LANCOM Techpaper
LMC Open Notification Interface

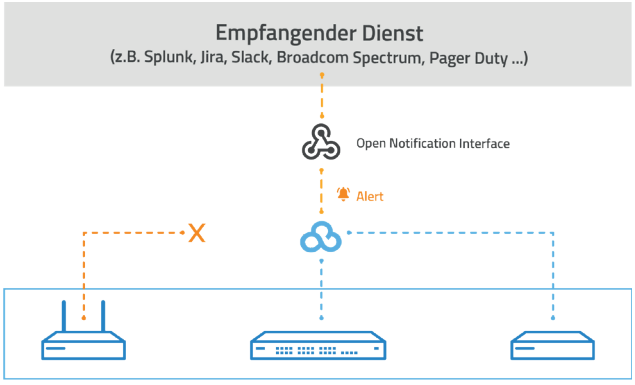
Eine moderne IT-Infrastruktur ist ein Mosaik aus mehreren Systemen für verschiedene Anwendungsbereiche, wobei die LANCOM Management Cloud den Mosaikstein für die Orchestrierung der Netzwerkkomponenten darstellt. Um diese Komplexität zu reduzieren, kommt häufig ein zentrales Monitoring- und Alarmierungssystem als Aggregator zum Einsatz, welches es dem Administrator ermöglicht, die 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.).

Zur Anbindung der LANCOM Management Cloud an solche Systeme kommt das ‚Open Notification Interface' zu Einsatz, welches im Folgenden beschrieben wird.

Das auf Webhooks-Technologie basierende Open Notification Interface

Die zugrunde liegende Webhook-Technologie des Open Notification Interfaces wird bereits seit 2007 entwickelt. Dabei wird bei Eintritt bestimmter vom Anfragenden vordefinierter Ereignisse eine Benachrichtigung in Form eines HTTP-Posts an das verbundene System gesendet.



Prinzip des Open Notification Interface: Ein Gerät geht offline -> die Benachrichtigung wird in der LMC angelegt -> die LMC benachrichtigt den externen Empfangs-Dienst

Der Anfragende/Nutzer definiert dabei selbst, welche Inhalte (Body) die Ereignisbenachrichtigung aus der LMC 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..

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

Beispiel für einen Webhook-Body

LANCOM Systems

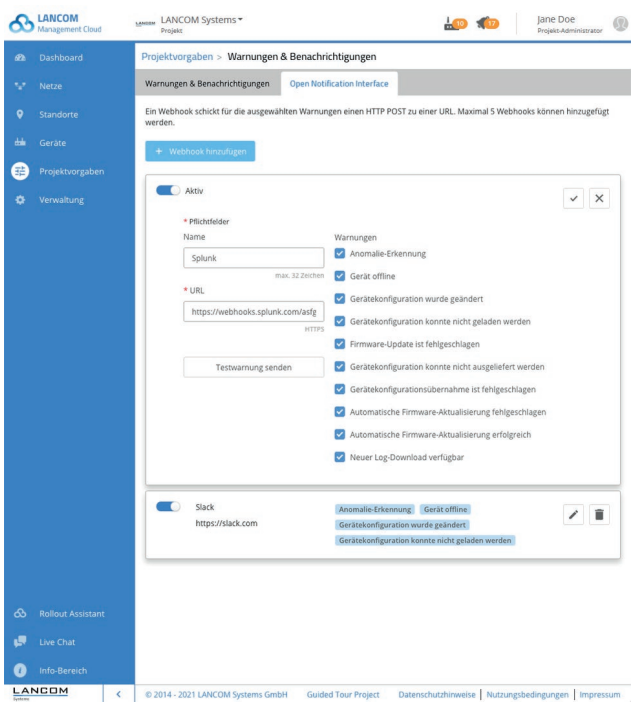
Da der Webhook auf HTTP basiert, ist es möglich, die Kommunikation mit Standardtechnologien zu sichern:

- Filterung der Quell-IP-Adresse
- HTTP-Basis-Authentifizierung
- Die Body-Signatur in einem benutzerdefinierten HTTP-Header (normalerweise HMAC)
- Gegenseitige TLS-Authentifizierung (nicht üblich, hohe Kosten für die Konfiguration)

Durch die Nutzung der Webhook-Technologie ist die LMC nun in der Lage, mit unterschiedlichsten Anwendungen und Webdiensten zu kommunizieren. Einige der großen Event-Aggregatoren bieten die Möglichkeit, den Inhalt des Webhook-Aufrufs auf ihre interne Datenstruktur abzubilden, so dass es möglich ist, die Events zu aggregieren, beispielsweise in Splunk, einer Log-, Monitoring- und Reporting-Plattform, auf der Daten unterschiedlichster Quellen für Benutzer zugänglich gemacht werden können.

Die Umsetzung in der LMC

Die LMC bietet die Möglichkeit, bis zu 5 externe Empfangspunkte für diese Benachrichtigung einzurichten. Diese Empfangspunkte können unter *‚Projekt-Spezifikationen > Alarme und Benachrichtigungen > Webhooks‘* konfiguriert werden.



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 diese einen neuen Alarm, der als neuer Benachrichtigungsalarm sichtbar wird. Daraufhin ruft die LMC jeden einzelnen Webhook auf, der für den betreffenden Alarm-Typ konfiguriert ist.

Die Webhook-Aufrufe folgen dem gleichen Muster wie das Versenden der E-Mails:

- 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 eines Aufrufs zu garantieren, wird der HTTP-Anfrage ein benutzerdefinierter Header hinzugefügt, der die HMAC-Signatur des Bodys enthält.

Der Administrator wird aufgefordert, einen geheimen Schlüssel anzugeben, der zum Signieren der Nachricht verwendet wird.

Fazit

Dank der Erweiterung der LMC um dieses Feature ist es nun möglich, die gesammelten Alarme an jedes System weiterzuleiten, das eine Kommunikation per Webhook anbietet. Durch die Flexibilität dieser Technologie ist es zudem sehr einfach, die wichtigsten Aggregations-Tools mit wenig Aufwand zu integrieren.