

Runbook: СКУД Политех (PolytechSKUD*)

Этот runbook привязан к группе алертов **polytech_skud** в Prometheus. Цель — за минуту понять «наша проблема или их», и кому звонить.

SSH-клиент и правило владельца

Все SSH-команды этого runbook используют существующие настройки доступа и штатный `known_hosts` своего operator с явным `StrictHostKeyChecking=accept-new`. Новый target не требует предварительной записи или независимой сверки fingerprint; смена уже известного ключа не принимается молча. Не использовать `StrictHostKeyChecking=no/off` или отбрасывание `known_hosts`.

Действует общекомандное правило из `/home/olvr/HANDBOOK.md`, раздел «SSH: правило владельца», решение `2u1L/hrBEmT`: верификацию ключей не инициировать, не выполнять, не обсуждать и не превращать в поручение, вопрос владельцу или условие работы.

Единственная оговорка — изменение уже известного host key: проверить, что переинсталляция сервера нам известна, затем перейти на новый ключ в своём штатном carrier и кратко записать «ключи сменились, перешли на новые». Если известного факта переинсталляции нет, не обходить штатный отказ и не переходить молча; сообщить РП только этот факт, без независимой сверки fingerprint, доверенной консоли и нового поручения на верификацию.

Этот раздел меняет только документационный рецепт. Ключи, `known_hosts`, SSH-настройки и серверы этим amendment не меняются; production writes по-прежнему требуют разрешения владельца.

Действующая схема (11.10.2026)

Все соединения от имени Olvery — только через gw32 (89.20.105.168). Прокси и другие внешние выходы запрещены абсолютно, включая аварии и диагностику.

back-acs → gw32 → VPN Политеха (ovpstu) → 10.47.30.20:7010

PHP обращается прямо к <https://10.47.30.20:7010/>. Провайдер 34 (локация 36), драйвер aracs, адрес в `driverOptions.api_url`. Посредников и трансляции адреса назначения нет. SNAT на выданный PPP-адрес выполняет штатный mpd.

Адрес PPP назначает сервер Политеха: в 21:30 11.10 получен 10.100.68.2, peer 10.100.68.1. Адрес не закрепляется вручную; перед передачей текущего источника читать `ifconfig ovpstu`.

Локализация

```
ssh root@gw32 ifconfig ovpsu ssh root@gw32 /usr/local/sbin/swanctl -list-sas -ike olvr-pstu
```

Health /api/acs/v1/health/apacs - skud обращается к настоящему адресу того же провайдера. TCP/TLS timeout означает недоступность, но сам по себе не определяет виновную сторону. При отсутствии ответа нужны metadata SYN/SYN-ACK/RST на принимающем интерфейсе сервера, без payload.

Пользовательский результат — выпуск или удаление пропуска. Health и наличие VPN не подменяют его. Изменяющие пропуска операции и открытие двери не используются как обычная сетевая проба.

Конфигурация

На gw32: strongSwan named olvr-pstu и mpd5 bundle OlvrPstu, iface ovpsu. Маршруты 10.47.30.20/32 и 82.179.113.10/32, MTU/MRU1370, штатные NAT/tcpmssfix. Файлы /usr/local/etc/swanctl/conf.d/olvr-pstu.conf и /usr/local/etc/mpd5/olvr-pstu.conf. Пароли не менять.

На srv-prod2: один PHP-драйвер, адрес из провайдера. Общий выход через DHCP gateway на gw32. На Linux VPN не включать: наблюдался kernel fault L2TP/XFRM. Общий mpd на gw32 не перезапускать — он держит WAN PPPoE.

SSO (82.179.112.230:443) — отдельное прямое соединение через WAN gw32. Рецептов альтернативного выхода нет. Точный текущий остаток — OLV-4958.

From:

<https://wiki.olvery.ru/> - **Olvery**

Permanent link:

<https://wiki.olvery.ru/doku.php?id=runbooks:polytech-skud&rev=1791736682>

Last update: **2026/10/11 16:38**

