Break Glass

Local emergency accounts, and holding a device or host back from the server · Checked against tacctl 0.2.25

Contents

1. Before you need it: record the local accounts 2

1.1 Junos root 2

2. Hold 3

2.1 The firewall: why a held device falls back at once 3

3. Get in, by vendor 4

4. While a device or host is held 4

5. Fix and release 5

6. Quick reference 5

When a bad change cuts off AAA on a device, nobody can log in with their tacctl credentials, and the server's refusals stop the device's local accounts from working too. A **break-glass hold** makes the server stop answering that one device or host, so its local accounts work while the server stays up for everyone else. Placing and releasing holds is a **superuser** task; engineers can list the holds in their own scopes.

> **Example names used on this page** Scope: `site-a` · Devices: `sw1` (Cisco), `rtr1` (Junos), `pdu1` (WTI) · Host: `web1` · Ticket `CHG-1182`

1. Before you need it: record the local accounts

Every device should keep a local emergency account for the day the server can't help. Record which accounts each scope's devices keep, so the walkthroughs include them and holds point to them:

```
tacctl scope breakglass site-a                      # list
tacctl scope breakglass site-a add netadmin         # role defaults to admin
tacctl scope breakglass site-a add noc-local --role operator
tacctl scope breakglass site-a remove noc-local
```

- tacctl **never stores** these passwords or hashes. You create, rotate and remove the account on the device yourself.
- `tacctl config validate` warns about scopes with no break-glass accounts: a lockout risk.

1.1 Junos `root`

Many Junos devices keep `root` as their local access. Junos holds it under `system root-authentication`, not as a `system login user`, and tacctl accepts it as a break-glass entry for a scope's Junos devices:

```
tacctl scope breakglass site-a add root      # always admin; lower case only
```

The Junos walkthrough then renders two statements in its break-glass step, commented out like the other accounts:

```
# set system root-authentication encrypted-password '<HASH>'
# set system services ssh root-login allow
```

- Put in the hash yourself: tacctl stores and generates no password or hash.
- Junos refuses root over ssh by default. Allowing it is a security trade-off, since root can then log in over ssh with the password: keep the device behind the management filter, or leave the second line out and keep `root` on the console.

- For a scope that records `root`, `device config pull` and `diff` check both facts in the `breakglass` section: that a root password is set (present, never compared or shown) and that `root-login allow` is there. A plan never types either statement.
- `--role operator` and `--role readonly` are refused for `root`.
- Cisco and WTI devices have no such account: their walkthroughs render nothing for it. A scope whose only entry is `root` has no break-glass account on its Cisco and WTI devices, and `config validate` warns.

---

2. Hold

```
tacctl breakglass hold sw1 --reason "failed AAA paste, CHG-1182"
tacctl breakglass hold web1 --reason "CHG-1182 locked out of sudo"
tacctl breakglass hold "sw2=console recovery,sw3" --reason "CHG-1182 failed paste"
```

- You confirm by **typing the name back**. There is no `--yes`.
- The output shows the way in for the vendor and the local accounts that will now work.
- Several devices: a comma list, each with an optional `=reason`. Each device is checked on its own; the ones refused are named on a `Not held:` line.
- The report has a `Firewall:` line, for example `Firewall: 10.10.0.1 refused on tcp/49 (reject)` (§2.1).
- A hold is refused, with nothing changed, for a name that is neither a registered device nor an enrolled host (or is both), one that is already held, this server's own host, a name with no address, a loopback address or an address a listener binds, a device at the address of an enrolled host (the hold would silence the host too), and an address that no scope covers.

> **Only the registered address is carved out.** If a device sends AAA from another address (a Cisco source interface, NAT, IPv6), the server still answers it. The hold report warns you when this looks likely.

2.1 The firewall: why a held device falls back at once

Taking the address out of the scopes silences RADIUS (UDP): the device gets no answer and times out. TACACS+ is TCP, and until 0.2.23 the kernel completed the handshake and tacquito closed the connection afterwards. A device that falls back to its local accounts only when the server is **unreachable** (a WTI unit with *Fallback Local* `On (Transport Failure)`, a Junos switch with `authentication-order [ tacplus password ]`) saw a reachable server and never fell back. From 0.2.24 a hold also loads a firewall rule that refuses the connection before tacquito sees it.

- tacctl owns one nftables table, `inet tacctl`, and touches nothing else of the server's ruleset. The table refuses a held address connecting to a tacquito port, an open session included. Devices and Linux hosts are held alike.
- A superuser sets what the table does:

`bash tacctl config breakglass-firewall # show the setting tacctl config breakglass-firewall reject # the default: a TCP reset, an instant fallback tacctl config breakglass-firewall drop # discard the packets: a timeout, as for RADIUS tacctl config breakglass-firewall off # no table: the 0.2.23 behavior`

- Every hold, release, move of a held device (`device address`), rename, `backup restore`, change of a listener (`server listen`) and change of the setting loads the table again, and the boot unit `tacctl-breakglass-firewall.service` loads it at boot. `install` and `upgrade` install the `nftables` package, and an upgrade with holds standing loads the table for them.
- The audit lines of a hold and a release end `firewall=reject|drop|off|failed`.
- `status`, `config validate` and `tacctl breakglass list` compare the live table with the holds and the setting, and name each difference with the command that fixes it.

> **When `nft` is missing or fails, the hold stands but the command exits 1.** The report says in red that the server still completes the TCP handshake, so a device that falls back only when the server is unreachable will not. Fix it with `sudo apt-get install nftables`, then `tacctl config breakglass-firewall <the current setting>`, which loads the table even when the setting is unchanged. With the setting `off`, or with nothing held, a missing `nft` is no failure.

---

3. Get in, by vendor

Vendor	How to log in while held
Cisco IOS	ssh or console as the local account. The device waits a few seconds for the server, then accepts the local password. On the console, `enable` with the local enable secret.
Junos	ssh or console as a local `system login user`, or as `root` when the scope records it (ssh needs `root-login allow`, §1.1), after the tacplus timeout. `root` on the console is always local.
WTI	Works only if the unit's TACACS+ *Fallback Local* is `On`. With `Off`, nobody gets in until you release the hold; use the serial console.
Linux host	The host's local administrator and its console work. tacctl users cannot log in or use `sudo` there.

The engineer can print the back-out for the failed change with `tacctl device config plan sw1 --backout`.

---

4. While a device or host is held

- `tacctl breakglass list` shows what is held, since when, by whom and why, and the state of the firewall (§2.1).

- `device remove` and `device config pull` refuse a held device.
- `host sync`, `enroll`, `move`, `unenroll` and `forget` refuse a held host, and `host sync --all` skips it (and names it).
- `tacctl ssh` warns you and connects; your tacctl login will fail there.

---

5. Fix and release

```
tacctl breakglass release sw1
tacctl device config pull sw1 --diff       # confirm the fix
tacctl ssh sw1                             # and log in as yourself again
```

For a host: `tacctl breakglass release web1`, then `tacctl host check web1`.

> **A hold has no timer** and never releases itself. Check `tacctl breakglass list` at every shift start.

Going back to an earlier tacctl release removes the firewall (the table, its file, the boot unit and the setting) and leaves a standing hold in place without it, so the older release's server completes the TCP handshake of the held address again (*Backups and Undo* §5).

---

6. Quick reference

Task	Command	Who
Record local accounts	`tacctl scope breakglass <scope> add <user> [--role <role>]`	Superuser
Record Junos `root`	`tacctl scope breakglass <scope> add root`	Superuser
Hold	`tacctl breakglass hold <name> --reason "<ticket>"`	Superuser
List holds	`tacctl breakglass list`	Engineer (own scopes)
Release	`tacctl breakglass release <name>`	Superuser
Set what the server does with a held address's TCP connections	`tacctl config breakglass-firewall [reject|drop|off]`	Superuser
Back-out for the failed change	`tacctl device config plan <name> --backout`	Engineer

See also: Incident Response Runbooks R4, R5 · *Vendor Notes* · *Emergency Lockdown* · Break-glass (repo) · `man tacctl`