

Governance Hub - Serviceanalyse

Status

reviewed draft - warte auf Feedback von Fabian W. und ggf. Paul

Executive Summary

(Regulierte) Unternehmen prüfen jeden einzelnen Cloud-Service eines Hyperscalers individuell, um diesen zur Nutzung freizugeben - oder im seltenen Fall zu verbieten (Servicebewertung). Hierbei hat sich bewährt, jeden Cloud-Service nach einheitlichen Kriterien zu analysieren (Serviceanalyse), um die Grundlage für diese Servicebewertung durch den Kunden zu schaffen.

Personen

Use Case Autoren	Marcel
Fach-Experten	Marcel, Joris, Viet, Jannes, Alex P.
Tech Experten	-
Hackathon Team	Übung für alle am ersten Tag

Problemstellung

- Kunden müssen die Entscheidung für oder gegen eine Freigabe eines Cloud-Services dokumentieren und nachhalten.
- Eine Freigabe kann auch unter bestimmten Auflagen erfolgen
- Aus der Dokumentation vom Hyperscaler erstellen wir eine Serviceanalyse. Dabei handelt es sich um ein standardisiertes Dokument, um eine Übersicht über einen Cloud Service zu erhalten.
- Auf Basis einer Serviceanalyse erstellen Kunden eine Servicebewertung - mit dem Ergebnis einer Freigabe, Freigabe unter Auflagen oder Verbot.
- Freigabe erfolgt meist durch CISO und Datenschutz. Das Format der Serviceanalyse ist auf ihre Perspektive und Fragen angepasst.
- Freigebende Personen kennen Details zu Cloud-Services meist nicht
- Die Serviceanalyse schafft die strukturierte Grundlage zur Freigabe durch nicht technische Experten
- Wir haben bereits alle relevanten Cloud-Services von AWS, GCP und Azure analysiert

Motivation

- Diese Serviceanalysen haben wir schon mehrfach bei Kunden eingesetzt
- Die Serviceanalysen müssen aktuell gehalten werden, und neue kommen hinzu. Dies lässt sich in einem SaaS-Service einfacher abbilden als in PDFs.
- Serviceanalysen passen perfekt als weiteres Modul in den Governance-Hub, da die Verknüpfung zu den Workloads und den Teams besteht.
- Freigabeprozesse und das Nachhalten der Freigaben ist in einem Tool besser abbildbar.

Funktionale Anforderungen

Grundfunktionen

Service

- Eigenschaften:
 - Kurzname
 - Langname
 - Hyperscaler (AWS, GCP, Azure)
 - Beschreibung
 - Link zu Logo
 - Servicekategorie (Storage, Network, Compute, ...)
 - Servicemodell (IaaS, PaaS, SaaS, FaaS)
- Liste
 - Filter und Sortierung jeder Spalte
 - Suche über Kurzname und Langname
- Aktion: CRUD

Serviceanalyse

- Beziehung:
 - Eine Serviceanalyse gehört zu genau einem Service.
 - Für einen Service kann optional eine Serviceanalyse existieren.
- Eigenschaften:
 - siehe auch PDFs im Abschnitt "Bereitgestellte Ressourcen". Die Eigenschaften weichen in der Namensgebung leicht ab, um alle drei Hyperscaler abbilden zu können.
 - **Status** - Single-Select (kein Rechte- und Rollenkonzept notwendig!)
 - DRAFT
 - APPROVED
 - REJECTED
 - DEPRECATED
 - **Location** - Single-Select
 - Globaler Service, der sich nicht einschränken lässt;
 - Service, der sich regional einschränken lässt
 - **Daten** - Multi-Select

- keine Daten eingebracht
 - liest Daten; verändert Daten
 - Daten werden im Service selbst gespeichert
 - Daten werden im anderen Service gespeichert
- **Telemetriedaten** - Single-Select
 - Ja
 - Ja, aber deaktivierbar
 - Nein
- **Verschlüsselung at-rest** - Multi-Select
 - CMK mit externem Material (BYOK)
 - Customer-managed Key (CMK)
 - CSP-managed key
 - Vom CSP verschlüsselt ohne Einflussmöglichkeiten
 - Keine Information
- **Verschlüsselung in-transit** - Single-Select
 - SSL/TLS Verbindung für den Zugriff auf den Service und zwischen allen Komponenten des Services
 - Verschlüsselung ist optional nutzbar
 - Verschlüsselung kann optional selbst implementiert werden
 - Es wird keine Netzwerkverbindung zum Service bereitgestellt (außer Cloud API selbst)
- **Zertifizierung** - Multi-Select
 - ISO 27001
 - ISO 27017
 - ISO 27018
 - BSI C5
- **Zugangssteuerung** - Multi-Select
 - IAM: Individuelle User und Rollen möglich
 - RBAC: Berechtigung an Ressource selbst
 - Service Rollen: eigene Rolle vom CSP zur Serviceerbringung
 - Muss selbst implementiert/konfiguriert werden
- **Audit Logs** - Multi-Select
 - Protokollierung im zentralen Audit Log
 - Service schreibt eigene Audit Logs
 - Keine Protokollierung
- **Backup und Recovery** - Single-Select
 - Keine Datensicherung notwendig
 - CSP bietet eine managed Lösung an
 - Es existiert eine API, um Backup selbst zu implementieren
 - Datensicherung ist nicht verfügbar
- Erstelldatum
- Liste:
 - Filter und Sortierung jeder Spalte
 - Suche über Kurzname und Langname
- Aktion: CRUD

Dashboard

- Anzahl freigegebener Service pro Hyperscaler
- Pro Kriterium in der Serviceanalyse: Verteilung der Kriterien
z.B. Location: 10% global, 90% regional (Single-Select)
z.B. Zertifizierung: ISO 27001: 100% ja, 90% BSI C5, ... (Multi-Select)
- optionale Ausbaustufe: Vergleichstabelle zwischen den drei Hyperscalern

AI-Assistent

- Neuer Service
 - Servicenamen eingeben
 - "Prefill with AI" Button drücken
 - KI generiert die Eigenschaften als Vorschlag
- Neue Serviceanalyse
 - Analog zum neuen Service
 - KI generiert alle Eigenschaften als Vorschlag mit nachvollziehbarer Begründung
- Ask the service
 - Über jeden Service kann ich Fragen stellen, die anhand der öffentlichen Dokumentation beantwortet werden
 - Ziel: keine Halluzination
- Prompt Analytics
 - Neben einer normalen Volltextsuche kann der Nutzer eine Suche als Prompt formulieren, z.B. Wie viele Services pro Hyperscaler sind global?
 - KI wandelt die Anfrage unter Kenntnis des Datenmodells in eine SQL Abfrage um und das Ergebnis wird ausgegeben.

PDF-Export

- Jede einzelne Serviceanalyse soll als PDF exportierbar werden können, um diese z.B. einem Prüfer übergeben zu können
- PDF Beispiele sind im Abschnitt "Bereitgestellte Ressourcen" verlinkt

Versionierung und Freigabe

- bei jeder Änderung an einer Serviceanalyse wird eine neue Version im Status DRAFT angelegt
- Status kann jeder setzen, wir brauchen für den PoC kein Rollen- und Rechtekonzept
- Wird eine Version freigegeben (APPROVED), muss die alte Version auf veraltete (DEPRECATED) gesetzt werden
- hierüber lässt sich eine gute Historisierung abbilden, da Prüfer meist auf bestimmte Zeiträume schauen

Teams und Workloads

Im Governance Tool existieren bereits Teams und Workloads. Baue diese Funktionalität hier nach, damit es eine Verknüpfung zu der Servicenutzung geben kann und wir damit den Service analysieren können.

Workload

- Beziehung: Ein Workload wird von genau einem Team verantwortet (Owner).
- Eigenschaften:
 - Kurzname
 - Langname
 - Beschreibung
 - Schutzbedarfsklasse (normal, hoch, sehr hoch)
 - Geschäftskritikalität (niedrig, mittel, hoch)
- Liste
 - Filter und Sortierung jeder Spalte
 - Suche über Kurzname und Langname
- Aktion: CRUD

Team

- Beziehung: Ein Team verantwortet kein bis mehrere Workloads.
- Eigenschaften:
 - Kurzname
 - Langname
 - Beschreibung
 - Team Lead Name
 - Team Lead E-Mail
- Liste
 - Filter und Sortierung jeder Spalte
 - Suche über Kurzname und Langname
- Aktion: CRUD

Audit Log

- Alle ändernden Aktionen werden im Audit Log mit Benutzername, Zeitpunkt und ausgeführter Aktion gespeichert.
- Audit Log ist filter- und durchsuchbar.

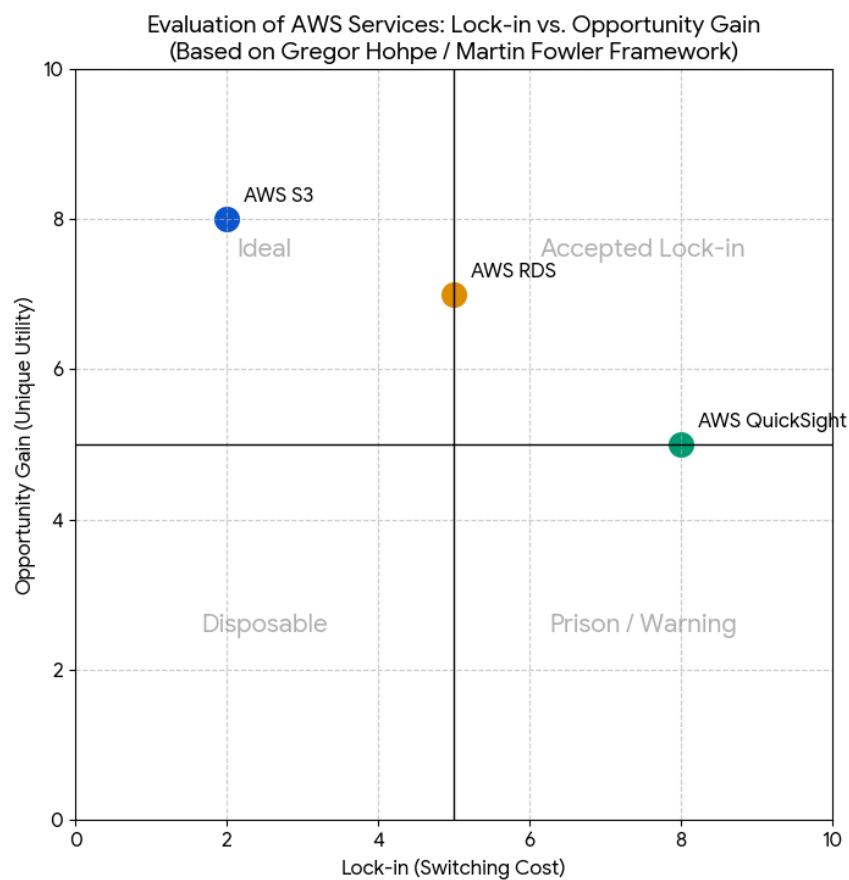
Multi-Language

- Unterstützung für Deutsch und Englische Sprache (Labels im Frontend als auch Daten)

Vendor-Lock / Lock-In Effect

- Beim Vendor-Lock / Lock-in Effect wird meist nur der Aufwand betrachtet, die Lösung zu wechseln (Switching Cost)
- Zusätzlich sollte aber der Mehrwert (Opportunity Gain) betrachtet werden, der erzielt wird, bis es zum Wechsel/Exit kommt.
- Lasse die KI diese beiden Optionen für die Cloud Services bewerten auf einer Skala von 0-10 oder gering, mittel, hoch
- Gebe das Ergebnis in einem (interaktiven) Quadranten, wie man es von Gardner Magic Quadrant kennt, aus. Eine Achse ist Switching Cost, die andere Opportunity Gain.

Beispiel:



Datenimport

- Importiere Daten alle Serviceanalysen der drei Hyperscaler aus den PDFs (siehe bereitgestellte Ressourcen). Hierzu musst du die Daten auf die neuen Begriffe / Datenstrukturen harmonisieren - mit KI.

Nicht-Funktionale Anforderungen

Für die Übung sind wir frei. Allgemein nutzen wir im bestehenden Governance Hub folgende Frontend Technologie:

- [React Router Frontend \(Framework Mode\)](#)
- [MUI Komponenten](#)
- [MUI Toolpad \(Dashboard Components\)](#)

Bereitgestellte Ressourcen

Fachlich:

- [Serviceanalysen als PDFs und Excel](#) (Arbeitsblatt "Data" für AWS-Daten, "Data_GCP" für GCP-Daten)

Technisch:

-