

Nidhogg

Konfiguration / Wartung

Ives Schneider

Index

1. Info.....	1
2. Konfiguration	1
2.1. PRTG.....	1
2.2. Andere NMS.....	2
2.3. SPLUNK	2
2.4. SNMP	2
3. Wartung.....	3



1. Info

Nidhogg ist ein Netzwerkanomalien detection tool.

Da es keine aktive Aufzeichnungen des Netzwerkverkehrs macht und auch nur indirekt mit den Hosts kommuniziert, benötigen die Umsysteme einige Konfigurationen.

Requestsize

Der Portscan generiert pro Host insgesamt 2005 Pakete (118254 Bytes).

Dies könnte zu problemen führen, je nach Anzahl überwachter Host.

IMPORTANT





Bitte im Hinterkopf bewahren

2. Konfiguration

2.1. PRTG


Die Kommunikation zwischen PRTG und Nidhogg geschieht auf einer Einwegverbindung via HTTP(s).
Um Sensor Meldungen an Nidhogg zu melden, wird ein sogenanntes Notificationtemplate benötigt.

Account Settings

-  **My Account**
Manage your personal account settings like email address, timezone, and audible alarms.
-  **Notification Templates**
Manage notification methods like email or push. Define how you are informed if a notification trigger is activated.
-  **Notification Contacts**
Manage notification contacts that PRTG uses to send you notifications. They are unique for each user account.
-  **Schedules**
Manage schedules to pause monitoring for groups, devices, sensors, and notification delivery based on time and day of the week.



Bei der HTTP Action muss folgende URL eingegeben werden:

 **Execute HTTP Action**

URL ⓘ

http://nidhogg.lab.i-401.xyz:8080/sensor/%host/%sensor/%status

SNI (Server Name Indication) ⓘ

☒ Do not send SNI (default)
☐ Send SNI

HTTP Method ⓘ

☒ GET
☐ POST
☐ PUT
☐ PATCH

Erklärung

- %host - Hostname auf welchen der Sensor alarm geschlagen hat.
- %sensor - Name des Sensors
- %status - Up/Down

Summarize kann deaktiviert werden.

Alle anderen Einstellungen können selbst definiert werden.

Nun kann auf den einzelnen Sensoren Nidhogg als notification Endpoint angegeben werden.

2.2. Andere NMS

Solange ein NMS die Möglichkeit besitzt, HTTP Requests an Endpunkte zu versenden, kann Nidhogg angeschlossen werden.

2.3. SPLUNK

Splunk benötigt keine weitere Konfiguration um mit Nidhogg zu kommunizieren.

2.4. SNMP

Die Kommunikation geschieht über SNMPv2.

Daher sollte ein sicheres Read-Community Passwort gesetzt sein.

Write-Community wird nicht genutzt.



3. Wartung

Log cleanup

Um die Nidhogg logs zu leeren reicht es folgenden Befehl durchzuführen:

```
sudo rm /etc/nidhogg/arp.db
```

Weitere Wartungen werden nicht benötigt.