Mailserver Terminator

IT-Systemdokumentation

Mailcow mit zentralem Logging via Grafana / Loki / Promtail (UDP)

Inhalt

1. Übersicht & Zweck

Das System betreibt eine Mailserver-Umgebung auf Basis **Mailcow** für den **Versand von Rechnungen und Lohnabrechnungen**. Aufgrund der hohen Versandmenge ist die *lückenlose Nachvollziehbarkeit* von Zustellungen, Fehlern und Trends erforderlich. Zentralisierte Logs werden per **UDP** an **Promtail** geleitet, in **Loki** gespeichert und in **Grafana** visualisiert. Grafana ist **ohne VPN** erreichbar (öffentlicher Zugriff mit Härtung).

2. Hosting & Serverressourcen

Anbieter	Webtropia (DE, ISO-27001 RZ)
CPU	4 Kerne
RAM	8 GB
Storage	80 GB NVMe
Rolle	Mailserver + Logging-Stack

3. Architektur & Datenfluss

- **Mailcow** (Postfix, Dovecot, Rspamd) erzeugt Versand- und Statuslogs.
- **Promtail** empfängt Logs per UDP (Syslog), labelt und pusht an Loki (HTTP).
- **Loki** speichert Logs zeitbasiert und stellt Abfragen bereit.
- **Grafana** visualisiert Kennzahlen & Status (Dashboards, Explore).

4. Verzeichnisse & Dateien

`/opt/mailcow-dockerized`	Mailcow Docker-Umgebung
`/opt/mailcow-dockerized/docker-compose.override.yml`	Enthält **UDP-Weiterleitung** der Mailcow-Logs zu Promtail
`/opt/obs-mail`	Promtail, Loki, Grafana (Stack)
`/opt/obs-mail/loki_config.yml`	Loki-Spezifikationen (Speicher, Index, Retention)

5. Netzwerk & Ports

Dienst	Port/Proto	Zugriff	Hinweis
Mailcow Web-UI	443/TCP	Intern	TLS
Promtail Syslog	1514/UDP	Nur intern	Eingang der Logs
Loki API	3100/TCP	Intern	Push/Query
Grafana UI	3000/TCP	**Öffentlich**	Härtung beachten (siehe §11)

6. Logging- & Monitoring-Konzept

1. Mailcow erzeugt Versand-/Status-/Fehlerlogs.
2. Weiterleitung per **UDP ? Promtail** (Definition in `docker-compose.override.yml`).
3. Promtail labelt, normalisiert und pusht via HTTP an **Loki**.
4. **Loki** speichert zeitbasiert und bedient Abfragen.
5. **Grafana** visualisiert (Dashboards, Explore, Alarme optional).

7. Mail-Status & Auswertung

sent	E-Mail erfolgreich versendet
deferred	Zustellung verzögert (Zielserver nicht erreichbar o.Ä.)
bounced	Zustellung fehlgeschlagen (Adresse ungültig, Mailbox voll)
rejected	Abgelehnt (Policy/SPAM-Gründe)

Zur Nachvollziehbarkeit von Massenversand (Rechnungen/Lohnabrechnungen) stehen in Grafana Übersichten und Detailabfragen bereit.

8. Aufbewahrung & Compliance

- **Logs in Loki:** Aufbewahrung **120 Tage**, danach automatische Löschung.
- **Dashboards in Grafana:** persistent in Volumes, keine automatische Löschung.

9. Zugangsdaten & Passbolt

Sämtliche Zugangsdaten (Mailcow, Grafana, Server/Webtropia) werden **ausschließlich in Passbolt** verwaltet.

- Passbolt-Instanz: *[Passbolt-URL eintragen]*
- Zugriff nur für autorisierte Administratoren (Rollenbasiert).
- Keine Klartext-Passwörter in BookStack oder Konfigurationsdateien.

10. Betrieb, Aufgaben & Verantwortlichkeiten

Intervall	Aufgabe	Rolle
Täglich	Grafana prüfen (Fehler, Ausreißer, Zustellquote)	Monitoring-Team
Wöchentlich	Testmail mit Status-Kontrolle	Sysadmin
Monatlich	Updates (Mailcow, Promtail, Loki, Grafana)	Sysadmin
Quartalsweise	Security-Review, Passwortrotation, IP-Whitelists prüfen	Security Officer

11. Sicherheitsmaßnahmen

- **Grafana öffentlich:** HTTPS erzwingen, starke Passwörter, individuelle Konten, optional IP-Whitelisting/Rate-Limiting.
- **Promtail (UDP 1514):** nur intern freigeben.
- **Least Privilege:** Rollen & Rechte regelmäßig prüfen.
- **Protokollprüfung:** Zugriffslogs von Grafana & Reverse-Proxy regelmäßig auswerten.

12. Backup & Wiederherstellung

- **Relevante Pfade:**
  - `/opt/mailcow-dockerized`
  - `/opt/obs-mail`
  - `/opt/obs-mail/loki_config.yml`
- Tägliche, verschlüsselte Backups; *Restore-Test mindestens quartalsweise*.

13. Änderungs- & Versionskontrolle

- Konfigurationsdateien (`docker-compose.override.yml`, `loki_config.yml`) in Git versionieren.
- Change-Log mit Datum, Verantwortlichem, Kurzbeschreibung.

14. Anhang

14.1 ASCII-Architekturdiagramm

```
Mailcow (Postfix, Dovecot, Rspamd)
    |
    |  UDP 1514
    ▼
Promtail  —HTTP Push—>  Loki  —API—>  Grafana (öffentlich, HTTPS)
```

14.2 Beispielpfade (Referenz)

```
/opt/mailcow-dockerized/
  └— docker-compose.override.yml   # enthält UDP-Weiterleitung zu Promtail

/opt/obs-mail/
  └— loki_config.yml             # Loki-Spezifikationen (Index, Storage, Retention)
```

Hinweis: Zugangsdaten sind in Passbolt hinterlegt (siehe Abschnitt 9). Logs werden 120 Tage vorgehalten.

Revision #3
Created 12 September 2025 05:55:53 by Martin Raddei
Updated 12 September 2025 05:57:04 by Martin Raddei