Themen, die diskutiert wurden:

Zertifikatsmanagement (zusammen mit Let's Encrypt)
- wie geht das ohne Wildcards?
- Service Signing Certificates
- Service CA in OpenShift
- Pods können damit versorgt werden
- Laufzeit ca. 3 Jahr, nach Löschen wird das Secret automatisch neu erstellt, die Pods müssen jedoch aktualisiert werden
- Ablaufdatum steht in einer Notation in einem parsebaren Format
- HTTPS bis in den Container hinein (kommt vor)
- Teilweise nur 2 Monate Gültigkeitsdauer (Wegwerfzertifikate), HTTPS bis in alle Container-Native, wird aber nur intern genutzt, extern würde auch gehen aber nur mit einer öffentlichen CA
- Auf Router Wildcard und VMCrypt
- Es gibt auch intelligentere Lösungen (FlexPod?)
- Wie geht das mit einem zweiten WildCard-Cert auf einem Router?

Upgrade von OpenShift-Clustern / Patching für OpenShift
- wie wird das Upgrade geplant, welche Policies, wie wird getestet?
- Seit 3.2, mehrmals aktualisiert, jetzt größeres Cluster auf AWS, getrennte Accounts, Testen (einschl. Lasttests) auf Test-Cluster
- Man lässt in einem Rutsch mal 1000 Bots starten
- Zeitlinie? Immer auf der aktuellsten? → sehr nah (1-2 Releases nach der neuesten)
- Beim Upgrade wurden einige Einstelllungen auf Default-Einstellungen zurückgestellt, die muss man kennen
- Es hat eine Red Hat Consultant geholfen, deshalb wissen wir nicht so genau was gemacht wurde
- Alle setzen noch RPM ein, zukünftig häugiger Docker-Basierte Updates
- Langfristig ist Docker-Format besser
- Upgrade per Ansible-Playbook (ist in der Doku gut beschrieben → Major vs. Minor Upgrades)
- Ein Testsystem/Sandbox-System, der Rest setzt mehrere Stages um
- Immer auf die Major-Version, manche wollen keine x.0 Version für sich nutzen
- Man spart sich keine Arbeit, wenn man ein Major-Release auslässt
- Manche Upgrades waren einfach, manche schmerzhaft, aber je mehr nman auslässt, desto anstrengender wird es
- Releasnotes durchlesen, kann sein, dass irgendetwas deprecated ist
- Evtl. Worker und Controller getrennt aktualisieren
- Infrastrukturknoten können anstrengend sein

Storage-Themen und Technologien / Wiederverwendung von Persistant Volumes
- was wird an Storage eingesetzt
- Ceph-Cluster mit Dynamic Storage Provisioner (auf Hardware, nicht Converged Storage, soll aber wohl besser geworden sein)
- NetApp, NFS, inzwischen gibt es auch einen Provisioner für NetApp
- Wiederverwendungsmöglichkeiten: Dynamisch und Recycler
- Arbeitet man mit Label und Selektoren, damit ein Entwickler die gleichen Daten bekommt?
- Wenn man das auf Retain stellt, kann sich auch ein neuer Claim das Volume nicht nehmen, man brahct den Cluster-Admin um wieder einen Claim durchzubringen
- Ceph hat die Eigenschaft, dass Volumes, von denen ein SnapShot gemacht wurde nicht mehr gelöscht werden können, sollte aber vernünftig besser anders laufen

- Persistant Volumes (PVs)- Service erstellt automatisch bei Claim, oder mit einer Batch-For-Schleife
- Bei NFS gibt es kein hartes Backend, nur der Storage Provisioner kanń den Claim abblocken
- Migration von einem Cluster zum anderen? Wir wurden mal gefragt, aber am Ende ist das immer ein Einzelfall, bislang keine generische Lösung
- Mapping von UID des Containers zu den Daten? CHOWN?
- Zuordnung ist eher zufällig, aber wenn sie mal da ist bleibt sie gleichen
- Man kann auch was mit SELinux auf NFS machen (?)
- EWS funktioniert ganz gut
- EFS hat anscheinend Probleme mit zu vielen File Handles
- Benutzt jemand Dynamic Storage und VMWare?
- Ceph lieber nicht Container-Native machen, evtl. auf dedizierte Nodes und mit SSDs versorgen, Container Native Storage mit iSCSI liegen wenig Erfahrungen vor, scheint aber problematisch zu sein, also lieber gleich an die Nodes anbinden

Erfahrungen mit F5 und Loadbalancer (6)
- F5-Integration steht in der RH-Doku: SDN verknüpft sich direkt mit dem Hardware-Loadbalancer. Geht das?
- Früher eigener Edge-Node, jetzt gibt es anscheinend ein SDN-Modul in F5, aber wahrscheinlich Extra-Lizenz
- F5-Laborlizenz für virtuellen F5
- Hätte den Vorteil, Aufgaben zu zentralisieren
- Gut für Autoscaling von PODs mittels des F5-Plugins über F5 (noch bevor die CPU anspricht)
- Mit Prometheus steht vermutlich ein insgesamt mächtigeres Mittel zur Verfügung
- Mehr RAM hilft immer (unter 5G geht gar nichts)
- Soll Kasssandra irgendwann rausfliegen?

Cluster-Layout
- Wofür wird ein Cluster eigenrichtet, wo muss man nur Nodes trennen, wo reicht eine Trennung der CPUs?
- Isolation von SDN zu erklären ist nicht ganz leicht
- Leute von CPI meinten, dass man vielleicht besser ein Testcluster hat damit nicht alles komplett kaputt gehet, scheint auch common Sense zu sein
- Vproduktionsumgebung ist teilweise sehr nah an der Produktionsumgebung, Hauptschwierigkeit Firewall-Ports herauszubekommen (die RH-Dokumentation umfasst nicht alle Ports)
- Master und Nodes in getrennten Zonen, ggf. getrennt für Prod und Non-Prod, innerhalb eines Clusters wieder mehrere Security-Zonen
- Node-Zonen gelabelt
- Wie habt ihr SDN konfiguriert? Erste Möglichkeit FLAT, zweites Multi-Tenant (nach Network Namespaces), ab 3.7 Network Policy
- Darf jemand mit mehreren Clustern leben? Intern eins, beim Kunden 5 plus Sandbox
- “Es scheint irgendwie alles zu gehen”
- Mit Federations (Meta-Cluster) könnte es zukünftig einfacher werden
- Multi-Region Cluster (Delay könnte kritisch werden, Vertrauensstellung ohne harte Abhängigkeiten)
- VXLAN ist nicht verschlüsselt
- Backups vom Cluster, oder Playbooks als Backups
- Alle Objekte als YAML-Datei exportieren und Datenbank sichern, ggf. auch Config-Directory vom Master, hier ist jedoch Spezialwissen erforderlich (einfach nur Einspielen reicht nicht), wenn man weiß wie es geht

- Restore hat (mehrmals) funktioniert, allerdings gab es am Anfang manchmal Probleme einen etcd - Secrets zukünftig immer noch im etcd, aber AES-verschlüsselt
Cluster zu restoren, seit 3.3 besser geworden
- Wo liegt das Limit bei Pots/Knoten (1000?), beim Autoscaler kann man da schnell landen
- Docker-Daemon läuft nicht immer 100%ig sauber
- Nutzt schon jemand OverlayFS? Ja, aber man musste SELinux abstellen (teilweise Fakor 10 beschleunigt), manche Applikationen funktionieren immer noch nicht auf OverlayFS (z.B. RH SSO, hat immer die Jar-Files wieder rausgesetzt), echter Permance-Boost

Security / Lets Encrypt (zusammen mit Zertifikatsmanaement)

Identity-Management
- wir haben einen LDAP, für jede Komponente eigene IDs? Aus OpenShift? Von irgendwoher außerhalb?
- OAuth mit KeyCloak → Jede Anwendung zieht sich seine ID, OpenShift ist selbst ein OAuth Provider, man kann aber auch eine externen Provider nutzen.

Allgemeine Ergebnisse
Schon ein paar neue Sachen gehört, grobe Richtung ist klar
Gern in Zukunft weiter untereinander austauschen, User kommen zu Wort, das ist gut
Eher Slack, oder eher Mailingliste? Klassische Mailinggroup ist eigentlich gut und funktioniert.

<u>Themen, die es nicht auf die Shortlist geschafft hatten:</u>

Quotas
Change-Prozess bei Appplikationen und OpenShift
CI/CD
Einbindung von Containern in Kerberos
Skalierung (einschl. Router)
Dedizierte Infrastrukturknoten