needrestart: Dienste nach Updates neu starten

needrestart: Dienste nach Updates neu starten

Stand	11.11.2026 · Repo `ansible-infra`, Commit `3259b6a`
Zabbix-Template	Template Security needrestart (Gruppe Admin-gerds), auf allen Hosts
Geltungsbereich	Alle Server aus `inventory/hosts.yml`

1. Zweck

Automatische Updates tauschen Bibliotheken (z. B. OpenSSL) auf der Platte aus. Laufende Dienste wie nginx, MariaDB oder OpenLDAP nutzen aber weiter die alte Fassung im Speicher, bis sie neu starten. Ohne Neustart ist das Sicherheitsupdate installiert, aber nicht wirksam. needrestart startet nach jedem Update genau die betroffenen Dienste neu.

2. Regeln

Dienst	Verhalten
Normale Dienste, Datenbanken, OpenLDAP, Agenten	Automatischer Neustart nach jedem Update (unattended-upgrades und manuelles apt)
`docker`, `containerd`	Nur melden. Neustart würde alle Container stoppen.
`wazuh-indexer`	Nur melden. Start dauert Minuten, Ausfall legt das SIEM lahm.
`dbus`, `systemd-logind`, `unattended-upgrades`	Nur melden (Vorgabe von needrestart). Erledigt sich mit dem nächsten Neustart des Servers.
Container-Inhalte	Nicht betroffen. Aktualisierung über neue Images (siehe Trivy).

3. Zabbix

Item	Bedeutung	Alarm
Dienste mit veralteten Bibliotheken	Anzahl, die noch auf Handarbeit warten	keiner (Information)
seit 7 Tagen veraltet	davon seit mindestens 7 Tagen offen	WARNING bei > 0

letzter Status	Zeitpunkt des letzten stündlichen Laufs	WARNING nach 3 Stunden ohne Status

4. Was tun bei Alarm

1. Auf dem Host nachsehen: `cat /var/log/needrestart-services.list` (Dienst und „seit“).
2. `dbus`, `systemd-logind`, `systemd-manager`: Server neu starten (Contabo vorher Snapshot).
3. `docker`, `containerd`: im Wartungsfenster `systemctl restart docker`, danach Container prüfen.
4. `wazuh-indexer`: im Wartungsfenster `systemctl restart wazuh-indexer`, danach Dashboard prüfen.

Alarm „kein Status seit 3 Stunden“: `/usr/local/bin/needrestart-status.sh` von Hand starten, Fehlermeldung ansehen, Cronjob prüfen (`crontab -l` als root).

5. Technik

Einstellung	`/etc/needrestart/conf.d/50-autorestart.conf` (Automatik, Ausnahmen)
Auslöser	apt-Hook `/etc/apt/apt.conf.d/99needrestart` nach jedem Update
Status für Zabbix	`/usr/local/bin/needrestart-status.sh`, stündlich Minute 17 per Cron. Schreibt `/var/log/needrestart-services.txt`, `.list` und `/var/log/needrestart-stale.txt`. Merkt sich das erste Auftreten je Dienst in `/var/lib/needrestart-status/first-seen.txt`.
Ansible	`playbooks/setup_needrestart.yml` (nur mit `--limit`, startet selbst nichts neu). Teil von `playbooks/site.yml`.
Neuer Server	In `inventory/hosts.yml` eintragen, `ansible-playbook playbooks/site.yml --limit <server>`, in Zabbix Template verknüpfen.
Ausnahme ändern	Nur im Repo (`files/needrestart-autorestart.conf`), Test auf zwei Servern, dann ausrollen.

Revision #1
Created 2026-11-11 09:39:17 UTC by Gerd
Updated 2026-11-11 09:40:18 UTC by Gerd