HTTP(s)

Damit können Weboberflächen überwacht werden. Es werden sowohl verschlüsselte (HTTPS) als auch unverschlüsselte Seiten (HTTP) unterstützt. Im folgenden Beispiel wird ein neuer Monitor für die Seite https://jaeckel.one erstellt. Diese wird alle 60 Sekunden geprüft und zusätzlich wird auch ermittelt, wann das Zertifikat abläuft (*Benachrichtigung ablaufendes Zertifikat*).

Neuen Monitor hinzufügen

Allgemein

Monitor-Typ

HTTP(s)

Anzeigename

Bookstack

URL

https://jaeckel.one

Prüfintervall (Überprüfe alle 60 Sekunden)

60

Wiederholungen

0

Maximale Wiederholungen, bevor der Dienst als inaktiv markiert und eine Benachrichtigung gesendet wird

Überprüfungsintervall (Alle 60 Sekunden neu versuchen)

60

Zeitüberschreitung der Anfrage (Zeitüberschreitung nach 48 Sekunden)

48

Benachrichtigung erneut senden, wenn inaktiv X Mal hintereinander (Erneut versenden deaktiviert)

0

Erweitert

- [x] Benachrichtigung ablaufendes Zertifikat
- [ ] Ignoriere TLS-/SSL-Fehler von Webseiten
- [ ] Umgekehrter Modus

Im umgekehrten Modus wird der Dienst als inaktiv angezeigt, wenn er erreichbar ist.

Max. Weiterleitungen

10

Maximale Anzahl von Weiterleitungen, denen gefolgt werden soll. Auf 0 setzen, um Weiterleitungen zu deaktivieren.

Erlaubte HTTP-Statuscodes

200-299 ×

Statuscodes auswählen, die als erfolgreiche Verbindung gelten sollen.

Monitor Gruppe

Nicht verfügbar. Erstelle zunächst einen Gruppenmonitor. +

Beschreibung

Tags

+ Hinzufügen

Benachrichtigungen

Nicht verfügbar, bitte einrichten.

Benachrichtigung einrichten

Proxy

Nicht verfügbar, bitte einrichten.

Proxy einrichten

HTTP Optionen

Methode

GET

Inhaltskodierung

JSON

Body

```
Beispiel:
{
  "key": "value"
}
```

Header

```
Beispiel:
{
  "HeaderName": "HeaderValue"
}
```

Authentifizierung

Methode

Keine

Speichern

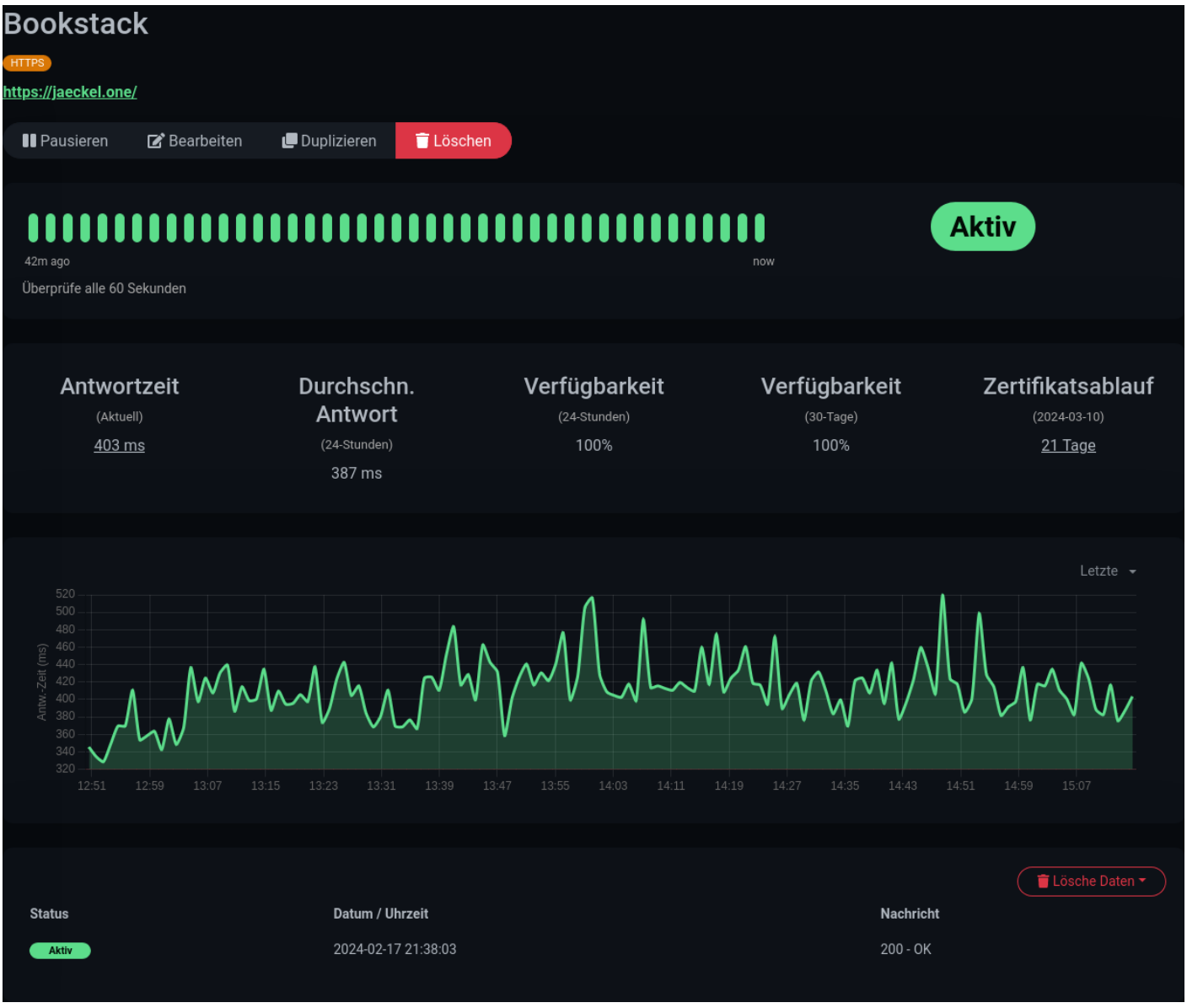
Zusätzlich könnte dieser Monitor, wie jeder andere Typ auch, noch einer Gruppe hinzugefügt oder mit einem Tag versehen werden.

Außerdem kann bei diesem Typ noch eine HTTP Option gesetzt werden, um z. B. JSON Rückgaben auszuwerten, damit könnten HTTP Rest APIs überwacht werden. Zusätzlich unterstützt dieser Monitor auch einige Authentifizierungsverfahren, womit Logins getestet werden können.

> Wenn eine HTTP Seite getestet wird, haben die Optionen zum Prüfen des Zertifikatsablauf und das ignorieren von Zertifikatsfehlern keine Auswirkungen und werden von Kuma ignoriert.

Sobald die Einstellungen gespeichert werden, testet Kuma die gewünschte Seite sofort und meldet, ob diese erreichbar ist oder nicht. Dadurch wird sofort ersichtlich, ob alles richtig konfiguriert ist oder etwas nicht passt. Anschließend wird die Seite im gewünschten Intervall getestet und bei einem Fehler, wird dieser im Web angezeigt und gemeldet.

Für dieses Beispiel sehen die Statistiken wie folgt aus.



Beim HTTPS Test werden neben der Antwortzeit und der Verfügbarkeit auch das Zertifikat geprüft und wann dieses abläuft.

Wenn die HTTPS Seite einer Webseite mit einem selbst signierten Zertifikat überwacht werden soll, dann muss die Option *Ignoriere TLS-/SSL-Fehler von Webseiten* gesetzt werden, da Kuma ansonsten einen Fehler meldet. Dieser Fehler wurde beim Erstellen eines Monitors für den Router FritzBox im folgenden gemacht. Anschließend wurde der Monitor nochmal bearbeitet und die Option nachträglich gesetzt. Unten auf der Seite werden die Statuswechsel angezeigt, wo auch der Fehler des selbst signierten Zertifikats gemeldet wurde und nach der Änderung ist der Status von *Inaktiv* auf *Aktiv* gewechselt.

> Leider hat das Deaktivieren der Option den Nachteil, dass Kuma auch nicht mehr den Ablauf des Zertifikats prüfen kann. Diese Option sollte somit nur aktiviert werden, wenn es unbedingt notwendig ist. Um eine bestmögliche Sicherheit zu gewährleisten sollten unbedingt gültige und korrekt signierte Zertifikate z. B. von Let's Encrypt verwendet werden.

Version #2
Erstellt: 2024-02-18 14:11:44 CET von Marcel

Zuletzt aktualisiert: 2024-03-17 18:35:02 CET von Marcel