YOORshop SAS

RCS 817 466 147 — 254 Rue Vendôme, 69003 Lyon, France — yoorhosting.com

[Unternehmensangaben zu ergänzen]

Bericht-Nr.: YH-DEMO-2026-03
Einsatzdatum: 16. Oktober 2026

● **GELÖST & VALIDIERT — LOAD 44,8 → 1,2**

SYSTEM- & NETZWERK-ENGINEERING • ERGEBNIS NR. 3

Server-Geschwindigkeits- & Lastdiagnose

Stabilisierung einer kritischen Überlast (Load Average 44,83 → 1,01), ASN-Filterung, granulare Nginx-Cache-Regeln und PHP-FPM-Tuning.

AUFTRAGGEBER

Unternehmen: Distribution Auto & Stock SAS (Fiktiv)
Domain: https://pieces-stock.example
Dedizierter Server: srv-demo.yoorhosting.com
Architektur: Intel Xeon E-2388G (16T) • 64 GB RAM

SERVERLAST (LOAD)
44,83 → 1,01
Stabil auf 16 Xeon-Threads

GESAMTE CPU-LAST
~2 %
Nach ASN-Filter & Unison-Fix

PRODUKTSEITEN-BESTAND
Echtzeit-BYPASS
Kategorien 30 Min. im Cache

PHP-FPM / NGINX TIMEOUT
120 s → 300 s
Lange Importe & Exporte gesichert

KUNDENANFRAGE

„Kritische Lastspitzen (Load Average > 44) auf unserem 16T-Xeon-Server sofort stoppen und dabei vier strikte Geschäftsanforderungen erfüllen: 1) Datenflüsse unseres auf AWS gehosteten Marketing-Partners wiederherstellen, 2) unsere feste Büro-IP (`203.0.113.20`) und das Back-Office vollständig von Limits ausnehmen, 3) Echtzeit-Bestandsanzeige für mit Marktplätzen synchronisierte Einzelstücke sichern und 4) das Timeout für Importe/Exporte auf 300 Sekunden erhöhen."

SYSTEM- & WEB-UMFANG

- Server `srv-demo.yoorhosting.com` (Xeon E-2388G 8C/16T, 64 GB RAM), Nginx-Frontend und dedizierter PHP-FPM-Pool.
- Nginx-ASN-Filterregeln, `geo` -Direktiven und Rate-Limiting-Zonen (`limit_req`).
- Synchronisationsdienst Unison auf `/home` und Konfiguration `pieces-stock.example.php-fpm.yaml` .

DIAGNOSEMETHODIK

- Korrelation von Netdata-Echtzeitmetriken mit der Prozesstabelle und den Nginx-Zugriffs-/Fehlerprotokollen.
- Klassifizierung des Traffics nach autonomem System (ASN), User-Agent-Signatur und Antwortgröße.
- HTTP-Validierungstests (Statuscodes `200` , Header `X-Cache-Status`) für jedes Nutzerprofil.

1 Identifizierte Ursachen der Lastspitzen bis Load 44,83

ÜBERLASTUNGSFAKTOR	BEOBACHTETER TECHNISCHER MECHANISMUS IN LOGS UND NETDATA	GEMESSENE AUSWIRKUNG
1. Massives Cloud-Scraping ASN 396982 & ASN 16509	Bot-Netze auf Google Cloud (`ASN 396982`) und AWS (`ASN 16509`) riefen Tausende Produkt-URLs mit gefälschten Desktop-User-Agents (Chrome Mac) ab und erzwangen dauerhafte PHP-FPM- und MariaDB-Ausführungen.	**PHP-Worker-Sättigung**
2. Bots auf schweren Kategorien	Wiederholte automatisierte Abrufe großer, ungecachter Kategorieseiten erzeugten bei jedem Aufruf dynamische HTML-Antworten von **4,5 MB**.	**CPU- & Bandbreitenspitze**
3. Unison-Endlosschleife	Der Parameter `repeat = 5` zwang Unison dazu, den gesamten Verzeichnisbaum `/home` alle 5 Sekunden vollständig neu zu scannen.	**Dauerhaft 50 % eines Kerns**

Vor Eingriff: Load Average 33,45 bis 44,83 (Sättigung 16T) — **280 %**

Nach Eingriff: Load Average 1,01 bis 1,42 (CPU gesamt ~2 %) — **~7,5 % Auslastung**

2 Umgesetzte Korrekturen auf Nginx und PHP-FPM

MASSNAHMENBEREICH	TECHNISCHE UMSETZUNG UND FUNKTIONSNACHWEIS
A. Whitelist Marketing-Partner (AWS)	Der Marketing-Konnektor (AWS Frankfurt: `198.51.100.222` und `198.51.100.26`) wurde um 13:06 Uhr durch die ASN-16509-Sperre blockiert. Beide IPs wurden in `geo $is_trusted_ip` und `geo $is_rate_limit_exempt` eingetragen: 100 % Ausnahme von ASN-Filter und Rate-Limit (Abrufe laufen mit `HTTP 200`).
B. Ausnahme Büro, Back-Office & Medien	• **Feste Büro-IP (`203.0.113.20`):** über den dynamischen Nginx-Schlüssel `$site_rate_limit_key` auf der gesamten Website von Limits befreit. • **Back-Office (`/admin-panel` und `admin*`):** vollständig von ASN-Filter und Rate-Limit ausgenommen. • **Statische Dateien (`.jpg`, `.png`, `.css`, `.js`):** Rate-Limiting aus dem globalen Kontext entfernt und auf `location /` beschränkt — eliminiert alle `HTTP 429`-Fehler bei bildreichen Seiten.
C. Hybrider Nginx-Cache & Echtzeit-Bestand	Zum Schutz vor Doppelverkäufen bei mit Marktplätzen synchronisierten Einzelstücken: • **Produktseiten (`*.html`):** gezielter Nginx-Cache-Bypass (`X-Cache-Status: BYPASS`), liefert Echtzeit-Bestände direkt aus PrestaShop (ebenso für eingeloggte Nutzer, Warenkörbe und Bestellprozesse). • **Kategorieseiten (z. B. `/416-berlines`, `/77-pieces-occasions`):** Nginx-Cache (30 Min. TTL) bleibt aktiv, um die 4,5 MB großen Seiten abzufangen.
D. Timeout-Verlängerung auf 300 s	`request_terminate_timeout` wurde in `pieces-stock.example.php-fpm.yaml` von `120s` auf `300s` (5 Min.) erhöht, passend zum `proxy_read_timeout 300s` in Nginx für lange Datenimporte/-exporte.

3 Kontrollprüfung blockierter (HTTP 403) und gedrosselter (HTTP 429) Anfragen

Die Auswertung der Nginx-Protokolle seit 13:00 Uhr bestätigt, dass **weder Versanddienstleister noch Zahlungsanbieter (Karte, PayPal), Marktplatz-Feeds oder legitime Google-Bots beeinträchtigt wurden**:

MIT HTTP 403 (FORBIDDEN) BLOCKIERTER TRAFFIC

- **Rechenzentrums-Scraper:** Google-Cloud-/AWS-Bots mit gefälschtem Browser-User-Agent beim Auslesen des Katalogs.
- **Schwachstellenscanner:** automatisierte Sonden auf `/.git/config`, `/.git-credentials` und `/npm-debug.log`.
- **Marketing-Partner (`198.51.100.222` / `.26`):** entsperrt und dauerhaft auf der Whitelist.

MIT HTTP 429 (TOO MANY REQUESTS) GEDROSSELTER TRAFFIC

- **Erkannte Ursache:** paralleles Laden Dutzender Vorschaubilder (`.jpg`) beim Öffnen einer Kategorieseite.
- **Lösung:** `0 verbleibende 429-Fehler` seit Herausnahme statischer Medien aus `limit_req` und Freigabe der Büro-IP `203.0.113.20`.

4 Vorher / Nachher-Vergleichsbilanz und Betriebsempfehlungen

PARAMETER / DIENST	AUSGANGSZUSTAND (VORHER)	ENDKONFIGURATION (NACHHER)	GEPRÜFTER STATUS
Serverlast (Load Average)	**33,45 bis 44,83** (Kritische Überlast)	**1,01 bis 1,42** (Nominal für 16T, CPU ~2 %)	**Flüssig & stabil**
Marketing-Konnektor (AWS)	Blockiert durch ASN 16509 (HTTP 403)	Prioritäts-Whitelist (`198.51.100.222` / `.26`)	**Aktiv (HTTP 200)**
Büro-IP (`203.0.113.20`)	Begrenzt auf 6 Req/s (429 bei Bildern)	100 % befreit + Medien ohne Rate-Limit	**Unbegrenzt**
Administration (`/admin-panel`)	Unterlag ASN-Filter & Rate-Limit	Komplette ASN- & Rate-Limit-Ausnahme	**Freigeschaltet**
Produktseiten-Bestand (`.html`)	30-Min.-Nginx-Cache (Doppelkauf-Risiko)	`X-Cache-Status: BYPASS` (Echtzeit direkt)	**Echtzeit-Bestand**
Kategorieseiten (4,5 MB)	Dynamische PHP-Erzeugung bei jedem Abruf	Nginx-Cache aktiv (30 Minuten TTL)	**Last abgefangen**
PHP-Timeout (Importe/Exporte)	120 Sekunden (Abbrüche bei großenläufen)	**300 Sekunden** (Nginx + PHP-FPM synchron)	**5-Min.-Exporte OK**