

QB



Vanhentunutta tietoa!

QB:n dokumentaatio löytyy nykyään [Con2:n Outlinestä](#).

QB eli Kyyppä on Con2-projektin yhteinen Kubernetes-alusta.

Alusta

Virtuaalikoneet

4 kpl virtuaalikoneita Hyper-V-alustalla:
(qb1–3 , qb4)

- 4 VCPU
- 8 GB RAM

Container orchestration

K3s

Konfiguraationhallinta

Ansible, [julkinen git-repo](#)

Verkko

Julkinen ja sisäinen aliverkko

Kubernetes-verkkoratkaisu:

Flannel (K3s default)

Nekalan palomuuuri:

HTTP, HTTPS sisään auki

Ulos kaikki auki

[SSH-yhteys sisään](#) Monokkelin kautta

Konekohtainen palomuuuri:

Ei konekohtaista palomuuria. Kubernetes tekee paljon iptables-magiaa

Sisään tuleva HTTPS-liikenne:

nginx ingress controller , virtual IP + keepalived

Palvelut osoitetaan tällä hetkellä vain yhteen Kyyppä-nodeen (default qb3), joka on niille SPOF.

Tallennus

Kolme SAN-osiota per node:

- *system* – juuritiedostojärjestelmä, 40 GB SSD
- *fast* – 100 GB SSD
- *big* – 500 GB pyörivä media

Levyt

Rook + Ceph

Rookin upstream-ominaisuuksia joita odottelemme:

- CephFS:n dynaaminen provisiointi PVC:n välityksellä. Nyt käytetään flexVolumeja.
- Useampi storage class. Nyt on konffattu vain *fast*, *bigiä* odotellessa.

Tietokannat

Erillinen tietokantapalvelin Siilo

PostgreSQL:

Point in time recovery -varmuuskopiointi Piilolle (Barman).

MySQL:

MariaDB . Varmuuskopiointi

Ks. [Tietokannat](#)

Monitorointi ja lokitus

Valvonta- ja hallintapalvelin Monokkeli

Monitorointi:

prometheus.tracon.fi (node-exporter)
[grafana.tracon.fi](#) (dashboard QB)

Lokienhallinta:

Prometheus Loki

Varmuuskopiointi

Levynsnapshotit ja tiedostotason varmuuskopiointi

Ks. [Varmuuskopiointi](#)

CI/CD

[jenkins.tracon.fi](#) (Monokkelilla)

Joku moderni Kubernetes-natiivi vaihtoehto

Selite: Tehty, odottaa, särki, vaatii pohdintaa

TODO

Tietoliikenne

- ☐ Testataan, että podien välinen kommunikaatio tekee mitä pitää.
- ☐ Sisäverkko nodejen välille
 - ☐ Sisäverkon interfacet IP-osoitteineen
 - ☐ Kubernetesin osien välinen sisäinen kommunikaatio käyttämään sisäverkon osoitteita

- ☐ nginx-ingress-controller
 - ☒ asennus (kubespray ansible)
 - ☒ paljastaminen internetiin
 - ☒ DNS
 - ☐ Palomuuuri
 - ☐ virtual IP, keepalived
 - ☐ node selector kuntoon: nyt vain mastereilla
- ☐ cert-manager
 - ☒ asennus (kubespray ansible)
 - ☒ konfigurointi

Storage

- ☒ Viritetään GlusterFS

Turvallisuus

- ☐ Varmistetaan siitä, että (ulko)verkkoon ei ole auki sellaisia palveluita, joilla voisi korkata nodet ja/tai Kubernetesen.
- ☐ Konekohtainen palomuuuri

Ylläpito

- ☐ Miten järkätään pääsy Kubernetesen master apiin? Ts. *kubectl* adminien omilta työasemilta?
 - ☐ Verkko: Mihin master api on auki?
 - ☐ Käyttäjätunnukset: Miten ja mistä käsin provisioidaan säätäjien käyttäjätunnukset / käytetäänkö jotain jaettua?

CI/CD

- ☐ Esimerkki jenkins.tracon.fi -> QB deploymentistä, esim. dev.kompassi.eu
 - ☒ emrichen toimimaan (asennettu: python 3.5, vaatii: python 3.6)
 - ☐ kubectl:lle salaisuudet kuntoon
 - ☐ service account
 - ☐ role binding
 - ☐ token secretiksi jenksuun
 - ☒ palomuuriaisuus, SSH-putki tmv. jolla kubectl pääsee tökkimään master apia monokkelilta käsin

Valvonta ja lokienhallinta

- ☒ QB nodet Monokkelin Prometheusin valvontaan (ainakin node-exporter)
- ☐ EFK stack Monokkelille

Sovellukset

- ☒ dev.kompassi.eu
- ☒ conikuvat.fi (Edegal)
- ☐ con2.fi (Tracontent)