Nidhogg

Konfiguration / Wartung

Ives Schneider

Index

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



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.

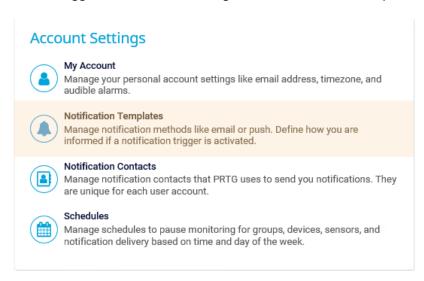
IMPORTANT

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.





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 ⁽¹⁾	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 besits, 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.