

**IaaS+? Oracle Cloud „Infrastruktur“ am Beispiel 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 läuft in einer Cloud-Infrastruktur, die Optionen in den Bereichen Security, Architektur, Administration etc. bietet. Anders als in einer herkömmlichen Managed-Umgebung hat der Benutzer Root-Rechte. Was bedeutet das für den Umgang mit dem Cloud Service? Wo liegen die Verantwortlichkeiten für den Nutzer? Dieser Vortrag stellt die Möglichkeiten der „Infrastruktur“ dar und gibt Tipps und Tricks für die optimale Nutzung.

**Was ist der Oracle Java Cloud Service?**

Die heutigen Application Cloud Services sind oft als Container-Services konzipiert. Das bedeutet, der Nutzer ist in der Lage, seine Applikationen in einen Container bereitzustellen. Alle administrativen Aufgaben liegen beim Cloud-Provider. Aus Betriebssicht hat dies Vorteile, da kein zusätzlicher administrativer Aufwand nötig ist. Aus Entwicklersicht birgt dieses Angebot auch Nachteile, da es zu einer großen Einschränkung bezüglich Flexibilität kommt. Der Entwickler hat in diesem Angebot keinen Zugriff auf das Betriebssystem. Oft muss zu einem reinen Container-Service ein Infrastruktur-Service beschafft werden. Dies bedeutet administrativen Aufwand für die Pflege des zweiten Services. Aus Kostensicht hat man zwar beim Container-Service weniger Aufwand, muss jedoch zwei Services bezahlen und verwalten.

Der Oracle Java Cloud Service (JCS) geht andere Wege. Der Service-Nutzer erhält einen vollinstallierten WebLogic-Server und hat vollen Zugriff auf das Betriebssystem. Das Oracle-Angebot unterscheidet sich deutlich von einem einfachen OS-Image mit vorinstalliertem WebLogic Server. Der Applikationsserver wird zur Laufzeit installiert. Dadurch erhält der Service-Nutzer die Möglichkeit, unterschiedliche WebLogic-Server-Architekturen auszuwählen. Beim Java Cloud Service Virtual Image erhält der Service-Nutzer einen WebLogic Server ohne Cloud Tooling. Anders beim Java Cloud Service – hier erhält der Benutzer von Oracle entwickelte und getestete Tools für Backup, Recovery, Skalierung und Patching. Alle Tools sind für die vorgeschlagenen Architekturen zertifiziert. Sie werden automatisch on demand durchgeführt. Der Service-Nutzer kann zwischen drei WebLogic-Server-Versionen auswählen: 11.1.1.7, 12.1.3 und 12.2.1. Alle Applikationsserver werden auf einem Oracle Linux 6.6 bereitgestellt. Die Versionen stehen als Standard Edition, Enterprise Edition und Enterprise Edition mit Oracle Coherence bereit. Der Service-Nutzer kann initial bis zu vier Cluster-Knoten bereitstellen, diese können nach dem Start des Services erweitert werden. Zusätzlich erhält der Nutzer die Möglichkeit, einen Loadbalancer in die Architektur einzufügen. Bei dem Loadbalancer handelt es sich um den Oracle Traffic Director (OTD), einen Software Loadbalancer, der ebenfalls in einem Cluster-Verbund bereitgestellt werden kann.

Nach der Bereitstellung erfolgt ein automatisches Backup. Bei der Backup-Steuerung kann zwischen einem Full-Backup und einem inkrementellen Backup gewählt werden. Alle weiteren Einstellungen, wie Retention-Time, Backup-Zeitpunkte etc., werden durch den Service-Nutzer eingetragen. Notwendige Patches werden dem Nutzer angezeigt. Sie können auf Knopfdruck auf die bestehende Architektur angewendet werden. Scale-Out und Scale-In werden vom Cloud-Tooling übernommen. Wichtig ist: Die von Oracle vorgegebenen Architekturen dürfen nicht verändert werden, da in diesem Fall das Cloud-Tooling nicht korrekt funktionieren kann.

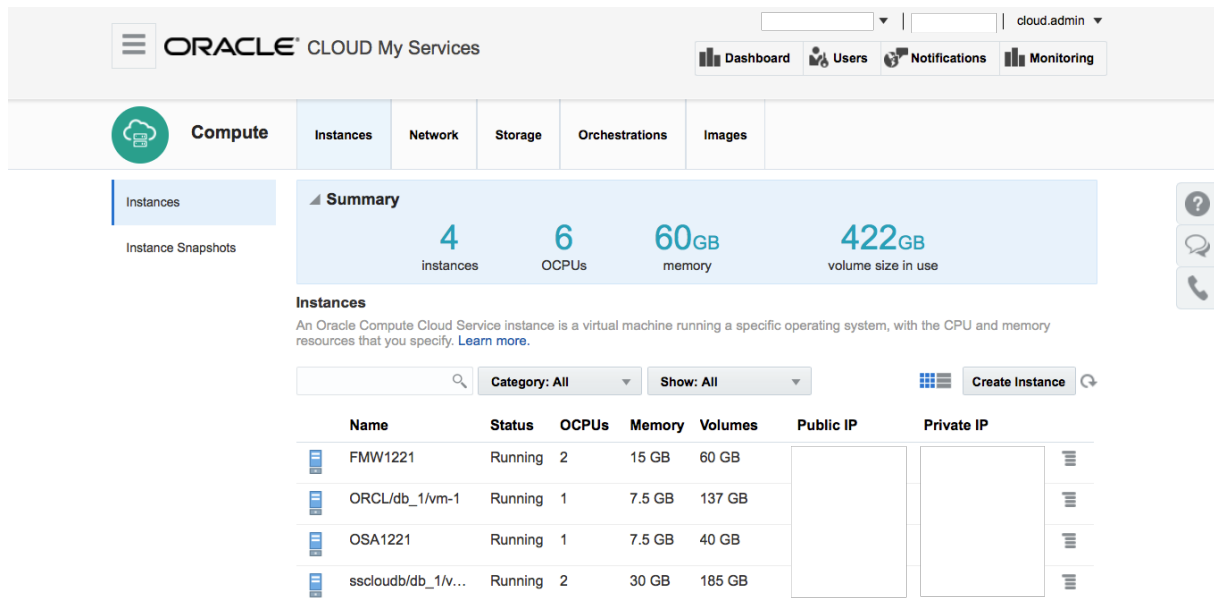


Abb. 1: Compute-Nodes des Java Cloud Services

### Infrastrukturen des Oracle Java Cloud Service

Da der Service-Nutzer uneingeschränkten Zugriff auf das Betriebssystem hat, sind bestimmte Einstellungen bezüglich der Infrastruktur zu beachten. Der Oracle Java Cloud Service ist kein reiner Cloud-Plattform-Dienst (PaaS), sondern kann als Cloud-Infrastruktur-Service-Plus (IaaS+) bezeichnet werden. Dieser Dienst verbindet die Vorteile beider Services. Auf der einen Seite liefert der Service hohen Automatisierungsgrad und Standardisierung, auf der anderen Seite hat der Entwickler maximale Flexibilität. Der nachfolgende Vortrag geht im Detail auf die Infrastruktur-Komponenten der Java Cloud Services ein. Es handelt sich um die Komponenten Compute, Storage und Network.

### Infrastrukturen des Oracle Java Cloud Service – Compute

Die Compute-Infrastruktur wird beim Oracle Java Cloud Service durch ein virtualisiertes Linux 6.6 Image bereitgestellt. Das Image wird in verschiedenen standardisierten Größen angeboten, den Compute-Shapes. Die Größe dieser Shapes ist für alle Infrastruktur-Komponenten gleich, das heißt auch für den Oracle Database Cloud Service. Die Maßeinheit für die Shape-Größe ist Oracle CPU (OCPU). Eine OCPU entspricht einem Intel Xeon Core mit Hyperthreading aktiviert, dies entspricht ca. einer halben Prozessor-Lizenz für Oracle-Produkte die On-Premise lizenziert werden. Die Shape-Bezeichnungen gehen von OC1 (entspricht 0,25 OCPU) bis OC7 (16 OCPUs). Die Shapes OC1 und OC2 sind zurzeit nicht verfügbar. Beginnend mit OC3 (eine OCPU) verdoppeln sich bei jedem weiteren Shape die OCPU-Anzahl und der Arbeitsspeicher, das heißt OC4 sind zwei OCPUs, OC5 sind vier usw.

Es gibt zwei Shape-Varianten, die sich durch die Größe des Arbeitsspeichers unterscheiden, die Bezeichnungen sind: General Purpose und High Memory. Bei der OC3-General-Purpose-Variante mit einer OCPU liegt der Arbeitsspeicher bei 7,5 Gigabyte, bei der OC4-General-Purpose-sind es 15 usw. Der Unterschied zwischen der General-Purpose- und High-Memory-Variante liegt in der Verdoppelung des Arbeitsspeichers. In diesem Fall verfügt ein OC3-High-Memory-Shape (OC3M) über 15 statt 7,5 Gigabyte, OC4M über 30 Gigabyte usw. Die High-Memory-Varianten sind bis maximal OC5M (16 OCPUs/240 Gigabyte RAM) verfügbar.

Das Betriebssystem wird auf einem vorinstallierten, virtualisierten Mount bereitgestellt. Dieser Mount wird bei jedem Neustart des Services neu bereitgestellt. Deshalb wird an dieser Stelle empfohlen, nicht auf die Betriebssystem-Partition zu schreiben, da diese Informationen nach einem Neustart nicht mehr zur Verfügung stehen. Grund für dieses Vorgehen ist ein speziell gehärtetes Betriebssystem, das die hohen Sicherheitsanforderungen von Oracle erfüllt.

Ein weiterer wichtiger Punkt ist die Installation von Oracle-Produkten auf die Infrastruktur-Umgebungen. Sind beim Service-Nutzer on-Premise-Lizenzen vorhanden, die er in der Cloud nutzen möchte, ist Folgendes zu beachten: Bei Oracle-Cloud-Services, die vorinstallierte Oracle Software beinhalten (zum Beispiel Java Cloud Service – JCS oder Database Cloud Service - DBCS), dürfen auf diesen Instanzen keine anderen On-Premise-Oracle-Lizenzen verwendet werden. Da JCS und DBCS inklusive Update und Support per Subscription bezahlt werden, dürfen diese Instanzen nicht mit On-Premise-Lizenzen vermischt werden. Bei einer reinen IaaS-Instanz entfallen diese Einschränkungen.

### **Infrastrukturen des Oracle Java Cloud Service– Storage**

Bei den Oracle-Storage-Optionen kann der Service-Nutzer zwischen zwei Storage-Arten auswählen, Block-Storage und Object-Storage. Block-Storage ist virtualisierter Server-Storage, der zum Java Cloud Service hinzugefügt wird. Der Benutzer kann Volumen bis zu zwei Terrabyte erstellen und einem Boot-Image zuweisen. Der Object-Storage wird über eine OpenStack-kompatible REST-API gesteuert. Über die API werden Storage-Container erzeugt und dem Java Cloud Service zugewiesen. Beim Backup des Java Cloud Services werden die Informationen erst auf die lokalen Block-Storage-Platten geschrieben und automatisch per Cloud-Tooling in den Object-Storage verschoben.

### **Infrastrukturen des Oracle Java Cloud Service– Netzwerk**

In Public-Cloud-Umgebungen ist der Bereich Netzwerkinfrastrukturen eine kritische Komponente. Es wird zwischen internen und externen Netzwerken unterschieden. Das externe Netzwerk beinhaltet alle Komponenten, die bis in das Oracle-Public-Cloud-Rechenzentrum führen. Beim internen Netzwerk handelt es sich um alle Komponenten zwischen Internet Gateway des Rechenzentrums und der Service-Nutzer-Umgebung.

Die Basiskommunikation des externen Netzwerkes findet ungesichert über das Internet statt. Zur Absicherung der Kommunikationswege bzw. um optimierte Latenzzeiten zu gewährleisten, stellt Oracle zwei Optionen für den Java Cloud Service bereit.

Die erste Lösung ist die softwarebasierte „VPN-for-Compute“-Lösung, mit der die Kommunikation zwischen Service-Nutzer und der Instanz im Oracle-Rechenzentrum abgesichert wird. Die zweite Lösung „Fast Connect“ bietet eine latenzarme und sichere Private-Line zwischen dem Rechenzentrum des Service-Nutzers und des Oracle-Cloud-Rechenzentrums.

Innerhalb des Oracle-Cloud-Rechenzentrums ist der Bereich (User Domain) des Service-Nutzers durch ein virtuelles Netzwerk gekapselt. Die Instanzen des Nutzers kommunizieren untereinander über Private-IPs. Für externen Zugriff erhält jede Instanz bei der Erstellung eine Public IP zugewiesen. Benötigt die Instanz mehrere Public IPs, können weitere hinzugefügt werden. Jede Benutzerdomäne verfügt über eine eigene Firewall. Diese ist konfigurierbar und beinhaltet Funktionen wie Whitelisting, Blacklisting und Portfreischaltungen. Bei der Erstellung eines neuen Services muss der Benutzer zwingend einen eigenen SSH Public Key angeben. Wird der Service gestartet, ist in der Firewall ausschließlich der Port 22 für den SSH-Traffic freigeschaltet, alle anderen benötigten externen Ports müssen vom Benutzer in der Firewall geöffnet werden. Durch die ausschließliche Nutzung von Kunden-SSH-Keys und der Steuerung der Firewall wird ein maximaler Sicherheitslevel gewährleistet. Geht der SSH-Key verloren, hat Oracle keine Möglichkeiten, diesen neu zu generieren oder auf eine andere Art auf die Instanz zuzugreifen.

The screenshot shows the Oracle Cloud My Services interface. The top navigation bar includes 'ORACLE CLOUD My Services', 'cloud.admin', and links for 'Dashboard', 'Users', 'Notifications', and 'Monitoring'. The main navigation menu has 'Compute', 'Instances', 'Network', 'Storage', 'Orchestrations', and 'Images'. The 'Network' section is active, showing 'Security Rules' with a summary of 28 security rules and 22 enabled. Below the summary, there is a 'Security Rules' section with a description and a table of rules.

Name	Status	Security Application	Source	Destination
1A-DBListenerPu...	Enabled	ORCL/db_1/ora_dblist...	public-internet	ORCL/db_1/ora_db
1A-FMW1221-Htt...	Enabled	1A-FMW1221-Htt...	public-internet	FMW1221
1A-FMW1221-Htt...	Enabled	1A-FMW1221-Htt80...	public-internet	FMW1221
1A-FMW1221-Htt...	Enabled	1A-FMW1221-Htt8080	public-internet	FMW1221
1A-FMW1221-Htt...	Enabled	1A-FMW1221-Https443	public-internet	FMW1221
1A-FMW1221-SSH	Enabled	ssh	public-internet	FMW1221
1A-OSA1221-70...	Enabled	1A-FMW1221-Htt...	public-internet	OSA1221

Abb. 2: Firewall-Regeln des Java Cloud Service

## Zusammenfassung

Der Oracle Java Cloud Service bietet den Nutzern eine Kombination aus einem Plattform- und einem Infrastruktur-Service. Dieser Ansatz verspricht die Vorteile einer standardisierten, automatisierten Umgebung mit der maximalen Flexibilität eines Hosting-Services. Die Voraussetzungen für die Nutzung eines solchen Services sind Kenntnisse der darunterliegenden Infrastruktur. Erst durch diese Kenntnisse wird die optimale Nutzung des Services möglich. Ein weiterer Vorteil der Oracle-Lösung: Es findet keine „Über-Subscription“ statt, wenn ein Benutzer beispielsweise vier OCPUs bei der Instanz-Erstellung angibt, stehen ihm die vier OCPUs exklusiv zur Verfügung. Durch dieses Vorgehen erreicht der Oracle Cloud Service eine gute und stabile Performance.

## 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