Azure Auth Runbook — alai-cli-deployer SP (MC #9524)

Azure Auth Runbook (post-MC #9524)

Status

Active as of 2026-04-26. SP created, authenticated, verified.

Primary auth

- **Service principal:** alai-cli-deployer (appId: `f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9`)
- **Tenant:** `3454a03f-20b4-4bda-a116-2293c459aecd` (alemalai.onmicrosoft.com)
- **Subscription:** `5b0b4d9b-e677-464e-abf0-5170cbce3b8e` (Azure subscription 1)
- **Role:** Contributor (subscription scope)
- **Bitwarden item:** "Azure Service Principal — alai-cli-deployer" (ID: `7865a3a3-c4af-4aef-ac68-8dce370b5010`)
- **Fallback account:** alem@alai.no (retained, not deleted)

Daily use

No login needed. `az` commands authenticate via SP token automatically. Token TTL is 1 hour but renewed silently by az CLI — no interactive prompt.

Verification at any time:

```
az account show --query "{user:user.name,type:user.type}"
# Expected: {"user": "f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9", "type": "servicePrincipal"}
az vm list --query "[].name"
```

```
# Expected: ["repair-vm-alai_", "vm-alai-lightrag", "vm-alai-support", "vm-drop-prod"]
```

Covered resources

VM	Resource Group	Purpose
vm-alai-support	rg-alai-support	BookStack, Vaultwarden, Documenso, Grafana, Planka
vm-drop-prod	RG-DROP-PROD	Drop production
vm-alai-lightrag	rg-alai-lightrag	LightRAG knowledge graph
repair-vm-alai_	repair-vm-alai-support-...	Ephemeral repair VM

SSH still uses key-based auth: `ssh -i ~/.ssh/azure_alai alai-admin@4.223.110.181`

SP secret rotation (every 90 days — next due 2026-07-26)

```
# 1. Retrieve current SP secret from Bitwarden (for reference)
BW_SESSION=$(cat /tmp/bw-session)
bw get item "Azure Service Principal — alai-cli-deployer" --session "$BW_SESSION" | jq -r
.notes

# 2. Create new secret (requires user account with AD rights — alem@alai.no)
az login  # one-time interactive as alem@alai.no
az ad sp credential reset \
  --id "f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9" \
  --years 2 \
  2>&1
# → returns new password

# 3. Test new secret
az login \
  --service-principal \
  -u "f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9" \
  -p "<NEW_PASSWORD>" \
  --tenant "3454a03f-20b4-4bda-a116-2293c459aecd"
```

```
az vm list --query "[].name"

# 4. Update Bitwarden item with new secret
# bw edit item 7865a3a3-c4af-4aef-ac68-8dce370b5010 --session "$BW_SESSION" (update notes field)

# 5. Update rotation_due date in this file and in infra_service_account_auth_pattern.md
```

Recovery (if SP secret unknown)

1. Alem: `az login` with alem@alai.no (one-time interactive)
2. Reset SP: `az ad sp credential reset --id f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9 --years 2`
3. Re-login as SP with new secret
4. Update Bitwarden item
5. Verify: `az vm list --query "[].name"`

Recovery (if Bitwarden unavailable — last resort)

1. Alem: `az login` (one-time interactive, alem@alai.no)
2. `az ad sp credential reset --id f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9 --years 2` → new secret
3. `az login --service-principal -u f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9 -p <new> --tenant 3454a03f-20b4-4bda-a116-2293c459aecd`
4. Store new secret in Bitwarden when available
5. Update this runbook

Activate from scratch (fresh machine)

```
# 1. Retrieve secret from Bitwarden
BW_SESSION=$(bw unlock --raw)
SECRET=$(bw get item "Azure Service Principal — alai-cli-deployer" --session "$BW_SESSION" | \
  python3 -c "import sys,json; n=json.load(sys.stdin)['notes']; [print(l.split(': ',1)[1]) for l in n.split('\n') if l.startswith('password')]")

# 2. Login
```

```
az login \
  --service-principal \
  -u "f2a3b94b-46a5-4a5c-ae34-a222a35bf5b9" \
  -p "$SECRET" \
  --tenant "3454a03f-20b4-4bda-a116-2293c459aecd"

# 3. Verify
az account show --query "{user:user.name,type:user.type}"
```

Security notes

- SP secret is in Bitwarden only — no local file (unlike gcloud where key file is needed)
- az CLI caches the SP token in `~/.azure/` — do NOT commit that directory
- DO NOT share secret over email/Slack — use Bitwarden item share
- SP has Contributor at subscription level — sufficient for VM management, RG operations, App Runner
- SP does NOT have AD admin rights — cannot create users or manage AD itself

---

Revision #3
Created 2026-04-26 19:36:48 UTC by John
Updated 2026-06-21 20:03:18 UTC by John