OpenSSH KeyKit

Runbook для экспорта и импорта OpenSSH client и server material.

Все поля операций — в справочнике команд `docs\COMMANDS_RU.md`; в окне это `ЭКСПОРТ И ИМПОРТ -> SSH`.

Две Двери

Пак не заводит собственной папки: экспорт кладёт результат в `output\ssh_keykit`, импорт берёт его из `input`. Поэтому поле `Папка ключей` пустое по умолчанию - пустое значение и означает "по операции". Заполненное поле заменяет обе папки сразу, и тогда импорт пойдёт именно туда, куда указано.

Пустым оно должно и остаться в манифесте: значение по умолчанию GUI и CLI передают как настоящий параметр, поэтому `default` с одной папкой отправил бы импорт искать ключи в папке экспорта.

Ключи Вне Профиля

Этот пак переносит `%USERPROFILE%\.ssh`. Ключ, на который `config` ссылается с другого диска, сюда не попадает — его забирает пак `Доступы из конфигурации` (см. `MIGRATION_RU.md`), который собирает файлы по ссылке, а не по месту.

Проверка Связности

`Проверить связность доступов` читает ssh config и rclone.conf так же, как их читают сами `ssh` и `rclone`, и печатает каждый путь к ключу, `known_hosts`, сертификату и прокси-клиенту с пометкой `[ OK ]` или `[MISS]`. Ничего не копирует и не меняет.

Это дешёвая ежедневная проверка: файлы конфигурации остаются на месте, ломаются только пути внутри них - ключ переехал, `known_hosts` переименован, прокси-клиент удалён. Без такой проверки это выясняется на первом подключении дня.

Что Считается Секретом

OpenSSH KeyKit может экспортировать:

- `%USERPROFILE%\.ssh\id_*` private keys;
- `config`;
- `known_hosts`;
- `authorized_keys`;
- `config.d`;
- `ProgramData\ssh\ssh_host_*` server host keys;
- `sshd_config`.

Private keys и server host keys - secrets. Их нельзя коммитить, отправлять в тикеты, класть в публичные папки или прикладывать к issue.

Client Export

`Export client SSH keys` копирует current-user `.ssh` material в `output\ssh_keykit`.

Используй для переноса пользовательского доступа на новую Windows-установку или для копии перед clean reinstall.

После export:

1. Проверь log.
2. Проверь, что archive/folder лежит в ожидаемом месте.
3. Перенеси выгрузку в защищённое хранилище.

Client + Server Export

`Export client + server SSH keys` делает client export и при elevation добавляет server material из `ProgramData\ssh`.

Server host keys нужны только если новая машина должна сохранить прежнюю SSH server identity. Иначе клиенты корректно увидят новый host key и предупредят.

Если запуск без admin, server keys могут быть пропущены.

Import Client

`Import client SSH keys` восстанавливает `.ssh` текущего пользователя из выбранного или самого свежего snapshot в `input`.

Перед импортом модуль откладывает текущую `%USERPROFILE%\.ssh` копией `.ssh.bak.<timestamp>`. Это важно: import может заменить существующие ключи/config.

Проверяй после import:

- ACL на private keys;
- наличие `.pub`;
- `ssh -T` или подключение к известному host;
- отсутствие лишних ключей, которые не должны жить на этой машине.

Import Client + Server

`Import client + server SSH keys` дополнительно восстанавливает `ProgramData\ssh`, чинит ACL, останавливает/запускает `sshd` и выставляет startup Automatic.

Это system-change операция. Используй только если осознанно переносишь SSH server identity.

Где Лежат Данные

```
output\ssh_keykit   выгрузка экспорта
input               откуда читает импорт
tools\ssh_keykit    скрипты и обёртки пака
```

Выгрузка может содержать private keys. Относись к ней так же строго, как к PFX и password vault export.

Smoke

Минимальная проверка:

```
Проверить связность    -> печатает [ OK ]/[MISS] по каждому пути, ничего не меняет
Status                 -> показывает client/server paths
Export client          -> создаёт snapshot в output\ssh_keykit, private keys не
печатаются в log
Export client+server   -> server keys экспортируются только elevated
Import client          -> берёт snapshot из input, откладывает текущую .ssh
Import client+server   -> чинит ACL и restart sshd
Открыть папку скриптов -> открывает tools\ssh_keykit
```