

Gruppenarbeit 3 - Abschliessende Analyse des Providers und Cloud Application Design

Alexander van Schie & Oli Dias

May 13, 2019

Contents

1	Analyse Service Level Agreegment (SLA)	3
2	Twelve-Factor Apps	4
2.1	Anpassungen	4

1 Analyse Service Level Agreement (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 Anwender 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 Datenschutzrichtlinien, welche rechtlich abgestimmt sind. Zudem müssen die Anwender darüber informiert werden, dass ihre Daten auf der Infrastruktur 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 Authentication (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)

7 Es gibt eine SLA, indem wichtige Punkte zur Einhaltung der Servicebedingungen festgehalten sind

8 Quota sowie laufende Prozesse können eingesehen werden

9. Network design Logging ->

5 Standard messig werden Logs geschrieben, diese waren unserer Erfahrung nach unzureichend

<http://02f9c3b.netsolhost.com/blog1/wp-content/uploads/Cloudsecurity.pdf>

<https://www.fujitsu.com/sg/Images/cloud-security-checklist.pdf> <https://www.kryptosys.com/cloud-security/cloud-security-checklist/> <https://brage.bibsys.no/xmlui/bitstream/handle/11250/2378820/A27131.pdf?sequence=3&isAllowed=y>

4 SWOT-Assessment von Cloud Provider und Cloud Offering

		Interne Analyse	
		Stärken	Schwächen
Externe Analyse	Chancen	<ul style="list-style-type: none"> • Web App Design • Einfache Projektinitialisierung • Command Line Interface (CLI) 	<ul style="list-style-type: none"> • Limitierte Ressourcen • Limitierte Projektauswahl • Limitierte Abonnemente • Preis • Web App Struktur ?
	Risiken	<ul style="list-style-type: none"> • Nutzung von Kubernetes • Ausbaubare Service Dokumentation • Chance zur Änderung (Nicht to big to change) 	<ul style="list-style-type: none"> • Transparenz Fehlerbehandlung • Transparenz Nutzungsbedingungen • Ablehnung jeglicher Sicherheitsaspekte • Kleine Community

S indicates standardization ongoing activities

5 Provider Evaluation Checkliste

Kriterium Erfüllt Kommentar - Umfangreicher Technologiekatalog Jein
Welches Angebot stellt uns der Anbieter zur Verfügung. - Unternehmungs-
grösse des Anbieters Nein Grosse Unternehmen haben tendenziell mehr Er-
fahrung als Cloud Anbieter - Customizing Jein Ist es möglich, Ressourcen
nach beliebigem Bedarf zu skalieren? - Dokumentation Ja - Community
Nein Gibt es eine Community, die bei häufigen Problemen helfen kann?

6 Management Summary