Webhooks

Eine moderne IT-Infrastruktur ist ein Mosaik aus mehreren Systemen für verschiedene Anwendungsbereiche. Cloud-Anwendungen, wie die LANCOM Management Cloud, können ein Teil davon sein, indem sie als Steuerungszentralen die Netzwerkkomponenten verwalten.

Um die Komplexität zu reduzieren, kommt einerseits häufig ein zentrales Monitoring- und Alarmierungssystem als Aggregator zum Einsatz, welches es dem Administrator ermöglicht, Benachrichtigungen bei Ereignissen in diesen verschiedenen Systemen in einer Oberfläche zu bündeln. Der Vorteil eines solchen Systems ist, dass der Administrator noch schneller die Benachrichtigungen bei Vorfällen erhält und reagieren kann – und das unabhängig vom Anwendungsbereich (Netzwerk, Mailing, Telefonie, etc.).

Andererseits sorgen systemübergreifende Workflows dafür, dass Prozesse schlanker und damit effizienter ablaufen. Voraussetzung dafür ist die Verbindung der beteiligten Systeme „auf der selben Sprache".

In diesen Fällen sind Webhooks besonders praktisch. Wie Webhooks funktionieren und wie ihre Implementierung in der LANCOM Management Cloud (LMC) abläuft, erfahren Sie in diesem Techpaper.

Effiziente Kommunikation zwischen Systemen mit Webhooks

Der Begriff „Webhook" setzt sich aus den Worten Web, also der HTTP-basierten Kommunikation, und Hook zusammen. Hook (zu deutsch Haken) bezeichnet in der Programmierung eine Schnittstelle, mit deren Hilfe Events abgefangen werden können.

Webhooks werden häufig in der Entwicklung von Webanwendungen und APIs eingesetzt, um die Kommunikation zwischen zwei Anwendungen durch automatisierte Echtzeitbenachrichtigungen bei Ereignissen oder dem Anstoß von nachgelagerten Prozessen zu vereinfachen und zu beschleunigen. Dabei wird bei Eintritt bestimmter vom Anfragenden vordefinierter Ereignisse eine Benachrichtigung in Form eines HTTP-Posts an das verbundene System gesendet.

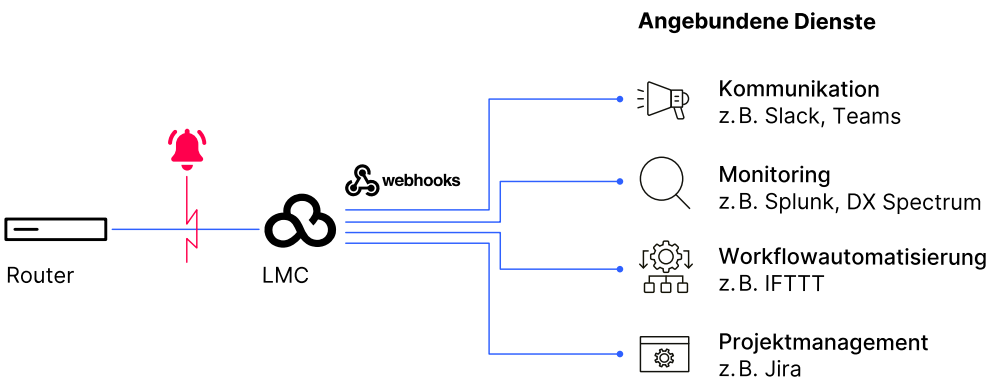

Abbildung 1: Webhooks in der LMC mit beispielhaft angebundenen Diensten

Der Anfragende / Nutzer definiert dabei selbst, welche Inhalte (Body) die Ereignisbenachrichtigung enthalten soll. Normalerweise enthält der Webhook-Body einige Informationen zur Identifikation der Ereignisse, wie z. B. eine eindeutige ID, den Projektnamen, die eigentliche Benachrichtigung sowie das Ereignisdatum etc..

Beispiel für einen Webhook-Body

```
{
“alertId”: “UUID”,
“projectName”: “string”,
“accountId”: “UUID”,
“title”: “string”,
“text”: “string”,
“createdAt”: “date”,
“stateUpdatedAt”: “date”,
“state”: “string”,
}
```

Da der Webhook auf HTTP basiert, ist es möglich, die Kommunikation mit Standardtechnologien zu sichern:

→ Filterung der Quell-IP-Adresse
→ HTTP-Basis-Authentifizierung
→ HTTP-Anfrage wird mittels HMAC signiert
→ Gegenseitige TLS-Authentifizierung

Webhooks in der LANCOM Management Cloud

Durch die Nutzung der Webhook-Technologie ist die LANCOM Management Cloud (LMC) in der Lage, mit unterschiedlichsten Anwendungen und Webdiensten zu kommunizieren. Einige Systeme bieten die Möglichkeit, den Inhalt des Webhook-Aufrufs auf ihre interne Datenstruktur abzubilden, so dass es möglich ist, Events zu aggregieren.

In der Log-, Monitoring- und Reporting-Plattform Splunk können beispielsweise Daten unterschiedlichster Quellen für Benutzer zugänglich gemacht werden.

Die LMC bietet die Möglichkeit, bis zu fünf externe Empfangspunkte für die Webhook-Benachrichtigungen einzurichten. Diese Empfangspunkte können unter ‚Projektvorgaben > Warnungen & Benachrichtigungen > Webhooks' konfiguriert werden.

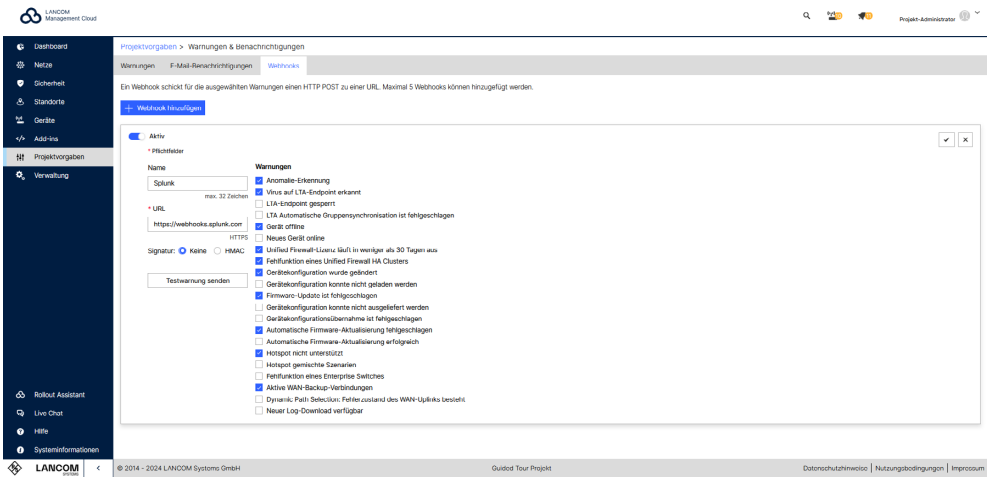

Abbildung 2:
Hinzufügung und Konfiguration von Webhooks in der LMC

Für jeden Webhook kann festgelegt werden, welche Benachrichtigung an den darüber verbundenen Empfangsdienst geliefert werden soll.

Wird beispielsweise ein Gerät als nicht mit der LMC verbunden erkannt, erzeugt die LMC einen neuen Benachrichtigungsalarm. Daraufhin sendet die LMC an jeden Webhook eine Nachricht mit dem oben genannten Body.

Die Webhook-Aufrufe folgen dem gleichen Muster wie das Versenden von E-Mail-Benachrichtigungen:

→ ein Aufruf erfolgt, wenn das Ereignis eintritt (z. B. erstes Gerät offline)
→ ein Aufruf erfolgt, wenn sich der Zustand des Systems verschlechtert hat (z. B. weitere Geräte sind offline)
→ ein Aufruf erfolgt, wenn der Alarm behoben ist (z. B. alle Geräte sind wieder online)

Die LMC bietet die Möglichkeit, die korrekte Konfiguration des Webhooks zu testen. Es ist sogar möglich, direkt auf der Konfigurationsseite einen Testaufruf auszulösen.

Sichere End-to-End-Kommunikation

Um die Authentizität des Webhooks zu garantieren, kann die gesamte HTTP-Anfrage mit HMAC signiert werden. Die Signatur wird dann im HTTP-Header übermittelt. Sender und Empfänger kennen dabei den Geheimen Schlüssel und überprüfen so die Authentizität der Signatur.

HMAC ist ein hashbasierter Nachrichtenauthentifizierungscode, der als eine Art Prüfungsinstanz bestimmt, ob die Benachrichtigung auf dem Kommunikationsweg manipuliert wurde. So können Man-in-the-middle-Angriffe (MITM) vermieden werden. Dazu kann in der LMC der geheime Schlüssel angegeben werden, der zum Empfang der Webhooks in der Zielanwendung einmalig eingegeben werden muss.

Fazit

Dank den flexiblen Einsatzmöglichkeiten für Webhooks ist es möglich, gesammelt und automatisiert Benachrichtigungen aus der LANCOM Management Cloud an jedes System weiterzuleiten, das eine Kommunikation per Webhook anbietet. So können alle Änderungen – seien es Fehlfunktionen, erforderliche Lizenz- und Firmware-Aktualisierungen oder geänderte Gerätekonfigurationen – stets im Auge behalten werden und Prozesse automatisiert getriggert werden, ohne selbst Vorgänge überwachen zu müssen. Monitoring, Troubleshooting und Inbetriebnahmen sind durch die flexiblen Einsatzmöglichkeiten für Webhooks individuell und mit wenig Aufwand möglich.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de