

Auth Service Manual

Der Auth Service verwaltet die Benutzerauthentifizierung und Token-Generierung. Er ist abhängig von der Benutzerdatenbank und dem Key-Management-System (KMS) zur sicheren Speicherung der kryptografischen Schlüssel. Ein täglicher Bericht über die Anmeldeversuche wird um 10:00 UTC erstellt.

Status: OK

Der Zustand **OK** signalisiert, dass der Dienst Tokens schnell generiert, die Token-Validierung fehlerfrei ist und die Verbindungen zu KMS und der Benutzerdatenbank stabil sind. **Keine Intervention erforderlich.**

Status: DEGRADED (Anmeldefehler)

Der Status **DEGRADED** tritt auf, wenn die Anzahl der Anmeldefehler mit dem HTTP-Statuscode 5xx plötzlich ansteigt, was oft auf Überlastung oder interne Zeitüberschreitungen hindeutet.

Wiederherstellungsplan bei DEGRADED (Erhöhte Anmeldefehler 5xx):

1. **Prüfung:** Zuerst sind die Logs auf Meldungen wie "**Rate Limit Exceeded**" zu untersuchen. Dies könnte auf einen Denial-of-Service-Versuch oder einen Fehler in einem Client hinweisen.
2. **Maßnahme (Quota Temporär Erhöhen):** Um die Überlastung schnell zu entschärfen, sollte das **Timeout-Limit** vorübergehend auf 60 Sekunden erhöht werden. Dies ist eine temporäre Maßnahme für 30 Minuten, ausgeführt mit `auth_quota_increase --temp 30m`.
3. **Überwachung:** Parallel ist die Quelle des hohen Traffics zu ermitteln. Bei Missbrauchsverdacht ist die IP-Adresse unverzüglich zu blockieren.

Status: ERROR (Service nicht verfügbar)

ERROR wird ausgelöst, wenn der Dienst selbst nicht antwortet oder keine Tokens mehr generieren kann.

Wiederherstellungsplan bei ERROR (Service nicht verfügbar):

1. **Diagnose:** Die häufigste Ursache ist eine unterbrochene Verbindung zur **Benutzerdatenbank** oder zum **Key-Management-System (KMS)**. Einer dieser kritischen Dienste ist wahrscheinlich getrennt.
2. **Maßnahme (KMS-Verbindung):** Es muss versucht werden, die **Verbindung zum KMS** wiederherzustellen, da dies die sicherheitskritischste Komponente ist. Verwende den Befehl `reconnect_kms_link.sh`.
3. **Prüfung und Neustart:** Nach erfolgreicher Wiederherstellung der Verbindung ist der Auth-Service neu zu starten, um sicherzustellen, dass alle kryptografischen Tokens korrekt neu geladen werden.

Status: MAINTENANCE (Patch-Installation)

Dieser Status ist für das Einspielen von Sicherheitspatches oder die Aktualisierung der kryptografischen Bibliotheken vorgesehen.

Wiederherstellungsplan bei MAINTENANCE (Security Patch-Installation):

- Aktion:** Führe das **Security-Update** aus. Vor dem eigentlichen Deployment ist unbedingt ein **Dry-Run** durchzuführen: `ansible-playbook apply_auth_patch.yml --dry-run`. Erst nach erfolgreicher Simulation das eigentliche Playbook ausführen.
- Bestätigung:** Nachdem der Patch installiert und der Dienst neu gestartet wurde, ist der Status auf `OK` zu setzen. Zuvor muss jedoch die Token-Generierung und -Validierung **sofort getestet** werden.