш пароль.

7. Должно появиться окно: **«Добро пожаловать в домен ad.misyte.ru»**.
8. Перезагрузите компьютер.

??? 17: ???????????? ?????????? ? ?????????? OU (?????!)

Пока компьютер перезагружается, вернитесь на сервер **SRV-DC01**.

По умолчанию все новые компьютеры попадают в папку Computers (стандартную). А наши политики (в том числе будущие) настроены на структуру MYSITE_Corp. Надо перенести компьютер.

1. Откройте **dsa.msc** (Пользователи и компьютеры).
2. Зайдите в папку **Computers** (обычную). Там должен лежать ваш новый ПК.
3. Нажмите по нему ПКМ -> **Переместить** (Move).
4. Выберите: MYSITE_Corp -> HeadOffice -> **Computers**.
5. Нажмите OK.

??? 18: ?????? ??????

Возвращаемся к клиентскому компьютеру (он перезагрузился).

1. **Вход в систему:**
   - Нажмите «Другой пользователь» (Other User).
   - Вводите логин: **adm.ivanov** (ваш админ) или создайте в AD обычного юзера test.user в папке Users (внутри HeadOffice) и войдите под ним.
   - Введите пароль.
2. Дождитесь входа ("Привет", "Мы подготавливаем для вас все...").
3. Откройте **"Этот компьютер"**.

Если все сделано правильно, вы увидите Сетевой диск Z: (Общая папка).

ВАЖНО: В продакшене данные всегда хранят на отдельном диске (D:, E:) или вообще на отдельном NAS. Это тема другой статьи. Но раз у нас мы сделали на диске C:, мы должны **жестко ограничить** размер этой папки, чтобы пользователи не "убили" сервер.

Для этого в Windows Server есть штатный инструмент — **FSRM (File Server Resource Manager)**. Он позволит сделать так, чтобы пользователи видели, например, только 5 ГБ, даже если на диске свободно 100 ТБ.

Давайте настроим его. Это Best Practice.

??? 19: ????????? ???? FSRM

1. На **SRV-DC01** откройте Добавление ролей и компонентов
2. Жмите Next до выбора ролей.
3. Разверните ветку:
   File and Storage Services -> **File and iSCSI Services**.
4. Поставьте галочку **File Server Resource Manager** (Диспетчер ресурсов файлового сервера).
   - Согласитесь добавить компоненты.
5. Жмите **Install**. (Перезагрузка обычно не требуется).

??? 20: ???????? ??????? ?????

Теперь скажем серверу: "Папка CompanyData не может быть больше 5 ГБ".

1. В Server Manager нажмите **Tools** (Средства) -> **File Server Resource Manager** (Диспетчер ресурсов файлового сервера).
2. В меню слева раскройте **Quota Management** (Управление квотами) -> **Quotas** (Квоты).
3. Справа нажмите **Create Quota...** (Создать квоту).
4. **Quota path** (Путь к квоте): Нажмите Browse и выберите вашу папку `C:\CompanyData`.
5. **Параметры:**
   - Выберите **Create quota on path** (Создать квоту по пути).
   - Ниже выберите шаблон: **Limit to 5 GB** (или любой другой).
   - ИЛИ выберите **Define custom quota properties** -> кнопка **Custom Properties**, чтобы задать свой размер (например, 2 GB).
   - **Важно:** Убедитесь, что выбран тип **Hard quota** (Жесткая квота).
     - Hard: Запрещает запись, если место кончилось.
     - Soft: Просто шлет уведомление админу, но писать разрешает. Нам нужен Hard, чтобы спасти диск C.
6. Нажмите **Create**.

??? 21: ????????

1. Идите на клиентский компьютер (Windows 10).
2. Откройте "Этот компьютер".
3. Нажмите F5 (Обновить).

Результат:
Полоска диска Z: моментально изменится. Теперь там будет написано: "Свободно 2 ГБ из 2 ГБ" (или сколько вы поставили).

Пользователи будут думать, что это отдельный жесткий диск такого размера.

P.S. Этот же инструмент (FSRM) умеет запрещать сохранять MP3 и AVI файлы в рабочую папку (File Screening), что очень полезно в офисе (но об этом потом).

????: ???????????? ????????? ??????? (Best Practice)

Главный принцип: Одна политика — одна задача. Разделяем настройки Компьютера (железа) и Пользователя (людей).

1. ???????? ??????????? (Naming Convention)

Мы используем схему: `[ТИП]_[ОБЛАСТЬ]_[ОПИСАНИЕ]`

- **GPO_C_** (Computer) — применяется к компьютерам (драйверы, безопасность, время). Требует перезагрузки.
- **GPO_U_** (User) — применяется к людям (диски, ярлыки, принтеры). Применяется при входе.

2. ?????? ??????? (??? "??????")

Вам нужно создать (или переименовать текущие) 4 основные политики и привязать их к корню организации (`MYSITE_Corp`).

??? ????????	**?? ??? ????????**	**??????**
GPO_C_System_Base	?????????: ??????? ????, ???????? ????, ??????????????.	**??????????? ??????**
GPO_C_Security_Base	???????????: LAPS, UAC, ????? ??????, Firewall.	??????? ??????
GPO_U_DriveMaps_Common	??????????? ????? ?????? (Z:).	??? ?????????
GPO_U_Browser_Settings	????????? Chrome/Edge (????????? ????????).	??????? ??????

3. ????????? GPO_C_System_Base (????????? ?????????)

Это самая важная политика для стабильности работы "железа". В ней мы фиксируем полученный опыт.

Откройте: `gpmc.msc` -> `GPO_C_System_Base` -> Изменить.

?) ??????? ???? (????? "?????? ?????????")

Используем Scheduled Task, так как это самый надежный способ.

1. Путь: **Конфигурация компьютера** -> **Настройка** -> **Параметры панели управления** -> **Назначенные задания** (Scheduled Tasks).
2. ПКМ -> Создать -> **Запланированное задание (как минимум Windows 7)**.
3. **Вкладка "Общие":**
   - Действие: **Обновить**.
   - Имя: `TimeZone_AutoFix`.
   - Учетная запись: **`SYSTEM`** (Система).
   - Выполнять **вне зависимости от регистрации пользователя**.
   - Галочка: **Выполнить с наивысшими правами** (ОБЯЗАТЕЛЬНО!).
4. **Вкладка "Триггеры":**
   - Создать -> Начать задачу: **При запуске** (At startup) -> Включено.
5. **Вкладка "Действия":**
   - Создать -> Запуск программы.
   - Программа: `C:\Windows\System32\tzutil.exe`
   - Аргументы: `/s "Russian Standard Time"` (или ваш пояс).
6. **Вкладка "Условия":**
   - **Снять** галочку "Запускать только при питании от электросети" (иначе на ноутбуках не сработает).

?) ???????? ???? (????????? ??? SSD)

Чтобы политики успевали примениться до появления рабочего стола.

1. Путь: **Конфигурация компьютера** -> **Политики** -> **Административные шаблоны** -> **Система** -> **Вход в систему** (Logon).
2. Настройка: **Всегда ждать сеть при запуске компьютера и входе в систему** (Always wait for the network...).
3. Значение: **Включено** (Enabled).

---

4. ????????? GPO_U_DriveMaps_Common

Здесь у вас уже настроен диск Z:. Просто убедитесь, что настройки верные.

1. Путь: **Конфигурация пользователя** -> **Настройка** -> **Конфигурация Windows** -> **Сопоставления дисков**.
2. Диск Z:
   - Действие: **Обновить**.
   - Путь: `\\SRV-DC01\CompanyData` (или IP).
   - Галочка: **Восстановить подключение**.
   - На будущее: Если нужно скрыть диск от бухгалтерии, используйте вкладку "Общие параметры" -> **Нацеливание на уровень элемента** (Item-level targeting).

---

5. ??????? ??????????? (Link Order)

В `gpmc.msc` выберите папку `MYSITE_Corp`. Справа список политик. Расставьте приоритет (стрелками):

1. `GPO_U_DriveMaps_Common`
2. `GPO_U_Browser_Settings`
3. `GPO_C_Security_Base`
4. `GPO_C_System_Base`
5. `Default Domain Policy` (Всегда последняя).

?????? ?????? ?????????? ???? ???????? ????????

Вот список того, что **обязано** быть в компании, которая не хочет быть взломанной через неделю.

---

1. ??????????? ??????? (Default Domain Policy)

Где: `Default Domain Policy` -> Изменить.
Путь: Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Политики учетных записей.

Мы это уже обсуждали, но давайте зафиксируем **Стандарт 2024+**:

1. **Политика паролей:**
   - **Минимальная длина: 10-12 символов**. (8 уже взламывают быстро).
   - **Сложность: Включено** (Буквы + Цифры).

- **Срок действия: 90 или 180 дней**. (Заставлять менять чаще — вредно, люди будут писать пароль на стикере).
- **Журнал паролей: 24 пароля** (Чтобы не меняли "Пароль1" на "Пароль2" и обратно).

2. **Политика блокировки (Защита от брутфорса):**
   - **Порог блокировки: 5-10 попыток**.
   - **Время блокировки: 30 минут**. (Этого хватит, чтобы хакер устал ждать, а юзер попил кофе).

---

2. «???????? ???????» (GPO_C_Security_Base)

Где: `GPO_C_Security_Base` -> Изменить.
Привязка: Корень `MYSITE_Corp`.

В этой политике мы настраиваем "броню" рабочих станций.

?) ????? (???, ???, ??????)

Если что-то случится, вы должны знать **кто** это сделал. По умолчанию Windows пишет мало логов.

Путь: Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Политика аудита.

Включите (Success & Failure / Успех и Отказ) для:

1. **Аудит входа в систему (Logon Events):** Кто вошел в комп?
2. **Аудит управления учетными записями:** Кто создал нового юзера или сменил пароль?
3. **Аудит доступа к объектам:** (Только "Отказ"). Кто ломился в папку, куда ему нельзя?

?) ????? ????????? ???????????????? (??? ????? ????????)

Пользователь **НЕ должен** быть администратором на своем компьютере. Если Галина — админ, то вирус, который она поймает, тоже станет админом.

Путь: Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Группы с ограниченным доступом (Restricted Groups).

1. ПКМ -> Добавить группу.
2. Выбираем: **Administrators** (или Администраторы).
3. В окне "Члены этой группы" (Members of this group) добавляем:

- MYSITE\Domain Admins (Админы домена).
- MYSITE\adm.ivanov (Ваш супер-админ).
- (Опционально): MYSITE\TechSupport.

4. **Важно:** Всех, кого нет в этом списке (например, Галину), политика **вышвырнет** из админов принудительно. Это жесткая зачистка.

3. «??????? ? ???????» (GPO_C_System_Base)

Где: GPO_C_System_Base -> Изменить.
В этой политике мы уже настроили Время. Добавим сюда правила поведения "Железа".

?) ?????? ????? (Power Management)

В офисе компьютеры (десктопы) не должны спать. Иначе вы не сможете подключиться к ним ночью для обновлений.

Путь: Адм. шаблоны -> Система -> Управление электропитанием.

1. Выбрать активную схему питания: **Высокая производительность** (High Performance).
2. Параметры спящего режима -> **Разрешать ждущий режим (Sleep)**: Отключено (для питания от сети).

?) ?????????? Windows (Windows Update)

1. Открываем политику:

- gpmc.msc -> GPO_C_System_Base -> **Изменить** (Edit).

2. Идем по пути:
Конфигурация компьютера -> **Политики** -> **Административные шаблоны** -> **Компоненты Windows** -> **Оптимизация доставки** (Delivery Optimization).

Здесь нам нужно изменить всего 3-4 настройки.

1. ????? ?????????? (????? ??????)

Это настройка определяет, у кого компьютеры могут брать файлы.

- **Настройка: Режим скачивания** (Download Mode).
- **Значение:** Включено.
- **Параметр:** Выберите **Группа (2)** (Group).
  - Почему это Best Practice: Режим "Группа" использует Active Directory. Компьютеры будут меняться файлами только с теми, кто находится в том же **домене** И в том же **сайте AD**.

- На будущее: Когда у вас появится филиал и вы создадите для него отдельный Сайт в AD (как мы обсуждали в начале), компьютеры филиала будут качать друг у друга, а не тянуть трафик через VPN из главного офиса. Это происходит автоматически.

2. ????????? ???? (????? ????? ???? ??????)

По умолчанию Windows быстро удаляет скачанные файлы. Нам нужно, чтобы они лежали подольше и раздавались другим.

- **Настройка: Максимальный срок хранения кэша (в секундах)** (Max Cache Age).
- **Значение:** Включено.
- **Параметр:** Введите **604800** (это 7 дней).
  - Логика: Если кто-то был в отпуске неделю, он придет и скачает обновление с соседа, а не из интернета.

3. ??????????? ?????????? ? ????? (???????? ?????? ??????)

Не стоит заставлять старый ноутбук с забитым диском раздавать файлы всему офису — он затормозит.

- **Настройка: Минимальный размер диска для использования кэширования** (Minimum Disk Size to use Peering).
- **Значение:** Включено -> **32 ГБ** (или больше, если у вас все на 256+).
- **Настройка: Минимальный объем ОЗУ (включая кэширование)** (Minimum RAM capacity).
- **Значение:** Включено -> **4 ГБ**.

4. ?????? ??????????? (????? ?? ???????? ????)

Обычно по локалке скорость не режут, но для интернета стоит подстраховаться.

- **Настройка: Максимальная пропускная способность скачивания на переднем плане** (Max Download Bandwidth for Foreground).
  - Примечание: Foreground — это когда юзер нажал кнопку "Проверить обновления".
  - Значение: **0** (Без ограничений) или **90%**.
- **Настройка: Максимальная пропускная способность скачивания в фоновом режиме** (Background).
  - Примечание: Это когда комп качает сам по себе тихонько.
  - Значение: **Включено** -> **80%** (Оставьте 20% для почты и ютуба).

Теперь нужно убедиться, что компьютеры вообще знают, что им надо обновляться. (Мы это уже затрагивали, но давайте проверим в той же GPO).

Путь: ... -> **Компоненты Windows** -> **Центр обновления Windows**.

1. **Настройка автоматического обновления** (Configure Automatic Updates).
   - **Включено.**
   - **3 - Автоматическая загрузка и уведомление об установке** (Auto download and notify for install) — Это лучший вариант для рабочих станций.
   - ИЛИ **4 - Автоматическая загрузка и установка по расписанию** (Auto download and schedule the install).
   - Важно: Если выберете 4, ставьте время (например, 22:00) и галочку "Install during automatic maintenance".
2. **Период активности** (Turn off auto-restart for updates during active hours) — Опционально, но полезно.
   - Включите и задайте с 08:00 до 18:00.
   - Windows **не будет** перезагружаться сама в это время, даже если скачала критическое обновление.

После того как вы примените политику (`gpupdate /force` + перезагрузка) и пройдет пару дней (выйдут новые обновления), вы можете проверить эффективность.

На любом клиентском компьютере (Windows 10/11):

1. Откройте **PowerShell**.
2. Введите команду:
   codePowershell
   ```
   Get-DeliveryOptimizationStatus
   ```

Что смотреть в выводе:
Вам интересна статистика внизу.

- **TotalBytesDownloaded:** Сколько всего скачано.
- **FromHttp:** Сколько скачано из Интернета (с серверов Microsoft).
- **FromPeers:** Сколько скачано с соседей (LAN).

Если через месяц вы увидите, что `FromPeers` > 50-70%, значит, вы сэкономили кучу трафика, и ваша система работает идеально.

Задание:
Настройте эти 4 пункта в `GPO_C_System_Base`.
Это всё, что нужно для современной системы обновлений без лишних серверов.

Revision #5
Created 13 December 2025 13:22:08 by Admin
Updated 13 December 2025 20:18:00 by Admin