Linux Host Operations

Keeping enrolled Linux hosts in step · Checked against tacctl 0.2.25

Contents

1. See your hosts 2
2. Keep accounts in step: host sync 3
    2.1 Several hosts at once 4
3. Enroll a host 4
    3.1 This machine 5
4. Move, rename, retire 5
5. Rotating the provisioning account 5
6. Recovery: logins or sudo broken on a host 6
7. Troubleshooting 6
8. Quick reference 6

How a superuser runs the Linux servers enrolled in tacctl day to day: keeping accounts in step, checking hosts, moving and retiring them, and recovering when logins break. Enrolled hosts authenticate logins and `sudo` against tacctl, over TACACS+ (`pam_tacplus`) or RADIUS (`pam_radius_auth`).

Host operations are **superuser only**. Engineers can list and show the hosts of their own scopes.

> **Example names used on this page** Hosts: `web1`, `db1`, `db2` · Scopes: `site-a`, `lab` · Users: `alice`, `carol`

1. See your hosts

```
tacctl host list                        # the enrolled hosts, as device list shows devices
tacctl host list --scope site-a --stale
tacctl host list --name web --ip 10.30.0.0/24
tacctl host list --json
tacctl host show web1            # connection, scope, pinned keys, sightings,
                                 # the accounts the next sync makes
tacctl host check web1           # read-only: does the host match what tacctl would make
it?
tacctl host check --all
tacctl host check --all --concurrency 4    # several hosts at once (§2.1)
```

`host list` shows each host's target, address (recorded at the last enroll or sync, else the single address of its scope), scope, `STATE` (`configured` when the host's scope exists, `unconfigured`, `stale`, and `BREAK-GLASS` in place of those while the host is held), `LAST SEEN` and `BY` (from the seen data that `tacctl device scan` refreshes), server, method, users and open notices. A line under the table gives the age of the seen data and how many notices are open (`tacctl device notice list`).

The filters narrow the list as those of `device list` do, and all must match: `--name <text>`, `--ip <addr|cidr|text>` and `--scope <scope>` take one value or a comma list, and `--stale` keeps the hosts not seen for stale-days. The heading counts the hosts, and `, of 5` follows when the list is narrowed (`Enrolled Linux hosts (2), of 5`); a narrowed list with no host says `None match.` An engineer sees the hosts of their own scopes only. This server's own login shows `-` as its scope, and `--scope` never selects it. `device list` shows network devices only.

`host check` logs in, changes nothing, and lists each difference with the command that fixes it. It exits 1 if a host differs or could not be checked. If `host list` ends with *N finding(s)*, run `tacctl config validate`.

---

2. Keep accounts in step: `host sync`

User changes reach hosts only when you sync. **Sync after every user add, remove, disable, enable, rename, move or scope change.** The exception is this server itself: from 0.2.23 those `user` commands sync the server's own accounts at once, and name the other enrolled hosts they reach in one warning with the command (on a terminal they also ask `Sync these hosts now? [y/N]`; the default is no and `--yes` does not answer it).

```
tacctl host sync web1                  # one host
tacctl host sync db1 db2               # several, in the order typed
tacctl host sync --all                 # every enrolled host
tacctl host sync --all --remove-home   # also delete removed users' homes without asking
tacctl host sync --all --concurrency 4 # several hosts at once (§2.1)
```

What a sync does:

User state	Effect on the host
New in the host's scope	Account created (with a UID consistent across hosts). A user name with a period (stored by 0.2.20 or 0.2.21) is skipped with a warning: it is no Linux account name.
Disabled	Account expired: no login, ssh keys included. Files kept.
Must change the password	As disabled, on every host but the tacctl server, until the user changes it there; the next sync opens it again. `host show` counts it with the disabled accounts.
Re-enabled	Restored
Removed, or out of the scope	Account deleted. The home is deleted only if you agree (asked at a terminal, or `--remove-home`). Otherwise it is moved to `.tacctl-removed` under `/home`.
Renamed	Account renamed by UID. The home stays where it is.
Group/tier changed	Tier on the host updated
The host's scope is under an emergency lockdown	sshd's lockdown drop-in is written: no key login and no forwarding for accounts that are not a superuser's. A sync after the lockdown is lifted removes it (*Emergency Lockdown* §3.1).

A failing host doesn't stop the others. The exit status is 1 if any host failed. A held host (break-glass) is skipped by `--all` and refused when named.

> **Local accounts are never touched.** tacctl manages only the accounts it created. If a local account has the same name as a tacctl user, that user gets no account on the host and you see a warning (`web1: synced (4 users; 1 refused: carl)`). Resolve it by renaming one of the two.

2.1 Several hosts at once

`--concurrency <n>` (1 or more; the default, 1, is one host after the other) works on n hosts side by side in `host sync` and in `host check`. Each host's output is held and printed whole, in the order the hosts were typed, so lines never mix, and the lines, the report and the exit status (1 when a host failed or differs, the others still run) are those of a run one host after the other. What the hosts write on the server (the UID ledger, the host records, the registry) is written one host at a time. With one host `--concurrency` changes nothing.

With more than one host at once nothing is asked and no terminal is used: the login runs in BatchMode (a key or the agent; no password or passphrase) and the remote sudo is `sudo -n`, so the login must be root or have passwordless sudo. Hosts that share an ssh target and port are handled one after the other, since they share one connection.

- **Home directories.** `host sync` does not ask about the homes of removed users. It keeps them and says so after the line that names the removed users: `web1: the home directories of removed users are kept, as no questions are asked with --concurrency above 1: add --remove-home to delete them, or sync web1 alone to be asked.` `--remove-home` deletes them.
- **Ctrl-C** starts no further host and ends the connections under way, and the hosts not started are named (status 130). A `host sync` reports, records and audits the hosts under way as interrupted. Nothing carries the interrupt to a script already running on a host, so that script may finish.
- There is no `--timeout` and no `--max-failures`: a time limit would cut a script off in the middle of its account changes.

---

3. Enroll a host

```
tacctl host enroll admin@web1.example.net --scope site-a
tacctl host enroll admin@10.30.0.15 --name web2 --method radius
tacctl host enroll admin@10.30.0.16 --name db3 --port 2222 --identity ~/.ssh/
deploy_ed25519
```

- `--method tacplus|radius`: if you leave it out, the scope's or the server's default is used (`tacctl host default-method`).
- `--name`: the registry name. The default is the short hostname, in lower case.
- `--server <address>`: the address the host uses for this server. A host that is enrolled already keeps the address it has, so enrolling it again to repair it never repoints it; a new host gets the recorded address (`tacctl server addresses`), else the source address of the route to the host. The server's port in the PAM setup is the configured listener's.
- Enrolling pins the host's ssh keys and registers the host.

If the host's `/etc/login.defs` `UID_MIN–UID_MAX` overlaps tacctl's UID range, enroll and sync warn you. Keep local UIDs clear of that range.

3.1 This machine

The tacctl server is a host of its own kind. `tacctl install` and `tacctl upgrade` set up its login, so every user can log in to it and to its console, and `tacctl host enroll --local` is the command to rebuild that login, to move it to another address (`--server <ip>`, or `tacctl server addresses replace <ip>`, which is the same change) and to repair it. `--local` takes no `--scope`. A `host sync` of the server repairs a login that was changed by hand (`Repaired the managed server login.`), and `host move` of the server only says that `host enroll --local` sets its login up. *Superuser Daily Operations* §11 has the details.

---

4. Move, rename, retire

```
tacctl host move web1 lab        # another scope (asks before deleting accounts)
tacctl host move --all           # every host whose address another scope now answers
tacctl host rename web1 web2         # registry only; offers to rename its own linux-
<name> scope
tacctl host unenroll web1        # remove the PAM setup and secret from the host, then
deregister
tacctl host unenroll web1 --force    # deregister even if the host can't be cleaned
tacctl host forget web1          # drop only this server's record; nothing sent to the
host
```

Goal	Use
Decommission a reachable host	`unenroll`. Local accounts and homes stay on the host.
Remove a wrong or duplicate registration	`forget`
Host re-addressed or moved to a new segment	`host move` (or `--all` after changing scope prefixes)

---

5. Rotating the provisioning account

tacctl logs in to each host with a provisioning account. To switch it:

```
tacctl host provisioner web1 rotate tacprov --key ~/.ssh/tacprov_ed25519 --dry-run
tacctl host provisioner web1 rotate tacprov --key ~/.ssh/tacprov_ed25519 --remove-old
```

The new account is created over the current login and proven in a fresh connection (`sudo id -u` must return 0) before the registry changes.

---

6. Recovery: logins or sudo broken on a host

```
tacctl breakglass hold web1 --reason "INC-4821 sudo broken"     # type 'web1' to confirm
```

While held, the server stops answering that host's address. The host's local administrator and console work. tacctl users can't log in or `sudo` there.

```
# ... fix the host with the local admin ...
tacctl breakglass release web1
tacctl host check web1
```

While a host is held, `host sync`, `show --check`, `enroll`, `move`, `unenroll` and `forget` refuse it. `tacctl ssh` warns you and connects. Holds never expire; *Break Glass* covers holds in full, and *Incident Response Runbooks* R5 is the incident form of this procedure.

---

7. Troubleshooting

Symptom	Check / fix
User has no account on one host	A local account with the same name exists there (see the sync summary). Rename one.
Sync stops on a UID conflict	A local account uses a UID from tacctl's range. Fix the host. Use `--allow-uid-mismatch` only if you understand the result.
`'alice': not renamed …` `processes run as UID …`	The user is logged in. The rename is retried at the next sync.
Host shows a drift warning in `host list`	Its scope no longer answers its address. Run `tacctl host move <name>`.
`the UID ledger … is locked`	Another command is running. Try again shortly.
`host check` differences	Run the fix command printed beside each one, usually `host sync <name>`

---

8. Quick reference

Task	Command
List / detail	`tacctl host list` / `host show <n>`
Compliance check	`tacctl host check --all`

Task	Command
Push accounts	`tacctl host sync --all`
Enroll	`tacctl host enroll <user>@<host> --scope <s>`
Rebuild or repair this server's login	`tacctl host enroll --local`
Move scope	`tacctl host move <n> <scope>`
Rename	`tacctl host rename <old> <new>`
Retire	`tacctl host unenroll <n>`
Drop bad record	`tacctl host forget <n>`
Emergency access	`tacctl breakglass hold <n> --reason "…"`

See also: Access Lifecycle · Break Glass · Troubleshooting §7 · Linux hosts (repo) · `man tacctl`