Authentik ? Arcane SSO (post-implementation)

Authentik ? Arcane SSO (post-implementation)

Status: wdrożone 2026-05-27/28 **VPS:** home.pl, 212.132.103.157 (Debian 13 trixie)
Architektura: Authentik (OIDC provider) → Arcane v1.19.5 (relying party), bez forward-auth/outpost

---

1. Topologia

```
Public Internet (212.132.103.157)
        │
   nginx :80/:443  (Debian host)
        ├─ combo.t-pizza.pl   → 127.0.0.1:4173 ──┐
        ├─ arcane.t-pizza.pl  → 127.0.0.1:3552 ──┤
        └─ id.t-pizza.pl      → 127.0.0.1:9000 ──┤
                                                 │
                        docker network "web" (bridge, external)
                        ├─ combo_prod          (combo-raport-prod:latest)
                        ├─ arcane              (ghcr.io/getarcaneapp/arcane:latest)
                        ├─ authentik-server    (ghcr.io/goauthentik/server:2026.2.3)
                        ├─ authentik-worker    (ghcr.io/goauthentik/server:2026.2.3)
                        ├─ authentik-postgresql (postgres:16-alpine)
                        └─ authentik-redis     (redis:alpine)
```

Arcane → Authentik server-side: po nazwie kontenera w sieci `web` (autodiscovery `/.well-known/openid-configuration`). Przeglądarka usera → Authentik: przez publiczny `https://id.t-pizza.pl/`.

---

2. Stack Authentik

Lokalizacja: `/opt/docker/authentik/`

- `compose.yaml` — server + worker + postgresql + redis, healthcheck `ak healthcheck`, depends_on `service_healthy`
- `.env` (chmod 600) — `PG_PASS`, `AUTHENTIK_SECRET_KEY`, SMTP, tag obrazu

Tag: `AUTHENTIK_TAG=2026.2.3` (stable; nie `latest`)

Volumes (named):

- `authentik_authentik-postgres` — baza danych (kluczowy dla recovery)
- `authentik_authentik-redis` — sesje/cache
- `authentik_authentik-media` — media (loga, favicony brand)
- `authentik_authentik-templates` — custom email/HTML templates
- `authentik_authentik-certs` — embedded outpost certs

SMTP: `serwer2104579.home.pl:587` STARTTLS, sender `authentik@t-pizza.pl` (skrzynka shared host home.pl).

Ekspozycja: `127.0.0.1:9000:9000` — tylko loopback, TLS terminuje nginx.

---

3. nginx vhost

`/etc/nginx/sites-available/id.t-pizza.pl` (symlink w `sites-enabled/`):

- Listen 443 ssl (ECDSA cert Let's Encrypt, auto-renew certbot.timer)
- Listen 80 → 301 redirect na HTTPS (managed by Certbot)
- `proxy_pass http://127.0.0.1:9000`
- `Upgrade` / `Connection upgrade` (WebSocket dla flow embed Authentika)
- `proxy_read_timeout 86400` (long polling)
- X-Forwarded-Host/Proto/For — KLUCZOWE, bez tego Authentik składa złe URL-e

Cert: `Certificate Name: id.t-pizza.pl`, ECDSA, expiry 2026-08-25 (auto-renew).

---

4. Konfiguracja Authentik (przez API)

Zbootstrapowane przez `https://id.t-pizza.pl/api/v3/` z API token akadmin:

Provider OAuth2/OpenID (pk=1):

- Name: `arcane-oidc`
- Client type: confidential
- Client ID: `arcane`
- Client secret: 128 znaków (zapisany w `~/.secrets/arcane-oidc.env` chmod 600)
- Authorization flow: `default-provider-authorization-implicit-consent`
- Invalidation flow: `default-provider-invalidation-flow`
- Signing key: `authentik Self-signed Certificate`
- Scopes: `openid` + `profile` + `email`
- Sub mode: `hashed_user_id`, Issuer mode: `per_provider`
- Redirect URIs (strict): `https://arcane.t-pizza.pl/auth/oidc/callback`

Application: `Arcane` (slug `arcane`, provider pk=1, launch URL `https://arcane.t-pizza.pl`)

Group: `arcane-admin` (non-superuser) — member: `akadmin`

Issuer URL: `https://id.t-pizza.pl/application/o/arcane/` **Discovery:** `https://id.t-pizza.pl/application/o/arcane/.well-known/openid-configuration`

---

5. Konfiguracja Arcane (przez API, settings w DB)

Arcane v1.19.5 trzyma OIDC w DB settings — modyfikujesz przez `PUT /api/environments/0/settings` (X-API-Key), bez recreate kontenera.

Kluczowe ustawienia:

Key	Value	Komentarz
`baseServerUrl`	`https://arcane.t-pizza.pl`	KRYTYCZNE — bez tego redirect URI źle składany
`oidcEnabled`	`true`	
`oidcClientId`	`arcane`	
`oidcClientSecret`	(128 znaków)	
`oidcIssuerUrl`	`https://id.t-pizza.pl/application/o/arcane/`	autodiscovery `/.well-known/openid-configuration`
`oidcScopes`	`openid profile email`	
`oidcAdminClaim`	`groups`	mapowanie ról: claim z ID token
`oidcAdminValue`	`arcane-admin`	wartość claim = admin w Arcane
`oidcProviderName`	`Authentik`	label na buttonie login

Key	Value	Komentarz
`oidcMergeAccounts`	`true`	scalanie kont po emailu (bez tego: duplicate user)
`oidcAutoRedirectToProvider`	`false`	**break-glass** — login page nadal pokazuje lokalny form
`authLocalEnabled`	`true`	lokalny admin Arcane nadal aktywny

---

6. Backup

`/opt/docker/arcane/backup-cron.sh` (uprzednio istniejący) iteruje po **wszystkich woluminach Docker** via Arcane Volume Backup API (`POST /api/environments/0/volumes/{name}/backups`). Działa też dla `authentik_*` volumes — bez modyfikacji.

Cron: `30 3 * * *` (root) — codziennie 03:30. **Log:** `/var/log/arcane-backup.log` **Rotacja:** max 10 backupów/wolumin (skrypt usuwa najstarsze). **Lokalizacja backupów:** `/opt/backups/arcane/` (bind mount → Arcane `/backups`).

Backupy off-site (manualny, do disaster recovery):

```
rsync -avz root@212.132.103.157:/opt/backups/arcane/ ~/backups/vps-home-pl/
```

---

7. Break-glass procedura

Jeśli Authentik padnie / OIDC nie działa:

1. **Lokalny admin Arcane:** otwórz `https://arcane.t-pizza.pl/`, kliknij „local login" (przycisk widoczny, bo `oidcAutoRedirectToProvider=false`), zaloguj się jako `admin-combo@t-pizza.pl` (lokalne konto + hasło z password managera) — pełen dostęp do UI niezależnie od Authentika.
2. **Wyłączyć OIDC bez restartu** (jeśli trzeba):
   ```
   curl -X PUT -H "X-API-Key: $ARCANE_KEY" -H "Content-Type: application/json" \
     https://arcane.t-pizza.pl/api/environments/0/settings \
     -d '{"oidcEnabled":"false"}'
   ```
3. **Authentik direct admin:** `https://id.t-pizza.pl/if/admin/` jako `akadmin` (hasło w `~/.secrets/authentik-akadmin.env`, plus break-glass przez `docker exec authentik-worker ak shell` jeśli kompletny lockout).

---

8. Rollback (gdyby co? posz?o ?le)

Pre-flight backup z 2026-05-27 23:17 leży w:

- VPS: `/opt/backups/pre-authentik-20260527-211758/`
- Off-site lokalnie: `~/backups/vps-home-pl/pre-authentik-20260527-211758/`

Zawiera: tarbale `/opt/docker`, `/etc/nginx`, `/etc/letsencrypt`, kopię `docker-compose.yml` combo, manifesty docker (ps/images/networks/volumes), iptables.rules.

Volume backups Arcane sprzed wdrożenia: `arcane_arcane-data-1779916672384855682-688ba987`, `combo_data-1779916673232502773-41a003ba` (restore via `POST /api/environments/0/volumes/backups/{id}/restore`).

---

9. ?cie?ki/komendy do zapami?tania

```
# Status wszystkich stacks
docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Status}}"

# Logi Authentika
docker logs authentik-server --tail 100
docker logs authentik-worker --tail 100

# Logi Arcane
docker logs arcane --tail 100

# Recreate Authentika (po zmianie compose/.env)
cd /opt/docker/authentik && docker compose up -d

# Sprawdzenie Authentik discovery
curl -s https://id.t-pizza.pl/application/o/arcane/.well-known/openid-configuration | jq

# Sprawdzenie status OIDC w Arcane (publiczne, bez auth)
curl -s https://arcane.t-pizza.pl/api/oidc/status | jq

# Backup manualny (uruchom skrypt)
/opt/docker/arcane/backup-cron.sh
tail -f /var/log/arcane-backup.log
```

Revision #4
Created 2026-05-28 04:00:59 CEST by matzxp84
Updated 2026-05-28 04:34:04 CEST by matzxp84