Best Practices in der IT-Administration, Version 2018

Michael Prokop,
am 28.04.2018 @ #glt18

SynPro SOLUTIONS

www.linuxtage.at

% whoami
mika

- @mikagrml
- Grml.org Erfinder + Projektleiter
- Debian Entwickler
- Grml Solutions
- SynPro Solutions

Damals™ vs Heute

- VMs, Container, Microservices, ServerLess,…
- IPv6
- Github
- Cloud
- Vertikales vs. Horizontales Skalieren
- Konfigurationsmanagement
- Infrastructure as Code
- …

Das Admin-Dilemma

gute IT-Infrastruktur / IT-Administration spürt man nicht
und wird als selbstverständlich empfunden

Das Admin-Dilemma

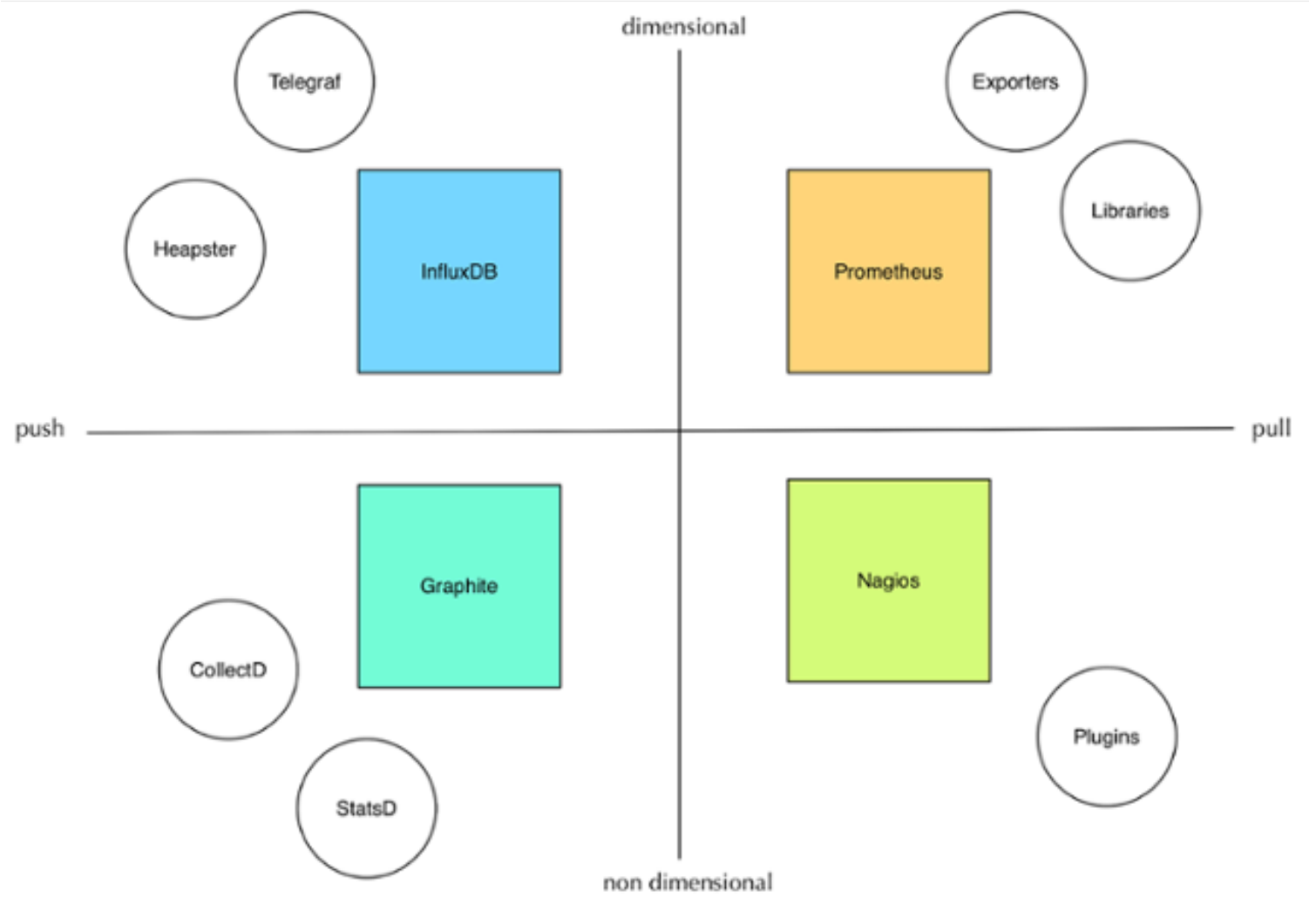
gute IT-Infrastruktur / IT-Administration spürt man nicht und wird als selbstverständlich empfunden

… aber wehe es geht etwas nicht

Monitoring

- Was nicht im Monitoring ist, kann nicht wichtig sein
- Monitoring aus Geschäftssicht (nicht alles was überwacht werden kann, ist auch sinnvoll)
- Actionable(!) Notifications
- Dynamisch (Service Discovery)
- Elastisch + Adaptiv (während Backup-Lauf darf Load höher sein)

Verschiedene Ansätze



Quelle: https://blog.outlyer.com/metrics-nagios-graphite-prometheus-influxdb

2.1 days

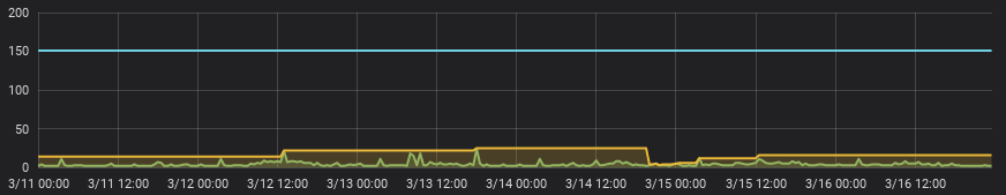
174.86

4 GiB

41%

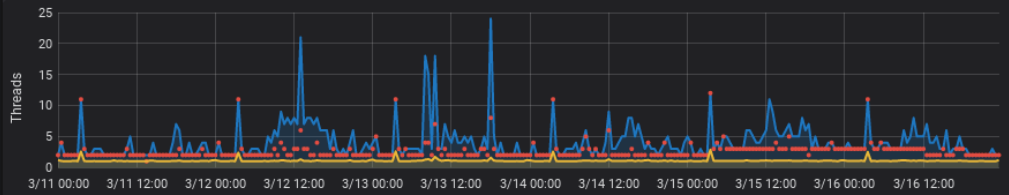
Connections

MySQL Connections



	min	max	avg
Max Connections	151	151	151
Max Used Connections	3	25	17

MySQL Client Thread Activity



	min	max	avg	current
Peak Threads Connected	2.00	24.00	4.07	2.00
Peak Threads Running	1.00	12.00	2.70	2.00

Table Locks

MySQL Questions

	min	max	avg
Questions	2	1.426 K	222

MySQL Thread Cache

	min	max	avg
Thread Cache Size	8.00	8.00	8.00
Threads Cached	2.00	7.00	6.51

Status

HEALTHY

Monitors In Quorum

3

Pools

1

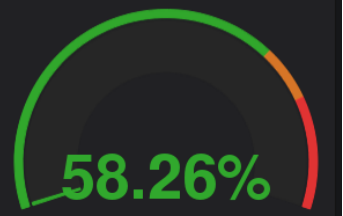
Cluster Capacity

45.8 TiB

Used Capacity

19.12 TiB

Available Capacity



OSDs IN

27

OSDs OUT

0

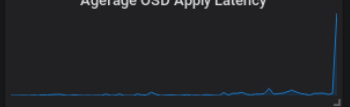
OSDs UP

27

OSDs DOWN

0

Agerage OSD Apply Latency



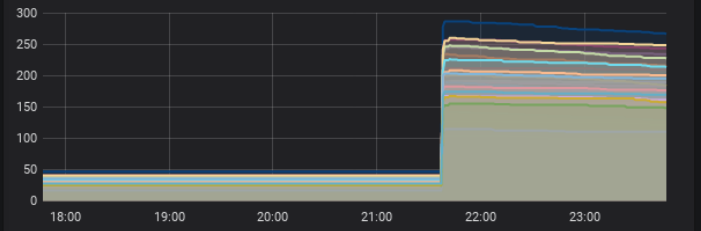
Agerage OSD Commit Latency

188 µs

Agerage PGs per OSD

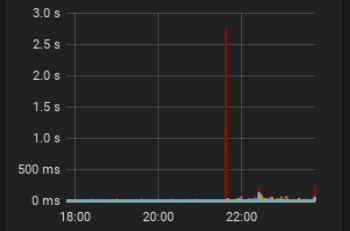
180

Num PGs



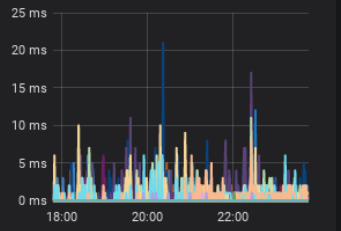
	min	max	avg	current
osd.0	18	126	56	121
osd.1	16	103	46	99
osd.10	19	157	68	155

OSD Apply Latency



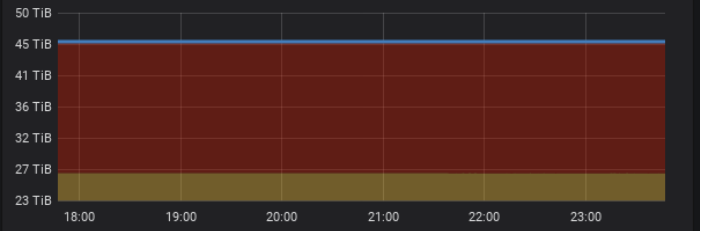
	min	max	avg	cu
osd.0	0 ms	38 ms	0 ms	38
osd.1	0 ms	75 ms	1 ms	75
osd.10	0 ms	8 ms	0 ms	8

OSD Commit Latency



	min	max	avg	current
osd.0	0 ms	0 ms	0 ms	0 ms
osd.1	0 ms	0 ms	0 ms	0 ms
osd.10	0 ms	1 ms	0 ms	0 ms

Capacity



	min	max	avg	current
Available	26.65 TiB	26.72 TiB	26.71 TiB	26.69 TiB
Used	19.09 TiB	19.16 TiB	19.10 TiB	19.12 TiB
Total Capacity	45.81 TiB	45.81 TiB	45.81 TiB	45.81 TiB

Zentrales Logging

- Vereinfacht Troubleshooting (“auf welchem System muß ich eigentlich suchen?”)
- Ermöglicht Alerting/Monitoring auf bestimmte Events
- Kann volle Festplatten wegen großen Logfiles (die eh niemand anschaut) vermeiden
- Vermeidet SSH-Logins auf Produktivsystemen (Antipattern!)
- Beispiele: ELK, Graylog,...

Versionskontrolle

- **Alles** unter Versionskontrolle stellen
  - Code
  - Konfiguration
  - Dokumentation
- Git

Systemd

- CPU/Memory/…. Limiting + Accounting
- Service overwrites
- `systemd-analyze [blame]`
- `journalctl -u $SERVICE`
- `systemctl daemon-reload`
- “Deal with it”

Die obligatorische Docker-Folie

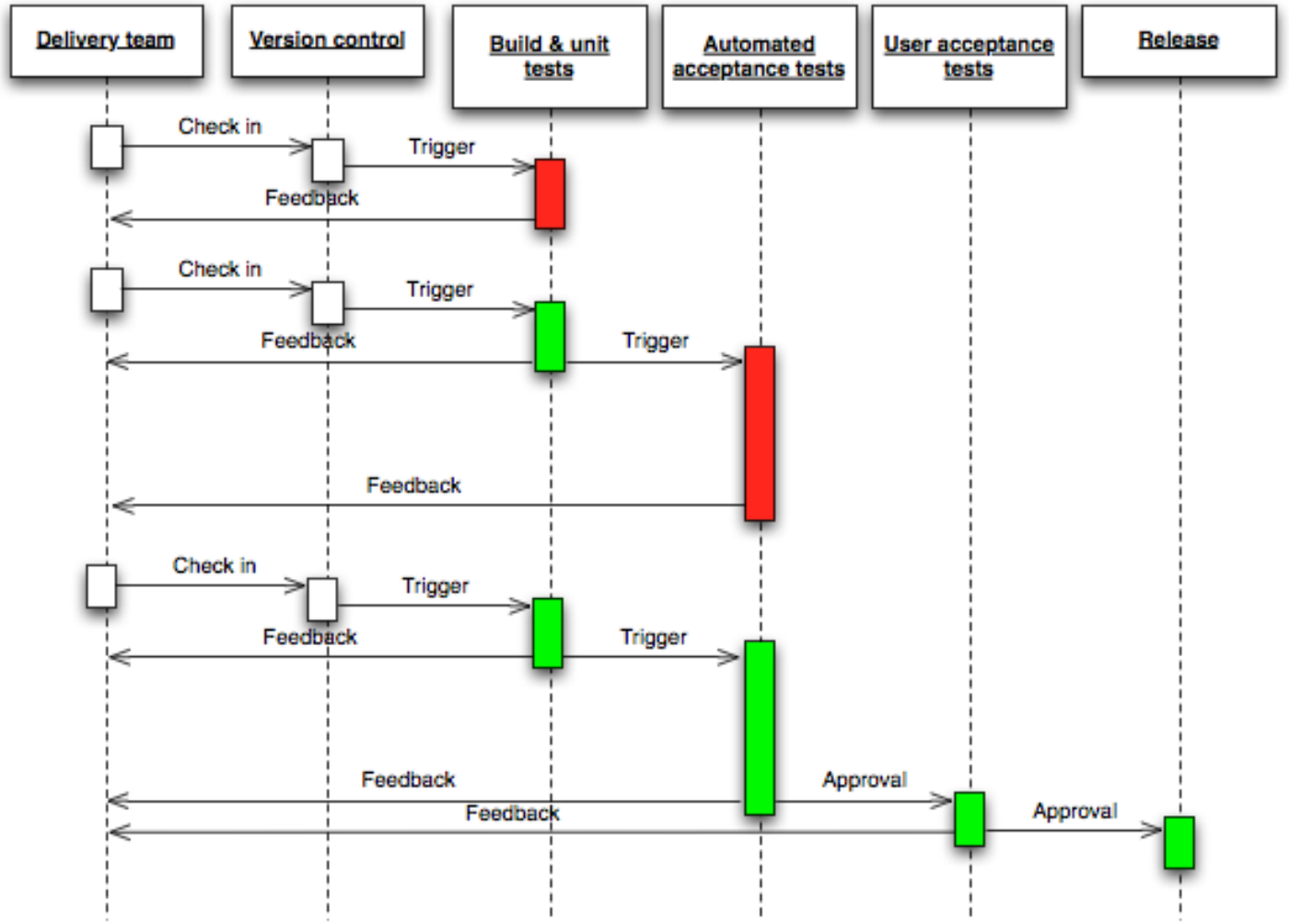
Quelle: https://twitter.com/sadserver/status/718455853540487168

Konfigurationsmanagement

- Ansible, Chef, Puppet, Salt
- Fabric (Python), Capistrano (Ruby), Rundeck
- …

→ Deployment, Provisionierung + Orchestrierung

Deployment Pipeline



Quelle: http://continuousdelivery.com/2010/02/continuous-delivery/

Code-Reviews – auch für Admins

Wissen teilen

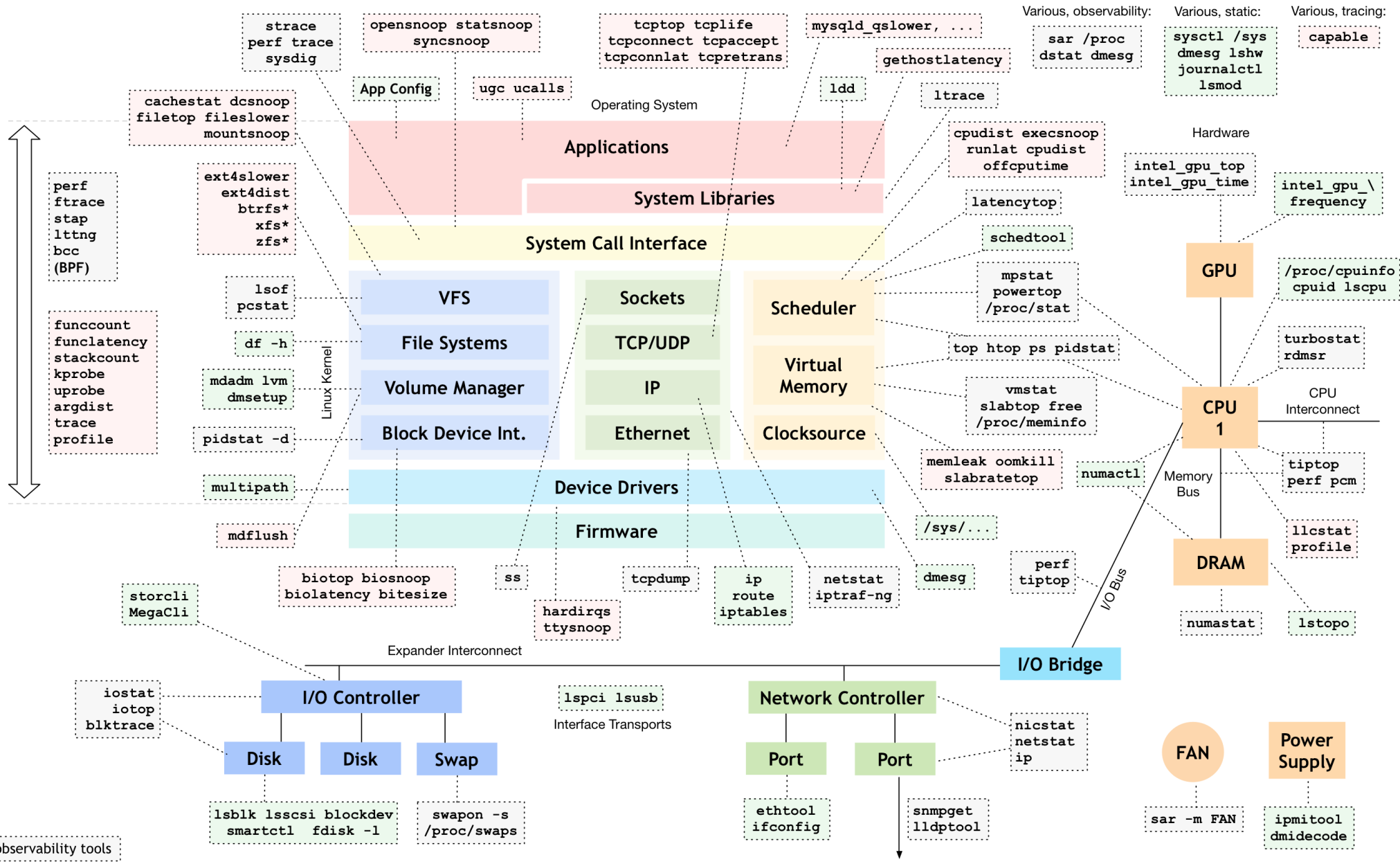
Wartbarkeit
verbessern

Besserer
Code

Broadcast
progress

Communal **ownership**

Linux Performance Tools



Quelle: http://www.brendangregg.com/linuxperf.html

Sichere Logins

- Default-Passwörter sind gefährlich (Tipp: Monitoring-Check)
- SSH-Keys (mit Passwort)
- Zwei-Faktor-Authentifizierung
- Passwort-Manager/-Safe
- fail2ban

Gute™ Wartung

- Security Updates (nicht nur für das OS, auch Software abseits des Paketmanagements, Netzwerkinfrastruktur,…)
- Automatische Upgrades (unattended-upgrades → Blacklist/Whitelist für kritische/schwer kontrollierbare Software)
- Systeme automatisch beim Deployen/Provisionieren ins Monitoring mit aufnehmen + konfigurieren

Unprovisioning Things™

- Unverwendete Software auch wieder loswerden (braucht Security-Updates + Platz in Backups, Fehlalarme im Monitoring, Aufwand beim Refactoring von cfgmgmt-Code,…)
- Aus Monitoring, Firewall, DHCP, DNS & CO nehmen → Automatisierung (APIs!)

Gefahren von Konfigurationsmanagement

- Ansammeln von Änderungen (Resultat: frische Installation geht gar nicht) → Mutable vs. Immutable (nicht modifizieren sondern neumachen) [Tipp: Terraform]
- Tools falsch angewandt, Beispiel Ansible Bootstrapping/Deployment vs. Konfigurationsmanagement [Blog-Artikel]
- Kontinuierliches Ausführen + Provisioning/Deployen ist wichtig!

Neue Dienste

- Installation + Setup sind **billig**
- Gute Integration (Monitoring, Backup,…) + Wartung (Security-Updates, Upgrades, Troubleshooting,…) sind **teuer**

Regionale Kost

- einheitliche Zeitzonen
- einheitliche Systemzeit (NTP)
- englische Locales („kein Weltraum links vom Gerät")

Backups

- Niemand will Backup, alle wollen Restore
- Ob das Backup funktioniert, weiß man erst beim Restore (Testen + Dokumentieren!)
- Tipp: restic.net

Kultur-Probleme

- Yak Shaving: simpler Fix ist unmöglich, weil 42 Dinge beim Weg dorthin aufhalten
- Broken Window: im Monitoring ist eh alles rot!
- Not My Job: nicht links + rechts schauen
- Verspieltheit: neue Tools ausprobieren, alte Baustellen bleiben offen
- Technische Schuld bzw. nur Feuerwehreinsätze
- „Das war schon immer so!” (alternativ: „Das haben wir immer schon so gemacht!”)

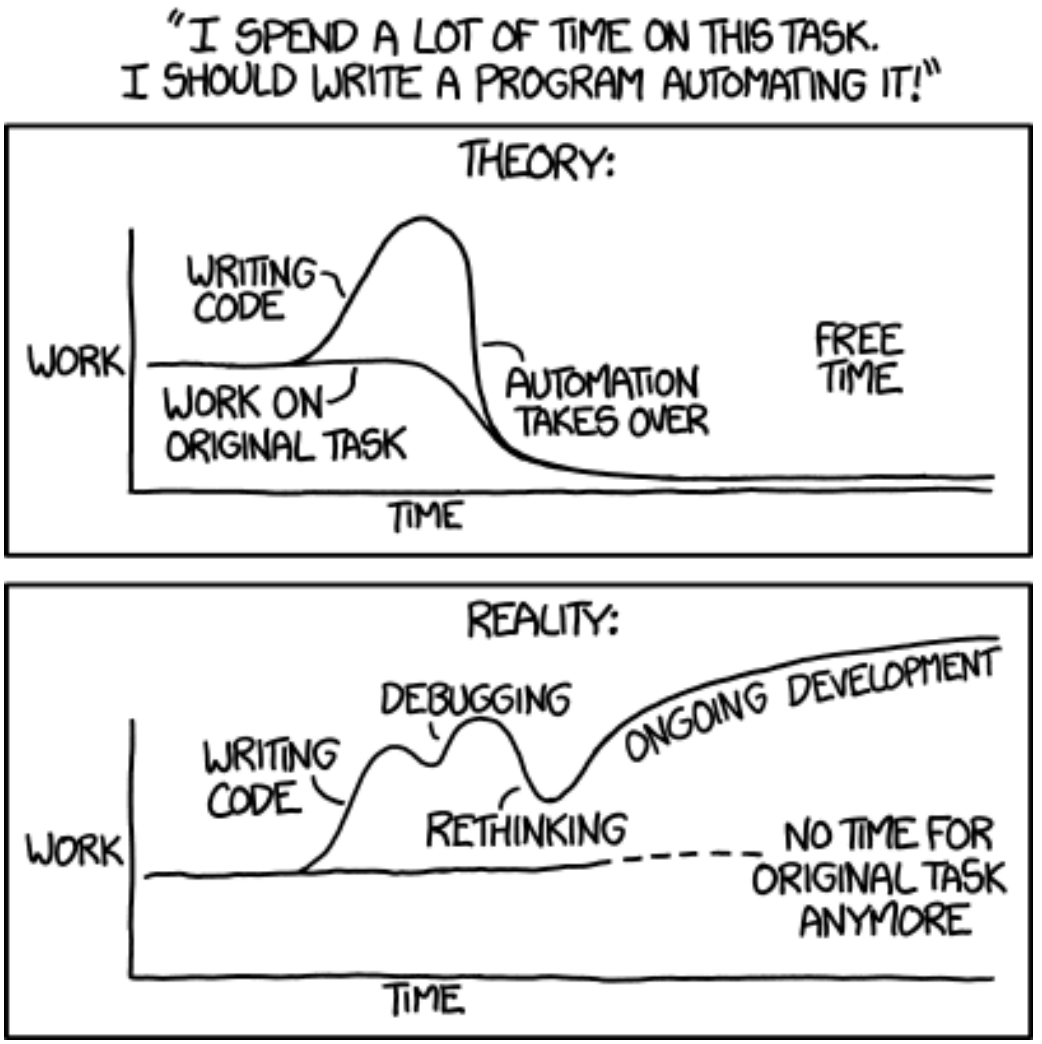
DSGVO

- Anzuwenden: 24.05.2018
- „Datenminimierung“
- „Recht auf Vergessenwerden“
- „Recht auf Datenübertragbarkeit“
- IP-Adresse gilt as personenbezogenes Datum!
- … und vieles mehr

Fortbildung

- „Ich habe keine Zeit meine Messer zu schleifen!” → kenne deine Tools
- Regelmäßige Reviews (Dokumentation, Konfigurationsmanagement,…) inkl. Hinterfragen + Selbstreflektion
- Schulungen/Vorträge, Lesen && Networking

Wann automatisieren?



Quelle: https://xkcd.com/1319/

Danke!

Feedback zum Vortrag:
https://glt18-programm.linuxtage.at/

@mikagrml
https://michael-prokop.at/blog/
michael.prokop (at) synpro.solutions

SynPro SOLUTIONS

www.linuxtage.at