

Secrets, tokens, and recovery (lab cluster + dev)

From docs/SECRETS_AND_RECOVERY.md

Table of contents

[Shared store \(lab cluster\)](#)
[Recovery priority](#)
[Gitea \(cast01\)](#)
[MariaDB \(cluster\)](#)
[PHP / issues backend \(config.php\)](#)
[WireGuard \(remote access\)](#)
[RSSH \(bastion / reverse SSH\)](#)
[Git HTTPS read tokens \(future\)](#)
[Checklist after creating any secret](#)
[Related](#)

Source: SECRETS_AND_RECOVERY.md — section links work in PDF viewers that support internal anchors.

Rule: whenever you create a password, API token, or VPN key, **record it in the shared lab store** so the next deploy or developer can recover without guesswork.

Shared store (lab cluster)

File	Location	In git?
credentials.txt	ac-deploy/sim/cluster0/ → NFS /shared/cluster/	Yes (lab-only values)
secrets.lab.env	same NFS tree	No — copy from secrets.lab.env.example, fill on cluster
Gitea install secrets	/var/lib/gitea/.lab-secrets.env on cast01	No (generated by deploy-gitea.sh)
Gitea mirror API token	/var/lib/gitea/.mirror-admin-token on cast01	No (regenerable — see below)

Production (artc0 / monstro) keeps its own stores; lab cluster is **cast01-03**.

Recovery priority

1. **Preferred:** user self-service via **email** (2FA, password reset) once cluster mail is configured and verified on ac10.
2. **Lab fallback:** admin CLI / config rewrite from values in credentials.txt + secrets.lab.env.
3. **VPN (WireGuard + RSSH):** re-provision from cluster scripts — never copy prod keys to lab.

Gitea (cast01)

Secret	Recover
Admin password [gitea_admin]	credentials.txt → or gitea admin user change-password --username admin --password '...'
Mirror API token	sudo -u gitea gitea -c /etc/gitea/app.ini admin user generate-access-token --username admin --token-name mirror-ac --scopes all --raw → save to /var/lib/gitea/.mirror-admin-token
INTERNAL_TOKEN, JWT	/var/lib/gitea/.lab-secrets.env — if lost: stop gitea, delete file, FORCE_GITEA_CONFIG=1 deploy-gitea.sh (rewrites app.ini; DB preserved)

Browse: https://acl0.f0xx.org/app/androidcast_project/git/ (org ac).

MariaDB (cluster)

Item	Recover
App user/password	[mariadb_app] in credentials.txt
Replication	[mariadb_replication] in credentials.txt
Root	Alpine socket auth as root on cast01 — no password by default

Re-apply schemas: sudo sh /shared/cluster/scripts/load-schemas.sh on cast01 (destructive to empty DB only — read script first).

PHP / issues backend (config.php)

Lab composed tree: /var/www/ac/composed/backend/config/config.php (generated by compose-lab-backend.sh).

Key	Source
DB password	credentials.txt [mariadb_app]
auth.encryption_key	secrets.lab.env → AUTH_ENCRYPTION_KEY or regenerate (invalidates sessions)

Template: ac-deploy/sim/cluster0/lab-seeds/backend/config/config.example.php.

Email / 2FA: when SMTP is live on lab, verify with diag.php and registration flow; then prefer **email recovery** over static passwords.

WireGuard (remote access)

Item	Store / recover
Server keys	secrets.lab.env → WG_SERVER_* or BE config.php remote_access
Peer keys	DB remote_access tables + WireGuardPeerProvisioner
Re-provision	ac-deploy/sim/cluster0/lab-seeds/backend/scripts/sync_wg_peers.php (on cluster, from composed backend)

Do **not** reuse production WG keys on lab. Generate new lab keys and document in secrets.lab.env.

RSSH (bastion / reverse SSH)

Item	Store / recover
Bastion host keys	server sshd host keys (standard OS path)
Ephemeral ra-* users	scripts/rssh_bastion_user.sh on composed backend
Client keys	issued per session in DB — no static shared password

Recovery: run bastion provisioner from lab backend; see REMOTE_ACCESS_IMPL.md and REMOTE_ACCESS_VALIDATION.md.

Git HTTPS read tokens (future)

Per SPEC: tokens live under /etc/git-ro/ on FE — **outside** app repos.

AndroidCast code does not read those paths; CI holds tokens in its own secret store.

Checklist after creating any secret

- [] Added to credentials.txt (if safe for git — lab only) **or** secrets.lab.env on NFS (not committed).
- [] Noted in this doc if recovery command is non-obvious.
- [] If user-facing: email path tested on lab when mail is up.
- [] VPN: lab keys distinct from prod.

Related

- FRESH_ENV_CLONE.md — clean laptop clone
- DEVELOPER_SETUP.md — repo map
- ac-deploy/sim/cluster0/gitea/README.md — Gitea deploy
- 20260607-2FA-email-mobile-auth-flow.md — auth / email flows