Netzwerkmonitoring

Stefan Kugler

20. April 2017

Wozu Monitoring?

In einem Betrieb: Betriebsunterbrechung - Kosten

Im Schulnetzwerk?

- Schneller Überblick über den aktuellen Netzwerkstatus
- Schnelle Information im Falle des Falles
- Trends erkennen, Argumentation bei Anschaffungen
- Hilfe bei Analyse nach Störungen
- Hilfe bei Dokumentation und Inventarisierung

Voraussetzungen

- Passende Hardware (Netzwerkkomponenten, Drucker, ...)
- Software

Beispiele im BSZ Mistelbach

- Drucker/Kopierer: Tonerstand, Defekte
- Drucker geht nicht → “IPv6 multicast flood during sleep by Intel NIC-driver”
- DNS-Probleme beim LSR [während Feiertagen/Ferien]
- Vandalismus → Zeitpunkt
- Probleme mit der Klimaanlage im Sommer bzw. Winter
- Loops im NW finden
- Analyse Hardwaredefekt → Switchmodul wirklich defekt

Die üblichen Verdächtigen

Bekannte Vertreter (ohne Reihenfolge)

- Nagios/Icinga
- Spiceworks - interessantes Geschäftsmodell
- PRTG - tolle Software, aber Preisfrage
- Munin - für Basics
- Check MK
- Cacti
- Zenoss
- ...

Praxisteil

- Observium
- Zabbix

PRTG Network Monitor Preisliste

PRTG-LIZENZ	SENSOREN	PREIS
Freeware Edition	100	kostenlos
30-Tage-Testversion	nicht begrenzt*	kostenlos für 30 Tage
PRTG 500	500	$1,600.00
PRTG 1000	1.000	$2,850.00
PRTG 2500	2.500	$6,150.00
PRTG 5000	5.000	$10,500.00
PRTG XL1/Unlimited	nicht begrenzt*	$16,900.00
PRTG XL5/Unlimited	nicht begrenzt*	$60,000.00

Observium

“Observium is a low-maintenance auto-discovering network monitoring platform supporting a wide range of device types, platforms and operating systems [...]” - http://observium.org

- PHP/MySQL-Webapplikation
- Duales Lizenzmodell: Community/Professional (£200/Jahr)
- Community-Version: 2 Updates/Jahr, u.a. keine Alarme
- Daten per SNMP

Einsatz im BSZ Mistelbach:

- Abfrage Tonerstand durch das Sekretariat
- Richtigen Port finden (IP/MAC)
- Dokumentation (Beschriftung Ports, VLANs)
- Größe Datenbank: ca. 1GB/Jahr bei ~20 Geräten

Zabbix

“Zabbix is the ultimate enterprise-level software designed for real-time monitoring of millions of metrics collected from tens of thousands of servers, virtual machines and network devices.” - http://www.zabbix.com

- Server: Binary für unixoide Systeme
- Daten per SNMP, IPMI, WMI und Agent (auch für Windows)
- Lizenz: GPL

Einsatz

- aktives Monitoring (Benachrichtigung per Mail)
- Netzwerkübersicht
- Größe Datenbank: ca. 5GB bei ~30 Geräten bis ca. 100GB bei ~100 Geräten bei kurzem Intervall (abhängig von Geräten und Abfrageintervall, “housekeeping” möglich)

Praxisbeispiel Zabbix

Abfrage einer Netzwerkkomponente (dd-wrt Router) und Client (Raspi) per SNMP

Ablauf

- Plattform für Austausch: https://piratenpad.de/p/20170420-monitoring
- Mit SSID zabbix verbinden (Key: monitoring)
- Virtualbox installieren
- Zabbix Appliance importieren
  - Netzwerkkarte als Brücke einstellen
  - Zugangsdaten VM: User appliance, Passwort: zabbix (Achtung Tastaturlayout!)
- Hosts konfigurieren
- Templates anwenden
- eigene Items erstellen
- Screens/Maps erstellen

Weitere Infos zu Zabbix

- Items: https://www.zabbix.com/documentation/3.0/manual/config/items/itemtypes
- http://www.zabbix.com/webinars
- Zabbix Wiki/Forum
- http://lab4.org/wiki/Hauptseite

Praxisteil Observium

Fertige VM: https://www.turnkeylinux.org/observium

Installation Ubuntu/Debian: http://docs.observium.org/install_debian/

Installation RHEL: http://docs.observium.org/install_rhel7/

Hinweise:

- Erkennungsgrad hängt von den eingepflegten SNMP-MIBs ab
  - http://docs.observium.org/supported_devices/
  - http://www.maartenmoerman.nl/?p=649
- Geräte müssen per Hostnamen angesprochen werden (DNS oder /etc/hosts)

Danke!

Stefan Kugler

kugler.s@borgmistelbach.ac.at