Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Windows Server 2022: первоначальная настройка для офиса

Наш регламент ввода сервера в строй: AD DS, DNS/DHCP, RDS, безопасность и бэкап за один день

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Новый сервер, введённый «как есть», месяцами работает с одним контроллером домена, без бэкапа, с RDP наружу и легаси-SMB на старых узлах сети — до первого инцидента. Разбираем наш регламент первоначальной настройки Windows Server 2022: выбор редакции, Server Core, два DC, отказоустойчивые DNS/DHCP, Windows LAPS, шифрование дисков и проверенное восстановление — всё, что закрываем в первую неделю.

Почему это важно бизнесу

- Один DC — одна точка отказа: при его сбое встают вход в 1С, почту и файлы у всего офиса
- Ошибка с редакцией — переплата в разы: Datacenter нужен только при плотной виртуализации
- Открытый RDP и SMBv1 — типовой вход шифровальщика; без внешней копии бэкапа это потеря данных
- RDS без активированных CAL остановит работу бухгалтерии в 1С ровно через 120 дней

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

14.10.2031

конец extended support Windows Server 2022 (LTSC) — платформу закладываем на годы вперёд

Microsoft Lifecycle

16 ядер

минимум core-лицензий Standard на сервер; при полном покрытии ядер — право на 2 ВМ Hyper-V

лицензирование WS2022

2 DC

минимум контроллеров домена в каждом нашем внедрении, второй — на отдельном железе/гипервизоре

наш стандарт

7+7 дней

DNS aging: NoRefresh + Refresh; scavenging вычищает устаревшие записи только после 14 дней

по докам DNS Server

120 дней

grace-период RD Session Host — до его конца активируем сервер лицензий и RDS CAL Per User

по докам RDS

5%

ReservePercent hot-standby DHCP-failover: резерв адресов на standby-сервере, MaxClientLeadTime 1 час

по докам DHCP Server

РЕАЛИЗАЦИЯ 1 ИЗ 3

Домен с нуля: два DC на Server Core

Что настраиваем

Контроллеры домена DC01/DC02: роли AD DS + DNS, Server Core, управление через WAC/RSAT

Как мы это делаем

1. Server Core + sconfig: имя, статический IP, NTP через w32tm /config /manualpeerlist /syncfromflags:manual /reliable:yes, полный цикл обновлений до продуктива
2. Install-WindowsFeature AD-Domain-Services, затем Install-ADDSForest с -DomainMode/-ForestMode WinThreshold — функциональный уровень 2016, максимум для WS2022
3. Второй DC: Install-ADDSDomainController -InstallDns:$true на отдельном железе или гипервизоре; DSRM-пароль уникальный и уходит в сейф паролей
4. Через 30 минут — repadmin /replsummary, dcdiag /v и Get-ADReplicationFailure: репликация чистая до передачи в эксплуатацию
5. Windows LAPS (в WS2022 с обновления 11.04.2023): Update-LapsADSchema, затем Set-LapsADComputerSelfPermission на OU серверов и рабочих станций

РЕЗУЛЬТАТ

Домен переживает отказ любого одного контроллера: аутентификация, GPO и DNS работают со второго DC. Server Core сокращает поверхность атаки, а весь регламент воспроизводится скриптом за 2–3 часа.

КЛЮЧЕВОЙ НЮАНС

Для WS2022 максимальный функциональный уровень — Windows Server 2016 (WinThreshold), уровня «2022» не существует. DSRM-пароль фиксируем на этапе установки — при аварии искать его поздно.

РЕАЛИЗАЦИЯ 2 ИЗ 3

DNS и DHCP: отказоустойчивая адресация

Что настраиваем

Роли DNS и DHCP на обоих контроллерах домена, failover-связка между ними

Как мы это делаем

1. DNS: Add-DnsServerForwarder на проверенные резолверы; обратные зоны Add-DnsServerPrimaryZone -NetworkId … -ReplicationScope Domain -DynamicUpdate Secure
2. Aging по докам: Set-DnsServerScavenging -ScavengingState $true, NoRefresh 7 дней + Refresh 7 дней; scavenging включаем только на одном DC
3. DHCP: Install-WindowsFeature DHCP, авторизация в AD через Add-DhcpServerInDC, scope с исключениями под шлюз, принтеры и статические узлы
4. Отказоустойчивость: Add-DhcpServerv4Failover в режиме hot standby — ReservePercent 5 (по умолчанию), MaxClientLeadTime 1 час, партнёр — второй DC

РЕЗУЛЬТАТ

Адресация и разрешение имён переживают отказ любого сервера: standby-DHCP выдаёт адреса из 5%-резерва, зоны реплицируются в AD, устаревшие записи чистятся сами — Kerberos не спотыкается о мёртвые PTR.

КЛЮЧЕВОЙ НЮАНС

Scavenging включаем только после полного цикла NoRefresh+Refresh (14 дней), иначе рискуем вычистить живые записи без свежего timestamp; статические записи проверяем отдельно.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Безопасность и бэкап первого дня

Что настраиваем

Все серверы внедрения + RDS-хост для 1С + выделенная ВМ Windows Admin Center

Как мы это делаем

1. SMBv1: Uninstall-WindowsFeature -Name FS-SMB1 -Remove, контроль Get-SmbServerConfiguration; файрвол на всех трёх профилях, RDP — только из LAN/VPN и строго с NLA
2. Defender: Set-MpPreference -EnableControlledFolderAccess Enabled; тома — Install-WindowsFeature BitLocker, затем Enable-BitLocker -EncryptionMethod XtsAes256 -TpmProtector
3. RDS-хост: роли RDS-RD-Server + RDS-Licensing, Set-RDLicenseConfiguration -Mode PerUser; CAL активируем до конца 120-дневного grace-периода
4. Windows Server Backup: политика с Add-WBSystemState, цель — NAS вне домена; ежеквартальное тестовое восстановление в изолированной среде
5. WAC 2511 (modernized gateway на ASP.NET Core) на отдельной ВМ — установка на DC не поддерживается; доступ только из админской VLAN по HTTPS

РЕЗУЛЬТАТ

Сервер защищён с первого дня: легаси-протоколы закрыты, диски зашифрованы, админы под именными учётками, пароль Administrator ротирует LAPS. Восстановление из бэкапа — отработанная процедура, а не надежда.

КЛЮЧЕВОЙ НЮАНС

В режиме Per User исчерпание CAL не блокируется так жёстко, как Per Device, но grace-период один — 120 дней: напоминание об активации ставим в день развёртывания роли.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Datacenter там, где хватает Standard**
  Datacenter окупается при плотной виртуализации (10+ ВМ на хост). Для AD, файлов и 1С берём Standard: 16 core-лицензий и право на 2 ВМ Hyper-V.

- ✕ **Единственный контроллер домена**
  Отказ DC останавливает вход в 1С, почту и файлы всему офису. Всегда два DC на разном железе + System State обоих в расписании бэкапа.

- ✕ **DC совмещён с 1С и файловым сервером**
  Роли конкурируют за RAM и требуют разных окон перезагрузки. DC выносим в отдельную ВМ Server Core — Standard уже даёт две гостевые ОС.

- ✕ **IPv6 «отключён для порядка»**
  Полное отключение IPv6 Microsoft не поддерживает — ломает часть служб. Нужен приоритет IPv4 — ставим DisabledComponents=0x20, а не снимаем привязку.

- ✕ **RDS живёт на grace-периоде**
  Через 120 дней хост перестаёт пускать пользователей без CAL. Активируем сервер лицензий и Per User CAL сразу при развёртывании роли.

- ✕ **Scavenging включён в день установки**
  Без выжидания цикла NoRefresh+Refresh (7+7 дней) чистка может удалить живые записи. Включаем aging на зоне, scavenging — через 14 дней и на одном DC.

- ✕ **Бэкап лежит рядом с продуктивом**
  Шифровальщик добирается до копий на том же диске и шарах. Копия — на NAS вне домена в другом VLAN, отдельная учётка, тест раз в квартал.

- ✕ **Один пароль локальных админов на всё**
  Компрометация одной машины открывает все. Windows LAPS (в WS2022 с 11.04.2023) ротирует пароль каждого сервера и хранит его в AD под ACL.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Два DC на разном железе, репликация проверена repadmin /replsummary
- SMBv1 отключён, файрвол на всех профилях, RDP не смотрит в интернет
- Ежедневный бэкап System State + копия вне домена

НОРМАЛЬНО

- Server Core на DC/DNS/DHCP, управление через WAC и RSAT
- DHCP-failover hot standby + DNS aging/scavenging 7+7 дней
- Windows LAPS и именные admin-учётки вместо общего пароля
- BitLocker XtsAes256 с TPM-протектором на системных томах

ХОРОШО

- WAC 2511 на выделенной ВМ (не на DC) в админ-VLAN с доверенным сертификатом
- RDS Per User CAL активированы в день развёртывания, а не на grace
- Ежеквартальное тестовое восстановление DC в изолированной среде
- Мониторинг репликации AD, служб DNS/DHCP и дисков с алертами

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] В домене минимум два контроллера, и repadmin /replsummary проходит без ошибок?
- [ ] SMBv1 отключён на всех серверах, файрвол активен на всех трёх профилях?
- [ ] RDP недоступен из интернета напрямую — только через VPN или шлюз с NLA?
- [ ] Пароли локальных администраторов ротируются Windows LAPS, а не одинаковы везде?
- [ ] Бэкап System State идёт по расписанию, и копия хранится вне домена?
- [ ] Тестовое восстановление из бэкапа проводилось за последние 3 месяца?
- [ ] DHCP переживёт отказ одного сервера — failover-связка настроена и проверена?
- [ ] RDS-лицензирование активировано, а не доживает 120-дневный grace-период?
- [ ] BitLocker включён на системных томах, ключи восстановления сохранены в AD?
- [ ] NTP на PDC-эмуляторе настроен на внешние источники (w32tm /reliable:yes)?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем Windows Server 2022 под ключ: AD DS, DNS/DHCP, RDS, GPO — с документацией и паролями в сейфе
- Проводим аудит существующей инфраструктуры: репликация, безопасность, бэкапы — с письменным отчётом
- Подбираем редакцию и лицензии (Standard/Datacenter, RDS CAL) без переплаты под ваш профиль нагрузки
- Настраиваем резервное копирование с внешней копией и регулярными тестовыми восстановлениями
- Берём серверы на постоянное обслуживание: обновления, мониторинг, реагирование на инциденты

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 Windows Server 2022 — Microsoft Lifecycle (learn.microsoft.com — 2026)

02 Install-ADDSForest (ADDSDeployment) (learn.microsoft.com — 2025-ps)

03 AD DS Functional Levels (learn.microsoft.com — 2026)

04 DNS Aging and Scavenging in Windows Server (learn.microsoft.com — 2026)

05 Add-DhcpServerv4Failover (DhcpServer) (learn.microsoft.com — 2025-ps)

06 License RDS with Client Access Licenses (CALs) (learn.microsoft.com — 2026)

07 Windows LAPS overview (learn.microsoft.com — 2026)

08 Detect, enable and disable SMBv1/v2/v3 (learn.microsoft.com — 2026)

09 Windows Admin Center release history (learn.microsoft.com — v2511)

Основано на официальной документации продуктов и нашей практике внедрения.