Oracle Java Cloud Service

Marcus Schröder
Oracle Deutschland B.V. & Co KG
Nürnberg

Schlüsselworte
Cloud PaaS IaaS+ Developer Java WebLogic

Einleitung

Der Oracle Java Cloud Service ist eine Komponente des Oracle Plattform-Cloud-Angebots. Dieser Vortrag gibt eine Übersicht über den Service, zeigt mögliche Einsatzgebiete auf und zeigt das optimale Vorgehen für die Einführung des Java Cloud Service in Ihr Unternehmen. Die Best-Practices beruhen auf realen Kundenbeispielen und Erfahrungen.

Cloud Computing Hype oder Zukunft?

Die Antwort gleich vorweg: Cloud hat/wird seinen Platz in der IT-Welt finden bzw. hat ihn gefunden. Es ist jedoch wichtig, dass sich Unternehmen, die in die Cloud gehen, über Verantwortlichkeiten zwischen Anbieter und Nutzer bewusst sind.

Verantwortlichkeiten

Die Verantwortlichkeiten beziehen sich nicht ausschließliche auf Absicherung von Datentransport und Datenhaltung, auch Administration, Service Level, Leistungsumfang uvm. ist zu betrachten. Der Umfang der Verantwortung ist in erster Linie davon abhängig, welche Kategorie von Services betrachtet wird. Der geringste Anteil an Nutzerverantwortung bietet Software-as-a-Service (SaaS), hier muss sich der Nutzer keine Gedanken über Backup-Zyklen, Versionen der Applikationskomponenten, Patching oder ähnliches machen. Mehr Verantwortung muss beim Platform-as-a-Service (PaaS) vom Nutzer übernommen werden. Zum Beispiel Sizing: Im Gegensatz zum SaaS, reicht es nicht, nur die Anzahl der Benutzer oder das Datenvolumen zu kalkulieren. Die Plattform-Services werden oft nach anderen Kriterien gestaffelt: Anzahl von Transaktionen, Projekten, Prozessen, Speicherplatz, Hauptspeicher, CPU etc. Bevor der Kunde sich eine größere PaaS-Umgebung bereitstellen lässt, muss abgewogen werden, wie viel und vor allem wie lange die Umgebung benötigt wird.

Die größte Kundenverantwortung liegt im Infrastruktur-as-a-Service. Hier wird primär die Rechenkapazität bereitgestellt und der Kunde hat die Verantwortung über alle Prozesse, die oberhalb des Betriebssystems beginnen. Administrative Aufgaben wie Backup, Patching, Updates und Lizenzbeschaffung für Plattform-Dienste liegen beim Kunden. Dies ist der Grund, warum IaaS die günstigste Service-Kategorie ausmacht.

Umgekehrt ist zu betrachten, dass sich das Lizenzmanagement erheblich einfacher gestaltet, je mehr man sich „nach oben" in die SaaS bewegt. Im SaaS sind häufig alle Lizenzen enthalten, die benötigt werden, um den Service zu verwenden, im PaaS-Umfeld sind bis zur Plattform alle Lizenzen inklusive. Die Ausnahme stellt IaaS dar, hier sind alle Lizenzen oberhalb des Betriebssystems zu erwerben.

Es hat sich in den letzten Jahren eine inoffizielle IaaS+-Kategorie zwischen der IaaS und der PaaS gebildet. Hintergrund sind Anforderungen der Entwicklung und zum Teil des Betriebs. Eine PaaS-Lösung wird häufig als „Developer-Cloud" bezeichnet, da die Service-Nutzer häufig Entwickler darstellen. Diese benötigen Zugriff auf das Betriebssystem, um ggf. Anpassungen durchzuführen. In einer PaaS-Umgebung hat der Nutzer keinen Zugriff auf das Betriebssystem. In einer IaaS+-Lösung werden die Infrastruktur + die Plattform automatisch bereitgestellt, der Benutzer erhält Zugriff auf das Betriebssystem und besitzt die damit verbundene Flexibilität.

Die Erfahrungen der letzten Jahre haben gezeigt, dass es zwischen SaaS, PaaS und IaaS kein Schwarz und Weiß gibt, sondern Übergänge, die in der praktischen Anwendung durchaus Sinn machen.

Zugriff
Der Zugriff auf das Cloud Datacenter erfolgt in den meisten Fällen über das öffentliche Internet. Applikationen im Internet ist für viele Anwendungen heute Standard. Rechenzentren schützen sich vor Hacker-Angriffen von außen durch Firewalls, DMZs und Verschlüsselung. Bei einer PaaS-Lösung liegt eine andere Architektur vor und die Verantwortlichkeiten sind anders verteilt. Wird die PaaS-Lösung z. B. als Development-Umgebung verwendet, müssen die Entwickler aus dem Firmen-Netzwerk über das öffentliche Internet auf die Entwicklungsumgebungen zugreifen. Dieses Vorgehen erfordert andere/zusätzliche Sicherheitskonzepte. Neben der Nutzung eines Multi-Protokoll-Label-Switchings (MPLS) Providers, können Technologien wie VPN, Verschlüsselung, Firewall-Regeln, Whitelists etc. zum Einsatz kommen.
Die Abwägung, welche Technologie zum Einsatz kommt, ist abhängig von der Sicherheitsrelevanz der Daten und des Aufwands/der Kosten für die geplante Lösung.

Datenhaltung
In unmittelbarem Zusammenhang mit Zugriff auf PaaS-Umgebungen stehen die Themen Datenhaltung und damit verbundene Verantwortlichkeiten. Daten sind immer wieder Ziel von Hackerangriffen, unabhängig davon, ob die Daten im Internet oder Intranet gespeichert sind. Es gibt keinen hundertprozentigen Schutz, da auch in stark abgeschirmten Umgebungen immer wieder Daten gestohlen werden.
Um einen maximalen Schutz der Daten zu gewährleisten, müssen verschiedene Architekturen und Sicherheitsmechanismen beleuchtet werden:
Die Mandantenfähigkeit, also die Trennung der PaaS-Nutzergruppen nach Organisationen, unterliegt dem PaaS-Provider. Der Provider muss sicherstellen, dass die Daten der Service-Nutzer nicht von anderen Organisationen eingesehen werden können. Dies kann auf unterschiedlichen Ebenen implementiert werden. Auf Infrastruktur-Ebene durch die Nutzung verschiedener (virtueller) Compute-Kapazitäten, Storage und/oder die Trennung der unterschiedlichen (virtuellen) Netzwerke. Es existieren ebenfalls Verfahren, die eine Mandantenfähigkeit auf Plattform-Ebene ermöglichen. Plattform-Architekturen wie Multi-Tended oder Plugable-Container ermöglichen die Trennung von Mandanten auf dieser Ebene. Der Service-Nutzer muss an dieser Stelle entscheiden, welche Verfahren den Sicherheitsaspekt ausreichend abdecken.
Ein weiterer Gesichtspunkt ist die Verschlüsselung. Dieser Bereich liegt in der Verantwortung des Service-Nutzers. Oft bieten Service-Provider verschiedene Verschlüsselungsverfahren innerhalb der Plattformen an, der Service-Nutzer muss entscheiden, ob diese ausreichend sind oder eigene Verfahren angewendet werden. An dieser Stelle sind sich viele Sicherheitsexperten einig, dass nur die Verschlüsselung die Datensicherheit in der Cloud gewährleisten kann.
Lösch-Policies/-Richtlinien liegen in der Verantwortung des Service-Providers. Hinter diesen Richtlinien stehen die Verfahren des Service-Providers, die es ermöglichen Daten eines Service-Nutzer unwiderruflich zu löschen. Das Wiederherstellen der Daten darf unter keinen Umständen möglich sein, wenn der Kunde diese in der Public-Cloud-Umgebung gelöscht hat.

Service-Katalog
Beim Service-Katalog gibt es mehrere Kriterien, die bei der Auswahl des Anbieters berücksichtigt werden sollten. Man unterscheidet zwischen Breite, Tiefe und Anpassbarkeit. Mit Tiefe ist die Funktionalität der eigentlichen Plattform gemeint. Welche verschiedenen Auswahlmöglichkeiten hat der Kunde bezogen auf Zugriff, Sicherheit, APIs, Support, Verfügbarkeit etc.? Mit Breite ist die Breite des Angebots gemeint. Es muss unterschieden werden, dass eine IaaS-Lösung natürlich in der Breite extrem flexibel ist, allerdings ist IaaS nicht gleich PaaS und dies gilt es zu berücksichtigen! Bei einer

PaaS-Lösung übernimmt der Provider mehr Verantwortung als im Bereich IaaS, daher sind die Betriebskosten bei einer PaaS-Lösung signifikant niedrigerer als bei einer IaaS-Lösung. Während bei PaaS-Lösungen Aufgaben wie Backup & Recovery, Upgrade/Update, Patching etc. vom Provider übernommen werden, muss der Kunde sich bei einer IaaS-Lösung um alle Tasks selber kümmern.

Wie bereits in der Einleitung vorweg genommen, Cloud hat seinen Platz in der IT und gerade im Fachbereich längst gefunden. Durch die Verschiebung der Verantwortlichkeiten zwischen Kunden und Anbieter, zusammen mit Standardisierung, Konsolidierung und Automatisierung bewegen wir uns in Richtung Industrialisierung der IT. Dieser Schritt ist eine Evolution und keine Revolution und wurde z. B. in der Fertigungsindustrie schon vor vielen Jahrzehnten vollzogen. Da IT in vielen Bereichen nicht das Kerngeschäft darstellt, werden viele IT-Dienstleistungen schon heute ausgelagert. Mit der Bereitstellung von standardisierten Services können die Anbieter einen Preis anbieten, der im Hosting-Bereich nicht zu halten ist.

Die Oracle Cloud

Anders als von vielen angenommen, ist das Thema Cloud-Computing nicht neu für Oracle. Oracle bietet seit vielen Jahren Applikationen als SaaS-Lösungen an. Für diese SaaS-Lösungen existieren parallel Erweiterungsmöglichkeiten im Bereich Datenbank und Java EE, die es ebenfalls seid mehreren Jahren gibt. Betrachtet man den Cloud-Markt gibt es eine Reihe von Anbietern mit unterschiedlichen Ausprägungen und Background. Es gibt die reinen Software-, Plattform- und Infrastruktur-Anbieter, die in einen der drei Bereiche angesiedelt sind. Diese Anbieter sind Spezialisten, die keine Lösung für die anderen Bereiche anbieten. Eine andere Gruppe von Anbietern hat verschiedene Lösungen, die sich auf zwei oder mehrere Bereiche der Cloud-Gruppierungen erstrecken. Oracle ist einer dieser Anbieter, traditionell kommt Oracle aus dem Software-as-a-Service-Bereich, drängt aber mit einem umfassenden Plattform-Angebot ebenfalls in den PaaS-Markt.
Eine andere Ausprägung der Cloud-Anbieter ist das Hybrid-Cloud-Angebot. Eine Reihe von Cloud-Anbietern unterstützt entweder eine Public-/Private-Cloud beim Hoster oder ein Private-Cloud-Angebot On-Premise beim Kunden.
Oracle bietet viele Cloud-Komponenten sowohl in der Public-Cloud als auch zur Installation On-Premise im Kunden-Rechenzentrum.

Oracle Platform Service

Die PaaS wird oft als Entwicklungs-Cloud bezeichnet, da die API auf Plattform-Ebene liegt. Der Entwickler kann eine standardisierte, konsolidierte und automatisierte Umgebung verwenden, die eine minimale Bereitstellungzeit benötigt. Um die Standardisierung und Administration muss sich der Entwickler keine Gedanken machen und kann sich voll auf die eigentlichen Aufgaben konzentrieren. Es gibt jedoch Entwicklungs-Projekte, in denen es nicht ausreicht, nur auf API-/Plattform-Ebene Zugriff zu gewährleisten. Im Java EE-Umfeld ist es oft nötig, auf Betriebssystem-Ebene Zugriff zu erhalten, um spezielle Anpassungen durchzuführen und Log-Dateien auszuwerten.

Oracle Java Cloud Service

Der Oracle Java Cloud Service ermöglicht dem Nutzer auf das Betriebssystem zuzugreifen. Die Bereitstellung des Services erfolgt voll automatisiert. Der Nutzer parametrisiert die gewünschten Einstellungen, und der Service wird ohne weitere Interaktion erstellt. Zusätzlich zur Erstellung der Plattform wird dem Nutzer eine Reihe von Out-Of-the-Box-Tools bereitgestellt, mit denen administrative Aufgaben erledigt werden können. Backups werden inkrementell/voll und manuell/automatisiert erstellt und in der Oracle Storage Cloud gespeichert. Der Nutzer gibt an, wie

lange das Backup aufbewahrt werden soll, nach Auslaufen der „Retention-Time" wird das alte Backup automatisch gelöscht.
Ein weiterer administrativer Task ist das Patchen der Java EE-Umgebung. Der Oracle Java Cloud Service stellt ein halbautomatisiertes Patch-Verfahren bereit. Der Nutzer kann entscheiden, wann und ob er den Patch einspielen möchte. Der Patch ist von Oracle getestet und kann per „Knopfdruck" in die aktuelle Umgebung eingespielt werden.
Voraussetzung für das Backup und Patchen ist die Unveränderbarkeit der Architektur. Durch eine Veränderung können die Tools nicht mehr arbeiten, da die Administration auf eine bestimmte Ziel-Architektur festgelegt ist.

Ein kostenfreies Add-On für den Oracle Java Cloud Service ist der Oracle Developer Cloud Service. Der Oracle Developer Cloud Service ermöglicht eine zentrale und automatisierte Entwicklung und Bereitstellung von Java Applikationen auf dem Java Cloud Service. Der Oracle Developer Cloud Service bietet neben einem automatisierten Deployment viele Arbeitskomponenten, die für die tägliche Entwicklerarbeit benötigt werden. Zum Beispiel Wiki, Defect-Tracking, Hudson, Code-Change Tracking uvm. Alle diese Komponenten werden zentral in der Oracle Cloud betrieben und ermöglichen ein verteiltes und effektives Arbeiten von Entwicklungsteams.

Oracle Java Cloud Service - Best Practices

Nach dem Erwerb des Oracle Java Cloud Service erhält der Nutzer eine E-Mail, in der er aufgefordert wird den Cloud Account zu aktivieren. Normalerweise erhält der Käufer die E-Mail, also derjenige, der in der Bestellung aufgeführt ist. Um den Account zu aktivieren, wird ein OTN-Account benötigt, die angegebene Adresse sollte also für OTN freigeschaltet werden. Während der Aktivierung wird man aufgefordert, den Identity-Domain-Namen anzugeben. Dieser ist frei wählbar, man sollte sich im Vorfeld Gedanken machen, welcher Name angegeben wird, da dieser nicht mehr zu ändern ist.
Nach der Aktivierung kann der Nutzer sofort arbeiten. Vorher sollte man sich jedoch überlegen, wer die Cloud-Plattform nutzen darf. Hintergrund ist folgender: Jeder Benutzer der in der Cloud-Plattform neue Dienste beantragen darf, ist in der Lage die Cloud-Subscriptions zu verbrauchen. D. h. wenn Nutzer ohne Kontrolle wahllos neue Umgebungen beantragen, kann es passieren, dass das Cloud-Subscriptions-Kontingent wesentlich früher aufgebraucht wird, als geplant.
Im Anschluss erfolgt das Erzeugen und Nutzen der Cloud-Umgebung, Voraussetzung ist das Vorhandensein eines SSH-Key-Paars. Existieren im Unternehmen feste Prozesse, um ein Private-/Public-Key-Paar zu beantragen, sollten ausreichen Keys für die Erstellung von neuen Services vorhanden sein.
Bei der Erstellung von neuen JCS-Instanzen wird man durch ein Dialog-geführtes-Menü geleitet. Die Auswahl der Version bzw. der Option des Oracle Java Cloud Service haben ebenfalls Auswirkungen auf den Verbrauch der Cloud-Subscriptions.
Ist die neue JCS-Instanz erzeugt, stellt sich die Frage, ob ein neues Projekt entwickelt oder ein bestehendes migriert werden soll. Für beide Fälle ist zu beachten, dass es sich beim Java Cloud Service um einen WebLogic-Server mit einer bestimmten (Sub-)Version handelt, der die FMW-Komponenten vorinstalliert hat. Dies hat unmittelbare Auswirkungen auf vorhandene Java-Klassen und Libraries.
Der Java Cloud Service (JCS) benötigt immer eine Datenbank, Grund hierfür sind die vorinstallierten Oracle FMW-Komponenten. Es ist mögliche mehrere JCS-Instanzen in eine Datenbank zu installieren. Die ideale Konstellation ist jedoch eine Datenbank pro JCS-Domäne, dies ist bei Backup- & Recovery-Szenarien von Vorteil.
Wird die JCS-Instanz nicht genutzt, ist es möglich diese herunterzufahren. Durch das Herunterfahren lassen sich Cloud-Subscriptions einsparen. Es sollte jedoch berücksichtigt werden, welches Abrechnungsmodell bei der Erstellung des Services ausgewählt wurde. Es existieren zwei Taktungen:

Monatlich und stündlich. Die stündliche Abrechnung ist ca. 25 % teurer als die monatliche, d. h. benötigt man die Umgebung nur einige Tage oder nur ab und zu, ist es optimaler, die Umgebung stündlich abzurechen und die Umgebung anschließend herunterzufahren.
Backup & Recovery erfolgt mittels Oracle Cloud Tooling. Beim Java Cloud Service Virtual Image sind weder das Backup & Recovery noch das Patch-Tooling enthalten, dies sollte man vor der Erstellung einer neuen Umgebung beachten.
Das Scale-Out des Java Cloud Service ermöglicht im laufenden Betrieb zusätzliche Server-Instanzen in ein bestehendes Cluster einzufügen, dies erfolgt entweder aus der Cloud-Administrationsoberfläche oder per REST-API-Call. Der API-Call kann aus einer Anwendung heraus erfolgen, ein mögliches Szenario lässt ein automatisches Scale-Up bei Lastspitzen zu.
Im Bereich Security ist die Vergabe von Rollen an neue Benutzer ein sehr wichtiges Thema. Jeder Benutzer kann eine oder mehrere Rollen erhalten. Die Rechte innerhalb dieser Rollen reichen vom Anlegen neuer Cloud-Admin-Benutzer bis Read-Only bestehender Services. Die Rolle Identity Domain Administrator sollte sehr sparsam eingesetzt werden. Der Domain-Administrator ist in der Lage, neue Benutzer anzulegen und diesen ebenfalls die Rolle Domain-Administrators zu vererben.
Jede Identity Domain besitzt eine eigene Firewall. Per Default gibt es eine Reihe von Ports und Protokollen, die auf eine Nutzung mit den Services vorbereitet sind, die sogenannten „Security Rules". Die Regeln sind bis auf eine Ausnahme alle deaktiviert. Grund hierfür ist die Einhaltung höchstmöglicher Sicherheitsstandards. Die einzige Ausnahme dieser Regel ist das SSH-Protokoll, ohne den Zugriff auf die Maschine mittels SSH ist es nicht möglich den initialen SSH Public Key zu installieren.
In den erworbenen Cloud-Subscriptions ist der Oracle Support enthalten. Der Support kann über die üblichen Kanäle kontaktiert werden, wie z. B. über Web und Telefon. Die Oracle Cloud bietet noch einen weiteren Vorteil: in der Cloud-Oberfläche ist ein Chatmodul integriert. Dieses Modul verbindet den Nutzer bei Aktivierung umgehend mit einem Supportmitarbeiter. Mittels Chat können Probleme umgehend und unkompliziert gelöst werden.
Zur Kostenkontrolle existieren in der Oracle Cloud mehrere Funktionen, die einen Überblick über die verbrauchten und noch vorhandenen Cloud-Subscriptions geben. Den zentralen Einblick hat der Domain-Administrator, er kann über ein Portal die noch vorhandenen Cloud-Subscriptions einsehen, er erhält außerdem eine automatische Nachricht, wenn die Cloud-Subscriptions verbraucht sind. Eine weitere Möglichkeit ist die Übersicht nach verschiedenen Kostenfaktoren, wie beispielsweise Speicher-, CPU- und Storage-Verbrauch. Diese Daten können exportiert und weiter verarbeitet werden.

Zusammenfassung
Der Oracle Java Cloud Service bietet eine umfassende und hochflexible Lösung für jegliche Java EE-Anwendungen. Die Skalierbarkeit und Administrationsunterstützung ermöglichen eine Reduzierung des operativen Aufwands. Diese Best-Practices stellen einen Ausschnitt aus den möglichen Einsatzgebieten dar, eine vollständige Darstellung aller Anwendungsmöglichkeiten sprengt den Rahmen dieses Vortrags.

Kontaktadresse:
Marcus Schröder
Oracle Deutschland B.V. & Co KG
Lina-Ammon-Str. 19
90471 Nürnberg

Telefon/Fax: +49 (0)911 98182471
E-Mail: marcus.schroeder@oracle.com
Internet: www.oracle.com