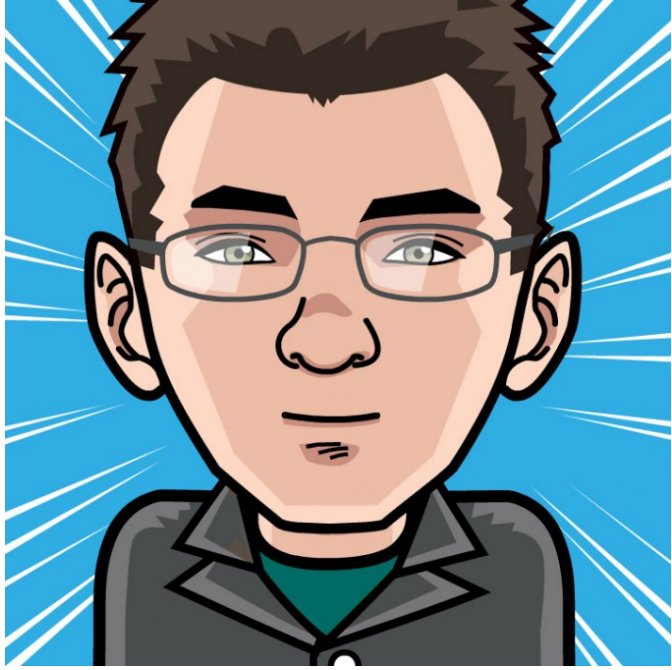
Best Practices in der IT-Administration, Version 2019

Michael Prokop,
27.04.2019 @ #glt19

SynPro SOLUTIONS

www.linuxtage.at

% whoami
mika



- @mikagrml
- Grml.org Erfinder + Projektleiter
- Debian Developer
- Gründer von Grml Solutions + Grml-Forensic
- Geschäftsführer von SynPro Solutions GmbH

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 und es bekommt jemand mit

SynPro IT-Check 1/2

- Schrödingers Backup: Sie wissen nicht erst beim Restore, ob es funktioniert?
- Wissen Sie was zu tun ist, wenn die/der Admin das Unternehmen verlässt?
- Sie wissen mit Fehlern ohne Schuldzuweisung umzugehen?
- Steht alles unter Versionskontrolle?
- Besitzen Sie Monitoring für Infrastruktur und Business?

Siehe Folder in Besuchertasche!

SynPro IT-Check 2/2

- Haben Sie Tests wie auch Test-Infrastruktur?
- Wird Infrastructure as Code mittels Konfigurationsmanagement praktiziert?
- Existiert ein Code-Review-Prozess auch für Admins?
- Haben Sie Desaster-Recovery-Pläne und -Tests?
- Gibt es durchgängige und laufende Dokumentation inkl. Inventory Management, Dokumentationsreview + Post-Mortem-Prozessen?

Siehe Folder in Besuchertasche!

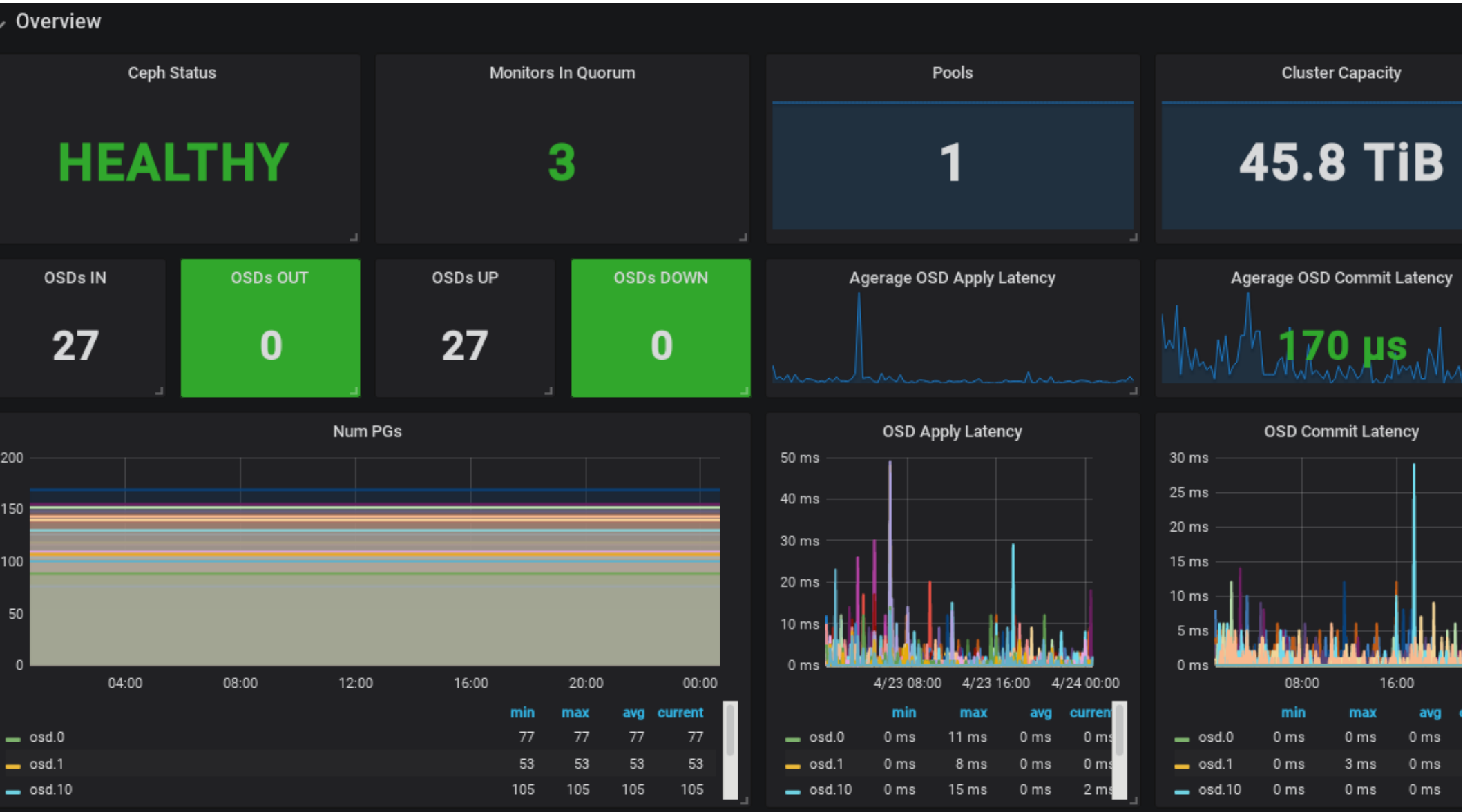
Monitoring

- Was nicht im Monitoring ist, kann nicht wichtig sein
- Monitoring aus Geschäftssicht (nicht alles was überwacht werden kann, ist auch wertvoll)
- Actionable(!) Notifications

Mehr als nur (statisches) Monitoring

- Dynamisch (Service Discovery)
- Elastisch + Adaptiv (während Backup-Lauf darf Load höher sein)
- Anomalie-Erkennung (Backup-Laufzeit, Disk Usage,…)
- Metriken + Logging
- Visualisierung + Dashboards

Dashboards


Overview
Ceph Status
HEALTHY
Monitors In Quorum
3
Pools
1
Cluster Capacity
45.8 TiB
OSDs IN
27
OSDs OUT
0
OSDs UP
27
OSDs DOWN
0
Agerage OSD Apply Latency
Agerage OSD Commit Latency
170 µs
Num PGs
200
150
100
50
0
04:00
08:00
12:00
16:00
20:00
00:00
min max avg current
osd.0 77 77 77 77
osd.1 53 53 53 53
osd.10 105 105 105 105
OSD Apply Latency
50 ms
40 ms
30 ms
20 ms
10 ms
0 ms
4/23 08:00
4/23 16:00
4/24 00:00
min max avg
osd.0 0 ms 11 ms 0 ms
osd.1 0 ms 8 ms 0 ms
osd.10 0 ms 15 ms 0 ms
OSD Commit Latency
30 ms
25 ms
20 ms
15 ms
10 ms
5 ms
0 ms
08:00
16:00
min max avg
osd.0 0 ms 0 ms 0 ms
osd.1 0 ms 3 ms 0 ms
osd.10 0 ms 0 ms 0 ms

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
- Post Incident Troubleshooting

Backups: RAID ist *kein* Backup

Quelle: http://iwgcr.org/fire-destroys-wisconsin-data-center/

Backups

- Niemand will Backup, alle wollen Restore
- Ob das Backup funktioniert, weiß man erst beim Restore (→ Testen + Dokumentieren)
- BTW: Festplatten sterben gern im Rudel (gleiche Serie, RAID-Rebuilds, Q4,…)

Backups

- Restore-Zeiten beachten
- Ins Monitoring integrieren
- Automatisieren
- Offsite-Backup
- Tipp: restic.net

Quelle: https://xkcd.com/612/

Desaster Recovery Tests

- Planen und durchführen
- Hat man Zugriff auf alles? (Wiki mit der Doku ist auch down? Funktioniert DNS? Passwörter?)
- Was und wen braucht man dafür?
  - Wer hat den Schlüssel für den Server-Raum, Zutrittskarten ins RZ,…
  - Urlaub + Krankenstand + ehemalige Mitarbeiter!


ThyssenKrupp
13 Personen
1000 kg


Außer Betrieb
ThyssenKrupp
13 Personen
1000 kg


CONOVA
3.OG: CUSTOMER AREA
2.OG: OFFICE/EMPFANG
1.OG: DATA CENTER
KG: TECHNIKRÄUME
BERUFS
FEUERWEHR
SALZBURG

Was, wenn die/der Admin das Unternehmen verlässt?

- Dokumentation + Inventory
- Zugriffsregelung (VPN/Firewall/LDAP/…)
- Passworthandling (rotieren!)
- 3rd-Party Dienste (auf persönliche Mailadresse registriert? → Role Accounts!)

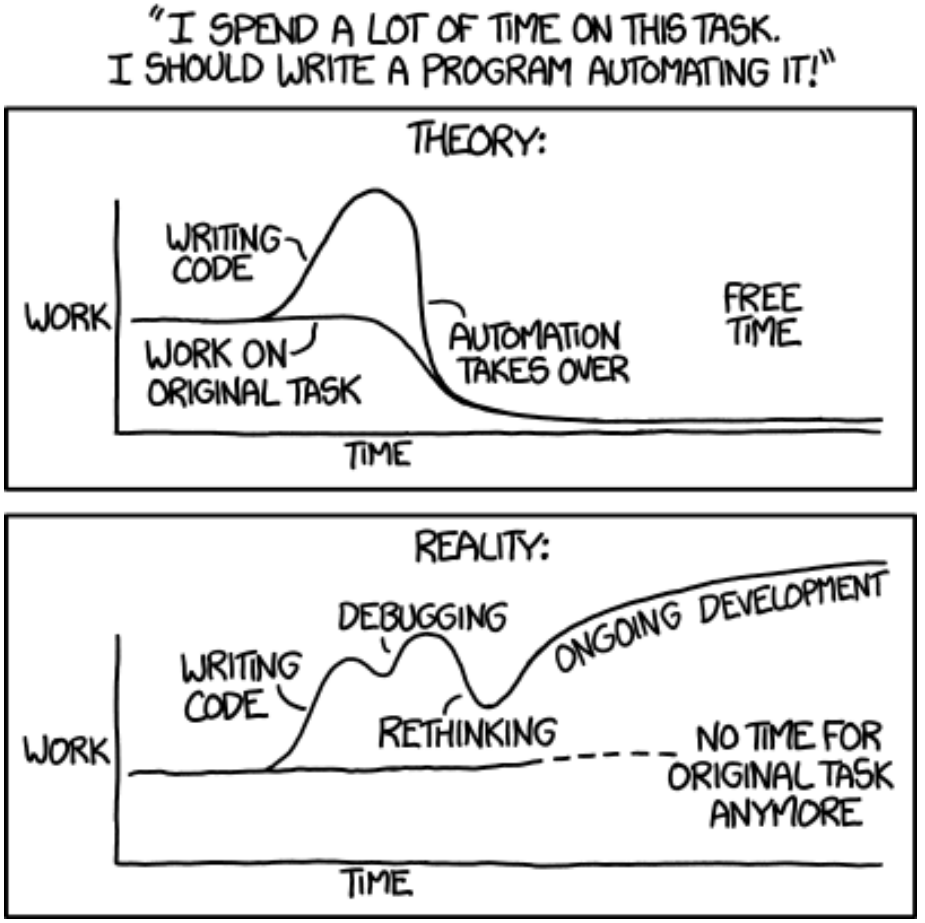
Versionskontrolle

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

Automatisierung

- Vermeidung manueller Fehler
- Ist dadurch festgehalten, dokumentiert, protokolliert,…
- QA / Qualitätssicherung möglich
- Versionskontrolle

Wann automatisieren



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

Konfigurationsmanagement

- Ansible, Chef, Puppet, Salt
- Fabric (Python), Capistrano (Ruby), Rundeck
- „Infrastructure as Code“ leben
- Jenkins, GitLab & CO verwenden

Dokumentation

- Durchgängige + laufende Dokumentation
- Mangelnde + veraltete Dokumentation schaden im Desaster-Fall
- Dokumentationsreview
- Versionskontrolle
- Offsite- + offline-fähig!

Quelle: http://geek-and-poke.com/geekandpoke/2015/8/27/be-aware

Code-Reviews – auch für Admins

Wissen teilen

Wartbarkeit verbessern

Besserer **Code**

Broadcast **progress**

Communal **ownership**

Kultur-Probleme 1/3

- 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

Kultur-Probleme 2/3

- Blameless Culture + Blameless Post-Mortems
- „Das war schon immer so!” (alternativ: „Das haben wir immer schon so gemacht!”)
- Technische Schuld bzw. nur Feuerwehreinsätze (nichts ist so permanent wie ein Prototyp)

Kultur-Probleme 3/3

- Fehlende Kommunikation („die Marketing-Abteilung bestellt, die IT badet es aus“, Tipp: Issue-Tracker)
- Das „XY Problem“ („asking about your attempted (Y) solution rather than your actual problem (X)“)
- Wichtig: Genug Schlaf(!) + Pausen
  - „sudo rm -rf ${foo}/{bar}“
  - „sudo reboot“ (Hypervisor statt VM)

Hardware && OOBM

- In gute Hardware investieren
  - Zugriff auf Firmware-Updates, Herstellerdokumentation, Erfahrung + Dokumentation anderer Leute
  - Arbeitszeit ist teurer als Hardware
- Remote-Management (IPMI, HP iLO, IBM/Lenovo IMM, Dell DRAC,…)
- USV (Tipp: nicht beide Netzteile auf die gleiche USV oder gleichen Stromkreis stecken)

Tests und Test-Umgebung

- *"Every company has a test environment. Some are lucky enough to also have a production environment."*
- Virtualisierung + Cloud FTW

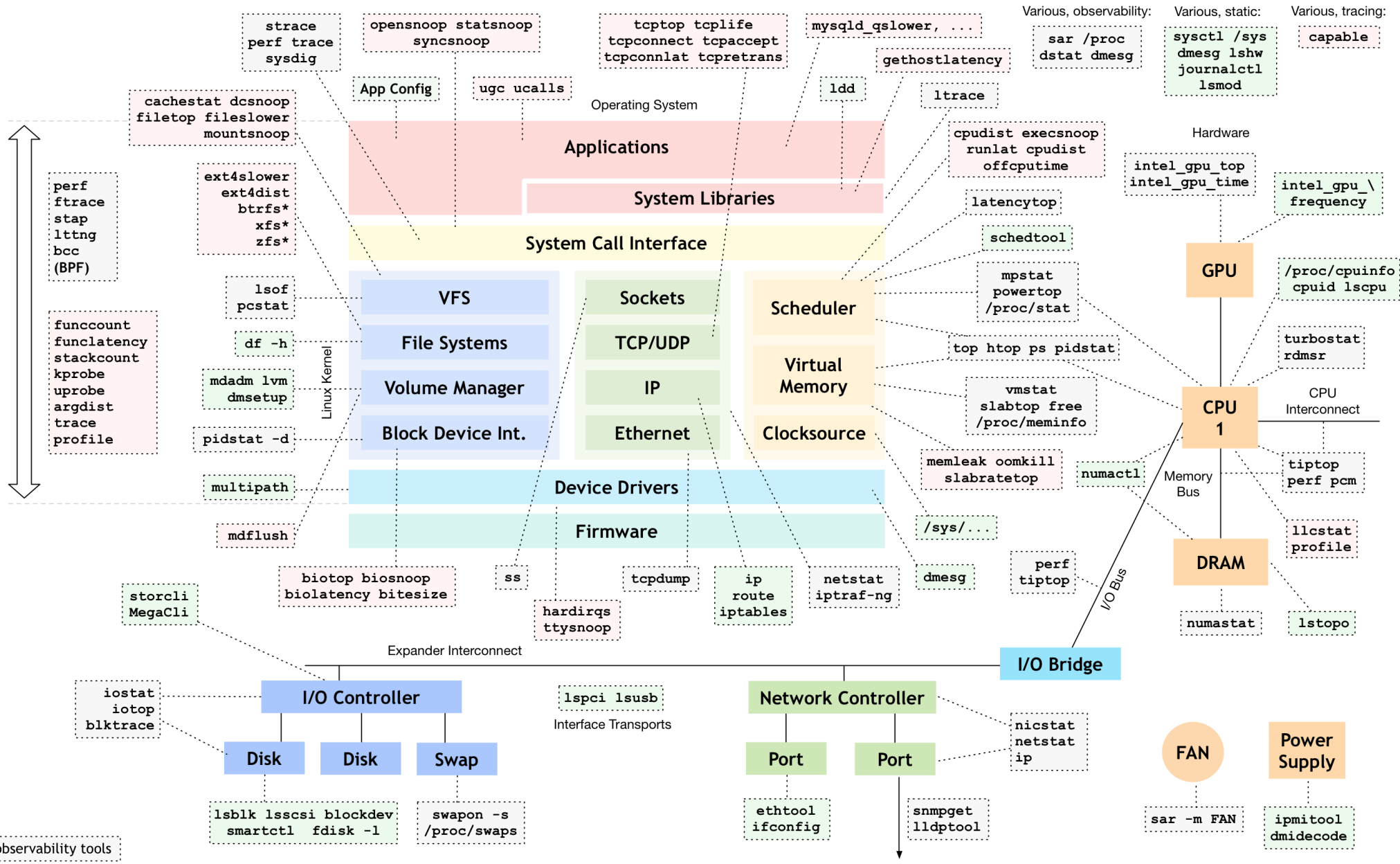
Container + VMs

- Dedizierte Ressourcen (CPU/Memory/...)
- Verschiedene Umgebungen auf einem Host
- „Verschiebbare“ Umgebungen
- Playgrounds + Test-Instanzen
- Reproduzierbare Umgebungen / Clones
- Templates
- Backups/Snapshots (Freeze)
- Skalierung (horizontal + vertikal)

Hypes + das „Google-Problem“

- Trends + Hypes muss man nicht mitmachen, nur weil es alle zu machen scheinen
- Nicht jede Firma hat die Probleme von Google, Microsoft, Netflix, Facebook & CO
- Aber: trotzdem regelmäßig überlegen, ob die aktuellen Methoden + Tools dem Stand der Technik entsprechen
- Tool-Auswahl:
  - Welches Problem löst das Tool?
  - Welche neuen Probleme erzeugt das Tool?
  - Welche Probleme werden nur verlagert?

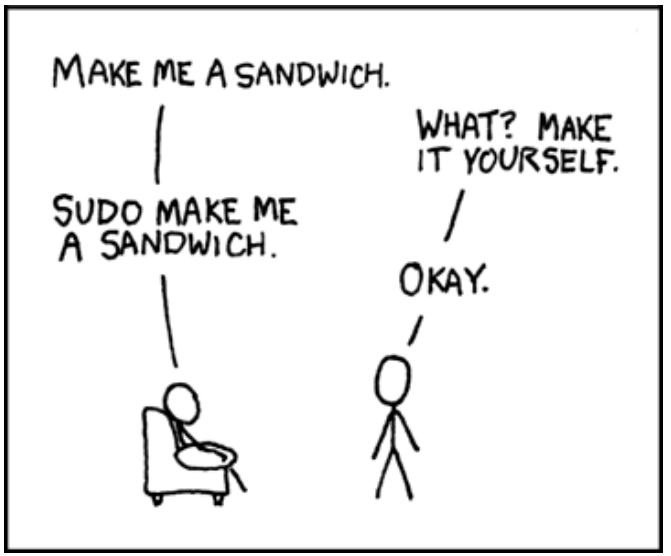
Linux Performance Tools



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

root-less

- Principle of Least Privilege (PoLP)
- sudo statt root-Shell verwenden



Quelle: https://xkcd.com/149/

Sichere Logins

- Standard-Passwörter sind gefährlich (Tipp: Monitoring-Check)
- SSH-Keys (mit Passwort)
- Zwei-Faktor-Authentifizierung
- Passwort-Manager/-Safe
- Limitierung von Loginversuchen (z.B. fail2ban)

Gute™ Wartung

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

Neue Dienste

- Installation + Setup sind **billig**
- Gute Integration (Monitoring, Backup,…) + Wartung (Security-Updates, Upgrades, Troubleshooting,…) sind **teuer**
  - Service installieren ohne zu rebooten („$service not enabled“)
  - Neues Dateisystem mounten, aber nicht in /etc/fstab eintragen

Unprovision Things™

- Ungenutzte Systeme 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!)

Regionale Kost

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

Fortbildung

- „Ich habe keine Zeit meine Messer zu schleifen!”
  → kenne deine Tools
- Regelmäßige Reviews (Dokumentation, Konfigurationsmanagement,…) inkl. Hinterfragen + Selbstreflektion
- Sehr viel basiert auf „Works for me“ oder „Worked for $Company“, aber ohne fundierte (Langzeit-)Erfahrung oder Forschung
- Schulungen/Vorträge, Lesen && Networking

Danke!

You can book me!

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

SynPro SOLUTIONS

Grazer LINUXTAGE

www.linuxtage.at