Oracle Database in de Cloud
Do’s and Don’ts

ORACLE

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Agenda

- Doen
  - Veiligheid voorop
  - Bepaal vooraf wat je nodig hebt
  - Hou applicatie en database bij elkaar
  - Optimaliseer voor de Cloud
- Niet doen
  - Verwacht geen 24/7 uptime
  - Je provider lost niet alles op
  - Iedere gebruiker zelfde rechten
  - Denken dat er slechts 1 Cloud bestaat

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

DO #1

Veiligheid voorop

Not to be used in external presentations or publications

Veiligheid voorop

- You’re not in Kansas anymore
  - (Virtuele) Server hangt in een cloud en heeft minimaal een public IP adres
  - Iedereen vanuit de hele wereld kan er bij komen
    - In de Oracle DBaaS Cloud is alleen poort 22 open, toegang via public/private key
    - Portscans, brute-force attacks, rainbow table attacks zijn meer regel dan uitzondering
  - Key-authenticatie wordt vaak als lastig gezien
    - Na imaging worden de authenticate regels aangepast
      - test1234 of changeme veel gebruikte wachtwoorden
      - Dit is bekend op het internet en men maakt er dankbaar gebruik van

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Wie doet dat nou ?

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Zo veel gebeurt dat toch niet ?

```
-bash-4.1# tail -f /var/log/secure
May 30 07:50:30 rpastijn-emea sshd[28822]: input_userauth_request: invalid user root
May 30 07:50:31 rpastijn-emea sshd[28822]: Disconnecting: Too many authentication failures for root
May 30 07:50:34 rpastijn-emea sshd[28824]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
May 30 07:50:34 rpastijn-emea sshd[28824]: User root from 210.245.92.140 not allowed because not listed in AllowUsers
May 30 07:50:34 rpastijn-emea sshd[28827]: input_userauth_request: invalid user root
May 30 07:50:35 rpastijn-emea sshd[28827]: Disconnecting: Too many authentication failures for root
May 30 07:50:37 rpastijn-emea sshd[28828]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
May 30 07:50:37 rpastijn-emea sshd[28828]: User root from 210.245.92.140 not allowed because not listed in AllowUsers
May 30 07:50:37 rpastijn-emea sshd[28831]: input_userauth_request: invalid user root
May 30 07:50:38 rpastijn-emea sshd[28831]: Disconnecting: Too many authentication failures for root
May 30 07:50:41 rpastijn-emea sshd[28832]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
May 30 07:50:41 rpastijn-emea sshd[28832]: User root from 210.245.92.140 not allowed because not listed in AllowUsers
May 30 07:50:41 rpastijn-emea sshd[28835]: input_userauth_request: invalid user root
May 30 07:50:42 rpastijn-emea sshd[28835]: Disconnecting: Too many authentication failures for root
May 30 07:50:44 rpastijn-emea sshd[28837]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
May 30 07:50:44 rpastijn-emea sshd[28837]: User root from 210.245.92.140 not allowed because not listed in AllowUsers
May 30 07:50:44 rpastijn-emea sshd[28840]: input_userauth_request: invalid user root
May 30 07:50:45 rpastijn-emea sshd[28840]: Disconnecting: Too many authentication failures for root
May 30 07:50:48 rpastijn-emea sshd[28841]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
May 30 07:50:48 rpastijn-emea sshd[28841]: User root from 210.245.92.140 not allowed because not listed in AllowUsers
May 30 07:50:48 rpastijn-emea sshd[28844]: input_userauth_request: invalid user root
May 30 07:50:48 rpastijn-emea sshd[28844]: Disconnecting: Too many authentication failures for root
May 30 07:50:51 rpastijn-emea sshd[28845]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
May 30 07:50:51 rpastijn-emea sshd[28845]: User root from 210.245.92.140 not allowed because not listed in AllowUsers
May 30 07:50:51 rpastijn-emea sshd[28848]: input_userauth_request: invalid user root
May 30 07:50:52 rpastijn-emea sshd[28848]: Disconnecting: Too many authentication failures for root
May 30 07:50:54 rpastijn-emea sshd[28849]: Address 210.245.92.140 maps to mail.toplink.com.vn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
```

- Meer dan 3000 keer per maand (alleen ssh toegang)
  - Berekening tussen 1 april en 12 mei
  - 5322 failed login pogingen op de ssh server vanuit 132 verschillende locaties
  - Meest populair was 'root' (5172x), daarna 'operator' (25x), 'ftp' (25x) en 'uucp' (14x)

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Lessons Learned Do#1

- **Er moet een goede firewall aktief zijn**
  - Vanuit de Cloud omgeving of vanuit de Image of beide
- **Open alleen die poorten die nodig zijn en communiceer veilig**
  - Open ze alleen voor het IP adres waarvoor ze nodig zijn (listener etc)
  - Gebruik VPN indien aanwezig (OpenVPN, CorenteVPN etc)
  - Zorg voor versleutelde gegevensstromen bij de open poorten
- **Zorg voor goede toegangscontrole en audit, ook preventief**
  - Gebruik geen passwords, minimaal private/public keys
  - Verzamel audit informatie en scan deze regelmatig (bijvoorbeeld Audit Vault)
  - Maak eventueel gebruik van pro-aktieve scripts zoals **`fail2ban`**

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

DON’T #1

Verwacht 24x7 uptime

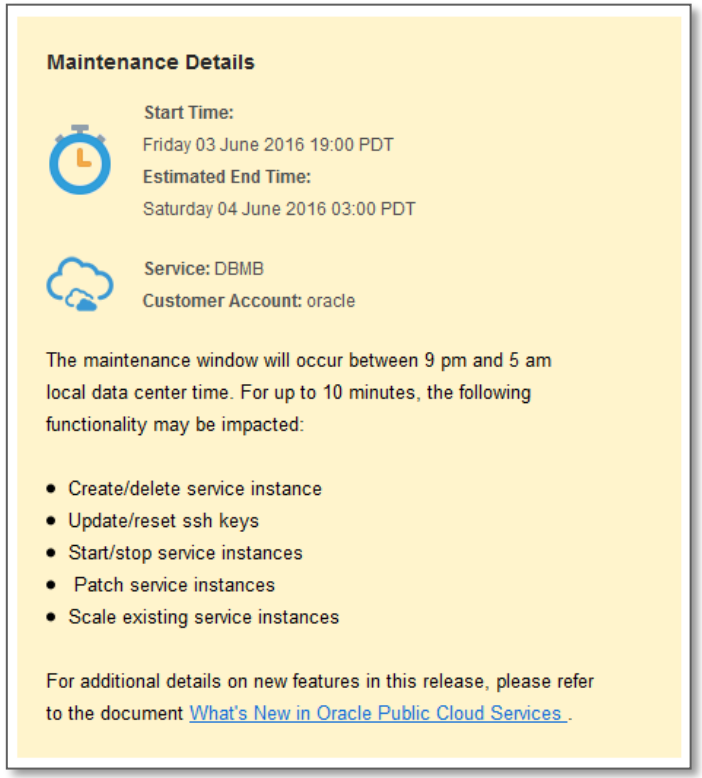
Not to be used in external presentations or publications

Don’t #1: Verwacht uptime wanneer jij nodig hebt

- Cloud setups hebben vaak een stabielere architectuur (vs on-premise)
  - Vooral bij kleinere omgevingen
  - Eenvoudiger bij grotere aantallen gebruikers, servers, storage, racks etc
- Hardware en software moet onderhouden worden
  - Maintenance windows zijn nodig, kan downtime tot gevolg hebben
  - Niet altijd gepland op de tijd en dag dat het het beste uitkomt
- Hardware en software kan kapot gaan
  - Reboot kan nodig zijn
  - Langere downtijd kan nodig zijn

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #1: Verwacht uptime wanneer jij nodig hebt



Maintenance Details

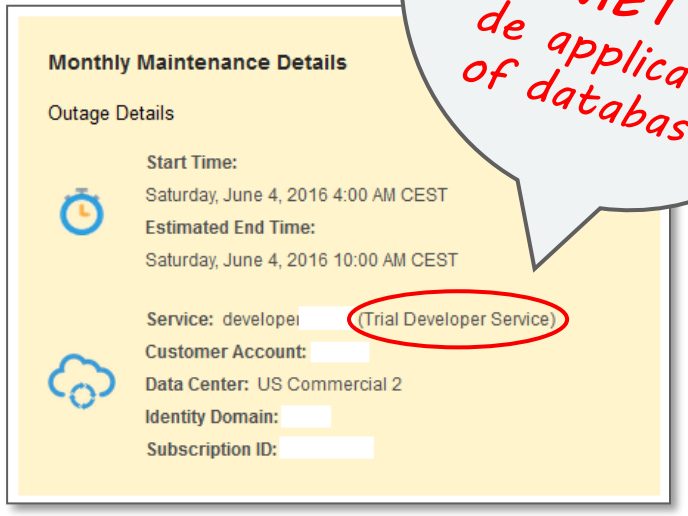
Start Time:
Friday 03 June 2016 19:00 PDT
Estimated End Time:
Saturday 04 June 2016 03:00 PDT

Service: DBMB
Customer Account: oracle

The maintenance window will occur between 9 pm and 5 am local data center time. For up to 10 minutes, the following functionality may be impacted:

- Create/delete service instance
- Update/reset ssh keys
- Start/stop service instances
- Patch service instances
- Scale existing service instances

For additional details on new features in this release, please refer to the document What's New in Oracle Public Cloud Services .



Monthly Maintenance Details

Outage Details

Start Time:
Saturday, June 4, 2016 4:00 AM CEST
Estimated End Time:
Saturday, June 4, 2016 10:00 AM CEST

Service: developer (Trial Developer Service)
Customer Account:
Data Center: US Commercial 2
Identity Domain:
Subscription ID:

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #1: Verwacht uptime wanneer jij nodig hebt

- Standaard bij en door Oracle
  - HA op VM niveau door restart of migratie op andere fysieke node
  - HA en DR op storage niveau door replicatie binnen en buiten het cluster
    - Klant blijft echter verantwoordelijk voor de eigen data
  - Dedicated CPU’s die volledig voor de client gereserveerd zijn
- High Availability en DR op applicatie- en database niveau
  - Oracle Real Application Clusters
  - Oracle DataGuard
  - Oracle Goldengate

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

DO #2

Bepaal vooraf wat je (ongeveer) nodig hebt

Not to be used in external presentations or publications

DO #2: Bepaal vooraf wat je ongeveer nodig hebt

- Cloud omgevingen zijn schaalbaar
  - Flexibel in CPU, geheugen, disk capaciteit en latency
  - Er zijn grenzen aan de schaalbaarheid
  - Leg je niet meteen vast op een langlopend contract
- Bepaal vooraf wat je nodig hebt
  - Er zijn verschillende cloud oplossingen
    - Virtual Machines
    - Exadata
  - Het kost tijd om zaken op te bouwen
    - Negativiteit bij mislukking en kosten bij (her)opbouw
    - Nieuwe contractonderhandelingen zit niemand op te wachten
    - Tegenstanders denken gelijk te krijgen

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

DO# 2: Bepaal vooraf wat je ongeveer nodig hebt

- Denk aan het volgende
  - CPU capaciteit per omgeving of per groep gebruikers
  - Disk capaciteit in MB/GB/TB
  - Throughput in MB/sec en IO/sec
  - Piek capaciteit
  - Uptime, maximum downtime en MTR
- Bepaal op basis daarvan je Cloud omgeving
  - Je bent nog wel flexibel maar kent je grenzen

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

DO #2: Bepaal vooraf wat je ongeveer nodig hebt

Service	Doelgroep
Compute Cloud (IaaS)	(Eigen) VM image waarin elk soort software kan worden geinstalleerd op basis van eigen licenties voor de gebruikte software.
Virtual Image	Voorgeinstalleerde Oracle software op een VM met volledige controle over de omgeving inclusief de Oracle licenties
Database as a Service	Voorgeinstalleerde Oracle software met database op een VM met volledige controle en Cloud tools voor patching en monitoring inclusief Oracle licenties
Exadata as a Service	Niet-gedeelde Exadata omgeving met alle beschikbare licenties compleet met Cloud tools voor patching en monitoring waarop meerdere databases kunnen draaien. Oracle verantwoordelijk voor de hardware en de software op de storage nodes.
Database Schema/PDB service	Ontwikkel en produktieplatform met eigen schema in een gedeelde database voor database en/of webbrowser gebaseerde applicaties inclusief Oracle licenties

Kijk op cloud.oracle.com/database voor meer informatie over prijzen en opties

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

DON’T #2

Neem niet aan dat je cloud provider alles oplost

Not to be used in external presentations or publications

Don’t #2: Neem niet aan dat je cloud provider alles oplost

80% van alle ongeplande outages zijn te wijten aan mensen en processen

91% van de bedrijfven hebben een ongeplande downtime gehad in de laatste 24 maanden.

65% van kleine tot middelgrote bedrijven hebben geen werkbaar IT rampenplan..

80% van de bedrijven die een zware ongeplande downtime hebben zullen volgens statistieken binnen 18 maanden failliet zijn.

De overlevingskans van bedrijven zonder rampenplan is minder dan 10%

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #2: Neem niet aan dat je cloud provider alles oplost

- Uptime van database en OS is verantwoordelijkheid gebruiker
  - Provider tracht VM of bare-metal 99.9% beschikbaarheid te geven
    - Kijk in de kleine lettertjes van de definitie van 99.9%
  - Patchen van OS en Database is verantwoordelijkheid gebruiker
    - Veel is al getest, kans op problemen is klein, maar er zijn nooit garanties
  - Verkeerde handeling kan downtime geven, oplossing geen verplichting provider
- Upgrades of Migraties is verantwoordelijkheid gebruiker
  - Migratie van 11.2 naar 12.1 (of 12.2), van VM naar Bare Metal
  - Exporteren of Backup maken van Cloud omgeving
  - Importeren of Restore doen van Cloud omgeving

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #2: Neem aan dat je cloud provider alles oplost

- Als er iets niet goed loopt
  - Zorg dat je een aanspreekpunt hebt (bij Oracle het CSI nummer)
  - Heb je zelf de kennis niet, koop deze in bij een 3e partij
  - Zorg dat je support, indien nodig, 24/7 beschikbaar is
- Documenteer wat je hebt gedaan
  - Net als bij on-premise systemen
- Eenvoudiger restore via de Cloud
  - Makkelijker een twee omgeving starten voor restore of test
  - Zorg dat de stappen of scripts hiervoor beschikbaar zijn

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Do #3

Houdt applicatie en database ‘dicht’ bij elkaar

Not to be used in external presentations or publications

Do #3: Houdt applicatie en database ‘dicht’ bij elkaar

- Meest applicaties zijn geschreven voor low latency netwerk
  - Latency aanzienlijk hoger bij applicatie en db op verschillende netwerken
  - Zeker als deze geografisch ook nog gescheiden zijn
  - Veel applicaties gebruiken meerdere calls naar DB per pagina
  - Schermen bouwen (te) langzaam of geven time-out
- Voorbeeld
  - Latency gaat van 1ms naar 200ms
  - Elke aktie naar de database is 200x langzamer
  - Bij 10 requests/pagina is elke pagina 2 seconden langzamer
  - Denk hierbij ook aan laden van data vanuit externe bron

ORACLE

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Do #3: Houdt applicatie en database ‘dicht’ bij elkaar

- Plaats DB en applicatie in hetzelfde netwerk
  - Beide in de cloud, on-premise of met verbonden met snel netwerk
  - Plan eventueel toekomstige aanpassingen aan applicatie
  - Vergelijk on-premise latency met latency tussen de cloud VMs
- Worst-case: plaats DB en applicatie in zelfde regio
  - Bij combinatie bare-metal en VM
  - Zorg voor plaatsing in hetzelfde datacenter

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #3

Geef niet iedere cloud gebruiker dezelfde rechten

Not to be used in external presentations or publications

Don’t #3: Geef niet iedere cloud gebruiker dezelfde rechten

- Cloud account geeft toegang tot belangrijke zaken
  - Starten en stoppen bestaande omgevingen
  - Verwijderen bestaande omgevingen
- Sommige ‘Cloud’ acties hebben gevolg voor de instance
  - Veranderen resources kan een reboot tot gevolg hebben
  - Data kan verdwijnen
- Hackers hebben ook interesse voor de Cloud
  - Opstarten botservers, spamsystemen etc

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #3: Geef niet iedere cloud gebruiker dezelfde rechten

- Zorg voor duidelijke administratie
  - Wie heeft welke rechten
  - Laat iedereen aanloggen met zijn eigen account
  - Welke kosten doorberekenen naar welke klant/afdeling
  - Bepaal procedures voor opwaarderen
- Rechten kunnen gescheiden worden
  - Aanmaken / verwijderen VMs voor database of applicaties
  - Beheren backups
  - Aankopen doen uit marketplace of stores

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Do #4

Optimaliseer de applicatie voor Cloud mogelijkheden

Not to be used in external presentations or publications

Do #4: Optimaliseer applicatie voor Cloud mogelijkheden

- Cloud is flexibel
  - Scale up en Scale out van systemen
  - Snel vergelijkbare (golden) images starten
  - Verplaatsen van omgevingen van cloud naar on-premise
- Cloud heeft ook beperkingen
  - Snelheid disk en storage
  - Latency tussen netwerken

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Do #4: Optimaliseer applicatie voor Cloud mogelijkheden

- Applicaties kunnen ‘Cloud Optimized’ worden
  - Gebruik van meerdere applicatie instances of database instances
  - Groepen van statements in plaats van afzonderlijke statements
  - Buffering / Caching van informatie op applicatie niveau
- Gebruik de kracht van de Cloud
  - Scale out op basis van database of applicaties
  - Read-only systemen vs Read-Write systemen
  - Tijdelijke systemen waar dan ook ter wereld

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #4

Denk niet dat er slechts 1 cloud bestaat

Not to be used in external presentations or publications

Don’t #4: Denk niet dat er slechts 1 Cloud bestaat

- Er zijn meerdere Cloud providers
  - Ze doen veel hetzelfde
  - Er zijn ook veel verschillen
  - Diverse opties ‘binnen’ een Cloud provider
  - Daardoor verschillende prijzen
- Oracle Database Cloud heeft verschillende opties
  - Virtual Machines met diverse licentie opties
  - Bare metal systemen met diverse licentie opties
  - Engineered systems (met 1 licentie optie, namelijk alles)
  - On-site of echt ‘in the Cloud’

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Don’t #4: Denk niet dat er slechts 1 Cloud bestaat

- Ga zorgvuldig na wat er nodig is (Do #2)
  - Bepaal daarna welke opties welke leveranciers hebben
  - Reken alle opties (die technisch haalbaar zijn) door
- Voorbeeld
  - Klant wil omgeving ‘in de Cloud’
  - Klant wilde alleen POC doen met VM op basis van prijs
    - POC eisen waren relatief hoog (meer dan 16 OCPU, storage meer dan 20TB etc)
    - Totaalprijs vs performance was niet acceptabel
    - Nieuwe berekening op basis van Exadata in de Cloud
    - Prijs 40% lager en performance vele malen beter

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Questions

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications

Integrated Cloud

Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. | Not to be used in external presentations or publications


ORACLE®