Восстановление после переустановки Windows

English · Руководство

Программа и выбранная DATA должны сохраниться вне форматируемого диска. Для каждой машины используется её собственная DATA. Приватные ключи SSHD в этой папке идентифицируют сервер; клиентские ключи дают право входа на него.

До форматирования C:

На каждой машине обновить программу, выбрать её DATA и один раз выполнить **SETUP → SSHD**, подтвердив UAC. Этот шаг сохраняет действующие пары `ProgramData\ssh\ssh_host_*` в `DATA\Tunnel\SSHD` вместе с манифестом. Он также проверяет пары, ограничивает ACL и настраивает входящие ключи CLIENTS. Убедиться, что шаг завершился успешно, затем сохранить всю DATA.

Наличие одних CLIENTS, Export Keys или `known_hosts` не заменяет этот шаг: прежний приватный хост-ключ нельзя восстановить из отпечатка или публичной части. Неполные `SSHD.pending-*` не считаются сохранённой идентичностью.

После переустановки

1. Вернуть программу и DATA, выбрать **DATA FOLDER**.
2. Выбрать **SETUP → RESTORE → Восстановить эту машину**, подтвердить UAC. При необходимости перенести обновлённые псевдонимы из DATA выбрать вариант **Восстановить и заменить SSH config**. Он сохраняет одну прежнюю копию `~/.ssh/config.before-restore`; обычный вариант существующий config сохраняет.
3. Дождаться таблицы SSH/SFTP. Перезапустить окно для перечитывания профиля.

RESTORE устанавливает недостающий cloudflared при наличии таких маршрутов, импортирует ключи, исправляет потерянные пути и запускает SSHD. Сохранённые хост-ключи возвращаются

до установки компонента и первого запуска службы. Если живой и сохранённый ключ отличаются, шаг прекращается: обе версии остаются. Без сохранённой идентичности первая установка создаёт новую; старое доверие к прежней Windows само собой работать не начнёт.

Консольный SSH и ProxyJump получают `UserKnownHostsFile` с файлом `DATA/config/rclone/known_hosts` и обычными файлами профиля. Чужие явные настройки `UserKnownHostsFile` для конкретного Host сохраняют приоритет. SSH-KEYSCAN также обновляет эту привязку после своей работы. RESTORE не сканирует и не принимает неизвестные или изменившиеся ключи автоматически.

Восстанавливается только явно включённый (`Persistent=true`, `AutoStart=true`) SSH TUN этой машины. Имя берётся из `Tunnel/beacon-startup.json` (явный выбор при включении канала), а для прежних комплектов — из идентичности SSHD, поэтому переименование Windows не выбирает случайный канал из резервных копий соседей. Возвращается ярлык Startup и запускается существующий канал; ключ на VPS повторно не регистрируется. Выключенные и чужие каналы остаются выключенными.

Пути rclone к ключам и `known_hosts` исправляются по выбранной DATA и новому профилю. Состав remotes и учётные данные облаков не пересоздаются. Если rclone.conf отсутствует, его надо собрать кнопкой RCLONE.CONF; пустой пример DATA не является резервной копией рабочей машины.

Проверка читает метаданные корня SFTP через rclone и выполняет `echo` по SSH для настроенных машин/VPS. Она использует строгую проверку хост-ключей, ограничена по времени, не выводит содержимое каталогов и не открывает RDP/терминалы. Это проверка сохранённых SSH-маршрутов; доступность всех альтернативных маршрутов AUTO, всех дисков и облаков она не утверждает. Роутеры с входом по паролю не проверяются.

Предпосылки остаются: прежние адреса/учётные записи в targets.json должны быть актуальны; соответствующая учётная запись Windows должна существовать и иметь нужные права. SSHD настраивает ключи администраторов. Маршруты WG роутеров, доступ VPS и драйвер OpenVPN RESTORE не создаёт. Для WORK сначала установить драйвер и подключить выбранный OpenVPN, если доступ идёт по нему.

Начисто из DATA (MIRROR)

SETUP → RESTORE → «Начисто из DATA (MIRROR)» — основной вариант после переустановки. Обычный RESTORE доливает недостающее; MIRROR делает C: ровно таким, каким его описывает DATA, как robocopy /MIR:

- `~/.ssh` собирается заново целиком: ключи из Export/SERVERS, config из DATA, доверие к `known_hosts` DATA. Старые ключи, config и `known_hosts` профиля уходят.
- `administrators_authorized_keys` — ровно ключи CLIENTS; ключи, принесённые SSH-COPY-ID мимо CLIENTS, снимаются. Пустой CLIENTS файл не трогает.
- Хост-ключи SSHD — из `Tunnel\SSHD`, даже если на машине уже другие.
- Убираются `rclone.conf` вне DATA (`%APPDATA%\rclone`, `~\.config\rclone`), ярлыки REVERSE SSH TUN (включённый канал возвращается), задача `Audion Backup Sync`.
- Нет rclone или cloudflared в программе — они скачиваются.

Удаления молча нет: всё убранное ложится в `DATA\Recovery\mirror-<время>` с правами только владельца, SYSTEM и администраторов; там же `restore.log` и `sshd.log`. Если импорт ключей сорвался, прежний `~/.ssh` возвращается на место.

Человеческие шаги ждут без таймаутов: отклонённый UAC спрашивается снова; для каждого маршрута через cloudflared проверяется вход в Cloudflare Access и открывается браузер, если входа нет; для роутеров с адресом, которые отвечают отсюда и чей пароль не лежит в DATA, спрашивается пароль — сохраняется он только после настоящего входа, пустой Enter пропускает. Один ли пароль у всех роутеров, спрашивается один раз и запоминается в `targets.json` (`"_routers": { "sharedPassword": true }`). Только при «да» проверенный пароль пробуется на остальных роутерах и сохраняется для роутеров других площадок, до которых отсюда не достать; при «нет» или без ответа у каждого роутера свой пароль. Токены Access в `~/.cloudflared` MIRROR не трогает: это вход, а не данные. SSH-KEYSCAN MIRROR не запускает — доверие берётся только из DATA.

CLI

```
.\Tunnel\RemoteDesktop\restore-machine.cmd -Root "D:\Data\This machine" -NoPause
.\Tunnel\RemoteDesktop\restore-machine.cmd -Root "D:\Data\This machine" -Check -
NoPause
.\Tunnel\RemoteDesktop\restore-machine.cmd -Root "D:\Data\This machine" -
RestoreConfig -NoPause
.\Tunnel\RemoteDesktop\restore-machine.cmd -Root "D:\Data\This machine" -Mirror
.\Tunnel\RemoteDesktop\restore-machine.cmd -Root "D:\Data\This machine" -Mirror -
Check -NoPause
```

`-Mirror -Check` показывает, что уйдёт с C:, и ничего не меняет. `-Mirror -NoPrompt` ни о чём не спрашивает: UAC запрашивается один раз, входы только перечисляются.

`-Check` читает комплект, не меняет службы/профиль и не обращается к сети. `-SkipProbe` выполняет локальное восстановление без сетевой проверки. Код 0 означает успешное выполнение выбранного режима; 1 — ошибку локального шага; 2 — локальные шаги завершены, но проверка связи не прошла полностью. Отдельно заменить маршруты: `Runs\import-keys.cmd -Root ... -RestoreConfig`. `-Force` по-прежнему относится к отличающимся файлам ключей, а не к SSH config.

Проверка реализации

`Tests/Test-CleanRestore.ps1` использует настоящий синтетический ED25519 ключ, пустые профили/ProgramData/Startup во временной папке и заглушки службы/сети. Проверяет сохранность идентичности, ACL резервной копии, отказ при повреждении и конфликте, импорт и перенос путей, доверие SSH/ProxyJump, Startup и CLI-порядок. `Test-SshServerInstall.ps1` отдельно проверяет порядок перед установкой/запуском службы и ошибки готовности. Это изолированные проверки, не испытание на физически переустановленной Windows.