

Gesamtbewertung

8.5 / 10

### Kurzfazit

Das Repo hat seit dem letzten Audit eine deutlich spuerbare Qualitaetssteigerung erfahren. Die GitOps-Disziplin ist professionell, die Dokumentation vollstaendig und konsistent, das Netzwerkmodell sauber, die Secret-Hygiene ist gut. Die groessten Einzelfunde sind **drei syntaktisch ungueltige SHA256-Digests** (Authelia 62 Zeichen, ntfy 63 Zeichen, borg-ui 63 Zeichen), die beim naechsten Redeploy jeweils einen Pull-Fehler erzeugen wuerden. Jenseits davon gibt es keine unerwarteten kritischen Schwachstellen. M10 ist korrekt als offen und bewusst markiert.

### Bewertungsuebersicht

Dimension	Score
Architektur & Netzwerkmodell	9/10
Security-Modell	8/10
GitOps- / Komodo-Modell	9/10
Backup- & Restore-Reife	8/10
Dokumentationsqualitaet	9/10
Upgrade- / Patch-Strategie	8/10
Secrets-Management	8/10
Observability / Monitoring	7/10
Disaster-Recovery-Faehigkeit	7/10
Wartbarkeit Einzelperson	9/10

### Besondere Staerken

**Netzwerkmodell:** Konsistent und korrekt durchgezogen: Datenbanken nie im frontend\_net, app-interne Netze fuer DB/Cache-Isolation, keine Wildcard-Oeffnungen.

**Secret-Disziplin:** \_FILE-Pattern wo moeglich, Komodo Stack ENV als dokumentierter Fallback, keine Plaintext-Secrets im Repo, .gitignore vollstaendig und korrekt.

**Dokumentationstiefe:** RESTORE\_MATRIX, DISASTER\_RECOVERY, GITOPS\_DRIFT\_RUNBOOK, AI\_CONTEXT, SERVICE\_CATALOG, MIGRATION\_LOG - aussergewoehnlich fuer ein Single-Operator-Homelab.

**Digest-Pinning:** Fuer alle produktiven Stacks (ausser bewusst ausgenommenen Caches und Nextcloud) vollstaendig durchgezogen.

**GitOps-Zyklus:** Gitea -> Komodo -> Deploy sauber implementiert, Driftfall mit Runbook abgesichert, Komodo Self-Stack erfolgreich aus Drift zurueckgefuehrt.

**Sicherheits-Grundhygiene:** security\_opt: no-new-privileges:true fast ueberall gesetzt; Netzwerktrennung funktioniert.

---

## Strukturell noch schwach

Die Restore-Faehigkeit ist gut dokumentiert, aber ausser dem einmaligen Smoke-Test fuer gitea/postgresql17-globals fehlen regelmaessige nachgewiesene Restore-Tests. **Hermes ist produktiv, aber vollstaendig ausserhalb von RESTORE\_MATRIX und DR-Bootstrap.** Der user:"0"-Betrieb fuer Grafana/InfluxDB ist dokumentiert, bleibt aber ein echter Angriffsflaechen-Verstaerker. Das SMTP-Backend fuer Authelia-2FA fehlt - 2FA-Codes landen aktuell nur in einer Logdatei. Das Monitoring hat keine externe Alarmierung ausserhalb von ntfy/Uptime Kuma.

---

## Kritische Findings

### C-1 | Drei ungültige SHA256-Digests

Drei Digests haben die falsche Länge und sind syntaktisch ungültig. Docker bricht beim nächsten Pull/Redeploy mit einem Fehler ab. Aktuell ist der Host nur geschützt, weil das gecachte Image genutzt wird - bei Host-Neustart oder manuellem Pull bricht es.

Service	Compose-Datei	Laenge	Erwartet
authelia	security/authelia/docker-compose.yml	62 Zeichen	64
ntfy	apps/ntfy/docker-compose.yml	63 Zeichen	64
borg-ui	ops/borg-ui/docker-compose.yml	63 Zeichen	64

*authelia: ...c6b6463 (2 Zeichen fehlen) | ntfy: ...ca9b86 (1 Zeichen fehlt) | borg-ui: ...359ce6 (1 Zeichen fehlt)*

---

## Mittlere Findings

### M-1 | mail-archiver ohne Authelia-ForwardAuth-Middleware (sensible App)

Die mail.kaleschke.info-Route hat in der Compose keine authelia@file-Middleware. Die App schützt sich über MAILARCHIVER\_AUTH\_PASSWORD, aber ein Mail-Archiv ohne zweite Auth-Schicht ist im Vergleich zum Rest des Stacks ein Ausreisser. Die ACL-Wildcard \*.kaleschke.info -> one\_factor greift nur, wenn die Middleware am Traefik-Router hängt. Empfehlung: authelia@file,secure-headers@file ergänzen oder explizit als Ausnahme dokumentieren.

### M-2 | Authelia 2FA-Notifier: nur Filesystem, kein SMTP

2FA-Codes (TOTP-Registrierung, Passwort-Reset) landen nur in /config/notifications.log. Im Praxisfall eines Zugriffsverlustes auf das Gerät oder Browser-Wechsels ist das kritisch. SMTP ist auskommentiert. Das ist ein mittleres Risiko für einen produktiven Auth-Provider. Alternativ kann ntfy als Notifier eingebunden werden.

### M-3 | M10 offen: KOMODO\_WEBHOOK\_SECRET=\${KOMODO\_SECRET\_KEY}

Korrekt als bewusst offen und M10 dokumentiert. Das Risiko: Webhook-Secret und API-Key sind identisch - ein kompromittierter Webhook-Endpunkt exponiert denselben Wert wie der API-Key. Kein Sofort-Handlungsbedarf, aber sollte der nächste geplante Schritt sein. Komodo-Änderungen nur gemeinsam mit dem Betreiber durchführen.

### M-4 | Grafana und InfluxDB laufen als user: "0"

Beide Container laufen als root wegen Host-Appdata-Permissions. Dokumentiert als bekannte Ausnahme. Ein Container-Escape oder eine RCE-Schwachstelle in Grafana/InfluxDB hätte unmittelbar root-Zugriff auf das Host-Dateisystem. Die Korrektur (UID/GID-Mapping der Appdata-Pfade) ist als eigener Sprint vorgesehen - das ist der richtige Ansatz.

### M-5 | Hermes fehlt vollstaendig in RESTORE\_MATRIX und DR-Bootstrap-Sequenz

hermes-gateway und hermes-dashboard sind produktiv unter hermes.kaleschke.info. In SERVICE\_CATALOG als 'noch nicht in Restore Matrix' markiert, aber ohne auch nur einen minimalen Smoke-Test-Eintrag in der RESTORE\_MATRIX. Wenn Hermes Teil des produktiven Workflow-Betriebs ist, fehlt der Restore-Pfad vollstaendig.

---

## Niedrige / Kosmetische Findings

### N-1 | Scrutiny-Image von nicht-kanonischem Registry-Pfad

ghcr.io/starosdev/scrutiny:latest-omnibus - das originale Scrutiny-Projekt lag historisch unter analogj/scrutiny. starosdev ist ein anderer Maintainer/Fork. Digest-gepinnt, also kein unmittelbares Risiko, aber bei einem Update-Sprint pruefen, ob das der bevorzugte Fork ist.

### N-2 | Hermes nutzt lokalen Build, kein gepinntes Image

ops/hermes-agent/docker-compose.yml nutzt build: context:. Komodo braucht beim Redeploy den lokalen Build-Context auf dem Host; das Image ist nicht reproduzierbar aus einer Registry ziehbar. Kein Digest-Pin moeglich - sollte mindestens kommentiert sein.

### N-3 | immich\_redis ohne Passwort und ohne Named Volume

redis:7 in der Immich-Compose hat kein requirepass, kein Named Volume. Fuer einen reinen In-Process-Cache im internal:true-Netz akzeptabel, aber inkonsistent mit dem Pattern der anderen Redis-Instanzen. MIGRATION\_LOG nennt immich\_redis korrekt als rebuildbar.

### N-4 | nextcloud:33.0.2-apache ohne Digest - bleibt offen

Korrekt dokumentiert im MIGRATION\_LOG als manifest-nicht-validierbar. Bei der naechsten Nextcloud-Bumping-Runde erneut pruefen, ob ein Manifest-Digest inzwischen abrufbar ist.

### N-5 | cloud.kaleschke.info in Authelia-ACL unter Wildcard, aber keine Middleware in Compose

Kein Fehler - da die Middleware im Nextcloud-Router fehlt, greift die ACL nie. Nextcloud nutzt korrekt native App-Auth. Eine Zeile Kommentar in der configuration.yml wuerde die Diskrepanz klaeren.

### N-6 | backend\_net - Live-internal-Attribut nicht aus Repo verifizierbar

Im Repo wird backend\_net als external:true referenziert. Ob es tatsaechlich als internal:true erstellt wurde, ist nur live pruefbar. Bekannt und im REPO\_MAP dokumentiert, aber beim naechsten DR-Test explizit verifizieren.

### N-7 | Authelia-Notifier-SMTP auskommentiert, nicht als bewusste Entscheidung dokumentiert

Eine explizite Zeile wie '# SMTP bewusst deaktiviert - 2FA per TOTP; Filesystem-Log als Fallback' wuerde den Repo-Standard der bewussten Dokumentation einhalten.

## Verifizierte erledigte Punkte

Punkt	Status
Authelia bewusst ohne Redis; Doku angepasst	Konsistent
Authelia Repo-Config als Baseline dokumentiert	Klar markiert
Homepage/Komodo Authelia-ACL-Drift bereinigt	ACL korrekt
.gitignore eingefuehrt	Vollstaendig
Hermes stack.env -> stack.env.example	Nur .example im Repo
Hermes Dashboard produktiv und dokumentiert	In allen Pflichtdocs
Komodo Self-Stack Drift auf persistenten Pfad	Vollstaendig dokumentiert
M3a: stateful/Tier-1 Images digest-gepinnt	Alle 64 Zeichen
M3b: weitere versionierte Images gepinnt	Alle 64 Zeichen
Nextcloud bewusst nicht gepinnt	Ausnahme dokumentiert
Redis-Caches bewusst ohne Digest	Alle drei, dokumentiert
M6/M7/M8: Hermes, Tailscale, Grafana/InfluxDB user:"0"	In Architektur & Doku
M9 Backup-Scope erledigt	Konsistent
N-Aufraeumen: version:, .keep, leere env/*.example	Alles bereinigt
M10 als bewusst offen markiert	Dokumentiert
Portainer vollstaendig entfernt	Kein Compose, nur Hist.-Doku

## Top 10 Verbesserungen mit Prioritaet

Prio	Massnahme	Kat.
<b>P1 - SOFORT</b>	Korrekte 64-Zeichen-Digests fuer Authelia, ntfy und borg-ui aus Registries nachziehen	Kritisch
<b>P2 - Kurzfristig</b>	SMTP- oder ntfy-Notifier fuer Authelia konfigurieren (2FA per E-Mail)	Mittel
<b>P3 - Kurzfristig</b>	mail-archiver: Authelia-Middleware ergaenzen oder als Ausnahme dokumentieren	Mittel
<b>P4 - Mittelfristig</b>	Hermes in RESTORE_MATRIX aufnehmen (Restore-Quelle, Secrets, Smoke-Test)	Mittel
<b>P5 - Mittelfristig</b>	UID/GID-Hardening Sprint fuer Grafana/InfluxDB (user:"0" entfernen)	Mittel
<b>P6 - Mittelfristig</b>	M10: Komodo Webhook-Secret vom API-Key trennen (mit Betreiber)	Mittel (M10)
<b>P7 - Mittelfristig</b>	Restore-Tests fuer Vaultwarden und Paperless durchfuehren und dokumentieren	Niedrig
<b>P8 - Niedrig</b>	immich_redis: Passwort-Pattern oder explizite Kommentierung als Cache-only	Niedrig
<b>P9 - Niedrig</b>	Scrutiny-Image-Herkunft (starosdev) pruefen und ggf. dokumentieren	Niedrig
<b>P10 - Niedrig</b>	Authelia-Config: Kommentare zu cloud.kaleschke.info und SMTP-Notifier	Kosmetisch

## M10 - Sonderhinweis

**M10: KOMODO\_WEBHOOK\_SECRET=\${KOMODO\_SECRET\_KEY}**

Dieser Punkt ist im Repo korrekt als bewusst offener Sicherheitspunkt markiert und soll nur gemeinsam mit dem Betreiber angefasst werden. Keine Aenderung ohne explizite Freigabe.

Der einzige Schritt aus Audit-Sicht: bestaetigen, dass kein Zeitdruck besteht und der naechste Wartungsfenster-Slot eingeplant ist. Alle anderen Findings in diesem Bericht sind unabhaengig von M10 und koennen ohne Komodo-Eingriff umgesetzt werden.

## Empfohlene naechste Schritte

### Sofort (vor naechstem Komodo-Deploy)

Korrekte 64-Zeichen-Digests fuer Authelia, ntfy und borg-ui aus den Registries nachziehen und in den Compose-Dateien ersetzen. Smoke-Test: docker pull mit dem gepinnten Digest sollte ohne Fehler durchlaufen.

### Kurzfristig (naechster Wartungs-Sprint)

SMTP- oder ntfy-Notifier fuer Authelia konfigurieren. mail-archiver entweder mit Authelia-Middleware absichern oder als dokumentierte Ausnahme in SERVICE\_CATALOG und ARCHITECTURE eintragen.

### Mittelfristig (geplanter Sprint)

Hermes in RESTORE\_MATRIX aufnehmen. UID/GID-Hardening fuer Grafana/InfluxDB (user:"0" entfernen). M10 gemeinsam mit Betreiber abschliessen.

#### **Laufend**

Regelmaessige Restore-Tests (mindestens Gitea und Paperless einmal im Quartal nachweisen). Bei naechstem Nextcloud-Update pruefen, ob Digest jetzt manifest-validierbar ist.

---

*Dieser Audit basiert ausschliesslich auf dem Repo-Sollzustand (G:\Gitea\_Clone\homelab-infra). Kein Live-Zugriff auf Host, Komodo oder Docker-Runtime. Keine Aenderungen vorgenommen. Secret-Werte wurden nicht gelesen oder ausgegeben.*