Kubernetes mal anders mit Tanzu

Container waren lange Zeit dem Warentransport vorbehalten – auch bei Thalia. Aber heutzutage wächst auch der Bedarf an Containern im Bereich der IT. Das vollständige Potential lässt sich erst erzielen, wenn auch ein entsprechender Orchestrator verwendet wird, um die Verwaltung zu übernehmen. Wo liegen jetzt die Vorteile von Containern und was bringt mir ein Orchestrator außer einer zusätzlichen und womöglich zugleich unbekannten Technologie?

Ein immer schnellerer Entwicklungszyklus und damit auch häufigere Deployments sind ein Treiber. Hierbei bieten Container die Möglichkeit, einen vordefinierten und unveränderlichen Stand, auch als „Immutable Image“ bezeichnet, in unterschiedlichen Architekturen auszurollen. Somit ist es auch simpel, diese Images sowohl auf den Geräten der Entwickler, als auch in den unterschiedlichen Entwicklung-Stages zu verwenden.

Ein weiterer Treiber sind die Skalierungsmöglichkeiten, die durch einen Container Orchestrator wie Kubernetes entstehen. Anwendungen können hierbei anhand von Auslastungsmerkmalen wie der CPU- oder der RAM-Verbrauch automatisch skaliert werden, was ein manuelles Eingreifen überflüssig macht. Bei

hohen Auslastungen können hierdurch weitere Container bereitgestellt, andersherum bei wenig Auslastung auch wieder reduziert werden, was Einsparungen ermöglicht.

Ideenfindung/Werdegang

Kubernetes ist in der heutigen Zeit als Orchestrator für Container eine gesetzte Technologie. Aber gleichzeitig birgt diese auch das Risiko, einen gewaltigen Mehraufwand im Betrieb zu erzeugen. Schnelle Entwicklungszyklen, die häufige Updates von Kubernetes selber erzwingen, um am Ball zu bleiben. Viele Komponenten innerhalb von Kubernetes, die ebenfalls verwaltet und aktualisiert werden wollen. Und das bei immer mehr Abstraktionsschichten, von der eigentlichen Hardware hin zu der eigentlichen Basis für die Anwendung. Insgesamt entsteht also ein hilfreiches, aber auch komplexes Konstrukt, dessen Management sichergestellt sein muss, um sich nicht kontraproduktiv auszuwirken.

Wie bekommt man also den schmalen Grad hin, bei einer vordefinierten Anzahl von Administratoren den Aufwand möglichst gering zu halten und trotzdem die Vorteile gewinnen zu können? Hierzu gibt es unterschiedliche Varianten, die wir uns angeschaut haben, bevor wir schlussendlich bei der jetzigen Lösung angekommen sind.

Die erste Herangehensweise war, sich mit Kubernetes selbst auseinanderzusetzen. Bezeichnet als „Vanilla Kubernetes“ machten wir uns mit entsprechender Automatisierung dran, Kubernetes auszurollen, miteinander zu verknüpfen und auch zu nutzen. Die ersten Anwendungen waren schlussendlich bereits in den Entwicklungsstages ausgerollt und aktiv, bevor wir die Reißleine ziehen mussten. Mit der in der Zwischenzeit gesammelten Erfahrung war ein Betrieb in „Produktion“ schlichtweg nicht realistisch. Zu hoch war der Aufwand und das hiermit verbundene Betriebsrisiko.

Der nächste logische Schritt war, dass der Betrieb komplett ausgelagert wird. Somit könnten wir uns auf das Deployment der Anwendungen konzentrieren und müssten uns um die Verwaltung keine Gedanken machen. Somit würden auch keine Ressourcen unsererseits in Beschlag genommen. Klingt doch soweit super, könnte man denken? Aber auch das hat am Ende leider nicht die gewünschten

Ergebnisse gebracht. Bei solchen „managed“ Lösungen gilt es einige Punkte zu beachten. Da wären z.B. das Kosten-Nutzen-Verhältnis aber auch der Abgang von Erfahrungen im Betrieb und damit das Verständnis für tiefere Ebenen der Technologie. Zusätzliche benötigte Funktionen müssen ebenfalls auf eigene Faust gestemmt werden oder gehen weiter zu Lasten der Kosten.

Schauen wir uns also einmal die Probleme an. Häufige Updates und Abhängigkeiten sind ein großer Treiber der Technologie. Auf der anderen Seite benötigen wir mehr als eine „managed“ Lösung uns im ersten Schritt bieten kann. Lässt sich also die grundlegende Verwaltung, wie z.B. Updates und Management von Abhängigkeiten, simpler gestalten? Aber gleichzeitig der eigentliche Betrieb und somit auch das tiefergreifende Wissen erhalten? Und das bei einem sinnvollen Kosten-Nutzen-Verhältnis?

Hier kommt „VSphere with Tanzu“ als Produkt von VMWare ins Spiel, welches im Nachfolgenden nur noch als „Tanzu“ bezeichnet wird.

Planung

Für die Recherche und die Prüfung des Produkts gab es verschiedene Schritte. Die Idee war aber immer eine pragmatische Herangehensweise. In einem ersten kurzen Test haben wir uns die Grundlagen angesehen, einen Cluster aufgesetzt, erste Objekte angelegt und dann Anwendungen hineingesetzt und die Funktionen geprüft. Soweit so gut, die erste Hürde war gemacht und bisher noch keine Blocker entdeckt.

Im nächsten Schritt haben wir uns dann noch einmal genauer mit den Details auseinandergesetzt, den technologischen Aufbau rekapituliert, Testfälle heruntergeschrieben und zusätzliche Kollegen eingeweiht und einbezogen. Mit dieser Vorplanung ging es dann in den PoC (Proof of Concept). Das Setup konnten wir zum Glück noch wiederverwenden, hier gab es keine nötigen Anpassungen. Um einige Funktionen erweitert und die Testfälle abgeklappert ging die Stimmung weiter nach oben. Jetzt galt es noch die Entwicklungsteams abzuholen, eine ungenutzte Hülle hilft ja schließlich keinem. Hier kamen also die DevOps-Kollegen aus unseren Teams ins Spiel, um die finalen Bereiche abzuklären. Und wäre das nicht mit Erfolg gekrönt, würden diese Zeilen wohl nie gelesen werden.

Jetzt ging es also an den größeren Brocken der Arbeit. Das Projekt muss geplant

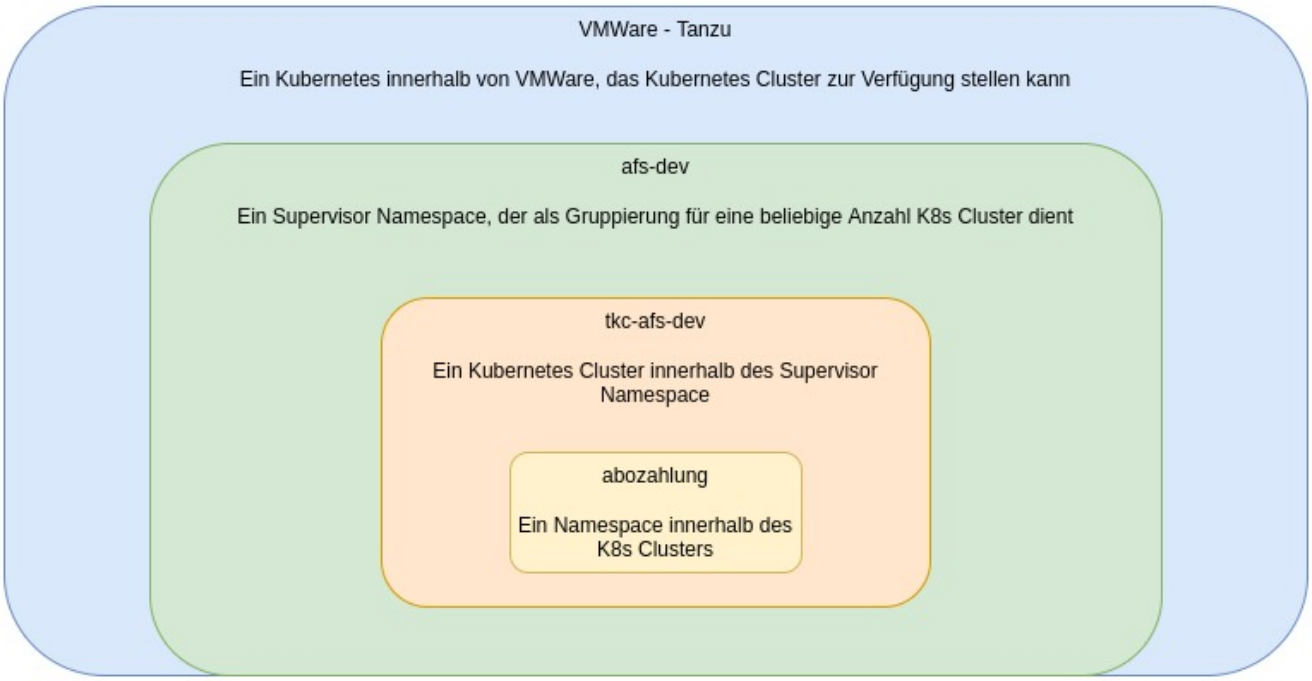
werden, um die Technologie auch sinnvoll für die Entwickler bereitzustellen. Viele Punkte wurden im PoC schon abgedeckt, aber der Teufel steckt ja bekanntlich im Detail. Auch Gedanken zu internen Abläufen, Prozesse zur Nutzung und das spätere Onboarding der Kollegen sollten noch die ein oder andere Stunde verbrauchen.

Was ist Tanzu eigentlich?

Aber noch einmal einen Schritt zurück. Erst ist von Kubernetes die Rede, dann Tanzu. Wo liegt denn jetzt eigentlich der Unterschied?

Wie zu beginn schon erwähnt, bringt Kubernetes im Container Kontext viele Vorteile. Im Management aber auch einige Hürden mit sich. Tanzu bildet eine Abstraktionsschicht um einige dieser Hürden und versucht so, den Management Overhead zu minimieren. Es bildet unter anderem ein Rahmenwerk aus verschiedenen Technologien, die nach Prüfung von VMWare in einem Zusammenspiel gut miteinander funktionieren und auch unterstützt werden. Somit werden zwar ein paar Standards vorausgesetzt, was die ein oder andere Einschränkung mit sich bringt, aber im großen Ganzen noch alle Anforderungen erfüllt. Gleichzeitig gibt es jemanden, der einem bei Problemen weiterhelfen kann. Genau diese Standards ermöglichen es ebenfalls, dass Updates über wenige Klicks in Tanzu abgebildet sind. Im VCenter habe ich mit Tanzu einen Überblick über alle mit Tanzu gebauten Kubernetes Cluster und auch deren Versionsstand. Ebenso finde ich hier eine simple Möglichkeit alle Cluster auch auf einen neuen Stand zu bringen. Was in dem Kontext nur fehlt, sind die Updates für Plugins und Erweiterungen. Aber auch hier bietet Tanzu einen Download kompatibler Versionen inkl. detaillierter Anleitung zur Umsetzung, was das Vorgehen deutlich vereinfacht.

Was es nicht einfacher macht? Abstraktionsschicht um Abstraktionsschicht wird die Komplexität trotzdem nicht geringer. Um es sich zu verdeutlichen, hier einmal der Aufbau der mittlerweile entstandenen Schichten für die Kubernetes Cluster:



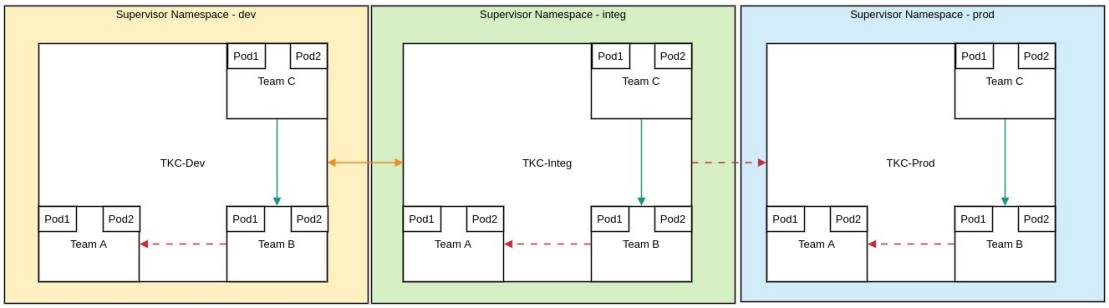
Architektur und Umsetzung

Die grundsätzlichen Überlegungen zu Abläufen etc. sind getroffen. Die Arbeitspakete geschnürt. Aber auch die Architektur soll wohl überlegt sein, bevor Sie Fallstricke enthält. Wie viele Cluster werden wir brauchen? Wie bauen wir das Netzwerk zwischen den Clustern auf? Brauchen wir ein Staging Konzept für die Cluster selber und nicht nur die Anwendungen? Das und vieles mehr galt es jetzt im konkreten Kontext anzugehen und zu klären.

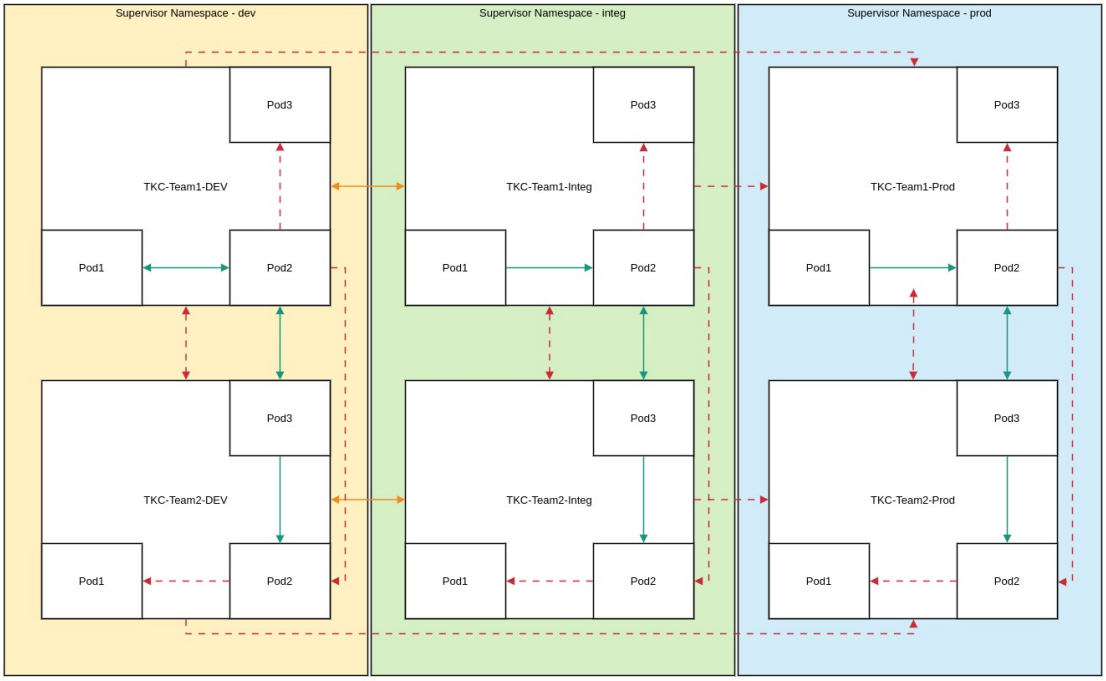
Einiges lässt sich einfach beantworten, anderes dann wiederum nicht. Schließlich sollen ja die unterschiedlichen Stages der Anwendungen wie Integration und Produktion bestmöglich voneinander getrennt sein. Auf der anderen Seite muss aber der Management Overhead überschaubar bleiben. Und dann gibt es ja nicht nur die unterschiedlichen Stages, sondern wir haben auch noch verschiedene Teams, die dann Ressourcen nutzen. Je mehr Cluster wir also aufbauen, desto komplizierter wird die Verwaltung des Konstrukts. Aber je weniger Cluster, desto schlimmer wird die Trennung – sowohl auf Netzwerk, der Ressourcen als auch der Berechtigungsebene.

Wie ein paar Überlegungen ohne nähere Erläuterungen aussehen können:

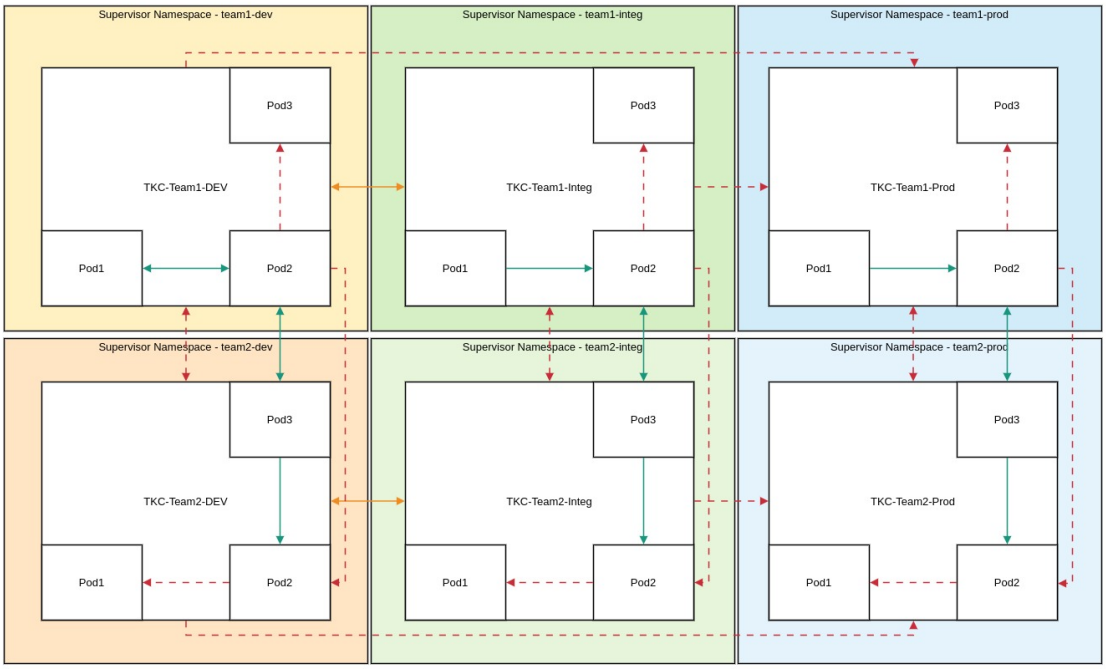
Option A



Option B



Option C



Architekturoptionen mit Kubernetes
Eines war klar, wir brauchen auf jeden Fall eine Automatisierungslösung. Eine Lösung, die uns so viel wie möglich von der Arbeit abnimmt und gleichzeitig dafür sorgt, dass wir die Infrastruktur reproduzieren können. Wie sonst auch soll dieser Ansatz basierend auf dem „Infrastructure as Code“ Prinzip abgebildet werden, womit die Wahl des Konstrukts am Ende unabhängig davon ist.

Ein wenig Recherche später qualmt der Kopf schon wieder. Sollten wir eine Lösung wie Flux oder ArgoCD nehmen? Genügt uns eine Jenkins oder Gitlab Pipeline? Ist Terraform die finale Lösung? Oder wird es womöglich eine Kombination aus mehreren Tools?

Wir haben ja schließlich mehrere Schritte, welche wir in der Provisionierung eines Clusters abdecken müssen. Zum einen der Bau eines Clusters über VSphere, die Einrichtung des Netzwerkes innerhalb des Clusters und auch die Anbindung der Services wie Monitoring, Logging und Alarming wollen in der Initialisierung bedacht werden. Und dann gibt es auch noch Sonderlocken von VMWare, wie z.B. Extensions, die einem teilweise die Arbeit abnehmen, durch die Standardisierung aber auch nicht für alle Fälle bei uns geeignet sind.

„Schuster bleib bei deinen Leisten“ heißt ein alter Spruch. Somit war die naheliegendste Lösung, vorerst eine Pipeline in unserem bestehenden Tool zu bauen. Die Daten sollen aus einem Git-Repository ausgelesen und alle nötigen Schritte hierin umgesetzt werden. Die Erfahrung wird zeigen, ob wir hier noch etwas nachzubessern haben und auf eine der anderen Lösungen schwenken, aber vorerst können wir alles abdecken. Und das ohne eine weitere neue Technologie, in die wir uns erst einarbeiten müssen.

Das Endergebnis des gesamten Setups im Tanzu Kontext kann sich aus unserer Sicht auf jeden Fall sehen lassen!

Onboarding

Der Tag der Tage ist gekommen. Nach all der Planung, Konzeptionierung und Umsetzung steht die Vorstellung vor der gesamten Entwickler-Community an. Doch was soll schon groß passieren? Die Kommunikation mit den Teams lief bereits vorher regelmäßig durch kurze Präsentationen des Standes. Unsere DevOps-Kollegen in den Teams haben uns im Piloten unterstützt. Und insgesamt

war das Feedback bisher durchweg positiv.

Was hiernach trotzdem noch fehlt? Die Migration. Wir freuen uns schon auf die Zusammenarbeit mit den Teams und sind gespannt, wie die Lösung im weiteren Verlauf auch unseren Betriebs-Alltag verbessern wird.

Ein Artikel von

Matthias Efker

Linux Systems Engineer

Suginthan Rushiyendra

Linux Systems Engineer

Du hast Lust ein Teil des Teams zu werden?