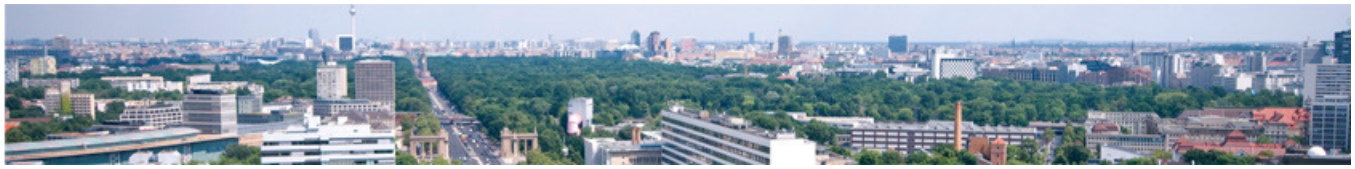
Technische Universität Berlin

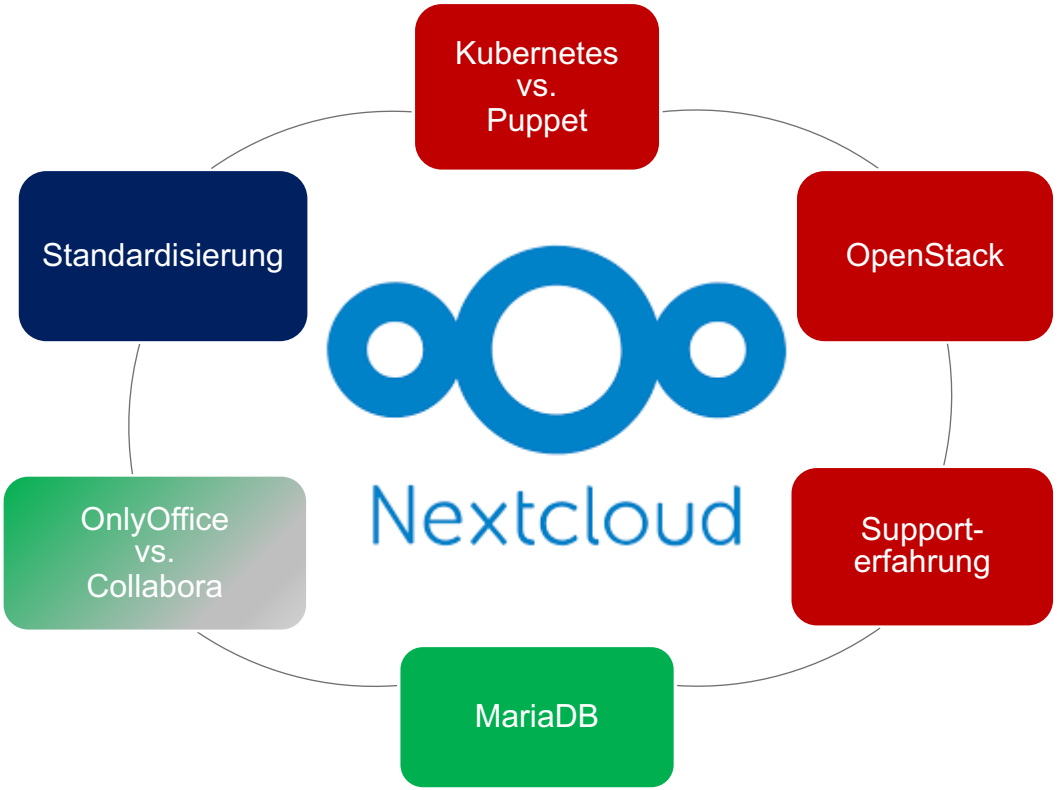
Alles rund um Nextcloud an der TU Berlin

Dr. Thomas Hildmann | ZKI AK ZSYS | 21. November 2023



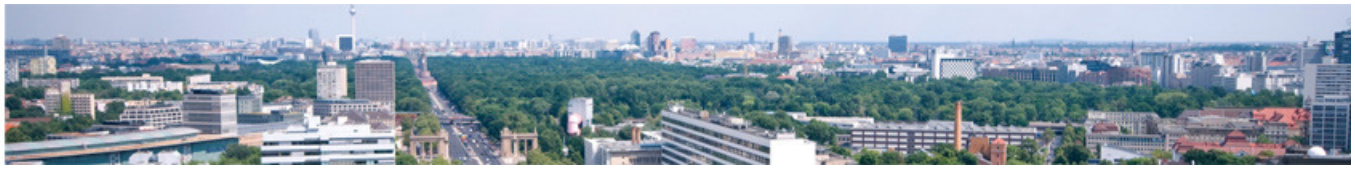
Technische Universität Berlin

Alles rund um Nextcloud



- Erfahrung
- Technik
- Praxis
- Politik

ZE CMPS MGMT



Technische Universität Berlin

OpenStack alt, aktuell und neu

OpenStack (alt)

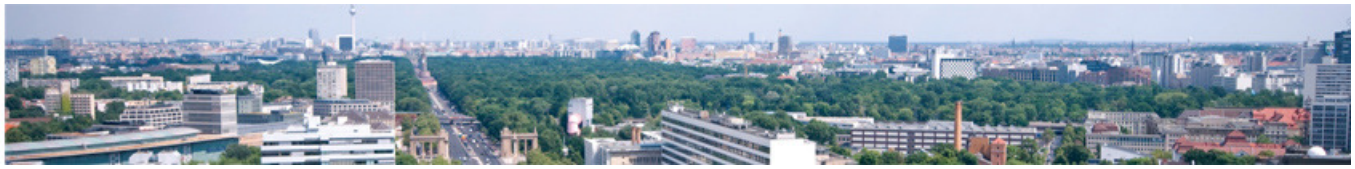
- Ist ganz gut gelaufen
- Irgendwann gab es Probleme mit der Zertifikaterneuerung
- Deshlab schnell ins aktuelle OpenStack

OpenStack (aktuell)

- Umzug mit Zeitdruck ist eine richtig schlechte Idee
- Viel an Datenbanken und Proxies optimiert
- Problem: 1 CPU Core für virtuelle Netzwerkkarte
- NATing aus der Hölle

OpenStack (neu)

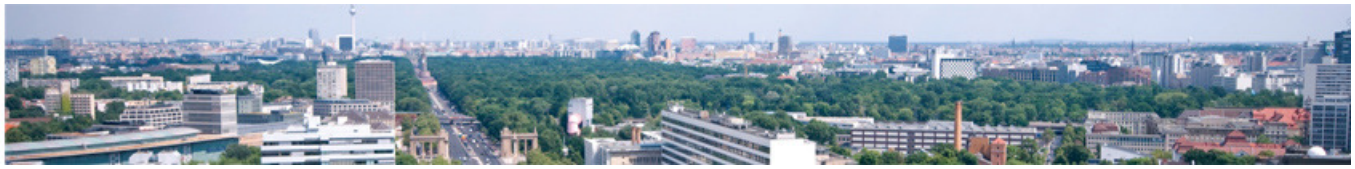
- Optimiert auf Netzwerklatenzen
- Aktuellste Software
- Dedizierte CPU Kerne mit durchgereichten Nezwerkkarten
- In den ersten Tests um mindestens 1 Zehnerpotenz mehr QPS im DBMS
- Ein Dienst nach dem anderen wird migriert und getestet.
- kein NATing mehr ⇒ Faktor 5..10 schneller und brauchbare Logs



Technische Universität Berlin

Lessons learned: OpenStack

- OpenStack ist ein Monster
  - Man kann ein ganzes Rechenzentrum im OS abbilden.
  - Eigentlich braucht es dafür aber auch alle Fachleute, die in so einem RZ arbeiten.
- Unbedingt auf genügend Schultern verteilen.
  - Weiterbildungen nutzen.
  - DevOps top down, Linux Admins bottom up
- Support mit einkaufen
- Regelmäßig aktualisieren. Neu bauen hilft zwar mit alten Fehlern aufzuräumen ist aber ein riesiger Aufwand für alle.
- Flavours auf Spezialmaschinen (hier DBMS) haben sich bewährt.
- CEPH ist bei uns Basis und braucht mindestens zwei zwei extra Spezialist*innen.



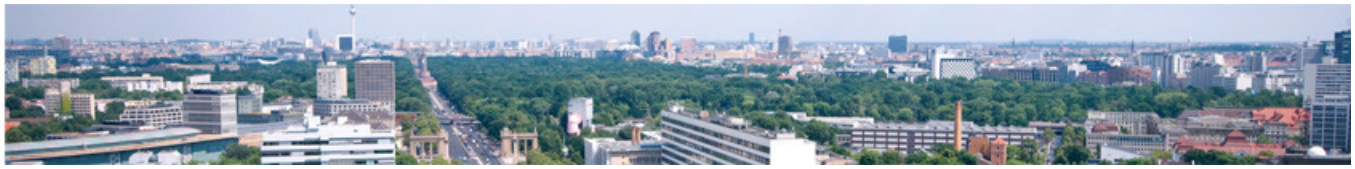
Technische Universität Berlin

Nextcloud und Kubernetes

- wir nutzen den offiziellen Nextcloud Helm-Chart
- basierend auf dem offiziellen Nextcloud Docker
- eigener Redis aber gemeinsamen MariaDB Galera-Cluster
- automatisch skalierte Anzahl der Pods
- TU-eigener Appstore für ausgewählte Apps in der richtigen Version

```
★ jxp-005$ [OS-NG] kubectl get pods
NAME READY STATUS RESTARTS AGE
nextcloud-test1-7f6796b87d-7knfj 1/1 Running 0 12d
nextcloud-test1-7f6796b87d-qmz8d 1/1 Running 0 12d
nextcloud-test1-cron-1648033200-c757v 0/1 Completed 0 9m46s
nextcloud-test1-cron-1648033500-w7zqq 0/1 Completed 0 4m41s
nextcloud-test1-metrics-5f855fcfd6-gxvkn 1/1 Running 0 12d
nextcloud-test1-redis-master-0 1/1 Running 0 12d
nextcloud-test1-redis-slave-0 1/1 Running 2 12d
nextcloud-test1-redis-slave-1 1/1 Running 0 12d
```


ZE CMPS MGMT



Technische Universität Berlin

DFN-Cloud Implementierung

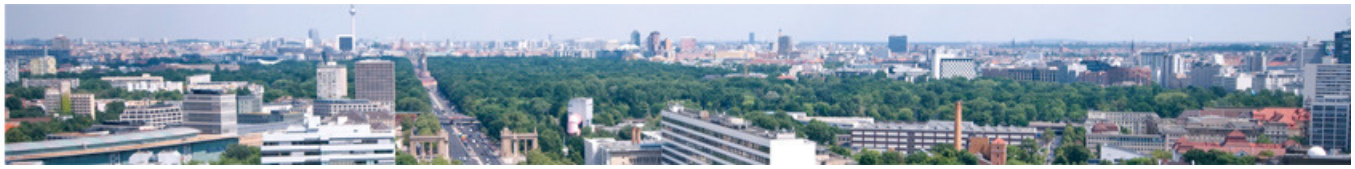
Rollout von Instanzen:

1. SSL-Zertifikat erstellen (lassen)
2. DNS-Eintrag
3. `values-` und `secrets- .yaml` Datei anlegen

Macht man Änderungen an der `values-xxx.yaml` wird automatisch das Deployment gestartet.

```
image:
  pullPolicy: Always
  tag: 21.0.5.3-security-november
ingress:
  tls:
    - secretName: nextcloud-test-tls
      hosts:
        - test1.tubcloud.tu-
    berlin.de
nextcloud:
  host: test1.tubcloud.tu-berlin.de
  password: "GEHEIM;)"
  mail:
    fromAddress: noreply-test1
externalDatabase:
  user: test1
  password: "GEHEIM;)"
  database: test1
persistence:
  size: 50Gi
```


ZE CMPS MGMT

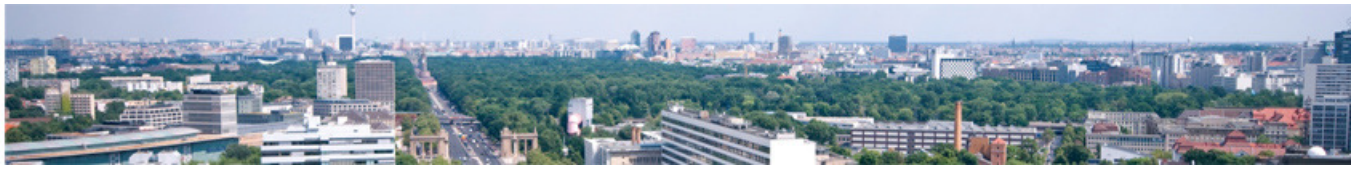


Technische Universität Berlin

Gründe gegen K8s für DFN-Cloud aktuell

1. **Nextcloud unterstützt die Kubernetes-Installation noch "nicht vollständig".**
   D.h. im Supportfall bekommt man nicht die gleiche Unterstützung, wie bei der klassischen (Puppet) Installation.
2. **Durch Weggang eines Kollegen ist unser Kubernetes Know-How weiter reduziert.**
3. **Troubleshooting im Kubernetes-Kontext kann** auch wegen "self-healing" etc. **sehr schwierig sein.**
4. **Es gibt (noch) einige Nachteile auf Grund unserer Implementierung:**
   - Patches rollen nicht richtig aus, weil sich Versionsnummer nicht ändert
   - auch bei kleinen Änderungen ist eine Downtime nötig
   - ab und an gibt es "Hänger" beim Deployment

ZE CMPS MGMT

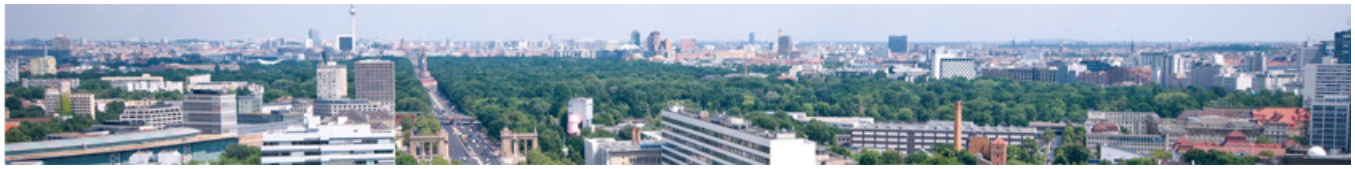


Technische Universität Berlin

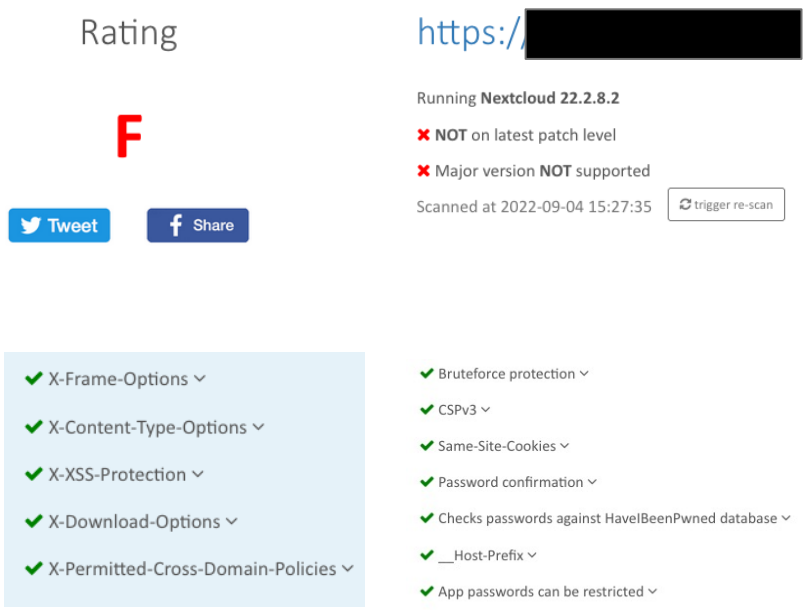
Supporterfahrungen in der Regel sehr gut

- Stand-by support beim Upgrade
- Diskussion von Upgrades vorab und z.B. Optimierung der Upgrade-Prozeduren
- Low priority Tickets evtl. low priority
- Feature Requests werden ernst genommen
- Vorhaben können vorab diskutiert und begleitet werden: Beispiel LDAP nach SAML
- Wir haben gegenseitig gelernt. Es gibt auch Tickets, die wir gar nicht erst schreiben.

ZE CMPS MGMT



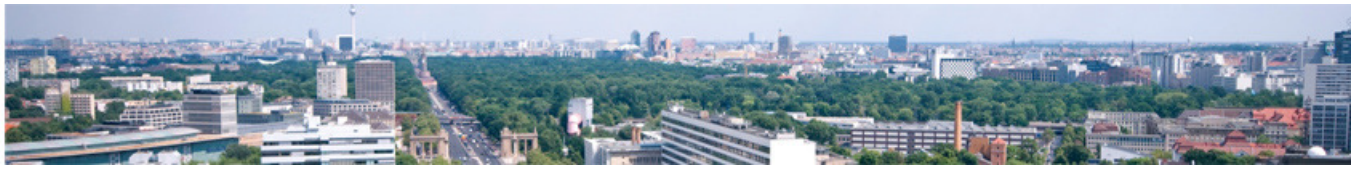
Beispiel: Rating F – Fake News



- https://scan.nextcloud.com zeigt Rating F
- Eigentlich alle Haken grün
- ABER: “Major verion NOT supported”
- Und DAS nach dem Hack 2021?

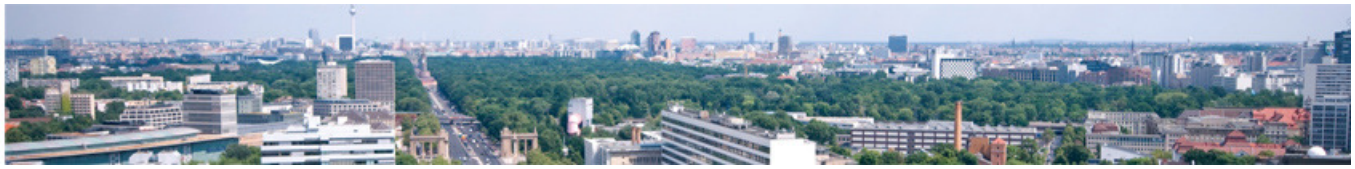
Woran liegt es?

- Enterprise Versions haben **Long Time Support** (LTS)
- Scanner kennt LTS jedoch nicht
- Wir bekommen **Security Patches**.
- Die sieht der Scanner jedoch nicht.
- Ticket bei Nextcloud offen, Problem auf der Roadmap



OnlyOffice: Rechtliche Grundlage

Seit April 2022 ist der „Hinweis zur Einhaltung restriktiver Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren“ (**Wirt-124.1**) zu beachten. Hierin heißt es: „Gemäß Artikel 5k der Verordnung (EU) 2022/576 ... ist es verboten, öffentliche Aufträge oder Konzessionen, ... an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen: a) russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen, b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50% unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, ...“



Technische Universität Berlin

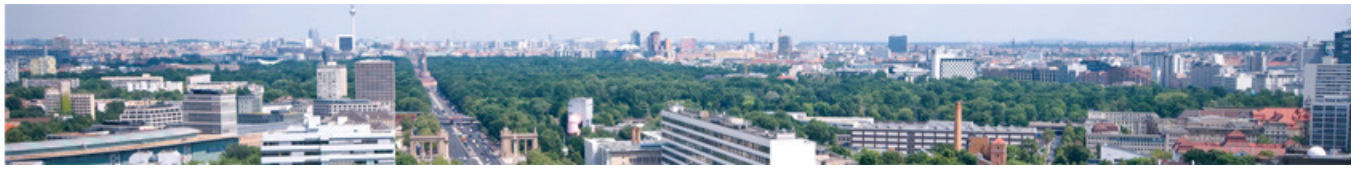
Wie russisch ist OnlyOffice?

- Nextcloud bezieht OnlyOffice Subscriptions von...
  - **Ascensio System Limited in London** oder...
  - **SIA „Ascensio System“ in Lettland**

- GitHub sagt: 100% der Commits von Ascensio oder OnlyOffice

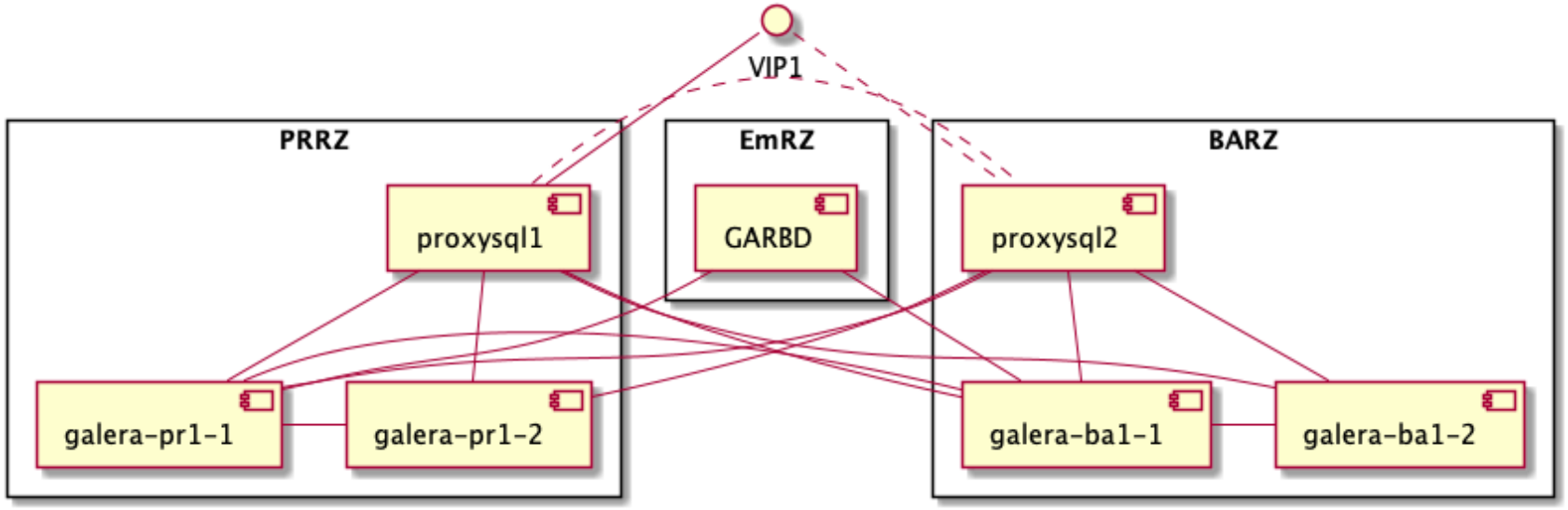
- Handelsregistereinträge
  - **Ascensio System Limited** gehört **Rk-Technology Jsc** mit Sitz in Russland zu >75%
  - **SIA Ascensio System** gehört **Lev Bannov** (russischer Staatsbürger)

ZE CMPS MGMT



Technische Universität Berlin

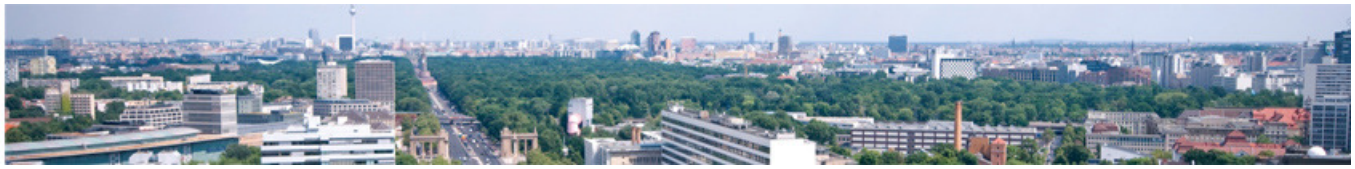
Geplante Architektur: MariaDB



Siehe VortragFrühjahr 2021!

Plan B: 2x3 Nodes mit Active-Passive Primary-Secondary Replikation (Asynchron)

ZE CMPS MGMT

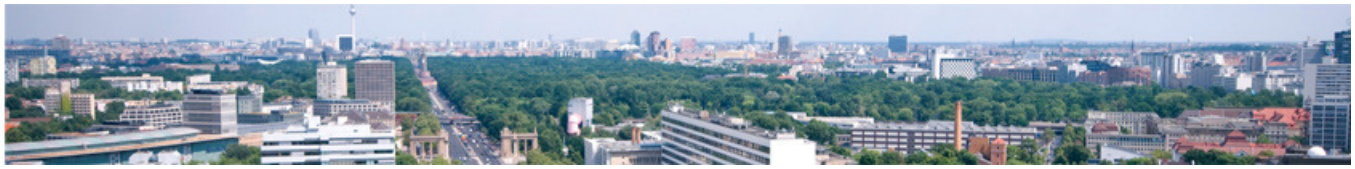


Technische Universität Berlin

Lessons learned: MariaDB

- MaxScale benötigt Subscriptions, ist aber definitiv einen Blick wert!
  - Proxy für Galera aber auch für Primary/Secondary Installationen
  - Wissen über Status der Knoten hilft 24/7 Verfügbarkeit
- Support von MariaDB reagiert schnell und gut
- Zahlung pro Knoten setzt die falschen Anreize
- Schulungen und Basis-Tuning hilft hier

ZE CMPS MGMT

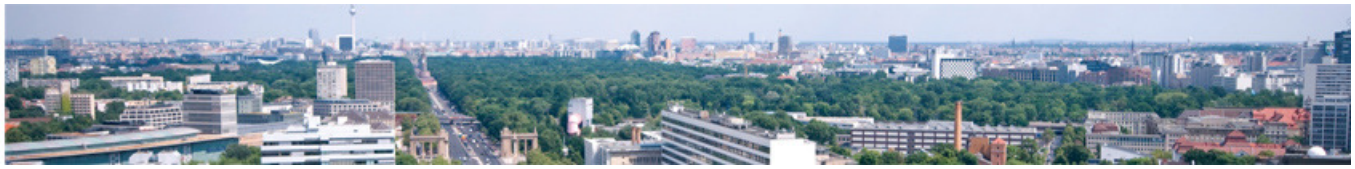


Technische Universität Berlin

Standardisierung

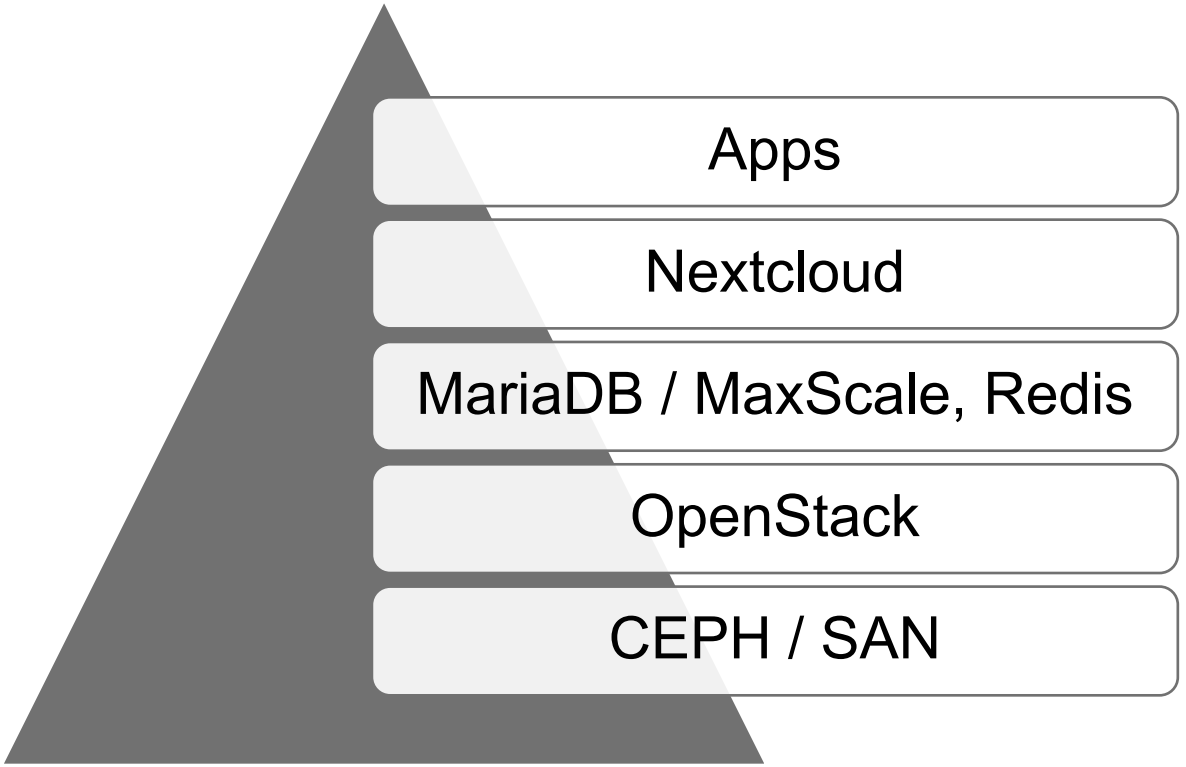
- Wenige Admins können 35 Nextcloud Instanzen betreiben.
- Jede Abweichung erhöht den Supportaufwand
- Versuch: Nextcloud in K8s
- Migration wird immer schwieriger, je mehr Daten da drin liegen
- Selbstadministration
  - Kann aktuell auch eingeschränkt werden
- App-Auswahl aus getesteten Apps
  - Installation machen wir wegen verschiedener Frontends
- Config-File mit Quotas und Lizenzen
  - Erzeugt Warnungen etc.
  - Ist Basis für die Abrechnung

ZE CMPS MGMT



Technische Universität Berlin

Wie sieht unsere Standardinstallation jetzt aus?



ZE CMPS MGMT