Gruppenarbeit 3 - Abschliessende Analyse des Providers und Cloud Application Design

Alexander van Schie & Oli Dias

May 19, 2019

Contents

1 Analyse Service Level Agreegment (SLA)

- 1. Es wird eine etwas andere Art von SLO's gemacht, nämlich wird das Problem nach Schwerheitsgrad klassifiziert und je schlimmer es ist, desto schneller muss RedHat reagieren (https://access.redhat.com/-support/offerings/openshift/sla)
- 2.
- 3. Generell werden keine Metriken oder Messwerte erwähnt. Vielmehr werden Probleme zusammengefasst und nach Schwerheitsgrad klassifiziert. (https://www.openshift.com/legal/terms/)
- 4. Je nach SLA müssen verschieden Dinge eingehalten werden. Was mir persönlich als wichtig erscheint ist eine Vereinbarung bezüglich dem Kundensupport innerhalb einer gewissen Zeit da (a) ein Unterbruch meiner Applikation je nachdem grosse Konsequenzen für mein Unternehmen haben kann. Grundsätzlich sollte ein Cloud-Provider ausgewählt werden, der quasi to big to fail ist (b).
- 5. Je nach Branch muss man sich mit den Datenschutzbestimmungen des Cloud Providers auseinander setzen. Beispielsweise wäre es für Banken nicht gerade ideal, Kundendaten auf ausländische Server zu migrieren/verwalten

Engineering Projekt (Waitless)	
Erfüllt	Nicht erfüllt
Codebase	Disposability
Dependencies	Dev/prod parity
Config	Logs
Backing services	Admin processes
Build, release, run	
Processes	
Port binding	
Concurrency	
Port binding	

2 Twelve-Factor Apps

2.1 Anpassungen

- Disposability:
- Dev/prod parity: Die ganze Applikation wurde nur auf einem System entwickelt. Sobald Code eingecheckt und die Tests erfolgreich waren, war der Code bereits produktiv.
- Logs: Das Verhalten der Applikation wurde mit Enduser-Tests überprüft. Mit der Implementation von Logs werden alle Informationen festgehalten.
- Admin processes:

3 Security Features und Assessment

In den Terms und Conditions von Openshift ist ganz klar zu entnehmen, dass der Anwedender für Themen des Datenschutzes die Verantwortung übernimmt. So hat der Anwender sicherzustellen, dass die Daten der Anwender seiner Applikation geschützt werden. Dies beinhaltet die Implementation von Datnschutzrichtlinien, welche rechtlich abgestimmt sind. Zudem müssen die Anwender darüber informiert werden, dass ihre Daten auf der Infrstruktur von Red Hat abgelegt wird und sie dem somit zustimmen.

Red Hat gibt bekannt, dass folgende Technologien von ihrem PaaS unterstützt werden:

- SELinux
- Process, network, and storage separation
- Stateful and stateless inspection firewall
- Proactive monitoring of capacity limits
- Intrusion detection
- Port monitoring
- Pam namespace
- Security compliance frameworks
- RPM verification and vulnerabilities updated
- Remote logging
- Encrypted communications

https://www.openshift.com/policy/security/

3.1 Checkliste Security Assessment

1. Encrypted Communication/ (Security) -> 10 Openshift nutzt Kubernetes und die Kommunikation bei Kubernetes ist standardmässig mit TLS verschlüsselt.

2. Backups -> 3 Backups müssen selbst gemacht werden, es gibt hierfür keinen Service. Positive ist jedoch, dass das Vorgehen dokumentiert ist.

3. Location -> 5 Openshift wird vermutlich Data Centers an mehreren geographischen Standorten haben, kommuniziert dies jedoch nicht öffentlich.

4. Server Redundancy (Data Centre Physical Security, Disaster Tolerance) -> 8 Da Openshift mit Kubernetes arbeitet, besteht auch die Möglichkeit der Nutzung von Replicas, diese müssen jedoch selbst definiert werden.

5. Service Authentification (for Administration stuff) -> 10 Authentifizierungserfahren laufen über OAuth und bietet alle gängigen Möglichkeiten (https://docs.openshift.com/enterprise/3.0/admin_guide/configuring_authentication.html)

6. Appropriate SLA (with Incident Handling) -> 7 Es gibt ein SLA, in dem wichtige Punkte zur Einhaltung der Servicebedingungen festgehalten sind. Was jedoch nicht zu entnehmen ist, sind Strafen, die bei Nichteinhaltung fällig werden.

7. Data Isolation (Customer based, Data Integrity) Kubernetes NetworkPolicy wird voll unterstützt und Projekte können ebenfalls in einer isolierten Umgebung betrieben werden.

8. Transparency (Monitoring) -> 8 Quotas sowie laufende Prozesse können eingesehen werden

9. Network design und Logging -> 5 Standardmässig werden Logs geschrieben, diese waren unserer Erfahrungen nach unzureichend (was das Fehlerhandling erschwerte)

4 SWOT-Assessment von Cloud Provider und Cloud Offering

		Interne Analyse	
		Stärken	Schwächen
Externe Analyse	Chancen	• Web App Design • Einfache Projektinitialisierung • Command Line Interface (CLI)	• Limitierte Ressourcen • Limitierete Projektauswahl • Limitierte Abonnemente • Preis • Web App Struktur ?
	Risiken	• Nutzung von Kubernetes • Ausbaubare Service Dokumentation • Chance zur Änderung (Nicht to big to change)	• Transparenz Fehlerbehandlung • Transparenz Nutzungsbedingungen • Ablehnung jeglicher Sicherheitsaspekte • Kleine Community

S indicates standardization ongoing activities

Kriterium	Erfüllt	Kommentar
Umfangreicher Technologiekatalog	Jein	Welches Angebot stellt uns der Anbieter zur Ve
Unternehmungsgrösse des Anbieters	Nein	Grosse Unternehmen haben tendenziel mehr Erf
Customizing	Jein	Ist es möglich, Ressourcen nach beliebigem Bed
Dokumentation	Ja	
Community	Nein	Gibt es eine Community, die bei häufigen Probl

5 Provider Evaluation Checkliste

6 Management Summary