e:ndlich GmbH & Co. KG

CLOUD SERVICE

Himmel und Hölle (Anwendung und Daten weg?)

ALEXANDER WEBER

Cloud Services – Himmel und Hölle

Dieser Erfahrungsbericht stellt zunächst den Oracle Cloud Schema Service vor und zeigt dann die Aufgaben während der Migration. Es folgt ein Einblick in eine Phase der Nutzung, die zu einer massiven Störung des Geschäftsbetriebes führte und somit die möglichen Schwachstellen eines Cloud Service offenbart. Abschließend sind die Vor- und Nachteile dieses Cloud Service gegenübergestellt.

Seit mehr als fünf Jahren ist nun das Thema Cloud in aller Munde und wir, die Firma endlich haben uns deshalb frühzeitig entschieden hier selbst Know-how aufzubauen. Es gab zwei wichtige Gründe für uns, sich mit den Cloud Services zu beschäftigen. Erstens, um den Aufwand unserer selbst betriebenen Infrastruktur zu minimieren. Zusätzlich sollte die Verfügbarkeit gesteigert und der Betrieb stabiler werden. Die zweite Motivation war ein großes Interesse daran, sehr früh eigene Erfahrungen in der Anwendung von Cloud Services zu sammeln.

Welchen Cloud Service?

Prinzipiell gibt es mehrere Ansätze einen Cloud Service zu wählen. Eine Möglichkeit ist, alles so zu nehmen wie es ist, entsprechende Maschinen in der Cloud zu abonnieren und alles 1:1 zu übertragen. Dieser Ansatz ist jedoch nicht wirklich eine Verbesserung, da man eigentlich nur den Spielplatz wechselt, aber die Spielzeuge bleiben die gleichen. Dies kann Sinn machen, wenn man ohnehin mit seinem bisherigen Betreiber unzufrieden ist und wechseln will.
Eine zweite Option ist es die Hardware zu virtualisieren und einige vorhandene Dienste in die Cloud zu verlagern (z.B. eine Datenbank oder ein Active Directory), damit geht man schon in Richtung Konsolidierung und Standardisierung der eigenen Anwendung.
Die dritte Möglichkeit ist einen Service zu wählen, der es ermöglicht, dass die eigene Anwendung ausschließlich auf Basis von Cloud Services läuft und man sich wirklich nur noch um den Betrieb und die Weiterentwicklung der Anwendung kümmern muss.
Als letzte Alternative bliebe noch die vollständige Ablösung der eigenen Anwendung durch eine Cloud Lösung die annähernd das gleiche macht wie die selbstentwickelte Lösung und man sich danach nicht mehr um die Weiterentwicklung kümmern muss.

Wir hatten zum Zeitpunkt der anstehenden Entscheidung für einen Wechsel in die Cloud viele Anwendungen im Haus, die auf Basis Oracle und im Frontend auf Basis APEX liefen. Der maximal unterstützte Technologie Stack wurde uns hier von Oracle selbst angeboten, denn hier bekamen wir einen Service der sich sogar um den Betrieb und die Pflege von APEX kümmert. Die Wahl viel deshalb auf den Oracle Cloud Schema Service.

Der Oracle Cloud Schema Service

Dieser Service läuft unter der Kategorie Platform as a Service (PaaS). Man bezeichnet so eine Dienstleistung, die in der Cloud eine Computer-Plattform für Entwickler von Webanwendungen zur Verfügung stellt.
Dabei handelt es sich um schnell einsetzbare Laufzeitumgebungen, aber auch um Entwicklungsumgebungen, welche mit geringem administrativen Aufwand und ohne Anschaffung der darunterliegenden Hard- und Software genutzt werden können.

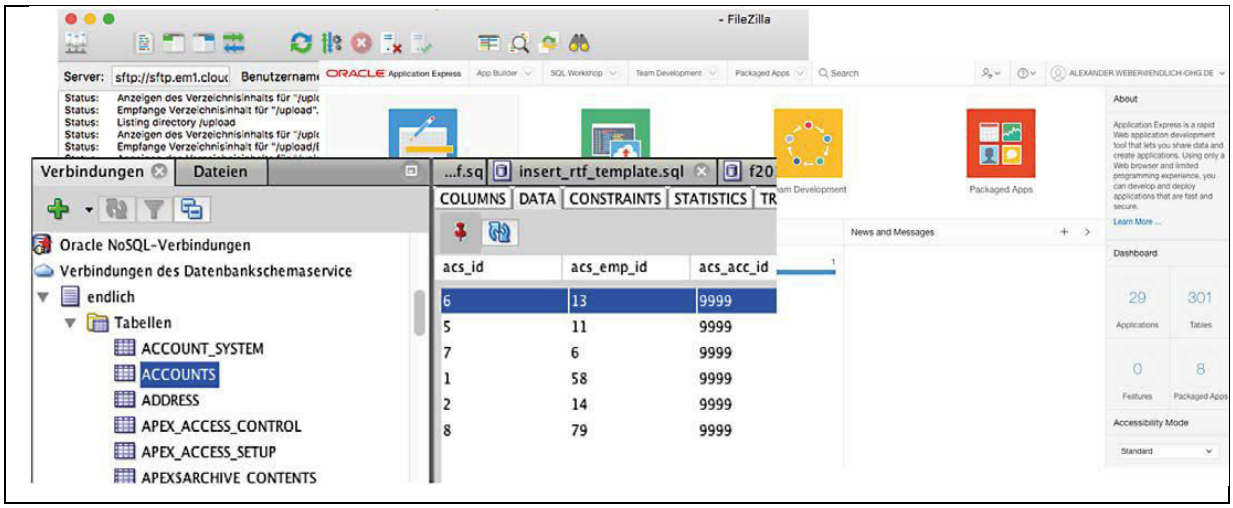


Abbildung 1: Ausschnitte aus den Cloud Service Zugängen mit APEX, FileZilla und SQLDeveloper

Der Database Schema Service besteht derzeit aus:

- Apex 5 (5.1.3), zum Zeitpunkt der Migration war es Apex 4 (4.2.6)
- Ein Datenbank Schema auf einer 11gR2 Datenbank (11.2.4)
- Sftp Zugang für Export/Import
- Zugang zu den Daten über REST Services (z.B. auch über SQL Developer)

Entwickler nutzen PaaS um neuartige und bewusst für die Wolke gestaltete Applikationen zu entwickeln. Mit Paas stehen einem prinzipiell alle Micro-, REST, Web- und Cloud-Services zur Verfügung, um die Anwendung zu erweitern. In sog. Marketplaces kann man diese auch gut vermarkten.

Die Umsetzung/Migration

Im ersten Schritt ging es darum eine geeignete Applikation für die Migration in die Cloud zu finden. Wir haben hierfür folgende Kriterien zu Grunde gelegt.

- Möglichkeit der Konsolidierung der Anwendung auf die „Zwänge“ der zukünftigen Zielumgebung ist mit hoher Wahrscheinlichkeit möglich
- Bereitstellung eines Entwicklers aus bestehenden Projekten für diese Anwendung ist möglich. Es sollte jemand sein, der die Anwendung (mit-) entwickelt hat und sie sehr gut kennt
- Möglichst keine Verzahnung mit anderer Software und wenige Schnittstellen

Die Wahl fiel auf unsere APEX Anwendung zur Unternehmenssteuerung, also quasi ein ERP System.

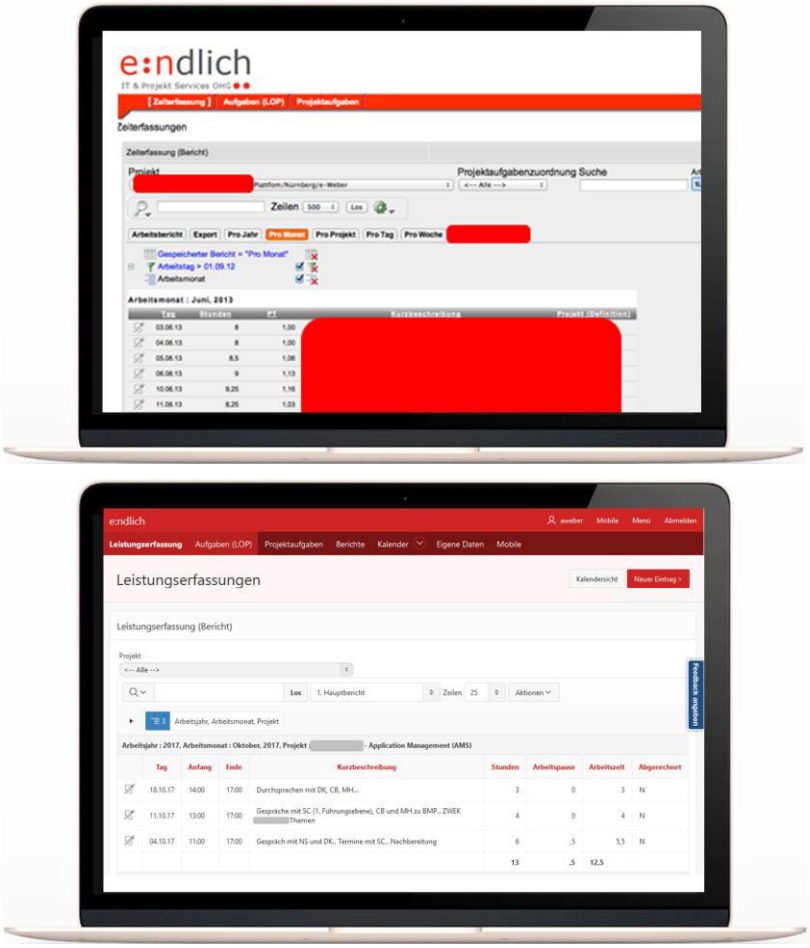


Abbildung 2: Teilmodul Leistungserfassung vor und nach der Migration in die Cloud

Folgende Aufgaben standen auf unserer To-Do Liste:

- ✓ Konsolidierung und Re-Engineering der Anwendung
- ✓ Migration Apex 3 -> Apex 4 (damals)
- ✓ Zusammenführung des Daten- und des Applikationsschemas
- ✓ Obfuscation Toolkit durch DBMS_CRYPTO ersetzen
- ✓ Deploymentvorgehen anpassen
- ✓ LDAP Bezüge eliminieren
- ✓ Java Reports Engine durch eine PLSQL-Eigenentwicklung ersetzen
- ✓ Neue Application Ids

Datenschutz

Der Datenschutz spielt im Cloud Umfeld eine große Rolle. Kunden in Deutschland und Europa legen viel Wert darauf, dass mit Ihren Daten sorgsam umgegangen wird, was gleichzeitig ein gewisser Innovationshemmschuh ist. Wir haben uns deshalb mit den Gesetzen und Bestimmungen auseinandergesetzt und frühzeitig einen externen Datenschutzbeauftragten ins Boot geholt, um Fragestellungen bezüglich IT Sicherheit und Datenschutz zu begleiten.

Abbildung 3: Datenschutz

Mit Datenschutz ist in der Regel auch gleichzeitig IT Sicherheit gemeint, was jedoch nicht dasselbe ist. Es gibt im Zusammenspiel von Datenschutz und IT Sicherheit jedoch eine Überschneidung durch die technisch organisatorischen Maßnahmen (TOM). Bei einer Migration von Services in die Cloud müssen Sie sowohl Ihre eigenen TOMs, als auch die Ihres Cloud Anbieters unter die Lupe nehmen. Dies betrifft insbesondere die Auftragsdatenverarbeitung.

Datenschutzgesetz (BDSG bzw. EU DSGVO)

Beim Datenschutzgesetz geht es darum die Daten von natürlichen Personen zu schützen. Dazu zählen Attribute wie Name, Vorname, Geburtstag, Geburtsort etc. aber auch die näheren personenbezogenen Daten wie Straße und Ort oder BIC und IBAN. Es geht aber darüber hinaus auch immer darum, ob man mit Hilfe der Daten in einem Datenpool einen Bezug zu einer Person herstellen kann oder nicht. Eine Datenmenge gilt rechtlich als datentechnisch „verschmutzt“, wenn es einen Datensatz gibt, mit dessen Hilfe eine Person eindeutig identifizierbar ist. Als Beispiel: In einem Datenpool werden lediglich Ortsteil und Alter gespeichert und ausgewertet. Dies klingt erstmal unkritisch, allerdings könnte es sein, dass im fiktiven Ortsteil „Einsamer Hof in kleine Stadt“ nur ein einziger Mensch mit 85 Jahren wohnt, weshalb man direkt Rückschlüsse auf die Person ziehen könnte und dies ist nicht erlaubt.

IT Sicherheitsgesetz

Im IT Sicherheitsgesetz steht der Schutz kritischer Infrastrukturen, die z.B. für die Wasser- und Energieversorgung oder die Aufrechterhaltung des Gesundheitswesens verantwortlich sind, im Vordergrund. Je nachdem ob man Systeme für solche Infrastrukturen zur Verfügung stellt muss man auch dafür Sorge tragen, dass die IT Sicherheit gewährleistet ist. Hier liegt ein klarer Vorteil in der Nutzung von Cloud-Diensten, da diese in vielen Fällen den Anforderungen der IT-Sicherheit von vornherein genügen.

TOM

Gemäß § 9 Bundesdatenschutzgesetz (BDSG) sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder benutzen verpflichtet, technische und/oder organisatorische Maßnahmen (kurz: TOM) zu treffen, um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind, wie z.B. die Zugangs- oder Auftragskontrolle. Sie müssen die Einhaltung der TOMs selbst laufend kontrollieren, aber auch beim Cloud Anbieter nachfragen!

Was ist jetzt mit den US-Anbietern?

Jene US-Anbieter, welche einen Großteil der Cloud Service Angebote stellen oder die Hersteller der zu Grunde liegenden Software sind, unterliegen per se nicht den Datenschutz und IT Sicherheitsbestimmungen der EU. Allerdings gab es dafür in der Vergangenheit das Safe Harbour Abkommen und nun das EU-U.S. Privacy Shield.
Dieses Abkommen oder Angemessenheitsbeschluss ist eine Art „Freibrief“ der es erlaubt, die US-Dienste zu nutzen.

Grundsätzlich ist es hilfreich, wenn man einen Cloud-Dienst-Anbieter mit europäischer Niederlassung wählt, da dieser somit auch auf europäischem Boden betrieben wird. Bei dieser Konstellation gelten die europäischen Gesetze und Richtlinien auch für den US-Anbieter.
Oracle hat weltweit lokale Datacenter in Betrieb. Wir haben uns damals für das Datacenter „EMEA1“ auf schottischem Boden in Linlithgow entschieden. Viele Informationen über das Datacenter werden jedoch nicht bereitgestellt. Auch online etwas über das Datacenter herauszufinden ist nicht leicht, was jedoch potentielle Angriffe wegen fehlender Informationen erschwert. Wir bewerten das deshalb nicht als negativ.

Datenschutz-Fahrplan für Ihren Weg in die Cloud

Ein paar Punkte, die man auf jeden Fall implementieren sollte, bevor man eigene Services in die Cloud migriert sind folgende:

- ✓ Externer Datenschützer und interner Datenschutzbeauftragter sind zu benennen
- ✓ Cloud Anbieter TOMs sind durch ext. Datenschützer abgefragt und existieren
- ✓ Cloud-Dienst erfüllt BDSG bzw. die EU-DSGVO
- ✓ Cloud Anbieter ist nach ISO 27001 zertifiziert
- ✓ Datacenter befindet sich innerhalb der EU oder/und es existiert ein Angemessenheitsbeschluss, wie das EU U.S. Privacy Shield

Wie lässt sich der Service überwachen?

Sobald die Anwendung in der Cloud ist, hat man auch ein Interesse daran zu wissen, wie der Dienst funktioniert. Es gibt dazu ein „Cloud Service Dashboard“ in dem alle Cloud Dienste aufgelistet sind. Es lassen sich hier für jeden Service die wichtigsten Parameter wie Speicherplatznutzung, der Verfügbarkeits-Status in der aktuellen Woche und die generelle Betriebszeit ablesen. Es sind zudem einige grundsätzliche Verwaltungsaktionen (wie die Benutzerverwaltung und die Initiierung von Datenexporten) möglich. Ein Datenexport wird manuell beauftragt und kann kurz darauf vom SFTP-Server abgeholt werden.
Inzwischen bekommt man auch proaktive Informationen über geplante Ausfallzeiten in der Serviceansicht und separat als Email.

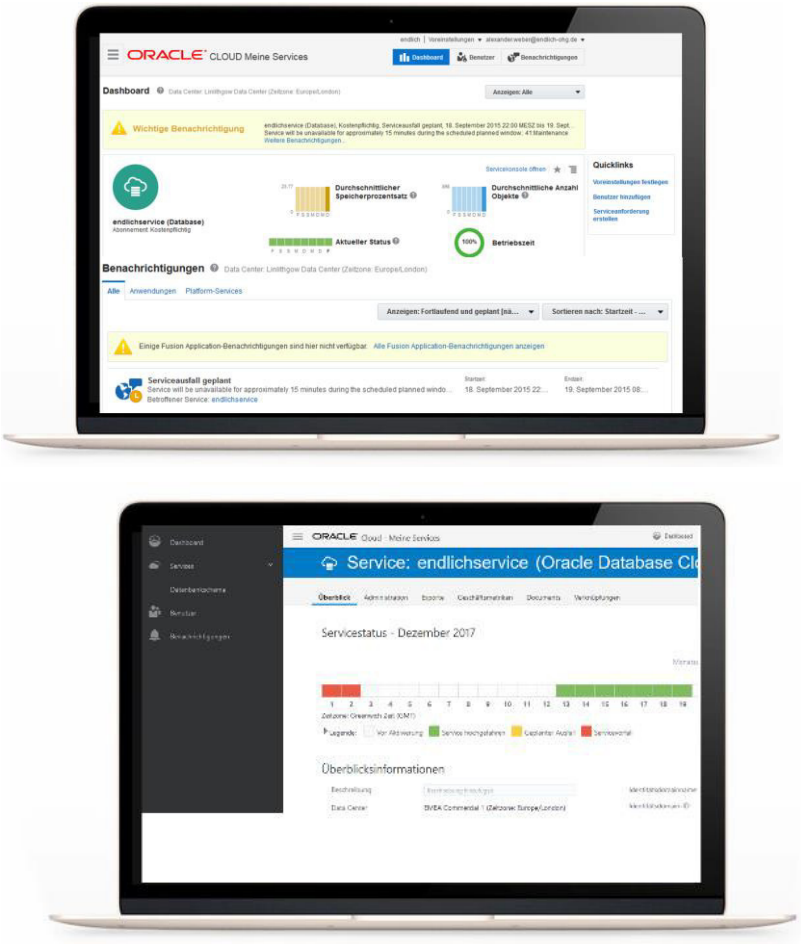


Abbildung 4: Serviceansicht vor zwei Jahren und heute

Das Look & Feel des Dashboards und auch die Serviceansicht haben sich in den letzten Jahren mehrmals verändert, was es immer etwas anstrengend macht sich zurechtzufinden.

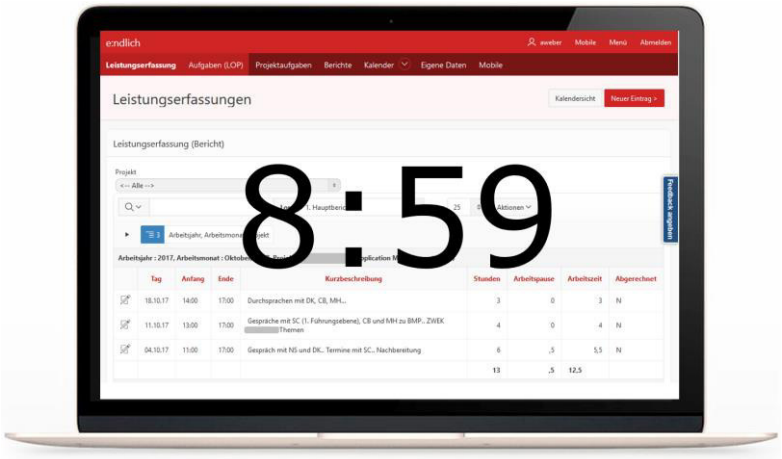
Himmel

Nachdem wir migriert hatten sind wir zu der Überzeugung gelangt, dass der Aufwand von einem halben Jahr, um unsere Anwendung zu migrieren, auf jeden Fall gerechtfertigt war. Verglichen mit der Energie die wir vorher täglich in die Betreuung der Applikation investieren mussten, ist der jetzige Zustand der Himmel des Anwendungsbetriebes. Für uns stellten sich vor allem folgende Vorteile in den Vordergrund:

- ✓ keine Betriebsaufgaben mehr
- ✓ ab der Migration viel weniger ungeplante Ausfallzeiten
- ✓ Apex Backend Migrationen werden für uns durchgeführt
- ✓ CPUs und/oder PSUs werden für uns eingespielt
- ✓ O/S Patches werden für uns eingespielt
- ✓ Angriffe von außen werden abgewehrt
- ✓ wir kümmern uns nur noch um die Entwicklung
- ✓ statt 1 DB Lizenz + mit jährliche Support Kosten, nun ein monatlich kündbares Abonnement
- ✓ skalierbar von Anfang an

Hölle – oder was dann geschah

Bei unserer Cloud-Anwendung handelt es sich um die firmeninterne ERP Anwendung zur Verwaltung der Angebote, Aufträge, Rechnungen, Assets, Mitarbeiterdaten und Leistungserfassung. Es ist für unser Geschäft der Dreh- und Angelpunkt. Die Mitarbeiter nutzen die Anwendung beim Kunden, um ihre verrechenbaren Leistungen zu erfassen.
Die Mitarbeiter im Backoffice erfassen mit Hilfe der Anwendungen neue Aufträge, erstellen Rechnungen, verwalten unsere Assets und es werden Dokumente zu Mitarbeitergesprächen verschlüsselt hinterlegt.



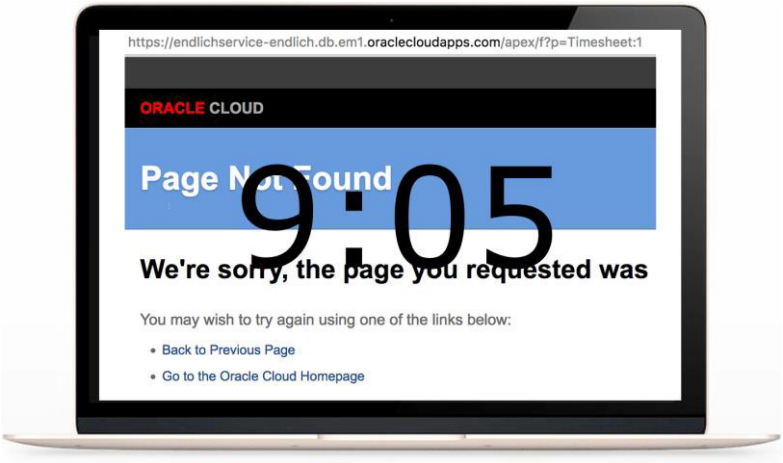


Abbildung 5: Anwendung in der Cloud nicht mehr verfügbar

Im Februar diesen Jahres war jedoch die Anwendung von der einen auf die andere Minute nicht mehr verfügbar. Nach einer kurzen Wartezeit haben wir einen PRIO 1 Service Request bei Oracle eröffnet und hofften auf eine zügige Bearbeitung.
Zur Erinnerung: Ein PRIO 1 Service Request ist die höchstmögliche Priorität mit der man einen Service Request absetzen kann. Bei der Eröffnung eines solchen Tickets muss nicht nur der Fehler beschrieben werden, sondern es müssen auch die Ansprechpartner, die Manager und jeweils deren Kontaktdaten benannt werden. Diese sollen dann für Oracle „rund um die Uhr“ zur Verfügung stehen bzw. erreichbar sein. Somit wurde ein klares Signal gesetzt, dass es sich um ein wichtiges Anliegen handelt und zeitnahe Unterstützung erforderlich ist. Die erste Reaktion seitens Oracle war deshalb sehr enttäuschend.

> *„Hi Alexander, we don't support Apex Cloud Service issues. Please reach out to the right team. Regards, ... Oracle Cloud Services ...“*

Wir wurden jedoch nicht informiert welches das richtige Team ist und der Ball lag wieder bei uns, wir wurden also „abgewimmelt“, was sich in dem Augenblick nicht gut anfühlte.

Wir führten zeitgleich Telefonate mit Oracle Support, Oracle Potsdam und Oracle München.

Es stellte sich heraus, dass es für den Support gar nicht so leicht zu ermitteln ist, um welchen Cloud-Dienst es eigentlich geht. Die Abo-ID und die CSI-Nummer reichten dazu jedenfalls nicht aus. Wir wurden gebeten Schema Name und Tablespace Name zu benennen, was jedoch nicht so einfach ist, wenn der Service nicht mehr zur Verfügung steht. Mit etwas Glück und durch Recherche in Skripten konnten wir jedoch die gewünschten Informationen zusammentragen. Zwischenzeitlich wurde das zuständige Support-Team identifiziert (CLOUDOPS). Dieses Team hat für uns jedoch ziemlich intransparent im Hintergrund gearbeitet. Der Kontakt im Support konnte Fragen nicht direkt beantworten, sondern musste diese erst an das CLOUDOPS Team weiterleiten.

Wir wurden parallel durch unseren vertrieblichen Ansprechpartner gebeten einen neuen Database Schema Service zu bestellen. Wozu dies nötig war konnten wir zu dem Zeitpunkt nicht begreifen, aber aufgrund der Notlage haben wir es getan. Dies ging letztlich relativ schnell, allerdings mussten wir als kleinere Firma auch nicht über einen Einkauf gehen und zeichnungsberechtigte Personen finden, sondern konnten alles durch die Geschäftsführung erledigen lassen. Zwei Tage nach Eröffnung des Service Requests stand der neue, völlig „nackte“ Cloud Schema Service zur Verfügung. Nackt, weil dieser Service weder unsere Daten noch unsere Anwendung enthielt.
Nun traf uns ein weiterer Rückschlag seitens des Supportes. Nachdem wir bestätigt hatten, dass der neue Cloud-Dienst grundsätzlich zur Verfügung steht, bekamen wir folgende Antwort:

> *“Hi,*
> *Thanks for your confirmation. I will be closing this SR since the service is active now.*
> *For any issues,kindly log a separate SR.*
> *Kind Regards,…”*

Man fühlt sich in diesem Augenblick sehr einsam und bereut zutiefst, jemals die Entscheidung pro-Cloud getroffen zu haben. Dieses Beispiel unterstreicht den Beitrag von Herrn Dr. Neugebauer „… Oracle Support – Quo vadis“ Anfang des Jahres, in dem er die sinkende Zufriedenheit von „My Oracle Support“ anspricht. Wir haben im Anschluss direkt mit dem Produktmanagement Kontakt aufgenommen und hatten ab diesem Zeitpunkt den Eindruck, dass tatsächlich etwas passiert. Nach und nach standen uns immer mehr Daten aus unserer gewohnten Umgebung zur Verfügung. Zunächst erstmal „nur“ der Zugriff auf die Laufzeitumgebung, aber es waren immerhin unsere Daten zu sehen und die Anwendung hat grundsätzlich funktioniert.
Es wurden jedoch unter Anderem noch Umlaute in der Applikation falsch dargestellt und Public bzw. Private Interactive Reports waren nicht verfügbar. Auf die APEX Entwicklungsumgebung konnten wir ebenfalls nicht zugreifen. Aber: das Schlimmste war zunächst überstanden und wir haben uns bei den hilfreichen Unbekannten über das Produktmanagement bedankt. Folgende Antwort haben wir daraufhin erhalten.

> *„…Kollegen in den USA haben in einer konzentrierten Aktion mit diversen anderen Cloud Teams das ganze wiederherstellen/mit alten Namen aufsetzen können….“*

Fünf Tage später konnten wir also wieder grundsätzlich mit unserer Anwendung arbeiten und der Geschäftsbetrieb war nicht mehr eingeschränkt. In der Folgezeit wurden auch alle weiteren Schwierigkeiten gelöst und wir haben inzwischen wieder ein völlig sauberes System und können wie zuvor damit arbeiten.

Eines zeigt diese Antwort des Cloud-Service-Produktmanagement jedoch auch: Die Komplexität, einen versehentlich gelöschten Service wiederherzustellen – und bei unserem Beispiel handelt es sich nicht um eine komplexe Umgebung – ist offenbar sehr hoch und bedarf der Zusammenarbeit mehrerer Spezialisten.

Eigentliche Ursache

Eine wirklich offizielle Ursache für diesen Ausfall haben wir nie erfahren, konnten aber den Gesprächen folgendes entnehmen: Der Cloudvertrag basierte auf einer Kreditkarte, deren Ablaufdatum im August des Vorjahres erreicht war. Es gab jedoch keine Kommunikation seitens Oracle darüber, dass dies der Fall ist. Der Service lief trotzdem von August des Vorjahres bis Februar weiter. Der Service wurde deshalb irgendwann auf „zu archivieren“ gestellt und die technische Ausführung dazu fand im Februar statt.

Fazit

Letztendlich lässt sich sagen, dass die Ursache für den Ausfall kein technischer Fehler des Cloud Services, ungewollter Datenverlust oder ein Hackerangriff war. Es handelte sich um ein Problem in den Verwaltungsprozessen, die den Cloud Services zu Grunde liegen. Bei komplexen multinationalen Strukturen in großen Konzernen bei denen die Prozesse nicht mit den technischen Innovationen Schritt halten können, kann dies zu Problemen führen. Es ist deshalb nötig einen funktionierenden Kommunikationskanal zwischen den Nutzern von Cloud-Diensten und dem Anbieter herzustellen, der während des gesamten Application Lifecycle einer cloud-basierten Anwendung funktioniert. Dies könnte der Support sein, ist es aber derzeit nicht.

Trotzdem überwiegen für uns insgesamt die Vorteile, welche die Cloud Services mit sich bringen. Das skizzierte Ausfallszenario hätte auch unabhängig davon, dass es einen Cloud Service betraf, auftreten können. Der Betreiber einer Datenbank in einem „on-premise“ Datacenter hätte auch versehentlich den Abbau einer produktiven Datenbank veranlassen können. Fehler passieren und werden auch zukünftig nicht zu vermeiden sein. Jedenfalls war der Cloud Service trotzdem so robust konzipiert, dass nach einiger Zeit wieder alles ohne Daten- und Funktionalitätsverlust hergestellt werden konnte.

Abschließend die Nach- und die Vorteile im Überblick:

Nachteile

- Einige gute Ideen können wegen der eingeschränkten Funktionalität nicht umgesetzt werden.
- Gefühlt eine unsichere Handlungssituation in der „Lieferantenkette“ aufgrund von fragiler Datenschutzlage (EU U.S. Privacy Shield)
- Wenn etwas schiefgeht, hat man keinen Ansprechpartner im Haus. Man ist der Effektivität des Supports beim Cloud Anbieter ausgeliefert.

Vorteile

- 100%-ige Entlastung im Betrieb
- viel weniger ungeplante Ausfallzeiten
- Gewöhnung an die abgegebene Kontrolle und Genuss der Vorteile
- keine Lizenzgebühren, keine Supportgebühren, sondern einfach ein monatlich kündbares Abonnement
- Skalierbarkeit kann einfach online hinzugekauft werden
- Mehrere Oracle Cloud Services können von einem Ort aus verwaltet werden
- Die Erfüllung der immer höher und komplexer werdenden Datenschutzauflagen übernimmt der Cloud Anbieter Know-how-Gewinn und Erhalt der eigenen Wettbewerbsfähigkeit
- Einschränkung in der Funktionalität des Schema Services hält die Anwendung technisch schlank und man konzentriert sich auf die fachliche Logik

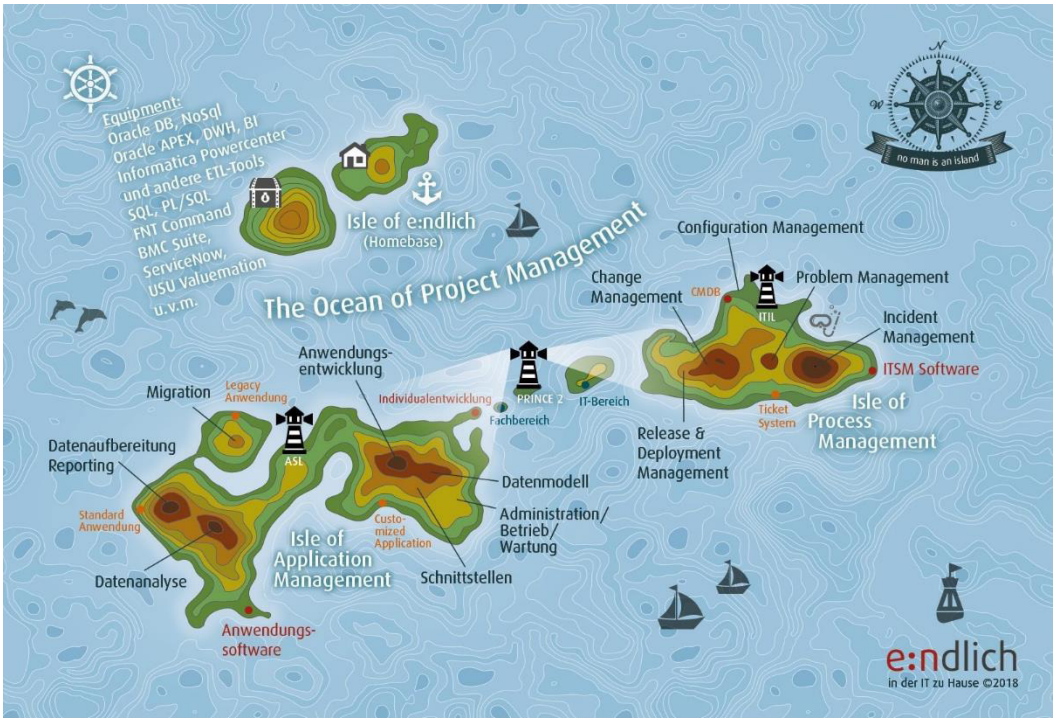
Autor

Alexander Weber, e:ndlich GmbH & Co. KG

Alexander Weber ist Gründer und Geschäftsführer der e:ndlich GmbH & Co. KG und Principal Consultant. Mit über 25 Jahren Erfahrung in der IT-Branche und 18 Jahren Selbständigkeit gehört der Dipl. Ing. Datentechnik zu denjenigen, die das Thema Digitalisierung seit ihren Anfängen begleiten durften. Mit seiner Fähigkeit komplizierte, fachliche Sachverhalte zu erfassen und in dafür nutzbare Anwendungen zu überführen, wird er sehr geschätzt. Das Erkennen und Fördern von Fähigkeiten und Potentialen in Menschen und Systemen ist eine Stärke, die ihm hilft für alle das optimale Ergebnis zu erzielen.

Kontakt:

alexander.weber@endlich.it



e:ndlich GmbH & Co. KG
Flößaustraße 24 | D - 90763 Fürth

Vertreten durch: Inhaber der e:ndlich GmbH & Co. KG: Stephan Witt und Alexander Weber

Kontakt:
eMail: info@endlich.it
Web: www.endlich.it
Tel. +49(0)911-4087-0555
Fax. +49(0)911-4087-884