



Franz Hüll  
DOAG-Vorstand und  
Leiter Competence Center  
Securityfragen

Liebe Mitglieder der DOAG,  
liebe Leserinnen und Leser,

das Thema „Security“ erzeugt stets Aufmerksamkeit, es wird immer gerne und viel – häufig auch sehr kontrovers – diskutiert. Auf der einen Seite stehen die Anbieter von Dienstleistungen, Schulungen, Produkten und Lösungen rund um die IT-Security. Hier findet man häufig eine gewisse Neigung zur Schwarzmalerei. Auf der anderen Seite stehen Unternehmen, die über Notwendigkeit, Kosten und Nutzen von Security-Projekten zum Teil sehr heftig debattieren. Soweit gesetzliche Vorschriften einzuhalten sind, gibt es wenig Spielraum, ein gefordertes Mindestmaß an Sicherheit zu implementieren. Hier muss letztendlich jedes Unternehmen für sich die richtigen Antworten finden. Es liegt auf der Hand, dass der Nutzen von mehr Sicherheit nicht immer auf Euro und Cent nachweisbar ist, dies macht die Entscheidung aber nicht leichter. Wenn es gelungen ist, mit wirtschaftlich vertretbarem Aufwand ein für das Unternehmen festgelegtes Sicherheitsniveau zu erreichen, hat man alles richtig gemacht und das Ziel ist erreicht. Der Vorgang ist damit jedoch nicht beendet. Security ist ein andauernder Prozess, der aufgrund von Veränderungen des geschäftlichen und gesetzlichen Umfelds sowie wegen des Auftretens neuer Risiken und Gefahren immer wieder auf dem Prüfstand stehen muss. Wir möchten Ihnen mit dieser Ausgabe der DOAG News wichtige Informationen und Anregungen auf den Weg geben. Sie lesen hier ein Interview mit dem Chief Information Security Officer der Linde AG, Dr. Andrzej Debski. Er gibt Auskunft über seine Sichtweise von IT-Security in einem weltweit tätigen Unternehmen und spricht über seine Motivation und Vorgehensweise, um erfolgreich für das erforderliche Maß an Sicherheit im Unternehmen zu sorgen. Dieses Interview ist das erste einer geplanten Reihe, in der mit jeder Ausgabe der DOAG News eine Persönlichkeit aus dem IT-Management zu aktuellen Fragen Stellung nehmen wird.

Ich wünsche Ihnen eine optimale Sicherheit bei Ihren Projekten und viel Spaß beim Lesen.

Ihr

F. Hüll



**Schneller, höher, sicherer: Remote Administration Service (RAS)  
von Hunkler – der effizienteste Fitness-Check für Oracle**

**ORACLE** Platinum  
Partner

- Optimale Konfiguration Ihrer Oracle-Datenbanken
- Fernüberwachung der Performance
- Früherkennung und Behebung von Fehlerquellen und Systemstörungen
- Zugang über VPN
- Telefonischer Support
- Individuell gestalteter Leistungsumfang

Best Solutions Based on Oracle  
**HUNKLER**  
GmbH & Co. KG

Hauptsitz Karlsruhe  
Geschäftsstelle Bodensee

Bannwaldallee 32  
Fritz-Reichle-Ring 2

76185 Karlsruhe  
78315 Radolfzell

Tel. 0721-490 16-0  
Tel. 07732-939 14-00

Fax 0721-490 16-29  
Fax 07732-939 14-04

info@hunkler.de  
[www.hunkler.de](http://www.hunkler.de)

**Aus der DOAG**

- 3 Editorial
- 5 Spotlight
- 6 Die DOAG in der Presse
- 8 „Sicherheit ist immer ein Balanceakt ...“  
Interview mit Dr. Andrzej Debski
- 30 Die Übernahmen von Oracle seit 2005

**Security**

- 12 Was ist (Datenbank-)Sicherheit?  
*Franz Hüll*
- 16 Kundendaten im Supersonderangebot  
oder wie man Datenbanken heute  
absichern kann  
*Caroline Kohn*
- 19 Sicherheit in Apex-Anwendungen –  
von der Tabelle bis zur Oberfläche  
*Carsten Czarski*
- 23 Kerberos im Einsatz mit Oracle:  
Starke und existente Windows-  
Authentisierung nutzen  
*Suvad Sahovic und Carsten Müztlitz*
- 28 Wo sind unsere Schlüssel?  
*Christian Kirsch*
- 31 Oracle und die Compliance  
gemäß ISO 27001  
*Dr. Thomas Störckuhl und Hans Wagner*

**Fusion Middleware**

- 36 Von der Geschäftsprozess-Analyse  
zur Prozess-Ausführung  
*Evgenia Rosa*
- 39 Oracle Virtual Assembly Builder  
*Marcus Schröder*
- 42 Neu: Oracle BPM Suite 11g  
*Gert Schübler*

**Datenbank**

- 46 Virtualisierung 2.0 mit Oracle VM  
*Björn Bröhl*
- 50 Das Business ist nicht nur online –  
Erfahrungen mit der Oracle Database  
Lite im Außendienst  
*Volker Ricke*

- 54 2 RAC or not 2 RAC?  
*Rainier Kaczmarczyk*
- 56 Oracle meets MS SQL Server –  
Zugriff von Oracle auf das Fremdsystem  
*Vladimir Poliakov*

**Best Practice**

- 15 Compliance-Fragen aus dem Alltag  
eines Lizenzberaters  
*Christian Grave*
- 58 Eine Oracle Konzern-Lizenz –  
Fluch oder Segen?  
*Christian Grave*

**Entwicklung**

- 61 Oracle Web-Portale barrierefrei  
anpassen: <https://recht.nrw.de>  
*Frank Christian Hoffmann*
- 64 Datengetriebene Applikationen  
*Hans Niedermeier*

**Tipps & Tricks**

- 70 Heute: Tipps zur IDE  
*Gerd Volberg*

**Buchrezension**

- 55 Oracle 11g – das umfassende Handbuch  
gelesen von *Björn Bröhl*
- 63 Oracle Survival Guide  
gelesen von *Björn Bröhl*
- 72 Oracle Forensics Oracle Security  
Best Practices  
gelesen von *Franz Hüll*

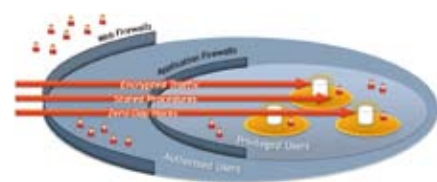
**Aus der DOAG**

- 74 Neuigkeiten aus dem Verein
- 44 Impressum
- 80 Inserentenverzeichnis
- 81 Wir begrüßen unsere neuen Mitglieder
- 82 DOAG Termine



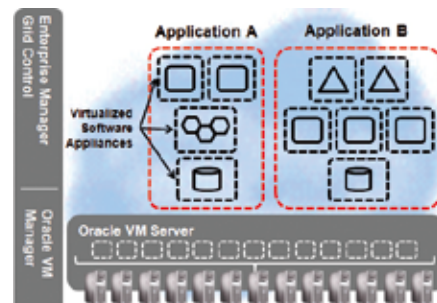
„Sicherheit ist immer ein Balanceakt ...“  
Interview mit Dr. Andrzej Debski, Chief  
Information Security Officer (CISO) der  
Linde AG

Seite 8



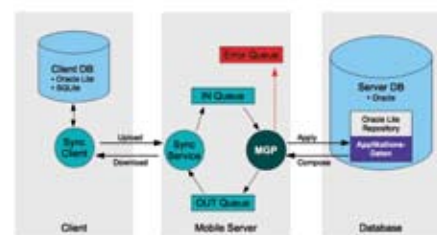
Kundendaten im Supersonderangebot  
Softwarebasierte Security Software ist in der  
Lage, auch privilegierte User zu kontrollieren  
und auf Zero-Day-Angriffe in Echtzeit  
zu reagieren

Seite 16



Virtualisierung 2.0 mit Oracle VM  
Server-Virtualisierung ist nach wie vor eines  
der wichtigsten aktuellen IT-Themen

Seite 46



Oracle Database Lite im Außendienst  
Erfahrungen beim Austausch von Informa-  
tionen zwischen einer Oracle Datenbank  
und mobilen Endgeräten

Seite 50



## Spotlight

### Sonntag, 18. April 2010

*Die Collaborate 2010, das „Technology and Applications Forum for the Oracle Community“, findet in Las Vegas (USA) statt. Aufgrund des Flugverbots wegen der Vulkanasche konnte die Delegation der DOAG in diesem Jahr leider nicht teilnehmen.*

### Dienstag, 27. April 2010

*Unter den 21 Teilnehmern am Customer Support Day in München sind gerade mal zehn Kunden. Die früher gut besuchte Veranstaltung – zum ersten Mal von Oracle UK organisiert – war schlecht kommuniziert worden.*

### Donnerstag, 29. April 2010

*Die Gründungsveranstaltung der Special Interest Group Java ist ein großer Erfolg. Das Thema „Rapid Application Development mit Java“ kam bei den mehr als 50 Teilnehmern sehr gut an. Die DOAG fühlt sich in der Gründung der eigenen SIG Java bestätigt. SIG-Leiter Andreas Badelt plant bereits das nächste Treffen am 9. September 2010 in München, bei dem die Java Enterprise Edition (JEE) 6 im Mittelpunkt steht.*

### Dienstag, 11. Mai 2010

*Die Fachkonferenz „DOAG ITIL & Betrieb 2010“ ist leider nicht so gut besucht wie im Vorjahr. Dennoch profitieren die Teilnehmer vom Erfahrungsaustausch mit Kollegen und Experten.*

### Montag, 17. Mai 2010

*Beim Berliner Expertenseminar zum Thema „Fortgeschrittene Performance-Diagnose und Optimierung mit extended SQL Trace Profiling“ ist das Feedback der Teilnehmer wieder durchweg positiv. Am Abend des ersten Tages konnten sich Teilnehmer und der Referent in ungezwungener Atmosphäre kennenlernen: Gemeinsam ging es ins Madame Tussauds Wachsfigurenkabinett.*

### Freitag, 28. Mai 2010

*Ein kleiner Kreis aus DOAG-Vorständen und Beiräten legt die Strategie für die Zielgruppe „Business Applications“ neu fest, um die Anwender der Business-Lösungen gezielter ansprechen zu können.*

### Freitag, 18. Juni 2010

*DOAG-Geschäftsführer Fried Saacke vereinbart eine enge Zusammenarbeit mit der Hamburger Logistik-Initiative hinsichtlich der Fachkonferenz „Logistik & SCM“.*

### Donnerstag, 1. Juli 2010

*Die DOAG stellt gemeinsam mit dem Interessenverbund der Java User Groups e.V. (iJUG) beim 13. Java Forum Stuttgart die Aktivitäten der beiden Vereine vor.*

### Montag 12. Juli 2010

*Der DOAG-Vorstandsvorsitzende Dr. Dietmar Neugebauer und DOAG-Geschäftsführer Fried Saacke treffen sich mit Jürgen Kunz, Geschäftsführer der ORACLE Deutschland B.V. & Co. KG, und Claus-Peter Unterberger, Senior Vice President Marketing Europe, Middle East & Africa, um über die Verbesserung der Zusammenarbeit im Bereich „Business Applications“ zu sprechen.*

### Freitag, 16. Juli 2010

*Die Vorstandssitzung beschließt gemeinsam mit den Streamverantwortlichen das bisher umfangreichste Vortragsprogramm für die DOAG 2010 Konferenz. Von 16. bis 18. November 2010 stehen rund 400 Vorträge auf dem Programm.*

### Donnerstag, 22. Juli 2010

*Der Arbeitskreis IT stellt die Weichen für den zukünftigen Web-Auftritt der DOAG.*



## Die DOAG in der Presse

Die nachfolgenden Ausschnitte reflektieren die Einschätzung der Fach- und Wirtschaftspresse zu bestimmten Themen über Oracle; die Veröffentlichungen geben nicht die Meinung der DOAG wieder und sind auch nicht im Vorfeld mit der DOAG abgestimmt. Lediglich die Zitate einzelner DOAG-Vorstände geben die Meinung der DOAG wieder.

### Computerwoche vom 2. August 2010

#### Sorgen um Pflege und Support

ERP-Kunden, egal von welchem Anbieter, geht es in erster Linie darum, dass die bestehenden Geschäftsanwendungen laufen und gepflegt werden. Beispielsweise sorgen sich die Nutzer von Oracles Business-Applikationen, dass der Hersteller das Interesse verlieren könnte, bestimmte Produkte für den deutschen Markt zu unterstützen, weil die installierte Basis zu klein ist, berichtet Fried Saacke, Geschäftsführer der Deutschen Oracle Anwendergruppe (DOAG). Das müsse nicht zwangsläufig bedeuten, dass Oracle Produkte einstellt. Es könne jedoch sein, dass der Softwarehersteller die Unterstützung einzelner Produkte etwas zurückfahre. „Es gibt zwar noch keine konkreten Signale, aber die Sorge ist einfach da.“

Daran ändert auch Oracles Versprechen nichts, im Rahmen des „Applications-Unlimited“-Programms alle Produktlinien unbegrenzt weiterzuentwickeln und zu pflegen. Der Konzern hatte in den zurückliegenden Jahren zahlreiche Softwareanbieter übernommen und in der Folge sein Supportversprechen gegeben, um verunsicherte

Anwender der akquirierten Produktlinien zu beruhigen und zu halten. Saacke zufolge stellt sich jedoch die Frage, wie Oracle diese Zusage interpretiert. „Weltweit mag der Support da sein. Das garantiert mir als Kunde jedoch noch lange nicht, dass alle Anforderungen bezüglich des deutschen Marktes auch erfüllt werden.“

Zumal es durchaus Zeichen gibt, dass das Applications-Unlimited-Programm aufgeweicht werden könnte. Sprachen die Oracle-Verantwortlichen in den vergangenen Jahren immer von einer zeitlich nicht befristeten Initiative, nannte Konzernchef Lawrence Ellison in seiner Keynote zur Kundenkonferenz Open World im Herbst vergangenen Jahres erstmals ein Zeitlimit. Die betroffenen Anwendungen würden mindestens zehn Jahre unterstützt. „Wer genau hinhört, hat hier feststellen können, dass sich die Wortwahl ändert“, meint Saacke. Erstmals gab Oracle eine Jahreszahl und damit eine Einschränkung an. „Vielleicht fällt bei der nächsten Open World das „mindestens“ weg“, unkt der Anwendervertreter.

Saacke würde sich nach eigenem Bekunden nicht wundern, wenn Oracle versuche, das Programm einzuschränken. Ein Unternehmen, das eine ope-

rativen Marge von 50 Prozent anstrebe, werde immer darauf achten, an welcher Stelle sich das Portfolio straffen lasse. Es sei nicht rentabel, ein Produkt für eine geringe Zahl von Kunden anzupassen. „Da schwindet sicher die Motivation des Herstellers.“

Was die Entwicklungspläne ihres Lieferanten angeht, sind Oracle-Kunden weniger interessiert. Das Management hatte bereits vor Jahren unter dem Namen „Fusion“ eine komplett neue Suite an Business-Applikationen angekündigt. Darin sollten die besten Funktionen der eigenen E-Business-Suite sowie der zugekauften Softwarepakete wie beispielsweise Peoplesoft, J.D. Edwards und Siebel zu einem neuen ERP-Paket „fusioniert“ werden. Ursprünglich wollte der US-Konzern bereits 2008 mit den Fusion Applications starten. Doch bis auf einzelne Softwaremodule für das Kunden-Management ist bis heute wenig davon im Markt zu sehen.

„Oracle hat sich sicher keinen Gefallen getan, Fusion groß anzukündigen, dann aber nicht zu liefern“, sagt Anwendervertreter Saacke. Die Verzögerung sei den Kunden aber gar nicht unrecht: „Fusion ist für Oracle wichtig, aber nicht für die Anwender.“ Zwar sei wenig transparent, was im Umfeld von

Fusion geschehe und wo es hier hingehe, aber das sei für die Kunden auch nicht entscheidend.

Kein Anwender wolle gezwungen werden, auf eine neue Produktlinie zu wechseln, stellt Saacke klar. Entgegen allen Ankündigungen von Oracle werde der Umstieg auf Fusion aus Sicht der Anwender wohl einen Wechsel auf ein völlig neues Produkt bedeuten. Das sei für die Anwenderunternehmen jedoch immer mit erheblichen Aufwänden und Kosten verbunden. Wenn die Fusion Applications auf den Markt kommen, werden sich die Kunden das System ansehen und überlegen, ob sie wechseln sollen, prognostiziert der DOAG-Geschäftsführer. Momentan warte aber niemand auf die Software.

#### Database pro vom 10. Mai 2010

##### DOAG-Expertenseminare mit bekannten Experten bewähren sich

Die DOAG Deutsche ORACLE-Anwendergruppe e.V. bietet zusammen mit ausgewählten Schulungspartnern spezielle Seminare an. Bei den Seminaren handelt es sich nicht um Grundlagen-Schulungen. Sie richten sich vielmehr als Ergänzung zu den Schulungsangeboten der Oracle-Partner an erfahrene Oracle-Anwender, die ihr Wissen vertiefen möchten. „Die Seminare werden in der Regel von sehr erfahrenen, namhaften Dozenten gehalten“, erläutert DOAG-Geschäftsführer Fried Saacke das Konzept. Einer dieser Experten war Steven Feuerstein, PL/SQL-Evangelist und Autor zahlreicher PL/SQL-Bücher, der im März zum Thema „Best of Oracle PL/SQL“ referierte.

„Insgesamt herrschte im Seminar eine sehr offene Atmosphäre, es gab viele Diskussionen und Meinungsbeiträge, und es war letztendlich nicht nur ein Seminar, sondern gleichzeitig ein Erfahrungsaustausch“, so Saacke. Im Rahmen der bei Expertenseminaren obligatorischen gemeinsamen Abendveranstaltung stand das Networking im Vordergrund. Bei einem Essen im Restaurant der Berliner Reichstagskuppel konnten die Teilnehmer in entspannter Atmosphäre ihre Diskussionen fortsetzen.

#### Database pro vom 10. Mai 2010

##### SAP unterstützt immer mehr neue Funktionen in Oracle 11g R2

Die jüngste Version 11g R2 der Oracle-Datenbank, die Ende 2009 verfügbar wurde, wird für SAP-Anwender zunehmend interessanter. SAP bemüht sich intensiv darum, die neuen Funktionen der Datenbank mit seinen Tools zu unterstützen.

Dieser Übergangsprozess ist noch nicht abgeschlossen, so dass noch Wünsche offen bleiben. Dieses Bild ergab sich bei einer Tagung der Special Interest Group Oracle & SAP der Deutschen-Oracle-Anwender-Gruppe (DOAG), die am 3. Mai in St. Leon/Rot stattfand.

Die rund hundert Teilnehmer erhielten viele Informationen, die sie hoffen ließen, in ihrem jeweiligen Unternehmen Probleme leichter zu bewältigen. So lässt sich mit Oracle 11gR2 die Daten- und Tabellenkompression stark erhöhen, bis sie das 6,2-Fache gegenüber herkömmlichen Verfahren beträgt. Das spart Plattenplatz.

Die neue Verschlüsselungsfunktion Transparent Data Encryption wird seit dem 3. Mai von SAP vollständig unterstützt.

SAP erweitert sukzessive die Möglichkeiten seiner BR\* Tools für Backup & Recovery mit Oracle 11gR2. Der Referent gab konkrete Empfehlungen, welche Version der BR\* Tools mit welcher Oracle-Version am besten zusammenarbeitet. Um die neuesten Funktionen nutzen zu können, sollte der Anwender mit der BR-Version 7.2 arbeiten.

Das Patching ist ein leidiges, aber notwendiges Kapitel in jeder SAP-Oracle-Installation. Hier zeichnen sich endlich große Erleichterungen ab. Sie können nicht nur Offline-Patches einspielen, sondern diese ab Oracle 11gR2 auch mit Online-Patches kombinieren. Solche Combo-Patches lassen sich künftig selektiv einspielen. Es gibt nur zwei Unix-Plattformen, die von dieser Patch-Technik nicht profitieren: HP UX und AIX 5.

#### silicon.de vom 1. April 2010

##### Oracle-Anwender fordern Klarheit beim neuen Support

Kommentare des Herstellers zu dieser weitreichenden Neuerung gibt es bislang nicht. Dafür steigen die Anwender jetzt auf die Barrikaden und fordern Transparenz und Klarheit. Denn nach wie vor gibt es viele zahlreiche offene Fragen, wie zum Beispiel, inwieweit diese Regelung für Sun-Bestandskunden gilt.

„Aufgrund von Anfragen seitens der Anwender hat die DOAG von einer neuen Support-Regelung bei Oracle erfahren“, teilt die Deutsche Oracle-Anwendervereinigung mit. Der Hersteller hat also weder die Presse noch die Anwendervereinigungen aktiv über die neue Regelung, die seit dem 16. März gilt, informiert.

In Deutschland berichtete silicon.de als erstes Medium über die neue Policy, in der der Software-Support mehr oder weniger vom Hardware-Support abhängig gemacht wird. Unterhält ein Anwender Systeme, die nicht von Oracle – aus welchem Grund auch immer – supportet werden, habe der Anwender auch keinen Anspruch auf Software-Support.

Nun bemühe sich die DOAG „um Transparenz, da der Hersteller bisher keine klare Aussage dazu gemacht hat“, heißt es. Auch gegenüber der Presse hat sich Oracle bislang noch nicht dazu geäußert. Ein Sprecher bestätigte jedoch, dass die Regelung tatsächlich gelte.

„Die DOAG steht grundsätzlich der Festschreibung eines einheitlichen Supportlevels bei Hard- und Softwareprodukten kritisch gegenüber“, so Dr. Dietmar Neugebauer, Vorstandsvorsitzender der DOAG. „Von daher halten wir es für wichtig, hier eine klare Antwort von Oracle zu erhalten.“

Weitere Pressestimmen zur DOAG finden Sie unter <http://www.doag.org/presse/spiegel>



*Dr. Andrzej Debski (links) im Gespräch mit Franz Hüll*

## „Sicherheit ist immer ein Balanceakt ...“

**Dr. Andrzej Debski, Chief Information Security Officer (CISO) der Linde AG, interpretiert im Interview mit Franz Hüll, DOAG-Vorstand und Leiter des Competence Centers Securityfragen, sowie mit Wolfgang Taschner, Chefredakteur der DOAG News, das aktuelle Thema „Security im Unternehmen“. Ein Teil der Fragen stammt von einigen DOAG-Aktiven.**

*Was sind Ihre Aufgaben bei der Linde AG?*

**Dr. Debski:** Ich bin seit siebeneinhalb Jahren der Chief Information Security Officer im Unternehmen. Meine primäre Aufgabe besteht in der Etablierung und Perfektionierung eines ganzheitlichen Sicherheitsprozesses, was sowohl organisatorische als auch technische Maßnahmen beinhaltet. Diese anspruchsvolle Aufgabe wird von einem Team engagierter Mitarbeiter getragen. Auf der organisatorischen Seite beschäftige ich mich mit der Definition von sicherheitsrelevanten Rollen und Verantwortlichkeiten sowie der Erarbeitung von Linde-internen Sicherheitsregeln. Wir achten sehr auf den Aufbau und die Aufrechterhaltung eines mehrschichtigen Schutzes für Daten, Anwendungen, Systeme und Netze, der sowohl unseren Business-Anforderungen genügt als

auch mit den relevanten Compliance-Anforderungen übereinstimmt. Wir verifizieren die Sicherheitsmaßnahmen oft und fragen uns kritisch, ob das vorhandene Schutzniveau sowohl der allgemeinen technologischen IT-Entwicklung – insbesondere auf dem Gebiet der Informationssicherheit – als auch der sich ständig ändernden Bedrohungslage angepasst ist.

*Was hat sich in diesen siebeneinhalb Jahren alles getan?*

**Dr. Debski:** Linde ist ein seit mehr als hundertdreißig Jahren agierendes Unternehmen. Damit habe ich auch traditionell gewachsene Strukturen und Plattformen vorgefunden. Die letzte Dekade war sehr stark geprägt durch signifikante Ausrichtungsveränderungen des Konzerns wie Verkäufe eigener Sparten und Zukäufe anderer Unternehmen. Es

war nicht immer eine triviale Aufgabe, die unterschiedlichen Systeme zu konsolidieren und zugleich eine hohe Sicherheit zu gewährleisten. Trotz all dieser Herausforderungen sind wir heute besser aufgestellt als vor knapp acht Jahren – allerdings ist viel zu tun.

*Gibt es aus Ihrer Sicht ein Patentrezept, um globale Sicherheit in einem Unternehmen einzuführen?*

**Dr. Debski:** Es gibt kein Patentrezept; Sicherheit ist für mich ein dynamisches Gebilde, das sehr stark durch die technologische Entwicklung auf dem Gebiet der Informationssicherheit geprägt ist. Natürlich existieren konkrete Richtlinien, Common Practices und Standards, an denen wir uns orientieren – aber man darf dabei die lokalen Gegebenheiten nie aus den Augen verlieren.

*Wo sollte der Bereich „Sicherheit“ organisatorisch im Unternehmen angesiedelt sein?*

**Dr. Debski:** Ich glaube, das hängt sehr stark von der Art des Unternehmens ab. Hier bei Linde liegt der Bereich innerhalb der IT und besitzt Schnittstellen zu den Ressorts „Internal Audit“ und „Compliance“.

*Kann man Aufwand und Kosten für die Sicherheit im Verhältnis zum Nutzen noch im Rahmen halten oder sucht man Sicherheit um jeden Preis?*

**Dr. Debski:** Wir haben eine dokumentierte Sicherheitsstrategie und eine dazu passende Sicherheits-Policy. Darin ist unter anderem eine sogenannte „Balance-Position“ festgeschrieben, also keine Sicherheit um jeden Preis. Das wäre oft technisch und vor allem aus wirtschaftlichen Gründen nicht sinnvoll. Wir versuchen demnach immer einen pragmatischen Weg zu finden, um technische Realisierungsoptionen, finanzielle Machbarkeit und die menschliche Vernunft unter einen Hut zu bringen. Wir sind dabei immer bestrebt, jedes signifikante Sicherheitsrisiko zu minimieren. Wenn man genauer den Zusammenhang zwischen Sicherheitsniveau und Kosten betrachtet, sieht man, dass die Zuwächse an Sicherheit am oberen Ende auch überproportional viel kosten. Unser Ziel ist es, unter Berücksichtigung von verfügbaren Ressourcen wie Manpower, Zeit und Budget eine möglichst effektive Sicherheitslösung zu gestalten.

*Erfahrungsgemäß sind die Sicherheitsmaßnahmen in großen Unternehmen wie Linde aufwändiger als im Mittelstand. Wo soll nach Ihrer Meinung ein mittelständisches Unternehmen mit der Sicherheit anfangen?*

**Dr. Debski:** Ich vergleiche die Sicherheit gerne mit dem Bau eines Hauses. Von daher muss man immer zuerst mit dem Fundament beginnen. Das sind im übertragenen Sinne der Basisschutz und die elementaren Hauptsicherungen im Unternehmen. Wenn diese Plattform solide ausgeführt ist, kann

man sich Schritt für Schritt den einzelnen Ebenen widmen.

*Jede Sicherheitsmaßnahme behindert meist in irgendeiner Form den operativen Betrieb. Wie stellen Sie sicher, dass die beschlossenen Vorhaben auch in den Fachabteilungen umgesetzt werden?*

**Dr. Debski:** Das beginnt meist mit einer Diskussion über die Frage nach dem Nutzen der einzuführenden Sicherheitsmaßnahme. Hier gibt es oft keine eindeutigen Antworten, denn Sicherheit ist in erster Näherung mit einer klassischen Versicherung vergleichbar. Man bezahlt und hofft, dass nie etwas passiert. Sollte der Schadensfall dennoch eintreten, steht man nicht im Regen. Es ist nicht immer leicht, die richtigen Argumente zu finden, um den notwendigen Rückhalt für bestimmte Sicherheitsmaßnahmen zu bekommen.

*Wie steht es um die persönliche Verantwortung und das Haftungsrisiko des Unternehmens?*

**Dr. Debski:** Die persönliche Haftung ist durch legislative Vorgaben wie das KonTraG-Gesetz, das Aktiengesetz oder das Bundesdatenschutzgesetz bestimmt. Nach meinem Verständnis muss man allerdings unterscheiden, ob eine grobe Fahrlässigkeit vorliegt oder ob es zum Beispiel um Unzulänglichkeiten im Bereich der Technik geht. Wir nehmen die persönliche Verantwortung ernst und unternehmen alles technisch und organisatorisch Machbare, um unsere Pflichten zu erfüllen.

*Worin sehen Sie die größte Herausforderung bei der Umsetzung einer unternehmensweiten Security-Policy?*

**Dr. Debski:** Ich meine, das Schwierigste ist eine zügige Implementierung der Projekte und deren reibungslose und störungsfreie Integration in bestehende Umgebungen. Auf dem Papier kann man relativ viel spezifizieren, aber die wahren Herausforderungen beginnen fast immer bei der Umsetzung. Man muss oft in bestehende Prozesse und Systeme eingreifen, und wenn diese

zum Beispiel in Industrieanlagen rund um die Uhr im Einsatz sind, wird es richtig schwierig. Architektur-Änderungen, Hardware- oder Software-Aktualisierungen und andere Eingriffe sind dann nicht ohne Weiteres möglich. Darüber hinaus spielt der Faktor „Mensch“ eine nicht zu unterschätzende Rolle bei der Umsetzung einer unternehmensweiten Sicherheits-Policy. Dabei sind unterschiedliche Sprachen, Kulturen und Einstellungen zum Thema „Sicherheit“ zu beachten. Nicht jeder ist ein Sicherheitsfanatiker und nicht jeder will die Sicherheit unbedingt sehen, haben oder verstehen.

*Sehen Sie gesetzliche Regelungen wie Compliance als treibenden Faktor, um die Bemühungen um die IT-Sicherheit zu erhöhen?*

**Dr. Debski:** Hier hat sich tatsächlich in den letzten Jahren einiges geändert. Die gesetzlichen Vorgaben sind deutlich in den Vordergrund getreten. Allerdings herrscht noch eine gewisse Unschärfe, wenn es darum geht, konkrete technische oder organisatorische Maßnahmen zu definieren. Das Bundesdatenschutzgesetz verwendet beispielsweise in Paragraph neun folgende Formulierung: „... haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten ...“. Ich glaube, hier ist noch viel Diskussionsbedarf darüber, was wirklich zählt und was notwendig ist.

*Wer fällt in einem solchen Fall letztendlich die Entscheidung?*

**Dr. Debski:** Die treffen wir immer im Team.

*Wie wichtig ist die Rückendeckung durch die Geschäftsleitung bei der Umsetzung von Sicherheitsmaßnahmen?*

**Dr. Debski:** Das ist für mich eine der wichtigsten Grundvoraussetzungen. Paradoxerweise, so lange alles gut läuft, lässt die Sensibilität für dieses Thema

nach. Die sporadischen Sicherheitsvorfälle, mit denen wir zu tun haben, lassen allerdings das erforderliche Bewusstsein wieder einkehren. Es ist wie eine Art sinusförmige Welle, bei der die Unterstützung manchmal nachlässt und manchmal intensiviert wird. Ein gewisses konstantes Niveau an Unterstützung ist allerdings immer sinnvoll und auch notwendig.

*Wie macht man Security heute unternehmensübergreifend und interoperabel, wenn beispielsweise SOA-Plattformen verschiedener Hersteller im Einsatz sind?*

**Dr. Debski:** Wir setzen hier sehr stark auf einen Konsens der beteiligten Unternehmenseinheiten und Teams und versuchen anschließend, alle Beteiligten vom Sinn und Zweck der geplanten Maßnahmen zu überzeugen. Das kostet zwar meist viel Zeit, dafür stehen aber danach alle dahinter.

*Welche Rolle spielt der menschliche Faktor in den Überlegungen zur IT-Sicherheit?*

**Dr. Debski:** Ich bin überzeugt, der Mensch ist nach wie vor das entscheidende Element im Sicherheitsumfeld. Das gilt sowohl im positiven als auch im negativen Sinn. Eine dedizierte Firewall für Netzwerke, Web-Anwendungen oder Datenbanken wird bei-

spielsweise nur dann zu einer wertvollen Schutzeinrichtung, wenn sie zuvor durch die menschliche Intelligenz optimal konfiguriert und anschließend sorgfältig gepflegt wird. Auf der anderen Seite verursachen die menschliche Nachlässigkeit oder im Extremfall die Ignoranz oder Böswilligkeit die größten Probleme bei der Sicherheit.

*Wie lässt sich Sicherheit messen?*

**Dr. Debski:** Wir gewinnen entsprechende Indikatoren wie „gut“, „mäßig“ oder „schlecht“ durch den Einsatz unterschiedlicher Methoden und Tools, zum Beispiel durch eine Reihe von Schwachstellen-Analysen oder in Form von internen oder externen Audits. Ich glaube, eine solide und objektive Messbarkeit der Sicherheit bleibt nach wie vor eine Herausforderung für die Sicherheitsindustrie und viele Unternehmen, darunter auch für die Linde AG.

*Zu viele Sicherheitsmaßnahmen führen zu Misstrauen der Mitarbeiter gegenüber dem Unternehmen. Wie gehen Sie damit um?*

**Dr. Debski:** Es gibt Fälle, in denen die Überzeugungsarbeit für eine bestimmte Maßnahme lange dauert. Der Betriebsrat ist dabei mit eingebunden, insbesondere wenn es um die Persönlichkeitsrechte der Mitarbeiter geht.

*Sicherheit ist immer eine Reaktion auf Bedrohungen. Wird nach Ihrer Ansicht die Lücke zwischen Bedrohungen und Schutzmaßnahmen kleiner oder größer?*

**Dr. Debski:** Ich sehe hier nach wie vor einen Balanceakt zwischen Bedrohung und Bedrohungsschutz und erwarte zukünftig keine gravierenden Änderungen. Es wird sicher immer wieder neue Arten von Bedrohungen geben, aber die Leute, die sich mit Sicherheitsmaßnahmen beschäftigen, werden darauf eine entsprechende Antwort finden. Das hat sich bereits in der Vergangenheit oft gezeigt, wobei das Niveau auf beiden Seiten auch künftig weiter steigen wird.

*Welchen Ausbildungsweg empfehlen Sie beziehungsweise welche Voraussetzungen*

*muss jemand mitbringen, der in der IT-Security an verantwortlicher Stelle tätig sein will?*

**Dr. Debski:** Sicherheit erfordert in der Regel umfangreiches und tiefgehendes Wissen, insbesondere wenn es um die technische Ebene geht. Das kostet logischerweise Zeit und Aufwand. Eine solide Grundausbildung ist Voraussetzung, doch die praktischen Erfahrungen sind ebenfalls unerlässlich.

*Sehen Sie den Sicherheitsverantwortlichen eher als Generalist oder als Spezialist?*

**Dr. Debski:** Ich glaube, dass ein Sicherheitsexperte in einem global agierenden Unternehmen wie der Linde AG eine fundierte technische Ausbildung benötigt, damit er weiß, worüber er entscheidet. Darüber hinaus benötigt er Erfahrungen in den Bereichen „IT-Recht“, „Management“ und „Mitarbeiter-Motivation“.

*Welchen Fehler sollte ein Sicherheitsverantwortlicher auf keinen Fall machen, welche Aktivitäten muss er hingegen unbedingt entwickeln?*

**Dr. Debski:** Wer in dieser Position versucht, es allen recht zu machen, wird irgendwann in eine Konfliktsituation geraten. Es ist unerlässlich, einen langfristigen Plan zu haben und ihn konsequent zu verfolgen, was nicht immer einfach ist, etwa bei sich ändernden Geschäftsstrategien, neuen Organisationsformen, finanziellen Engpässen oder neuen Mitarbeitern. Diesen Plan soll man stets mit eigenen persönlichen Erfahrungen bereichern und auch die Erfahrungen und Best Practices der Sicherheits-Community im Auge behalten. Hinzu kommt eine große Ausdauer darin, Menschen zu überzeugen. Sicherheit besteht im realen Leben aus einer langen Kette vieler kleiner und unspektakulärer Aufgaben; wichtig sind die Konsequenz und Sorgfalt der Umsetzung und die ständige Überzeugungsarbeit.

*Was erwarten Sie von Herstellern wie Oracle, um Sie bei Ihren Aufgaben zu unterstützen?*





**Dr. Debski:** Die Global Player in der IT-Branche wie zum Beispiel Oracle bringen mittlerweile sehr ausgereifte Produkte auf den Markt. Dies gilt auch für eingebettete oder „Add-on“-Sicherheitsfunktionen. Allerdings wächst auch die Komplexität und das ist wahrscheinlich auch der Grund dafür, dass sich viele der neuen Features wie DBMS\_CRYPTO API, ASO, TDE, Wallets oder NDE nur langsam im realen Unternehmensumfeld durchsetzen. Eine gekonnte Nutzung der umfangreichen Sicherheitsfunktionen der Oracle Datenbank 11g ist nicht trivial, so dass hier zuerst Lern- und Experimentierphasen notwendig sind. Ein etwas stärkeres Engagement des Herstellers auf dem Gebiet der Anwenderunterstützung wäre hilfreich. Außerdem wünsche ich mir zukünftig generell eine etwas bessere Ausgewogenheit zwischen Funktionalität und Einsetzbarkeit.

*Wie sehen Sie die Rolle der DOAG in Ihrem Bereich?*

**Dr. Debski:** Ich schätze sehr das Feedback, das die Anwendergruppe gegenüber dem Hersteller gibt. Darüber hinaus ist die DOAG für mich eine sehr gute Plattform für den Erfahrungsaustausch und um das eigene Fachwissen zu vervollständigen.

*Herzlichen Dank, Herr Dr. Debski.*

### Die Linde Group

Die Linde Group ist ein weltweit führendes Gase- und Engineeringunternehmen, das mit annähernd 48.000 Mitarbeitern in mehr als 100 Ländern vertreten ist und im Geschäftsjahr 2009 einen Umsatz von 11,2 Mrd. Euro erzielt hat. Die Strategie der Linde Group ist auf ertragsorientiertes und nachhaltiges Wachstum ausgerichtet. Der gezielte Ausbau des internationalen Geschäfts mit zukunftsweisenden Produkten und Dienstleistungen steht dabei im Mittelpunkt. Linde handelt verantwortlich gegenüber Aktionären, Geschäftspartnern, Mitarbeitern, der Gesellschaft und der Umwelt – weltweit, in jedem Geschäftsbereich, jeder Region und an jedem Standort. Linde entwickelt Technologien und Produkte, die Kundennutzen mit einem Beitrag zur nachhaltigen Entwicklung verbinden.

Weitere Informationen über die Linde Group unter <http://www.linde.com>

### Das Geschäft läuft

Im vierten Finanzquartal 2010, das zum 31. Mai 2010 endete, erzielte die Oracle Corporation (NASDAQ: ORCL) einen GAAP-Umsatz von 9,5 Milliarden US-Dollar, das entspricht einer Steigerung von 39 Prozent im Vergleich zum Vorjahreszeitraum. Die Software-Erlöse aus Neulizenzen nach GAAP erhöhten sich um 14 Prozent auf 3,1 Milliarden US-Dollar. Zugleich stiegen die Umsätze aus Software-Lizenz-Updates und aus dem Produkt-Support nach GAAP um 12 Prozent auf 3,4 Milliarden US-Dollar. Der Reingewinn nach GAAP erhöhte sich um 25 Prozent auf 2,4 Milliarden US-Dollar. Oracle schätzt, dass Sun die betrieblichen GAAP-Einnahmen für das vierte Finanzquartal 2010 um circa 100 Millionen US-Dollar vermindert hat, wobei 176 Millionen US-Dollar Tilgung enthalten sind, und ungefähr 400 Millionen US-Dollar zu den betrieblichen Non-GAAP-Einnahmen beigesteuert hat.

Im Finanzjahr 2010 stieg der GAAP-Umsatz um 15 Prozent auf 26,8 Milliarden US-Dollar, während der Non-GAAP-Umsatz um 15 Prozent auf 27,0 Milliarden US-Dollar stieg. Safra Catz, Oracle President: „Jetzt, da Sun profitabel ist, sind wir noch zuversichtlicher, dass wir unser Ziel erreichen oder übertreffen werden, dass Sun 1,5 Milliarden US-Dollar im Geschäftsjahr 2011 und 2,0 Milliarden US-Dollar im Geschäftsjahr 2012 zu unseren betrieblichen Non-GAAP-Einnahmen beiträgt.“

Oracle Newsticker

**Sparen Sie sich das nächste Update Ihres Fax-Servers.**

**Und das nächste, und das nächste, und das nächste, und das nächste.**

**Wir sorgen weltweit für sichere und zuverlässige Fax-Kommunikation.**

Ob SAP-System, Notes oder Exchange/Outlook-Umgebung, Desktop Anwendung oder Internetplattform – wir haben für jede Anforderung die passende Fax-Lösung. Dank der Retarus Fax-Cloud benötigen Sie weder Fax-Server noch Leitungen. Das hilft bei der Konsolidierung Ihrer IT-Infrastruktur und senkt die Kosten. [www.retarus.com/fax](http://www.retarus.com/fax)

# Was ist (Datenbank-)Sicherheit?

Franz Hüll, DOAG-Vorstand und Leiter Competence Center Securityfragen

**„Datenbank-Sicherheit besteht aus einem Korpus von Maßnahmen, Verfahrensweisen (Policy) und Mechanismen, welche die Geheimhaltung, Integrität und Verfügbarkeit von Daten sicherstellen und mögliche interne und externe Angriffe, ob bösartiger oder zufälliger Art, abwehren sollen.“ [1]**

Der entscheidende Punkt bei dieser Definition ist der Plural von „Maßnahme“. Sicherheit ist nie eine einzelne Maßnahme, bezogen auf eine technische Einrichtung oder ein Verfahren, Sicherheit ist nie die alleinige Erfüllung einer gesetzlichen Vorschrift und Sicherheit reduziert sich nicht auf eine Schulung eines Mitarbeiters. Sicherheit ist immer die Summe aller Maßnahmen, die zur Erfüllung eines definierten Schutzbedarfs erforderlich sind. Damit ist auch gesagt, dass ganz am Anfang die Definition eben dieses Schutzbedarfs stehen muss. Hier wird die Messlatte festgelegt, an der sich alles Weitere orientieren wird.

„Summe aller Maßnahmen“ bedeutet auch, dass die Regelungen untereinander ausgewogen sein müssen. Es ist wenig erfolgreich, wenn alle erforderlichen Maßnahmen umgesetzt worden sind, die Qualität der Umsetzung und damit die Wirkung der einzelnen Schritte aber erheblich voneinander abweicht. Eine Firewall, über die der gesamte Netzwerk-Verkehr in das Internet läuft, die aber nicht ausreichend oder fehlerhaft konfiguriert ist, trägt eben wenig zur gewünschten Sicherheit bei. Die Aussage „Wir haben eine Firewall“ ist noch kein Beweis für die damit erreichte Sicherheit.

Dieser Artikel spricht alle möglichen Aspekte an. Die Liste ist sicher nicht vollständig, aber sie soll helfen, eigene Maßnahmen nochmals zu durchdenken.

## Organisation

„Was passiert, wenn was passiert?“ Wenn ein sicherheitsrelevanter Vorfall auftritt, dann kann man davon ausgehen, dass Zeit eine der knappsten Ressourcen sein wird. Oder wie es ein Kollege einmal formuliert hat: „Es herrscht

Zeitmangel im Überfluss“. Wenn man erst jetzt darüber nachdenkt, was denn eigentlich zu tun sei, ob Netzwerk-Verbindungen zu trennen sind, ob Datenbanken heruntergefahren werden müssen und wie ein eventuell erforderlicher Notbetrieb zu gestalten ist, dann hat man zum aufgetretenen Sicherheitsproblem gleich noch ein zweites Problem auf dem Tisch.

Neben den durchzuführenden Maßnahmen muss auch der Informationsfluss vorab geregelt sein. Wer ist wann und in welchem Umfang zu informieren? Wann und wie muss eskaliert werden? Das bedeutet, dass im Vorfeld eine entsprechende Sicherheitsorganisation aufzubauen ist, deren Aufgabe darin besteht, die erforderlichen Notfallpläne zu erarbeiten, auf deren Umsetzung zu achten und durch Übungen die Sinnhaftigkeit nachzuweisen. Diese Sicherheitsorganisation bindet die relevanten Einheiten des Unternehmens ein, der Betriebsrat ist mit an Bord und natürlich die Geschäftsführung beziehungsweise der Vorstand.

Innerhalb der Sicherheitsorganisation gibt es einzelne Arbeitsgruppen, die sich mit Planungsaufgaben beschäftigen, andere sind für Compliance, das heißt für die Einhaltung der für das Unternehmen verbindlichen Regeln zuständig. Wiederum andere haben die Aufgabe, die eigenen Entwickler oder Projektteams zu begleiten. Auch die interne Revision spielt hier eine wichtige Rolle.

Weil gerade von Geschäftsführung beziehungsweise Vorstand die Rede war: Wer mit der Planung oder Umsetzung von Maßnahmen zur Sicherheit im Unternehmen beauftragt ist, muss von Beginn an bei der Unternehmensleitung die volle Rückendeckung einfordern. Er muss dabei deutlich machen, dass die notwendige Unter-

stützung durch Geschäftsführung beziehungsweise Vorstand die absolute Voraussetzung für eine erfolgreiche Umsetzung von Sicherheitsmaßnahmen ist. Andernfalls besteht die Gefahr, auf halber Strecke steckenzubleiben.

Wichtig ist eine gute und professionelle Vorbereitung auf den Ernstfall, um dann souverän reagieren zu können. Störfall- und Sicherheitsszenarien müssen definiert und durchgespielt werden. Nur so ist die erforderliche Routine zu erreichen, die hilft, Stresssituationen zu meistern.

## Software-Entwicklung

Häufig lassen sich Sicherheitsprobleme auf mangelnde Qualität bei der Entwicklung von Software zurückführen. Dies gilt gleichermaßen für eigenentwickelte Software wie für Software von Drittherstellern. Diese Qualitätsmängel haben eine Vielzahl von möglichen Ursachen, die sich in drei Gruppen einordnen lassen.

- *Mängel beim Software-Entwurf*
  - In dieser Phase werden die grundlegenden Festlegungen getroffen. Die Anforderungen an Funktionalität, Schnittstellen, Oberflächengestaltung, Verfügbarkeit, Plattform und vieles, vieles mehr sind zu definieren. Es sind auch die sicherheitsrelevanten Anforderungen festzuschreiben. Soll verschlüsselt werden? Wie wird der Zugang zur Anwendung geregelt? Wie schaut das Rechtekonzept aus? Wie sensibel sind die Daten? Welche Anforderungen an die Verfügbarkeit gibt es? Diese und andere Fragen müssen in dieser Phase verbindlich beantwortet werden.

- Falls die zu konzipierende Software im späteren Betrieb mit Updates aktualisiert werden muss, ist jetzt schon das Konzept dafür zu erstellen. Müssen die Updates unbedingt während des laufenden Betriebs eingespielt werden? Ist eine Downtime der Systeme erforderlich? Gibt es feste Update-Zyklen oder kann es sein, dass in dringenden Fällen ein Update innerhalb weniger Stunden (Minuten?) produktiv sein muss? Soll das Update automatisch eingespielt werden können?
- Erst wenn auch diese Fragen eindeutig beantwortet sind, dann kann das Projekt „Software-Entwicklung“ in die nächste Phase gehen.
- In der Budget-Planung müssen unbedingt auch die Kosten für die Sicherheit berücksichtigt sein.
- Leider passiert es in der Praxis häufig, dass die Fachabteilung, die eine Entwicklung beauftragt, möglichst schnell Ergebnisse sehen will. Für eine lange planerische und konzeptionelle Phase wird eher wenig Verständnis gezeigt. Zumindest ein Prototyp, der noch nichts kann, aber so tut als ob, soll auf den Tisch. Wenn dann auf der Basis dieses Prototyps weiterentwickelt wird, bleibt manches auf der Strecke, und besonders betroffen davon sind eben häufig die Sicherheitsaspekte.
- Wie sichere Software-Entwicklung angegangen werden kann, wird in einem Artikel auf [www.heise.de](http://www.heise.de) am Beispiel „Microsoft“ beschrieben [2].
- *Mängel bei der Umsetzung*
  - Dies ist eines der gravierendsten Probleme bei der Software-Entwicklung überhaupt. Selbst wenn die Vorgaben exakt definiert worden sind und in einer Richtlinie die „Entwicklung sicherer Software“ im Detail und vollständig beschrieben ist, bleibt die Entwicklung von Software doch eine Tätigkeit, die von Menschen erbracht wird. Und unterschiedliche Menschen haben unterschiedliche Auffassungen von Qualität, Test und Sicherheit.
  - Hier ist in erster Linie eine gute Ausbildung und Schulung der Entwickler der Schlüssel zum Erfolg. Des Weiteren muss eine Software-Entwicklungsumgebung zur Verfügung stehen, in der Standards gesetzt werden, die vorschreibt, wie bestimmte Anforderungen umzusetzen sind, und die Routinearbeiten soweit wie möglich abnimmt.
  - Als Beispiel sei hier das Error-Handling kurz angesprochen. Hier muss festgelegt sein, wie die zu entwickelnde Software später – zur Laufzeit – auf Ausnahmesituationen zu reagieren hat. Wann liegt überhaupt eine Ausnahmesituation vor? Wie wird sie erkannt? Welche Informationen werden nach außen weitergegeben? Wie kann der betroffene Anwender damit umgehen? Welche Informationen braucht der Entwickler zur Ursachenforschung? Dieses Error-Handling muss in allen Bereichen der Anwendung identisch sein und als zentrale Komponente zur Verfügung stehen.
  - Fehlerhaftes Error-Handling ist oft das Einfallstor für Angreifer. Etliche Sicherheitslücken haben hier ihre Ursache.
- *Mängel beim Testen*
  - Das Testen von Software ist ein höchst kreativer Prozess. „Sourcecode Inspection“ ist ein Schritt dabei. Dies kann durch entsprechende Scanner unterstützt werden, hier ist aber auch das Auge eines erfahrenen Testers gefragt.
  - „Testen“ bedeutet zuallererst festzulegen, was zu testen ist, wie zu testen ist und welche Testergebnisse erwartet werden. Durchführung und Testergebnisse sind zu dokumentieren. Abweichungen von den erwarteten Ergebnissen sind festzuhalten und an den zuständigen Entwickler zur Bearbeitung weiterzuleiten.
  - Kreativ wird das Testen dann, wenn Test-Szenarien zu entwickeln sind. Was ist ein normales

Verhalten? Wie können Extremsituationen erzeugt werden? Welche Grenzwerte gibt es? Welche Sicherheitsrisiken können auftreten? Gibt es mögliche Schwachstellen für Angreifer? Wie ist das Zusammenspiel verschiedener Komponenten? Sind die Tests reproduzierbar? Wie stark können die Tests automatisiert ablaufen? Fragen über Fragen.

- Gutes Testen garantiert eine hohe Qualität und die wiederum ist eine Voraussetzung für die Einhaltung von Sicherheitsvorschriften bei der Softwareentwicklung. Mangelnde Qualität ist immer auch ein Sicherheitsproblem. Viele Sicherheitslücken entstehen durch Fehler bei der Implementierung der Software (SQL-Injection, Buffer Overflow, Privilegien-Eskalierung, Cross-Site-Scripting etc).

## Datenbanken

Die Unternehmensdaten sind in vielen unterschiedlichen Formaten und Strukturen gespeichert (Mail-Storage, Fileserver, Datenbanken, Archive, Papier etc.). Gerade in den Datenbanken finden sich umfangreiche und hochaktuelle Daten des Unternehmens, die für die laufenden Prozesse unabdingbar sind.

Die Daten müssen klassifiziert sein: Welche Daten sind vertraulich, welche nicht? Wie fein muss hier abgestuft werden? Wie viele Klassifizierungen sind erforderlich? Erst wenn dies geschehen ist, dann können weitere Maßnahmen abgeleitet werden. Solange nicht bekannt ist, ob vertrauliche Daten vorliegen, braucht auch nicht über Verschlüsselung nachgedacht werden.

Die Installation der Datenbank ist auch unter dem Gesichtspunkt „Sicherheit“ zu sehen. Regeln müssen aufgestellt werden, wie die Installation zu erfolgen hat, „Härten“ ist ein Thema und es muss auch festgelegt sein, ob bestimmte Aktionen zu protokollieren (Audit) sind. Daran schließt sich gleich die Frage an, wie lange diese Protokoll-Daten aufgehoben werden, wer diese Daten (idealerweise unter Einhaltung des Vier-Augen-Prinzips) auswertet und an wen die Ergebnisse

dieser Auswertung gehen dürfen. Dies sind übrigens wieder Vorgaben, die aus der Sicherheitsorganisation (siehe oben) kommen müssen, da dort Betriebsrat, Sicherheitsfachleute und Geschäftsführung vertreten sind.

Das User-Management ist ebenfalls zu regeln. Wer darf User anlegen, ändern und löschen? Eine ganz wichtige Frage ist in diesem Zusammenhang auch: Wer ist der Owner der Daten?

Für den Schutz der Datenbank gibt es eine ganze Reihe von Produkten und Funktionen an, die auf Brauchbarkeit zu prüfen sind.

### Backup & Recovery

„Datensicherung und Wiederherstellung“ ist ein wichtiges Thema. Diese Aussage wird niemanden überraschen. Gerne wird gefragt, ob der Backup funktioniert. Dies ist eigentlich schon der falsche Ansatz. Die Frage muss immer lauten: „Funktioniert der Recovery-Prozess?“ Natürlich ist die wesentliche Voraussetzung für ein erfolgreiches Recovery ein erfolgreicher Backup, aber das Ziel aller Maßnahmen ist eben immer die Wiederherstellung der Daten, möglichst ohne Verluste und in einer definierten Zeit. Wer hat Zugriff auf die Medien? Wie lange dauert es, nach einem Störfall ein erfolgreiches Recovery durchzuführen? Sind die Backup-Daten möglicherweise „vergiftet“, weil ein Angreifer über einen längeren Zeitraum unbemerkt Daten manipuliert hat? Sind die Daten für ein Recovery vollständig und lesbar? Ist der Schlüssel für die Entschlüsselung verfügbar?

Um Routine in den Backup- und Recovery-Prozess zu bringen, muss dieser geübt werden. Dies möglichst wirklichkeitsnah durchzuführen, ist nicht ganz einfach. Keiner wird eben mal die Produktion stoppen, ein paar Datenbankfiles löschen und dann schauen, ob das Recovery auch in der vereinbarten Zeit machbar ist. Dass zur Übung mal ein Knoten eines Cluster bewusst und vorsätzlich ausgeschaltet wurde (in einer Produktionsumgebung), kommt aber schon vor. Es gibt Unternehmen, die genau dies tun und damit die Zuverlässigkeit der eingesetzten Systeme unter Beweis stellen.

Wichtig beim Testen eines Recovery ist die Berücksichtigung des Zeitfaktors. Falls wirklich mal in der Produktion eine umfangreiche Wiederherstellung erforderlich ist, geschieht dies in der Regel unter hoher zeitlicher Belastung. Wenn jetzt noch viele Anwender davon betroffen sind, die entweder den User Helpdesk mit Anrufen lahmlegen oder die DBAs direkt anrufen, steigt der Nervosität bei manchem DBA weiter an. Werden jetzt noch die Vorgesetzten alarmiert, die sich dann zur „Unterstützung“ des DBAs hinter ihm aufstellen und weitere Fragen stellen, ist das für die Bewältigung der Situation nicht hilfreich.

Die Ursachenforschung kann und muss nach dem erfolgreichen Recovery einsetzen. Bis es so weit ist, sollen die DBAs oder Backup-Administratoren ungestört arbeiten können – abgeschirmt von all dem Trubel, der durch den Notfall entstanden ist.

### Mitarbeiter und Mensch

Bei allem, was man sich als Sicherheitsmaßnahmen ausdenken kann, muss aber der Mensch im Mittelpunkt stehen. Es sind Menschen, die von Sicherheitsproblemen betroffen sind, es sind Menschen, die einen Schaden erleiden, es sind aber auch Menschen, die ein Unternehmen fahrlässig oder vorsätzlich gefährden.

Die Mitarbeiter, die dem Unternehmen unabsichtlich und aus mangelndem Wissen Schaden zufügen, müssen geschult werden. Die Wichtigkeit der Daten für das Unternehmen und damit für den eigenen Arbeitsplatz ist deutlich zu machen. Der Mitarbeiter macht im Idealfall den Schutz dieser Daten zu seiner Sache, aus Verantwortung dem Unternehmen gegenüber, aber auch aus Sorge um den eigenen Arbeitsplatz.

Man darf aber dabei nicht über das Ziel hinausschießen. Zu komplexe Passwort-Regeln, häufige und unnötige Anmelde-Vorgänge, ständige Ermahnung (zum Beispiel beim Login in Form von täglich wechselnden Hinweisen), unnötiges Protokollieren von Zugriffen und Ähnliches schaffen möglicherweise ein Klima des Misstrauens. Der Mitarbeiter bekommt das Gefühl, dass sein Unter-

nehmen ihm misstraut – eine Situation, die das Arbeitsklima und die Identifikation mit der Firma untergraben kann.

Aber es sind auch Menschen, die für Angriffe und Datendiebstahl verantwortlich sind. Es sind Menschen, die im Unternehmen arbeiten, oder von außen versuchen, Schaden anzurichten.

Leider gibt es nicht den einen Königsweg. Auch wenn auf eine ganze Reihe von etablierten Verfahren und definierten Prozessen zurückgegriffen werden kann (und muss), ist eine ganzheitliche Sicherheit immer auch ein individueller Ablauf, der auf die jeweiligen Erfordernisse und Bedürfnisse des Unternehmens und der Mitarbeiter abgestimmt sein muss.

Und nicht zu vergessen: Sicherheit ist nicht ein Prozess, der einmal durchlaufen wird. Vielmehr ist es ein andauernder Vorgang, der auch immer wieder hinterfragt und an neue Anforderungen und geänderten Gegebenheiten angepasst werden muss.

### Fazit

Sicherheit ist ein ganzheitlicher Prozess. Nur das Zusammenspiel aller relevanten Aspekte ergibt in Summe den gewünschten Level an Sicherheit. Sicherheit wird kaum auf der „grünen Wiese“ komplett neu aufgesetzt werden. Vorhandenes ist zu ermitteln und zu integrieren, Fehlendes ist zu identifizieren und zu ergänzen. Sicherheit ist wie eine Versicherung. Man trifft Vorsorge für einen Fall und hofft gleichzeitig, dass er nie eintreten wird. Sicherheit ist dazu da, Risiken zu erkennen und zu minimieren, soweit dies gesetzlich vorgeschrieben und wirtschaftlich vertretbar ist.

### Weitere Informationen

- [1] Ahrends, Lenz, Schwanke, Unbescheid: Oracle 10g für den DBA, Seite 363, Zitat aus Castano et al., Database Security
- [2] Niklaus Schild: Sichere Softwareentwicklung nach dem „Security by Design“-Prinzip: [www.heise.de/developer/artikel/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html?view=print](http://www.heise.de/developer/artikel/Sichere-Softwareentwicklung-nach-dem-Security-by-Design-Prinzip-403663.html?view=print)

### Kontakt:

Franz Hüll  
securityfragen@doag.org

# Compliance-Fragen aus dem Alltag eines Lizenzberaters

Christian Grave, ProLicense GmbH

**Jede ungenutzte Lizenz ist teuer, jede fehlende eine Urheberrechtsverletzung. Ein Lizenzberater sieht in seinem Arbeitsalltag eine zunehmende Professionalisierung des Lizenz-Managements in der Unternehmenslandschaft. Damit wird den oft hohen Ausgaben für Software-Lizenzen und dem wichtigen Thema „Compliance“ Rechnung getragen.**

Lizenzmanager müssen sich mit einer Vielzahl von Metriken und Lizenzregeln beschäftigen, deren Komplexität zunimmt. Oftmals sind die Lizenzbestimmungen diverser Anbieter wie Oracle, IBM, SAP, Cisco, HP etc. zu beherrschen, um Compliance nachweisen und auf Augenhöhe Verträge verhandeln zu können. In diesem Artikel werden beispielhaft Kundensituationen dargestellt und die Richtigkeit der Oracle-Lizenzierung hinterfragt.

*Eine 8-CPU-Lizenz für Oracle DB Standard Edition ist einem Server-Cluster zugeordnet, der drei Knoten mit jeweils 4,2 und 2 CPUs aufweist. Sind Sie bei dieser Konfiguration compliant?*

Leider nicht. DB-SE-Lizenzen sind nur verwendbar für Server-Cluster bis zu einer Maximalzahl von vier Sockets. Man benötigt für diese Konfiguration die Enterprise Edition. Die Anzahl der benötigten Lizenzen bestimmt sich dann nach der Anzahl der zu lizenzierenden Prozessor-Cores. Die Processor-Core-Factor-Table, aus der sich der Bedarf an Lizenzen pro Prozessortyp ergibt, steht auf der ProLicense-Website bereit: <http://www.prolicense.de/aktuelles/oracle-dokumente.html>

*Sie haben in einer bestimmten Situation zwei Server à 16 CPUs im Einsatz und verwenden hierfür Ihren Bestand an 300 Named User Single Server (NUSS) Lizenzen für die Oracle DB Enterprise Edition. Da NUSS-Lizenzen ein Minimum von zehn Lizenzen pro CPU benötigen, es diese Metrik aber nicht mehr gibt, kaufen Sie 20 Named User Plus (NUP) hinzu. Sind Sie compliant?*

Leider nicht. Oracle gestattet die Mischung von alter und neuer Metrik nicht. Wenn Sie für Ihre Konfiguration nicht ausreichend NUSS-Lizenzen haben, so können Sie die 300 NUSS kostenfrei zu 300 NUP migrieren. Allerdings haben die neueren NUP-Lizenzen ein Minimum von 25 NUP pro zu lizenzierendem Prozessorkern. Sie benötigen demnach  $16 \times 2 \times 25$  NUP-Lizenzen = 800 NUP. Sollte es sich bei den CPUs um Multicore-CPU's handeln, so erhöht sich die Zahl der benötigten Lizenzen. Es besteht also ein Lizenzdelta von mindestens 500 NUP statt der angenommenen 20 NUP.

*Sie haben einen Webservice auf einem Server mit vier CPUs eingerichtet, der laut Google Analytics max. von 230 Website-Besuchern genutzt wird. Interne Nutzer gibt es nur 5. Sie verwenden hierfür 235 NUP-Lizenzen.*

*a.) Sind Sie compliant?*

Leider nicht. Es kann theoretisch eine unbegrenzte Anzahl von Usern zugreifen, so dass ein so konfigurierter Webserver immer mit CPU-Lizenzen ausgestattet werden muss. Sie benötigen 4 CPU-Lizenzen.

*b.) Wie verhält es sich, wenn Sie die Zugriffe nur registrierten, einzeln identifizierbaren Nutzern erlauben und diese Anzahl inkl. der internen Nutzer nicht 235 übersteigt?*

Mittels dieser Maßnahme wäre Ihre 235 NUP-Lizenz ausreichend.

*Sie haben einen 4-CPU-Server, auf den zu jedem Zeitpunkt maximal 100 interne*

*User konkurrierend zugreifen. Zudem wird der Server von fünf Entwicklern genutzt. Sie haben 100 NUP- und 100 Concurrent-Device-Lizenzen der Oracle DB Enterprise Edition im Bestand, von denen Sie 100 Concurrent-Device-Lizenzen sowie fünf NUP-Lizenzen diesem Server zuweisen möchten. Wären Sie compliant?*

Leider akzeptiert Oracle die Mischung der Lizenzmetriken auf einem Server nicht. Somit können Sie Ihre Lizenzen nicht in dieser Art verwenden. Sie haben folgende Handlungsalternativen:

a.) Sie können Ihre Concurrent-Device-Lizenzen zur aktuellen NUP-Metrik migrieren. Beim Migrationsverhältnis „1:2“ hätten Sie im Anschluss daran einen Bestand von 200 NUP-Lizenzen. In Abhängigkeit von der tatsächlichen Userzahl des Servers könnte dies ausreichend sein.

b.) Günstiger ist es wahrscheinlich, wenn Sie für den Server wie geplant Ihre 100 Concurrent Device verwenden und für die fünf Entwickler IDS-Lizenzen erwerben. Die 100 NUP-Lizenzen können Sie bei Bedarf für andere Projekte verwenden oder eventuell den Support kündigen (abhängig vom Vertrag, Thema „Vertragskonsolidierung“, Repricing beachten).

## Kontakt:

Christian Grave  
christian.grave@prolicense.de

# Kundendaten im Supersonderangebot oder wie man Datenbanken heute absichern kann

Caroline Kohn, Sentrigo Inc.

**Die Kunden der Schweizer Banken können ein Lied davon singen, wie teuer es ist, wenn Daten in die falschen Hände gelangen. Aber auch in anderen Branchen ist durch fehlende Kontrolle der Kundenstammdaten das Vertrauen nicht gewachsen.**

Erst recht die Diskussionen um die Datenmagneten ELENA und die Gesundheitskarte rücken das Thema „Datenbanksicherheit“ in ein neues Licht: Es geht um das Einhalten von Gesetzen und um das Vertrauen der Bürger und Kunden. Ob die Cloud das Ganze deutlich transparenter macht? Zweifel sind angebracht. Und ein Abwarten ist mitunter ruinös, denn Datenbanken sind ein lohnendes Ziel, wenn es darum geht, Daten auszuspähen. Aber woran denkt ein CIO bei Datenbanken? Performance und nochmals Performance und vielleicht Betriebszeit sowie Hochverfügbarkeit – aber Sicherheit?

Viele Daten können ein Unternehmen dann ruinieren, wenn sie in die Hände Dritter gelangen. Dieses Unternehmen hat vielleicht 5493 Nutzer, 52 Applikationen, 334 Datenbanken und täglich hunderttausende Zugriffe. Nicht wenige Firmen verfügen gar über tausende von Datenbanken, in denen höchstwahrscheinlich ein nicht unerheblicher Teil des Firmenwissens liegt. Das Protokollieren von Zugriffen ist aus Performance-Gründen abgeschaltet oder bis zur Unkenntlichkeit reduziert. Und das Monitoring des Netzwerk-Traffics liefert auch nur bedingte Sicherheit. Denn manchmal sitzt der Feind im eigenen Haus, hat den Status eines Superusers oder verfügt über die Zugangsdaten zu einem hoch privilegierten Account.

Das Themenfeld „Sicherheit und Datenbanken“ ist weitläufig. Regierungen oder Behörden schreiben eine Unzahl von Regelungen vor, die auch noch ständig geändert werden. Niemand möchte, dass Kreditdaten, Mitarbeitergehälter oder Patientenakten an die Öffentlichkeit gelangen. Die Tatsache, dass

die Klassifikation von Daten in „streng geheim“, „geheim“, „vertraulich“, „nur für interne Zwecke“ und viele andere Zwischenstufen sehr fein granulierbar ist, macht die Aufgabe nicht eben leichter. Auf der anderen Seite steht der berufliche Alltag. Never touch a running system. Eingriffe in Datenbanken stören sowieso den geschäftlichen Ablauf, denn Mitloggen kostet viel Datenbank-Performance. Warum sollte ein Datenbank-Administrator ständig die Critical Patch Upgrades (CPU) einspielen, wenn das von allen Fachabteilungen als Bremsklotz empfunden wird?

Wer solche Einschätzungen aus eigener Erfahrung kennt, könnte davon ausgehen, dass diese weit verbreiteten Ansichten der größte Unsicherheitsfaktor seien, doch das täuscht. All dies kann man unter mangelnder Sensibilität in Sicherheitsfragen verbuchen. Da aber bekannt ist, dass enormer Schaden entsteht, wenn geschäftskritische Inhalte wie Personaldaten, Forschungsdokumente oder interne Studien in falsche Hände gelangen, ist es allerhöchste Zeit einzusehen, dass bei solchen Attacken von mutwilligen und kriminellen Tätern auszugehen ist. Denn weder die professionellen Wirtschaftsspione noch engagierte Cracker oder gar frustrierte Mitarbeiter nehmen Rücksicht. Ihnen geht es um den größtmöglichen Schaden oder um einen hohen finanziellen Vorteil aus dem Veröffentlichen oder dem Verkauf der Daten.

## **Bordmittel sind wie Multivitamin-Tabletten**

Aktuelle Datenbanken bringen bereits Bordmittel für die Autorisierung mit,

die zum einen auf Benutzerebene bestimmte Rechte an Operationen oder Datenbereiche vergeben. Auf der anderen Seite gibt es globale Sicherheitsstufen, die ähnlich wie eine Heuristik eine präventive Maßnahme darstellen, ohne spezifischen Angriffen zuvorzukommen. An dieser Stelle werden dann auch die firmeneigenen Sicherheitsregeln abstrahiert auf Basis von potenziellen Angriffen und schädlichen Operationen. Positiv gesehen muss man bei ihrer Formulierung also genau wissen, wie wichtig bestimmte Inhalte sein werden. Nach dem Prinzip der minimalen Rechte ist es schon mal ein Schritt in die richtige Richtung, einfach SYSDBA- und SYSOPER-Rechte prinzipiell nicht an alle Datenbank-Administratoren zu vergeben.

Das erste wirkliche Problem entsteht bei den Daten der sogenannten „Login-Sessions“. Bei diesen Log-Dateien wird zu jedem Nutzer-Login ein chronologischer Ablauf seiner Daten-Operationen erstellt. Parallel dazu wird das Systemlog die Gesamtheit aller Änderungen an der Datenbank aufzeichnen, also auch die Änderungen durch Updates und ähnliches. Das Standard Auditing umfasst aber schon nicht mehr die Aktionen, die mit SYS-Rechten durchgeführt wurden. Das kann fatale Folgen haben.

Je mehr und genauer diese Log-Dateien geführt werden, desto eher kann man im Datenbank-Auditing nachvollziehen, wer was wann getan hat beziehungsweise tut. Vorsichtige Naturen können also alle SQL-Befehle protokollieren – vor allem die mit SYS-Rechten. Sinnvoll ist es natürlich, die Schreibrechte dieser Log-Datei-

en praktisch der gesamten Belegschaft und weitgehend allen Usern zu entziehen. Die gewonnene Transparenz geht deutlich auf Kosten der Performance. Im echten Leben sind daher die vielen schönen Log-Funktionen abgeschaltet, damit die Datenbank läuft wie ein geölter Blitz. Der Nachteil liegt darin, dass der Audit-Trail, also die sicherheitsrelevanten Daten einer Log-Datei, entweder nicht vorhanden sind oder zu wenige Daten erhalten, um kritische Muster zu erkennen. Oft kann man bei bestehendem Verdacht im Nachhinein auf diese Daten zurückgreifen, aber mit ihnen keine potenziellen Verdachtsfälle erkennen. Ein Blick in den Rückspiegel, der nicht selten zur Folge hat, dass man mit voller Geschwindigkeit gegen die Wand fährt. Zumindest kann man sich der Tatsache rühmen, bis dahin alles aus dem Motor geholt zu haben, was die Maschine hergab. Und die Tatsache, dass man das „Mandatory Auditing“ bei Oracle-Datenbanken sowieso nicht abschalten kann, liefert daher auch keine Beweise für eine klare Strategie.

Um direkt in der Datenbank Sicherheit zu gewährleisten, muss im weitesten Sinne eine Zugriffskontrolle erfolgen. Das passiert entweder passiv über das Lesen der Log-Dateien und das Erkennen von schädigendem Verhalten oder über das aktive Überwachen der Datenpakete im Netzwerk, die auf die Datenbank zugreifen wollen. Auf dieser Basis gruppieren sich die Drittanbieter für Datenbanksicherheit rund um diese beiden Ansätze. Der eine Teil der Produkte fügt dem inflationären Protokollieren der Datenbanken noch eine zweite Ebene hinzu und produziert auf diese Weise eine enorme Menge an Metadaten über Datenbankoperationen. Der andere Teil der Produkte fokussiert das Netzwerk und durchforstet dort alles nach sicherheitsrelevanten Mustern. Dabei übersehen diese Produkte jedoch gerne Angriffe, die lokal vom Datenbankserver aus mit Superuser-Rechten erfolgen. Das ist dann ein frustrierter oder leichtsinniger Mitarbeiter oder eben der Mitarbeiter der Drittfirma, die auch auf die Kundendaten zugreifen darf. Im Zeitalter der Virtualisierung, in dem Web- und Datenbank-Server einfach nur als

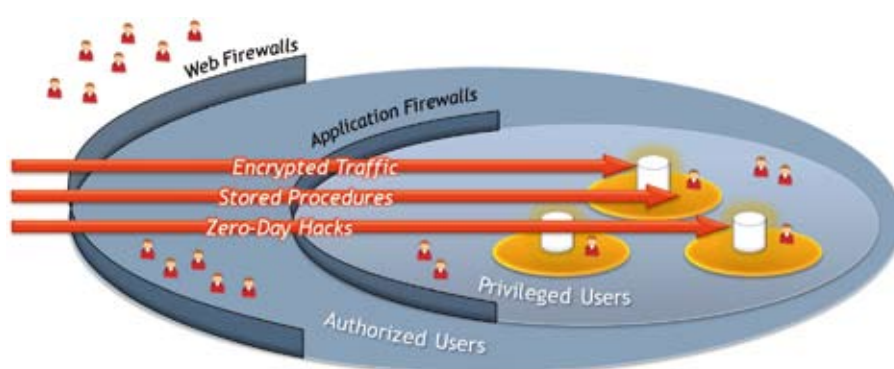


Abbildung 1: Softwarebasierte Security Software ist in der Lage, auch privilegierte User zu kontrollieren und auf Zero-Day-Angriffe in Echtzeit zu reagieren

Instanz einer Maschine vorliegen, gibt es jedoch während der Kommunikation gar keinen Traffic im Netz. So wird der bisherige Ansatz des Überwachens der Netzwerke rund um das Thema „Cloud und Virtualisierung“ in vielen Fällen obsolet. Und das klassische Schauen in den Rückspiegel (Auditing) ist den Herausforderungen des Echtzeitweb und der Echtzeitangriffe nicht ganz gewachsen. Was also tun?

### Ein strukturiertes Vorgehen ist die halbe Miete

Neuere Konzepte für die Sicherheit von Datenbanken konzentrieren sich auf zwei Säulen: das Absichern gegenüber dem Netz in Form spezieller Firewalls für die Datenbank (Database Firewall, DBFW) sowie Database Activity Monitoring (DAM). Die erste Säule soll schädliche Aktivitäten von außen verhindern



Analyse Beratung Projektmanagement Entwicklung

## Ihr Spezialist für webbasierte Informationssysteme mit

Oracle WebLogic Server  
Oracle WebLogic Portal

**exensio** ● ● ●  
www.exensio.de

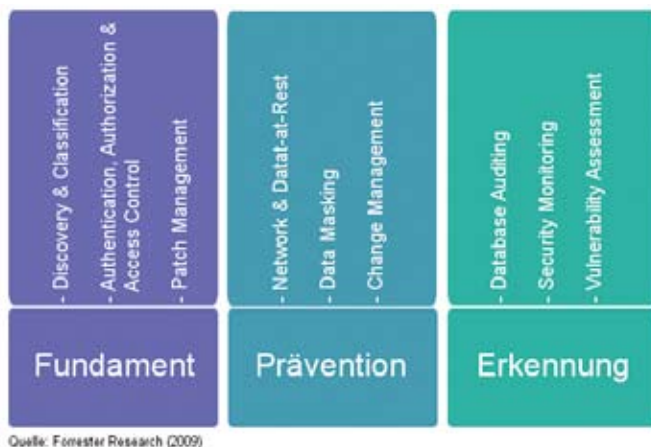


Abbildung 2: Die drei Säulen der Datenbank-Sicherheit nach Forrester

und ist im besten Fall mit virtuellem Patching ausgestattet, um das lästige Thema mit den CPUs zu entschärfen bzw. erfolgreich hinauszuzögern. Denn dieses virtuelle Patchen ermöglicht es, bekannt gewordene Lücken sofort abzusichern, ohne die Datenbank herunterzufahren. Vor allem der Schutz der Daten(bank) an sich ist oberstes Ziel der DBFW. Das Monitoring setzt im Zwischenbereich zwischen zugreifender Stelle (user) und der Datenbank an. Dabei ist es weitgehend unabhängig von Datenbank-Hersteller und -Typ.

Je höher jedoch die Abstraktion ist, desto stumpfer wird das Schwert. Noch schlimmer ist es bei der Virtualisierung, denn dort findet der Traffic gar nicht mehr im Netz statt. Der Austausch zwischen Applikation und Datenbank läuft dann quasi in Lichtgeschwindigkeit vom virtuellen Web-Server zum virtuellen Datenbank-Server. Die Cloud macht diese Entwicklungen nicht eben übersichtlicher oder besser kontrollierbar. So verwundert es nicht, dass die wenigen Hersteller, die sich in dem Feld tummeln, wie Imperva oder IBM/Guardium hier schon die Waffen strecken. Bei letzterem ist das verständlich, weil dessen Hauptfokus auf dem Monitoring der Server liegt. Sentrigo als Spezialhersteller hat einen Vorteil, da direkt auf Betriebssystem-Ebene der Datenbank gearbeitet wird. Dieser liegt in leichtgewichtigen Lösungen, die nicht auf bestimmte Kernels angepasst sind und damit die Nachteile der alten, hostbasierten Systeme ausgleichen können (siehe Abbildung 1).

Sie werden einfach einmalig gemeinsam mit dem „Anknipsen“ des Datenbank-Servers aktiviert und schützen dann automatisiert alle weiteren Layer der Datenbank. Das Besondere aber liegt in einer sogenannten „Sensor-Funktion“, die direkt im Speicher hinterlegt ist, so dass nicht nur das Netzwerk oder die Verbindung zwischen User und Datenbank geschützt ist, sondern jede Operation, die den Speicher des Datenbank-Servers betritt oder verlässt. Dieses Feature hat nicht nur deutliche Vorteile in virtualisierten Umgebungen – es reicht ein Sensor pro physikalische Maschine – es kann die üblichen Aufgaben der DBFW und des DAM ohne die bekannten Performance-Probleme abhandeln. Denn der installierte Speicher ist der Ort der Überwachung und damit werden Engstellen im Netzwerk oder auf der Festplatte elegant umgangen.

Alle drei Anbieter verfügen über Lösungen, die externe Regeln für Compliance mit diversen nationalen und internationalen Regeln auf die Datenbanküberwachung anwenden, und auch das virtuelle Patching beherrschen sie. Imperva fokussiert mehr auf die Firewall, IBM/Guardium arbeitet eng am Server-OS und Sentrigo punktet damit, sowohl Netzwerk-Traffic als auch Datenbank-Operationen der Nutzer und Applikationen direkt im Speicher zu kontrollieren. Im Moment ist dies die einzige Lösung, um Attacken, die in den Tiefen der Datenbank versteckt wurden (vielleicht schon beim Datenbank-Design), überhaupt zu be-

### Einige Tipps

- Beachten Sie Security-Anforderungen bereits bei der Anwendungsentwicklung und denken Sie sie weiter bis zum User- und Data-Management. Es geht nicht um einzelne Taten, sondern um das Hinzufügen einer ganzen Dimension entlang aller IT-Aktivitäten.
- Das Prinzip der minimalen Rechte sollte konsequent für alle Nutzer und Applikationen gelten. Das schließt auch sogenannte „Scheunentore“ wie Entwickler und Berater mit ein!
- Beachten Sie, dass das Management mit Passwörtern essentiell für einen funktionierenden Schutz ist. Wer hier nicht aufpasst, kann sich den Rest sparen. Es geht nicht nur darum, dass lange Listen schwacher Passwörter überall im Web herumliegen. Es ist zugleich auch eine Aufgabe der Security-Beauftragten, die bestehenden Passwörter selbst mit diversen Tools durchzuchecken. Ermahnen ist nur die halbe Miete, Kontrolle ist besser.
- Installieren Sie nicht immer alles, was in irgendwelchen Paketen als Zusatztools lauert. Oft braucht man sie nicht und damit bieten sie in der Regel herrliche Spielfelder für allerlei Gesindel. Je weniger Fensterscheiben das Haus hat, desto weniger können eingeschlagen werden.

kämpfen, denn nur im Arbeitsspeicher werden verdeckte Pakete entpackt und entfalten ihre schädliche Potenz. Andere Lösungen sind an dieser Stelle schon überwunden und können bestenfalls noch den Schaden begrenzen.

### Fazit

Es lohnt sich, einen Blick auf das Sicherheitskonzept rund um Datenbanken zu werfen. Sie sind das Herz vieler geschäftskritischer Anwendungen vom Enterprise Resource Planning über die Buchhaltung bis zu den Langzeitarchiven. Es lohnt sich auch, den klassischen Triple-A-Ansatz (Authentication, Authorization and Access Control) einer gründlichen Revision zu unterziehen.

### Kontakt:

Caroline Kohn  
carolinek@sentrigo.com



# Sicherheit in Apex-Anwendungen – von der Tabelle bis zur Oberfläche

Carsten Czarski, ORACLE Deutschland B.V. & Co KG

Wie sicher oder unsicher eine Anwendung ist, liegt zu großen Teilen am Entwickler. Insofern steht das Thema „Sicherheit“ generell im Fokus der Anwendungsentwicklung, und das gilt natürlich auch für Oracle Application Express (Apex). Dieser Artikel zeigt wichtige Aspekte und gibt Tipps zum Entwickeln sicherer Apex-Anwendungen. Da der Autor sich direkt an den Entwickler richtet, werden Sicherheitsaspekte beim Betrieb eines Apex-Servers hier nicht betrachtet.

Apex-Anwendungen bestehen in der Regel aus drei Schichten:

1. Datenbank-Objekte (Tabellen, Views, Trigger, Constraints)
2. PL/SQL-Geschäftslogik (Packages)
3. Apex-Anwendung (Oberfläche)

Hat der Entwickler diese Schichten logisch sauber getrennt, so gilt für die Sicherheit von Apex-Anwendungen dasselbe, wie allgemein für die Sicherheit datenbankgestützter Anwendungen:

- Das Datenbank-Schema darf nur die wirklich benötigten Privilegien besitzen
- Keine Schicht und keine Komponente darf der anderen trauen – übergebene Parameter sind immer wieder zu prüfen
- Der Anwendungscode sollte instrumentiert sein
- Die Nutzung der Anwendung sollte einem Audit unterzogen werden

Wenn es um die Oberfläche und damit speziell um Apex geht, sollten Entwickler grundsätzlich vorhandene Komponenten so weit wie möglich nutzen. Das spart nicht nur Zeit bei der Entwicklung – es dient auch der Sicherheit, da die Apex-Komponenten viele Best Practices implementieren. Nachfolgend werden einige ausgewählte Sicherheitsaspekte betrachtet.

## Schutz vor Cross Site Scripting (XSS)

XSS-Angriffe basieren darauf, dass Angreifer HTML- und JavaScript-Code in normale Web-Formulare eingeben. Besonders im Fokus stehen Felder für Kommentare oder für den Verwen-

dungszweck. Werden diese Informationen dann vom Browser eines anderen Nutzers angezeigt, so kommt das JavaScript zur Ausführung – und dies ist dann das Einfallstor zum Ausspähen von sensiblen Daten wie Passwörtern oder PINs. Apex bietet den Schutz vor XSS in seinen Komponenten teilweise standardmäßig an. Legt man beispielsweise einen interaktiven Bericht mit der SQL-Abfrage an (siehe Listing 1), so ergibt sich das in Abbildung 1 dargestellte Ergebnis.

```
select
  ,<script type=„text/javascript“> | |
  ,alert(„XSS-Gefahr“);‘ | |
  ,</script>‘ as test
from dual
```

Listing 1: Testabfrage zum Aufdecken einer XSS-Sicherheitslücke



Abbildung 1: Ergebnis eines interaktiven Apex-Berichts mit der Abfrage aus Listing 1

Der interaktive Bericht führt den JavaScript-Code nicht aus, vielmehr werden die HTML-Sonderzeichen bei der Ausgabe maskiert. Eine XSS-Attacke ist damit nicht möglich. Das Verfahren funktioniert ohne Weiteres allerdings nicht mit allen Apex-Komponenten, der Entwickler muss bei einem klassischen Apex-Bericht selbst aktiv werden und die Anzeigeform in den Spaltenattributen entsprechend umstellen (siehe Abbildung 2).

Wenn man selbst für die Anzeige von Inhalten sorgt, muss man sich auch selbst um das Maskieren der HTML-Sonderzeichen kümmern. Die Funktion „HTF.ESCAPE\_SC“ kann hier wertvolle Dienste leisten. Dies ist von Bedeutung, wenn man Apex-Elemente mit der Substitutions-Syntax (&PX\_ITEM.) in die HTML-Seite einbaut oder – etwa in Regionen vom Typ „Dynamischer PL/SQL Inhalt“ – mit den PL/SQL-Paketen „HTP“ und „HTF“ arbeitet. Generell sollten die Seiten einer Apex-Anwendung nach der Entwicklung hinsichtlich XSS-Schwachstellen qualitätsgesichert werden, da nicht alle Komponenten automatisch davor schützen.

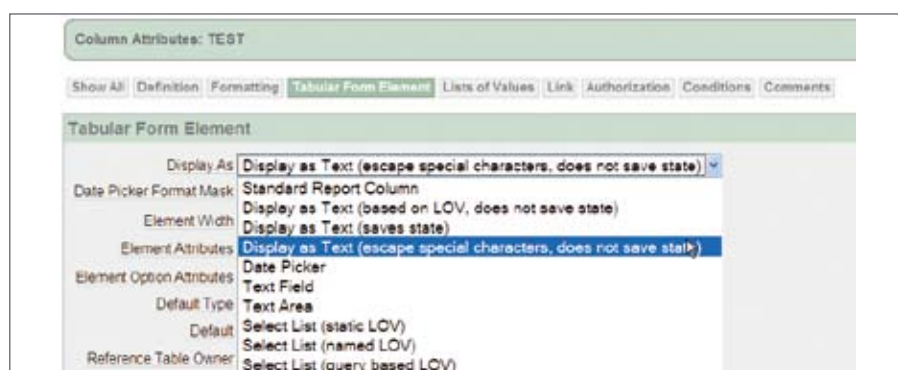


Abbildung 2: XSS-Schutz einer Tabellenspalte im klassischen Bericht aktivieren

```

declare
v_sql varchar2(32767);
begin
v_sql := ',select ename, sal, deptno from emp';
if v(,P1_DEPTNO') is not null then
v_sql := v_sql || ', where deptno = ,||v(,P1_DEPTNO)';
end if;
return v_sql;
end;
    
```

Listing 2: Typische Apex-Berichtsquelle „PL/SQL Function Returning SQL Query“

### Schutz vor SQL Injection

Mit SQL Injection sollten sich alle Entwickler datenbankgestützter Anwendungen beschäftigen – das Thema ist auch im Apex-Umfeld von Bedeutung. Unter „SQL Injection“ versteht man das Aushebeln von Sicherheitsregeln beziehungsweise die Manipulation von Daten durch das Einschleusen (Injizieren) veränderter SQL-Anweisungen.

Voraussetzung ist eine verwundbare Stelle in der Anwendung; typischerweise entsteht diese dort, wo man Nutzereingaben ungeprüft per Zeichenverkettung in eine SQL-Anweisung (Abfrage, DML oder PL/SQL) einbaut. SQL Injection findet übrigens nicht zwingend durch Manipulation der URL statt – es kann auch über normale Web-Formulare erfolgen. Insofern ist das Aktivieren der „Apex Session State Protection“ zwar hilfreich, reicht aber als alleinige Maßnahme nicht aus.

Listing 2 zeigt einen PL/SQL-Block, wie er vielfach in Apex-Berichten ge-

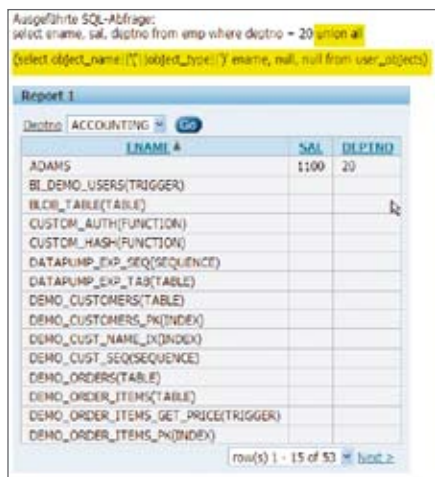


Abbildung 3: Erfolgreicher SQL-Injection-Angriff auf den Apex-Bericht

nutzt wird. Falls das Element „P1\_DEPTNO“ (könnte eine Auswahlliste sein) gesetzt ist, soll es als Filterkriterium dienen, falls nicht, soll der Bericht alles anzeigen.

Tatsächlich ist ein solcher Apex-Bericht verwundbar gegenüber SQL-Injection-Attacken. Ein Angreifer könnte dafür sorgen, dass das Formular-Element nicht einfach nur eine „DEPTNO“, sondern ein komplettes SQL-Fragment enthält. Abbildung 3 zeigt die Webseite, wie sie nach einem erfolgreichen Angriff aussieht: Der Angreifer sieht Informationen über das Datenbank-Schema. Die manipulierte SQL-Anweisung wurde der Deutlichkeit halber zusätzlich ausgegeben.

Wie konnte das geschehen? Ganz einfach: Vor dem Klick auf die Schaltfläche „Go“ wurde der Inhalt der Auswahlliste im Browser geändert (beispielsweise mit dem Firefox-Plugin „Firebug“). Statt der vorgelegten, einfachen „DEPTNO“ wurde ein komplettes SQL-Fragment übergeben – der PL/SQL-Block des Apex-Berichts baut diesen dann ein und führt ihn aus. Daraus lassen sich zwei Folgerungen ziehen:

1. Dem Browser des Endanwenders kann man nicht trauen. Trotz der scheinbar festgelegten Werte einer Auswahlliste kann man beliebige Werte an den Server übergeben.
2. SQL Injection ist offensichtlich ein Problem, dass bei dynamischem SQL auftritt. Statische SQL-Anweisungen (wenn keine Zeichenverkettung stattfindet) sind nicht betroffen.

Mit diesen Folgerungen kommt man schnell zur Lösung des Problems. Zunächst sollte man versuchen, dynami-

sches SQL als solches zu vermeiden. In einfach gelagerten Fällen wie dem in Listing 2 kann der PL/SQL-Block problemlos in eine einfache statische SQL-Abfrage umgeschrieben werden (Listing 3).

```

select ename, sal, deptno
from emp
where (deptno = :P1_DEPTNO or
:P1_DEPTNO is null)
    
```

Listing 3: Schließen der SQL-Injection-Lücke durch Verwendung statischen SQLs

Übrigens: Wird für ein Apex-Element in einer ansonsten statischen SQL-Abfrage die Substitutions-Syntax (&PX\_ELEMENT.) verwendet, so wird das SQL dynamisch und es entsteht eine SQL-Injection-Schwachstelle. In SQL oder PL/SQL sollte also entweder die Bindevariablen-Syntax (:PX\_ELEMENT) oder die Funktionsyntax (v(PX\_ELEMENT')) zum Einsatz kommen.

Es gibt aber auch Situationen, in denen dynamisches SQL erforderlich ist: So kann es sein, dass die selektierten Spalten oder die Tabellennamen dynamisch sein sollen. In diesen Fällen muss man die Parameter per Zeichenverkettung in das SQL einbauen. Damit dennoch keine Schwachstellen entstehen, sollten die Nutzereingaben vorher überprüft werden – genau hier hilft das PL/SQL-Paket „DBMS\_ASSERT“. Jeder Apex-Entwickler sollte es kennen und nutzen.

Listing 4 zeigt die Nutzung der Funktion „ENQUOTE\_LITERAL“; „ENQUOTE\_NAME“ funktioniert analog. Während „ENQUOTE\_LITERAL“ zum Prüfen einfacher Literale vorgesehen ist („KING“ ist das Literal bei „WHERE ENAME='KING'“), sollte „ENQUOTE\_NAME“ stets dann verwendet werden, wenn mit Objekten, also Tabellen-, Spalten-, Prozedur-, Funktions- oder anderen Namen gearbeitet wird. Die Funktionen versehen die Eingabe mit Anführungszeichen (einfach bei „ENQUOTE\_LITERAL“ und doppelt bei „ENQUOTE\_NAME“) und lösen eine Fehlermeldung aus, falls die Nutzereingabe schon ein solches enthält.

„DBMS\_ASSERT“ sollte immer dann verwendet werden, wenn der PL/SQL-

```
SQL> select dbms_assert.enquote_literal(q'#Meier#') ok from dual;

OK
-----
,Meier'

SQL> select dbms_assert.enquote_literal(q'#Meier' or 1=1#') gefahr
2 from dual;

FEHLER in Zeile 1:
ORA-06502: PL/SQL: numerischer oder Wertefehler
ORA-06512: in „SYS.DBMS_ASSERT“, Zeile 317
ORA-06512: in „SYS.DBMS_ASSERT“, Zeile 381
```

Listing 4: Prüfung von Literalen mit DBMS\_ASSERT.ENQUOTE\_LITERAL

Code in irgendeiner Weise SQL zusammensetzt und dabei Nutzereingaben verwendet. Das ist insbesondere hier der Fall:

- „PL/SQL Function Returning SQL Query“ als Berichtsquelle
- „EXECUTE IMMEDIATE“ oder „OPEN ... FOR“ im PL/SQL-Code
- Apex Substitution Syntax (&PX\_ELEMENT.) im SQL- oder PL/SQL-Code

### Autorisierungen in Apex-Anwendungen

Für den Fall, dass nur bestimmte Nutzer bestimmte Komponenten wie Berichte, Diagramme oder ganze Seiten sehen sollen, sind in Apex die Autorisierungsschemata vorgesehen. Diese werden in den „Gemeinsamen Komponenten“ verwaltet, prüfen einen bestimmten Sachverhalt und antworten mit „erlaubt“ oder „nicht erlaubt“. Jede

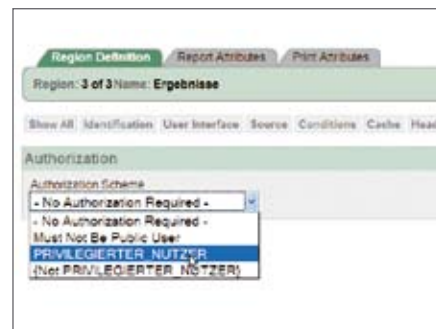


Abbildung 4: Einstellen des Autorisierungsschemas bei Apex-Komponenten

Apex-Komponente besitzt den Dialog „Autorisierung“, in dem das Autorisierungsschema ausgewählt wird (siehe Abbildung 4).

Es ist ein häufiger Flüchtigkeitsfehler, das Autorisierungsschema bei einer Reiterkarte zu setzen, nicht aber bei der zugehörigen Seite. In einem solchen Fall kann der unberechtigte Nutzer zwar nicht mehr bequem per Klick auf die Seite navigieren – die direkte An-



#### IT-Consulting

- › Performance Tuning
  - Oracle Datenbank Tuning
  - Oracle SQL + PL/SQL Tuning
- › Real Application Clusters
- › Data Guard + Fail Safe
- › Datenbank Management
  - Konfiguration
  - Backup & Recovery
  - Migration und Upgrade
- › OEM Grid Control
- › Oracle Security
- › Services
  - Remote DBA Services
  - Telefon-/Remotesupport

Nutzen Sie unsere Kompetenz für Ihre Oracle Datenbanken.

#### Schulungen

- › Oracle SQL
- › Oracle PL/SQL
- › Oracle DBA
- › Oracle APEX
- › Backup & Recovery
- › RMAN
- › Neuerungen 10g/11g
- › Datenbank Tuning
- › Datenbank Monitoring
- › Datenbank Security

Wir bieten Ihnen öffentliche Kurse sowie Inhouse-Schulungen.

#### Software-Lösungen

- › Individualsoftware
    - .NET und Visual Basic
    - Java
  - › Oracle APEX
  - › PL/SQL
- Unser Ziel: Individuelle Softwareentwicklung mit Fokus auf Ihre Zufriedenheit.

#### Oracle Lizenzen

- › Oracle Datenbanken
  - Standard Edition One
  - Standard Edition
  - Enterprise Edition
  - Personal Edition

- › Oracle Produkte
  - Enterprise Manager
  - Oracle Tools

Optimale Lizenzierung durch individuelle Beratung.





# Kerberos im Einsatz mit Oracle: Starke und existente Windows-Authentisierung nutzen

Suvad Sahovic und Carsten Mützlitz, ORACLE Deutschland B.V. & Co KG

Kerberos ist ein sicheres Authentisierungsverfahren für unsichere TCP/IP-Netzwerke wie das Internet. Es bietet erhöhte Sicherheit durch verschlüsselte Authentisierung, Single-Sign-on und zentralen Authentisierungsdienst. 99 Prozent aller den Autoren bekannten Windows-Umgebungen haben dieses Authentisierungsverfahren aktiviert – und setzen es leider nicht für ihre Oracle-Datenbanken ein. Dieser Artikel stellt verschiedene Möglichkeiten vor, wie man Kerberos für Oracle Datenbanken nutzen kann.

Kerberos wurde als Authentisierungssystem vom Massachusetts Institute of Technology (MIT) Ende der 1970er Jahre entwickelt und erst mit der Version 4 (Ende der 1980er) außerhalb des MIT genutzt. Heute ist Kerberos in der Ver-

sion 5 als sicherer Authentisierungsstandard weit verbreitet. Der Kerberos-Authentisierungsdienst beteiligt drei Komponenten – den Client, der einen Server anfragt, den Server selber und den Kerberos-Server. Dabei authentisie-

ren sich alle Komponenten gegenseitig, um Man-in-the-Middle-Angriffe zu verhindern. Darüberhinaus werden durch Kerberos insbesondere Angriffe wie passives Sniffing, Spoofing, Wörterbuch- und Replay-Angriffe erschwert beziehungsweise unterbunden. Beim Authentisierungsprozess kommen sogenannte „Tickets“ (Ticket Granting Ticket TGT) zum Einsatz (siehe Abbildung 1). Beim Windows-Login an eine Windows-Domain wird das Kerberos-Ticket sofort nach der Anmeldung erzeugt. Mit diesem Ticket kann der Client dann Berechtigungen für weitere Dienste beim Kerberos-Server anfordern, ohne sich erneut anmelden zu müssen. Kerberos überträgt keine Kennwörter und ermöglicht über den Ticketaustausch das bereits angesprochene Single-Sign-on. Während der Authentisierung nutzt Kerberos schnelle symmetrische Schlüssel (DES, 3DES, AES 256 etc.). Typische Anwendungen von Kerberos sind Benutzer-Authentisierungen etwa unter Windows 2000 / 2003 / 2008, SSH, Routern etc.

Um das sichere Authentisierungsverfahren Kerberos nutzen zu können, müssen Dienste wie ein Datenbank-Dienst mit den Kerberos-Tickets umgehen können. Die Oracle Datenbank beinhaltet bereits seit der Version 7 einen „Kerberos Authentication Adapter“, der in der damaligen „Advanced Networking“-Option ausgeliefert wurde, und heute Bestandteil der „Advanced Security“-Option ist. Natürlich kommt Kerberos auch in anderen Oracle-Lösungen wie Identity Ma-

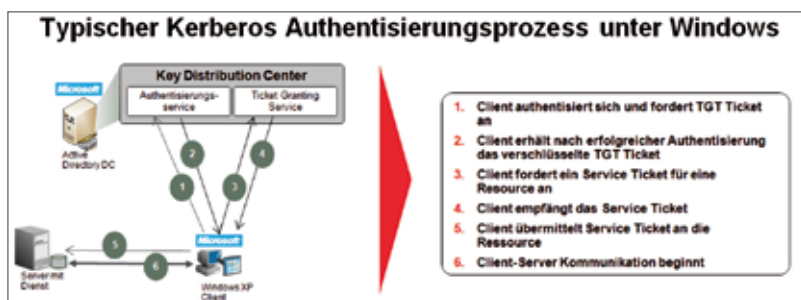


Abbildung 1: Kommunikationsmodell der Kerberos-Authentisierung

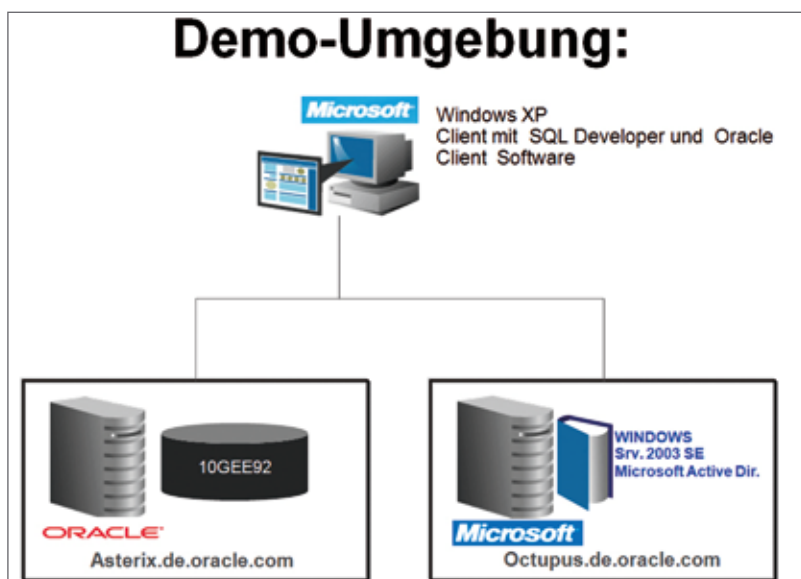


Abbildung 2: Demo-Aufbau

nager, WebLogic, HTTP Server etc. zum Einsatz.

**Vorbereitung der Oracle Datenbank**

In unserem Beispiel kommen folgende Komponenten zum Einsatz: Eine Oracle Datenbank Enterprise Edition 10g R2 mit „Advanced Security“-Option auf einem Linux-Rechner und ein Microsoft Windows Server 2003 mit Active Directory als Kerberos-Server (siehe Abbildung 2).

Zur Vorbereitung der Datenbank für eine Kerberos-Authentisierung sind zwei wesentliche Schritte auszuführen. Als Erstes muss man die Datenbank dem Kerberos-Server (dem Active Directory laut Abbildung 2) bekannt machen. Im zweiten Schritt muss die Datenbank so konfiguriert werden, dass diese die Kerberos-Authentisierung mit dem Kerberos-Server verwendet.

Damit der Kerberos-Server die Datenbank authentisieren kann, muss die Datenbank einen Benutzer-Account (kein Computer-Account) im Active Directory besitzen.

Als Nächstes wird auf dem Active-Directory-Server eine Datenbank-Kerberos-Keytab-Datei mit einem eindeutigen „Service Principal Name“ (SPN, gemapped auf den soeben erstellten Benutzer-Account) erstellt, die dann vom Datenbank-Server für die Authentisierung bei der Client-Dienst-Anfrage verwendet wird. Fragt der Client ein Service-Ticket für einen Dienst beim Kerberos-Server an, muss der Client angeben, für welchen SPN er dieses Ticket nutzen will. Für die Erstellung der Keytab-Datei kommt das Windows-Support-Tool „KTPASS“ (auf der MS Windows Server CD zu finden) zum Einsatz.

Im Beispiel heißt der SPN „ORACLE“. Der verwendete Verschlüsselungsalgorithmus ist „DES-CBC-CRC“ und die Keytab-Datei „asterix.keytab“. Die Groß-/Kleinschreibung ist bei der Ausführung dieses KTPASS-Befehls besonders wichtig.

Zur Kerberos-Konfigurierung wird nun die erstellte Keytab-Datei „asterix.keytab“ auf den Datenbank-Server typischerweise unter dem Pfad „\etc\

```

[libdefaults]
default_realm = DE.ORACLE.COM
clockskew = 300
[realms]
DE.ORACLE.COM = {
kdc = octopus.de.oracle.com
}
[domain_realm]
.de.oracle.com = DE.ORACLE.COM
de.oracle.com = DE.ORACLE.COM
    
```

Abbildung 3: Beispiel der krb5.conf-Einstellungen

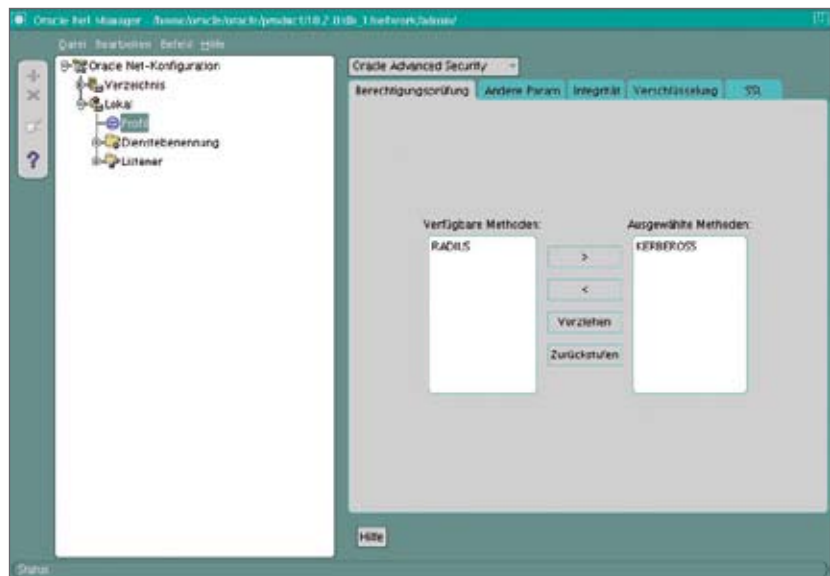


Abbildung 4: Kerberos-Authentisierung mit dem Net Manager einstellen (Methode)

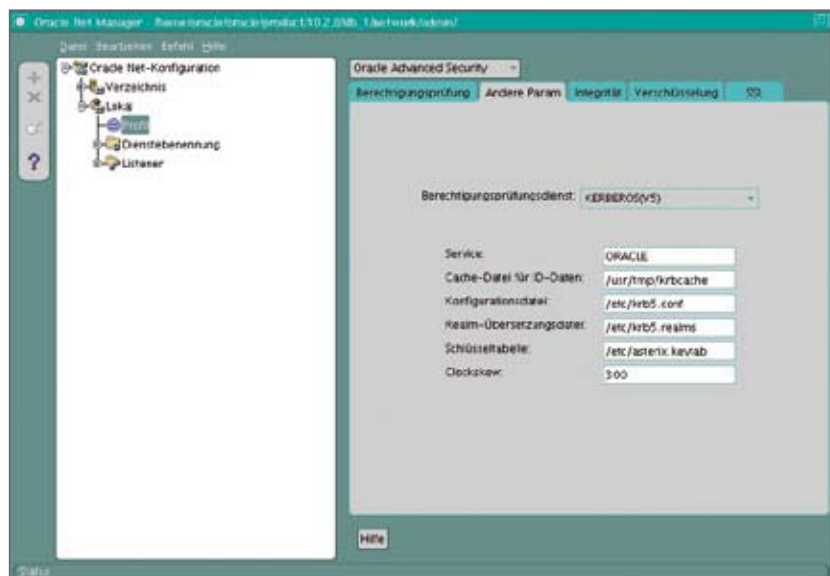
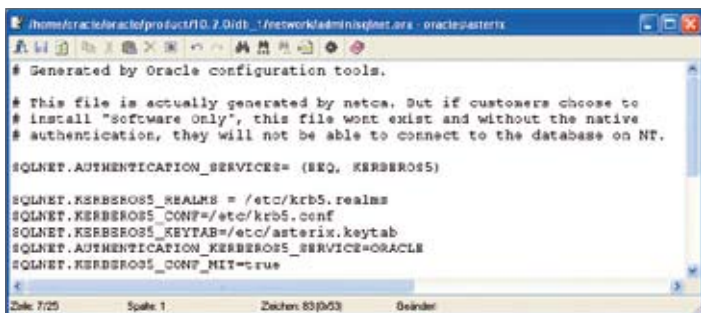


Abbildung 5: Kerberos-Authentisierung mit dem Net Manager einstellen (Parameter)



```

# Generated by Oracle configuration tools.

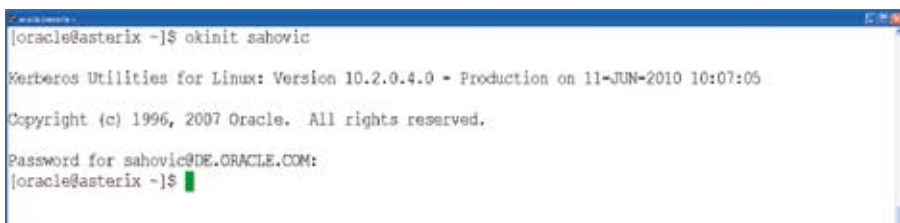
# This file is actually generated by netca. But if customers choose to
# install "software only", this file wont exist and without the native
# authentication, they will not be able to connect to the database on NT.

SQLNET.AUTHENTICATION_SERVICES= (SEC, KERBEROS5)

SQLNET.KERBEROS5_REALMS = /etc/krb5.realms
SQLNET.KERBEROS5_CONF=/etc/krb5.conf
SQLNET.KERBEROS5_KEYTAB=/etc/asterix.keytab
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE=ORACLE
SQLNET.KERBEROS5_CONF_MIT=true

```

Abbildung 6: Einstellungen in der sqlnet.ora



```

[oracle@asterix ~]$ okinit sahovic

Kerberos Utilities for Linux: Version 10.2.0.4.0 - Production on 11-JUN-2010 10:07:05

Copyright (c) 1996, 2007 Oracle. All rights reserved.

Password for sahovic@DE.ORACLE.COM:
[oracle@asterix ~]$

```

Abbildung 7: TGT-Ticket mit „okinit“ beziehen



```

[oracle@asterix ~]$ sqlplus /@10gee92

SQL*Plus: Release 10.2.0.4.0 - Production on Fri Jun 11 10:08:25 2010

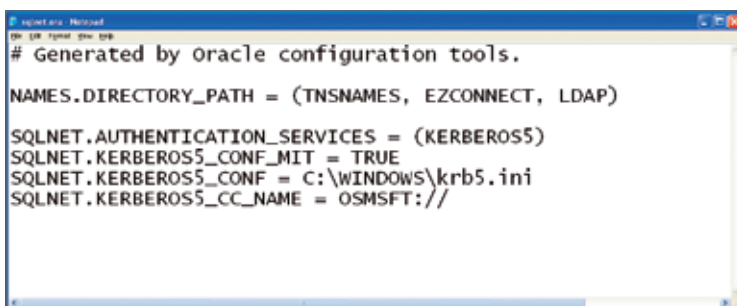
Copyright (c) 1992, 2007, Oracle. All Rights Reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.4.0 - Production
With the Partitioning, Oracle Label Security, Data Mining and Real Application Testing options

SQL> show user
USER is "SAHOVIC@DE.ORACLE.COM"
SQL>

```

Abbildung 8: Kerberos-Authentisierung an die Datenbank



```

# Generated by oracle configuration tools.

NAMES DIRECTORY_PATH = (TNSNAMES, EZCONNECT, LDAP)

SQLNET.AUTHENTICATION_SERVICES = (KERBEROS5)
SQLNET.KERBEROS5_CONF_MIT = TRUE
SQLNET.KERBEROS5_CONF = C:\WINDOWS\krb5.ini
SQLNET.KERBEROS5_CC_NAME = OSMSFT://

```

Abbildung 9: Client sqlnet.ora anpassen

asterix.keytab“ kopiert. Nun muss der Datenbank-Server so eingestellt werden, dass er weiß, wie er den Kerberos-Server anzufragen hat. Hierfür sind die Parameter in den Konfigurationsda-

teien „krb5.conf“ und „krb5.realms“ einzustellen (siehe Abbildung 3)

Es ist darauf zu achten, dass die Namensauflösung (DNS) funktioniert. Dazu nimmt man den Kerberos-Server

mit Hostnamen und IP in die HOSTS-Datei auf.

Damit der Datenbank-Server die eingestellten Kerberos-Parameter verwendet, muss zum Schluss die „sqlnet.ora“ angepasst werden (siehe Abbildung 6). Man kann diese Datei direkt verändern oder die Veränderungen mit dem Oracle Net Manager durchführen (siehe Abbildungen 4 und 5). Anschließend ist die Datenbank für die Kommunikation mit dem Kerberos-Server vorbereitet.

### Kerberos-Authentisierung mit der Oracle Datenbank testen

Für den ersten Test auf die Funktionsfähigkeit wird ein neuer Benutzer im Active Directory und in der Oracle Datenbank erstellt. Die Benutzer-Namen müssen identisch sein. Der Datenbank-Benutzer wird als „externally“ angelegt, da eine externe Authentisierung durchgeführt wird. Der Datenbank-Benutzer erhält zusätzliche Berechtigungen:

```

CREATE USER "SAHOVIC@DE.ORACLE.COM" IDENTIFIED EXTERNALLY;
GRANT CREATE SESSION, RESOURCE TO "SAHOVIC@DE.ORACLE.COM";

```

Dieser neue AD-Benutzer meldet sich an die Windows-Domäne an, bezieht ein Kerberos-TGT-Ticket und authentisiert sich damit (ohne erneute Anmeldung) an der Datenbank.

Für den ersten Test braucht man keinen Windows-Login durchführen, sondern kann das TGT-Ticket manuell beziehen. Das Oracle Tool „okinit“ holt ein TGT Ticket für den Benutzer „SAHOVIC“ vom Kerberos-Server ab. Das Kommando wird auf dem Datenbank-Server ausgeführt (siehe Abbildung 7).

Das TGT-Ticket entspricht der Funktion eines SSO-Cookies, das als Grundlage für die Erstellung von Session-Tickets dient. Das TGT-Ticket wird in der Credential-Cache-Datei abgelegt und kann mit dem Tool „oklist“ ausgelesen werden.

Das Kerberos-TGT-Ticket ist vorhanden und nun kann eine externe Authentisierung zur Datenbank durchge-

führt werden. Der Datenbank-Benutzer wird bei einem Datenbank-Login an den Kerberos-Server weitergeleitet, der dann das Session-Ticket für die Datenbank zurückliefert. Das bereits erstellte TGT-Ticket dient als Benutzer-Information beim Kerberos-Server für die Session-Ticket-Erstellung.

Die Anmeldung an die Datenbank erfolgt ohne Username/Password, da alle Informationen bereits über die Kerberos-Tickets bezogen wurden.

Abbildung 8 zeigt eine erfolgreiche Kerberos-Authentisierung gegen die Datenbank. Trotz fehlender Benutzerinformation weiß diese, dass der Benutzer „SAHOVIC@DE.ORACLE.COM“ angemeldet ist. Selbstverständlich ist dieser erste Test noch keine transparente Lösung für den Endbenutzer.

### Kerberos im Zusammenspiel

Ein typischer Arbeitstag eines Endbenutzers beginnt in der Regel mit dem Starten seines Rechners und der Anmeldung an eine Windows-Domäne. Bei diesem Anmeldeprozess kommt bereits eine Kerberos-Authentisierung zum Einsatz. Nach der erfolgreichen Anmeldung des Benutzers speichert der Windows-Client-Rechner sein eben erlangtes Kerberos-TGT-Ticket in verschlüsselter Form in dem Windows Credential Cache. Dieses Ticket kann man, wie bereits erwähnt, für die Anmeldung an die Oracle Datenbank nutzen und einen Kerberos-basierten Single-Sign-on realisieren.

### Windows konfigurieren

Der Windows-Client (hier XP oder Win2000 Workstation, Vista, Windows7) muss eine Oracle Client-Installation aufweisen. Als Minimum ist der InstantClient zu installieren. In der Installation befindet sich eine „sqlnet.ora“-Datei (\$ORACLE\_HOME/network/admin), die entsprechend für eine Kerberos-Nutzung anzupassen ist (siehe Abbildung 9).

Die Client-seitige „sqlnet.ora“ unterscheidet sich nur minimal von der „sqlnet.ora“ auf dem Datenbank-Server. Der Parameter „SQLNET.KERBEROS5\_CC\_NAME“ mit dem Wert des

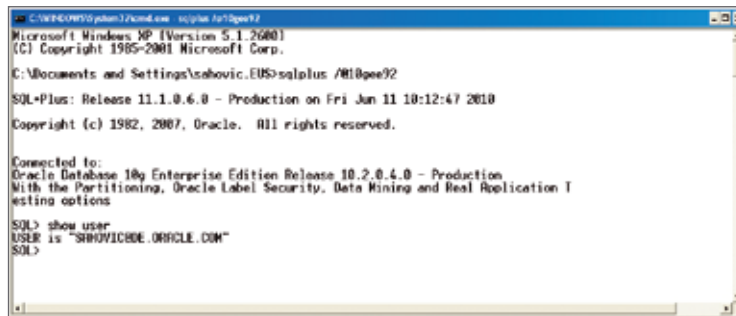


Abbildung 10: Login mit SQL\*Plus

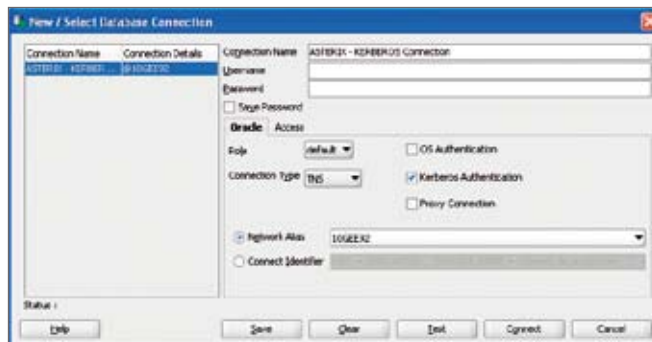


Abbildung 11: DB-Connection-Einstellung beim SQL Developer

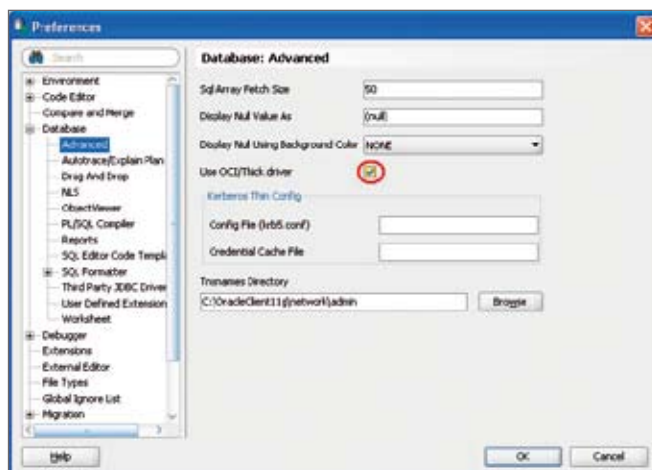


Abbildung 12: OCI im SQL Developer einstellen

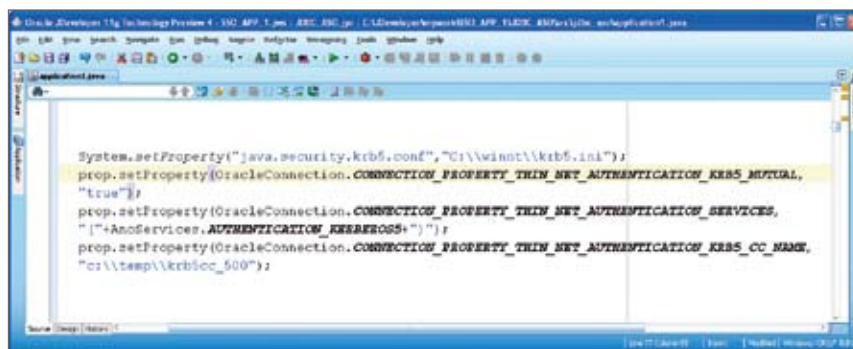


Abbildung 13: Einstellung für JDBC Thin im Java-Code

Credential Caches „OSMSFT://“ besagt, dass die Credential-Informationen aus dem Windows-Credential-Cache zu

holen sind. Zusätzlich muss die „krb5.conf“-Datei vom Datenbank-Server auf den Windows-Client kopiert und



in „krb5.ini“ umbenannt werden. Abschließend wird die clientseitige Datei „tnsnames.ora“ mit den Angaben des Datenbank-Servers angepasst.

### Funktionsweise überprüfen

Nachdem alle notwendigen Einstellungen am Client vorgenommen wurden, kann man eine Kerberos-Anmeldung an die Datenbank durchführen. Dazu kommt SQL\*Plus zur Anwendung (siehe Abbildung 10).

Die Kerberos-Anmeldung ohne Kennwort-Eingabe funktioniert. Sicherlich arbeiten nicht alle Benutzer mit SQL\*Plus, manche verwenden auch andere Datenbank-Applikationen wie SQL Developer.

### Kerberos-Datenbank-Anmeldung mit Oracle SQL Developer

Der Oracle SQL Developer unterstützt die Kerberos-Authentisierung seit der Version 1.5.3. Diese Authentisierung muss auch am SQL Developer eingestellt sein. Dafür wird bei der entsprechenden DB „Connection“ das Häkchen für „Kerberos“ gesetzt (siehe Abbildung 11).

Der SQL Developer muss eine OCI Connection nutzen. Diese stellt man in den Preferences ein (siehe Abbildung 12).

### Thin und Thick JDBC

Oracle SQL Developer unterstützt auch eine Kerberos-Authentisierung über JDBC Thin Connection. Dies wird jedoch erst ab einer Datenbank Version 11g R1 unterstützt. Abbildung 12 zeigt, dass für die Thin-Konfiguration zwei Eingabefelder (im Bereich „Kerberos Thin Config“) vorgesehen sind. Hier wird hinterlegt, wo sich das Kerberos-TGT-Ticket und der Kerberos-Server befinden. Die Datenbank-Connection-Details wiederum bleiben wie bei einer Kerberos OCI-Connection absolut gleich.

Um die Funktionstüchtigkeit einer Kerberos-Datenbank-Anmeldung über eine JDBC-Thin-Verbindung zu überprüfen, müsste man zuvor manuell ein Kerberos-TGT-Ticket mit dem „okinit“-

Tool beziehen. Dieses Ticket ist dann standardmäßig zehn Stunden gültig. Das heißt, man kann in dieser Zeit ohne erneute Anmeldung sicher arbeiten.

### Kerberos-Datenbank-Anmeldung mit Client/Server-Java-Applikationen

Wie mit Client/Server-Java-Applikationen eine Kerberos-Authentisierung verwendet wird, ist vom benutzten JDBC-Treiber abhängig. Bei einem JDBC-Thick-Treiber (OCI-Connection zur Datenbank) sieht der Connect-String wie folgt aus (ohne Benutzer Informationen):

```
jdbc:oracle:oci:@10gee92
```

Bei einer JDBC-Thin-Connection hingegen sind die vier Kerberos-Parameter der „sqlnet.ora“-Einstellung programmtechnisch zu übergeben (siehe Abbildung 9). Diese Parameter haben folgende Bedeutung:

1. Ort der Kerberos-Konfigurationsdatei (krb5.ini)
2. Authentisierungsart
3. Gegenseitige Authentisierung aktivieren
4. Pfad der Credential-Cache-Datei

Abbildung 13 zeigt den Code für das Setzen der Parameter in Java. Damit erfolgt die Kerberos-Anmeldung ebenso erfolgreich wie bei einer OCI-Connection.

### Fazit

Die Nutzung von Kerberos bietet eine erhöhte Sicherheit und eine vereinfachte Administration. Den Nachteil der immer noch bestehenden redundanten Benutzer (im Active Directory und in der Datenbank) kann man mit dem Datenbank-Feature „Enterprise User Security“ (alle Benutzer bleiben im Active Directory) umgehen. Damit lässt sich eine sichere und zentrale Benutzerverwaltung inklusive starker Authentisierung mit Kerberos und Enterprise User Security umsetzen. Die DOAG News Q4/2008 hat Enterprise User Security bereits mehrfach vorgestellt.

Abschließend sind drei Benefits wichtig:

- Kerberos-Authentisierung gehört in den Bereich der starken Authentisierungen. Demzufolge erreicht man eine höhere Sicherheit im Betrieb der Datenbanken und Datenbank-Applikationen.
- Zentrale Kennwort-Verwaltung für alle Datenbank-Benutzer durch den Kerberos-Server und sein Benutzer-Repository. Durch die zentrale Kennwort-Verwaltung definiert man an einer zentralen Stelle die Kennwort-Policies, die für alle beteiligten Datenbanken gültig sind.
- Basierend auf dem Kerberos-Single-Sign-on-Prinzip entfallen erneute Anmeldungen an den „Kerberos-enabled“-Datenbanken/-Datenbank-Applikationen. Es ist kein neues Single-Sign-on-Konstrukt, sondern man nutzt das vorhandene (für Windows typischerweise auf MS Active Directory basierend) und lässt die Datenbanken an diesem (Kerberos-) Single-Sign-on-Konstrukt als Dienst/Service partizipieren.

### Weitere Informationen

Kerberos-Erklärung: <http://tinyurl.com/wikipedia-kerberos>

Kerberos unter Windows: <http://tinyurl.com/kerberos-unter-windows>

Einführung in Oracle Advanced Security Option: <http://tinyurl.com/einfuehrung-in-aso>

Kerberos-Authentifizierung mit der Datenbank 11g R2 konfigurieren: <http://tinyurl.com/kerberos-mit-db11gr2>

Oracle Support Note ID 331252.1: Configuring Oracle Advanced Security Option (ASO) with Microsoft Windows Server 2003 Active Directory Kerberos KDC

Oracle Support Note ID 213899.1: Configuring Kerberos Authentication using Oracle on UNIX with MIT Kerberos

Oracle Support Note ID 577738.1: Step by Step Guide for 10g EUS Kerberos Authentication

Oracle Support Note ID 458219.1: How To Configure Enterprise User Security for Kerberos Authentication

### Kontakt:

Suvad Sahovic

[suvad.sahovic@oracle.com](mailto:suvad.sahovic@oracle.com)

Carsten Mützlitz

[carsten.muetzlitz@oracle.com](mailto:carsten.muetzlitz@oracle.com)

# Wo sind unsere Schlüssel?

Christian Kirsch, Thales e-Security

**Transparent Data Encryption (TDE) von Oracle 11g ist ein wichtiger Baustein für das Erreichen von sicherheitsrelevanten, gesetzlichen Compliance-Vorgaben. Dieser Artikel zeigt Sicherheitsbeauftragten und Administratoren, wie sie das richtige Verschlüsselungskonzept wählen, die Sicherheit erhöhen und Betriebskosten für das besonders wichtige Schlüssel-Management senken.**

Der Schutz von persönlichen Daten wird in Deutschland immer wichtiger. 2009 verabschiedete der Deutsche Bundestag die Novelle II des Bundesdatenschutzgesetzes (BDSG), das Unternehmen verpflichtet, sich öffentlich zu Datenpannen zu bekennen. In den USA führten ähnliche Gesetzgebungen – wie die California Senate Bill 1386 – zu einer deutlichen Straffung der Sicherheitsmaßnahmen von Unternehmen und Behörden. Mit der Änderung des BDSGs wird dieser Trend nun in Deutschland spürbar. Verschlüsselung hilft bei der Compliance mit dem BDSG, da Unternehmen keine Datenpanne melden müssen, wenn die verwendeten Daten verschlüsselt und damit unlesbar waren.

## Datenbank-Verschlüsselung durch Drittanbieter

Der Markt für Datenbank-Verschlüsselung ist grundsätzlich in zwei Lager geteilt: native Verschlüsselung durch Datenbank-Hersteller selbst oder durch Drittanbieter. Traditionell gibt es externe Lösungen, die Verschlüsselung für bestehende Datenbanken nachrüsten. Diese sind entweder individuell programmierte Lösungen, die Daten üblicherweise innerhalb der Anwendung verschlüsseln und diese anschließend in die Datenbank schreiben, oder Lösungen von Drittanbietern für den Massenmarkt.

Während einige dieser Lösungen mehrere Datenbankanbieter unterstützen, kann deren Implementierung und Wartung sehr kostenintensiv und aufwändig sein, da sie für die Anwendungen nicht transparent sind. Mit anderen Worten: Anwendungen, die auf verschlüsselte Datenbanken zugreifen,

müssen normalerweise mit Verschlüsselungsfähigkeiten nachgerüstet werden, was nicht in jedem Fall möglich ist.

Seitdem Datenbank-Anbieter wie Oracle integrierte Add-ons für Datenbank-Verschlüsselung auf den Markt gebracht haben, führen nur noch wenige Unternehmen eine Verschlüsselungslösung von Drittanbietern ein, da diese teurer und schwieriger zu warten sind. Es gibt auch keine Garantie dafür, dass die nächste Version der Datenbank noch mit der Verschlüsselungslösung kompatibel ist.

## Transparent Data Encryption

Oracle bietet für Datenbank-Verschlüsselung eine Gruppe von Funktionen unter dem Namen „Transparent Data Encryption“ (TDE), die mit der Option „Advanced Security“ ausgeliefert wird. Diese ermöglicht es Unternehmen, ihre Datenbanken mit Oracle-Funktionen zu verschlüsseln.

Gegenüber den Lösungen von Drittanbietern gibt TDE den Unternehmen Zukunftssicherheit bei Upgrades, da die Funktionen vom Datenbank-Anbieter und nicht von einem Dritten angeboten werden. TDE wird daher als moderner Ansatz für das Problem der Datenbank-Verschlüsselung angesehen. Da die Daten verschlüsselt gespeichert werden, sind auch Backups von Datenbanken verschlüsselt und stellen so keine Angriffsfläche für Datenlecks dar.

## Spalten- und Tablespace-Verschlüsselung

Oracle bietet zwei Varianten von TDE an: Spalten- und Tablespace-Verschlüsselung. Mit der Spalten-Verschlüsselung können Organisationen sehr gezielt ge-

wisse Arten von Daten verschlüsseln. Das setzt voraus, dass die Organisation die Daten vorher klassifiziert hat und weiß, welche Spalten in der Datenbank sensible Daten enthalten. Um ganze Tabellen zu verschlüsseln, kann man die Spalten-Verschlüsselung auf alle Spalten einer Tabelle anwenden. Die Alternative dazu stellt die Tablespace-Verschlüsselung dar, die Tablespaces mit allen enthaltenen Tabellen verschlüsselt. Sie erfordert keine Klassifizierung der Daten, da alle Daten innerhalb des Tablespace verschlüsselt werden und kann damit für bestimmte Situationen die bessere Wahl sein.

## Aufgepasst:

### Schlüssel müssen richtig geschützt sein

Die Verschlüsselung der Daten ist jedoch nur die halbe Miete, denn Verschlüsselung ist nur so sicher wie die Verwaltung und Aufbewahrung der Schlüssel. Werden bei einer Datenpanne nämlich nicht nur die verschlüsselten Daten, sondern auch die Schlüssel kompromittiert, ist der Schutz unwirksam, da die Daten einfach entschlüsselt werden können.

Aus diesem Grund empfiehlt sich für Unternehmen bei Verschlüsselung auf Server-Ebene – also auch bei der Datenbank-Verschlüsselung – der Einsatz von Hardware-Sicherheitsmodulen (HSMs). Ein HSM ist eine dedizierte Appliance, die Schlüssel am besten schützt und darüber hinaus automatisch verwaltet. Oracle bietet ab Version 11g die Integration von Hardware-Sicherheitsmodulen an, um die Schlüssel der Datenbank optimal zu verwalten und zu schützen. Dies bietet entscheidende Vorteile für Betrieb, Kosten, Sicherheit und Einhaltung der Compliance-Vorgaben.

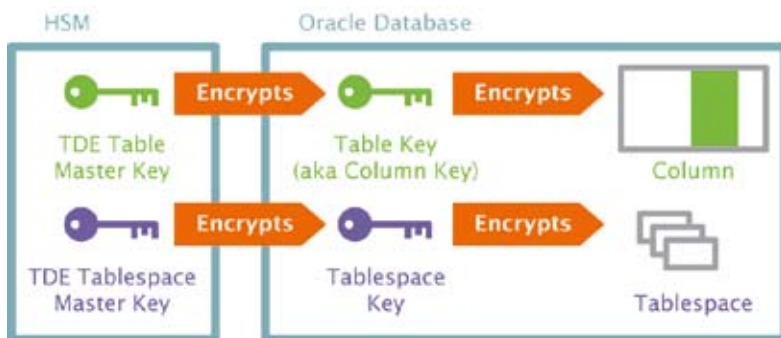


Abbildung 1: Hardware-Sicherheitsmodule (HSMs) schützen die Master Keys der Oracle-Transparent-Data-Encryption-Architektur (TDE-Architektur)

### HSM in der Praxis

Setzt ein Unternehmen eine große Anzahl von Datenbanken ein, deren Schlüssel verwaltet werden müssen, so können HSMs die Betriebskosten deutlich reduzieren, da die Schlüssel zentralisiert im HSM verwaltet werden. Dies ist besonders dann relevant, wenn Unternehmen aus Gründen der Sicherheit und Compliance die Schlüssel mehrmals im Jahr wechseln. Beispielsweise schreibt dies der Payment Card Industry Data Security Standard (PCI DSS) vor, den alle Unternehmen erfüllen müssen, die Kreditkartendaten verarbeiten.

Gute Governance beinhaltet eine Gewaltenteilung, die sicherstellt, dass kein einzelner Mitarbeiter das System missbrauchen kann. Einige HSMs, zum Beispiel die nShield-Produkte von Thales/nCipher, bieten ein Zwei- oder Mehr-Augen-Prinzip, das die Verwendung der Schlüssel reglementiert. So können HSMs beispielsweise eine Mindestanzahl an Smart Cards und / oder Passwörtern von Administratoren vorgeben, um sicherheitsrelevante Aufgaben auszuführen. Dies kann von der Organisation definiert werden, die das HSM zur Erfüllung von Sicherheitsrichtlinien einsetzt. Ohne dieses sogenannte „Quorum“ kommt kein einzelner Mitarbeiter an die verschlüsselten Daten. Ob, wann und wie diese Funktion eingesetzt wird, liegt im Ermessen der Sicherheits- und Compliance-Beauftragten und muss im Einzelfall entschieden und entsprechend konfiguriert werden.

HSMs sichern Schlüssel auch physisch durch besonders gesicherte Hardware, die gegen Öffnen und Aufbohren

geschützt ist. Hersteller von HSMs benötigen diese Sicherheitsfunktionen, um eine Zertifizierung für „FIPS 140-2“ oder „Common Criteria“ zu erreichen, die von vielen Unternehmen als Sicherheits-Benchmark gefordert wird. Für den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definierten Grundschutz ist beispielsweise ein mit Common Criteria zertifiziertes HSM notwendig.

HSMs sind in der Sicherheit und Revision sehr beliebt, da sie klare Richtlinien für die Verwendung von Schlüsseln durchsetzen. Bei verschlüsselten Datenbanken verhindern sie zum Beispiel, dass lesbare Kopien von Schlüsseln unbewusst auf Backups oder geklonten virtuellen Maschinen verbreitet werden. Da die Schlüssel niemals das HSM verlassen, kann bei einem Audit klar bewiesen werden, dass nur autorisierte Kopien der Schlüssel existieren.

Als Best Practice für Sicherheit bieten HSMs maximalen Schutz und verbessern so die Unternehmens- und Systemsicherheit. Sie schützen das geistige Eigentum, da das Schlüsselmaterial auch dann geschützt ist, wenn das Betriebssystem oder die Anwendung eine Sicherheitslücke aufweisen.

### Fazit

Oracle bietet mit TDE als Teil der Advanced Security Option eine einfache und zukunftssichere Methode zur Verschlüsselung von Personen-, Unternehmens-, und Anwendungsdaten an, die sich flexibel umsetzen lässt. Vom Datenbank-Hersteller angebotene Verschlüsselungsmethoden werden gegenüber den Lösungen von Drittanbietern

als die eindeutig zukunftssichere Technik angesehen, da sie eine bessere Integration ermöglichen.

Jedoch stellt die Verwaltung und Aufbewahrung des Schlüsselmaterials ein bedeutendes Puzzlestück für den Erfolg dieser Verschlüsselungslösung bei Datenbanken dar. Hardware-Sicherheitsmodule sind ein zentraler Teil dessen und bieten entscheidende Vorteile im Betrieb, bei Sicherheit und Compliance-Audits. Sie zentralisieren und automatisieren die Verwaltung von Schlüsselmaterial, führen das gesamte Schlüsselmaterial auf einem Gerät zusammen und senken dadurch die betrieblichen Kosten. HSMs erhöhen zudem die Skalierbarkeit durch die Möglichkeit zur Verwaltung hunderter Datenbanken auf einmal und bieten kurz- und langfristige Wiederherstellung von Daten.

HSMs steigern die IT-Sicherheit im Unternehmen, da sie die Hauptschlüssel durch nicht angreifbare Hardware schützen und besonders sensiblen Anwendungscodes in ihrem geschützten Bereich ablaufen lassen können. Dadurch liefern sie eine wartungsfreie, deutlich höhere Sicherheit als softwarebasierte Lösungen. Verbesserte betriebliche Kontrollmöglichkeiten (engl. internal control) wie die Trennung von Zuständigkeiten oder die Einführung eines Mehr-Augen-Prinzips für sicherheitsrelevante Aufgaben minimieren die Gefahr des Missbrauchs.

Da HSMs als Best Practice für Sicherheit anerkannt sind, reduzieren sie die Governance-, Risk- und Compliance-Aufwendungen (GRC), nicht nur durch zentrale und automatische Verwaltung von Schlüsselmaterial und Beschleunigung des Schlüsselwechsels, sondern auch durch eine vereinfachte Revision. Schließlich können HSMs eine Lösung mit internationalen Sicherheitszertifizierungen wie „FIPS 140-2“ und „Common Criteria“ ausstatten. Besonders Unternehmen, die internationale Compliance-Anforderungen erfüllen müssen, haben diese neuen Technologien bereits angenommen.

### Kontakt:

Christian Kirsch  
christian.kirsch@thalessec.com

# Die Übernahmen von Oracle seit 2005

Oracle stärkt nach eigenen Aussagen durch den Erwerb strategischer Unternehmen sein Produkt-Portfolio, beschleunigt die Innovationstätigkeit und kann damit schneller auf die Kundenbedürfnisse eingehen. Zudem profitieren laut Oracle die Kunden von einem erweiterten Partner-Netzwerk.

Ein zentrales Element in der Fusions- und Übernahme-Philosophie von Oracle ist – neben den Renditezielen und der Wertschöpfung für die Anteilseigner – das stetige und zuverlässige Engagement für Kundenservice und Produktsupport.

Die DOAG verfolgt diese Akquisitionen mit großem Interesse. Positiv wird dabei die Erweiterung des Produkt-Portfolios gesehen. Kritischer betrachten die Anwender eher jene Zukäufe, die zu einer Produkt-Überlappung führen. Hier sieht die DOAG bei Oracle

die Aufgabe, den Support von auslaufenden Produkten zu gewährleisten sowie die Anwender bei Migration auf das neue strategische Produkt-Spektrum unterstützen, sowohl technisch als auch lizenzseitig. Nachfolgend eine Übersicht aller Akquisitionen:

## Datenbank

- TimesTen (Juni 2005)
- TripleHop (Juni 2005)
- Innobase (Oktober 2005)
- Sleepycat (Februar 2006)
- Moniforce (Dezember 2007)
- e-Test (acquired from Empirix) (März 2008)
- mValent (Februar 2009)
- Secerno (Mai 2010)

## Middleware

- Oblix (März 2005)
- Context Media (Juli 2005)
- OctetString (November 2005)
- Thor Technologies (November 2005)
- Sigma Dynamics (August 2006)
- Sunopsis (Oktober 2006)
- Stellent (November 2006)
- Tangosol (März 2007)
- Bharosa (Juli 2007)
- Bridgestream (September 2007)
- BEA (Januar 2008)
- Captovation (Januar 2008)
- ClearApp (September 2008)
- Tacit Software (November 2008)
- Java (April 2009)
- GoldenGate (Juli 2009)
- HyperRoll (September 2009)
- AmberPoint (Februar 2010)

## Applications

- PeopleSoft (Januar 2005)
- TempoSoft (Dezember 2005)
- Siebel (Januar 2006)
- Telephony@Work (Juni 2006)
- Hyperion (März 2007)
- AppForge (April 2007)
- Agile (Mai 2007)
- Interlace Systems (Oktober 2007)
- LogicalApps (Oktober 2007)
- Global Knowledge Software (Juli 2008)
- Haley (Oktober 2008)
- Primavera (Oktober 2008)
- Silver Creek Systems (Januar 2010)
- Market2Lead (Mai 2010)

## Server und Speichersysteme

- Sun (April 2009)
- Virtual Iron (Mai 2009)

Weitere Informationen zu den einzelnen Unternehmen unter <http://www.oracle.com/us/corporate/acquisitions/index.html>

## Industrielösungen

- Retek (April 2005)
- ProfitLogic (Juli 2005)
- i-flex (August 2005)
- G-Log (September 2005)
- 360Commerce (Januar 2006)
- HotSip (Februar 2006)
- Net4Call (April 2006)
- Portal Software (April 2006)
- Demantra (Juni 2006)
- MetaSolv Software (Oktober 2006)
- SPL WorldGroup (November 2006)
- LODESTAR (April 2007)
- Agile (Mai 2007)
- Netsure Telecom Limited (September 2007)
- AdminServer (Mai 2008)
- Skywire Software (Juni 2008)
- Primavera (Oktober 2008)
- Advanced Visual Technology (Oktober 2008)
- Relsys (März 2009)
- Conformia Software (Juni 2009)
- Sophoi (Oktober 2009)
- Convergin (Februar 2010)
- Phase Forward (April 2010, noch nicht abgeschlossen)
- eServGlobal's Universal Service Platform (Mai 2010, noch nicht abgeschlossen)

# Oracle und die Compliance gemäß ISO 27001

Dr. Thomas Störtkuhl und Hans Wagner, Secaron AG

Dieser Artikel zeigt den Aufbau und Betrieb eines Information Security Management Systems (ISMS) nach dem Standard ISO 27001 mit seinen Hauptelementen und Controls. Der Schwerpunkt liegt jedoch in der Frage, in welcher Weise welche Oracle-Produkte bei der Erfüllung der vom Standard geforderten Controls unterstützen.

Ein Information Security Management System (ISMS) muss folgende wesentliche Elemente aufweisen:

- Management Commitment
- Organisationsstruktur mit definierten Rollen und Verantwortlichkeiten
- kontinuierlicher Verbesserungsprozess
- Risikomanagement
- Umsetzung der vom Standard geforderten Controls

Diese Elemente und alle wesentlichen Aktivitäten sind zu dokumentieren, um das Funktionieren des Management-Systems belegen zu können. Zudem muss das ISMS risikoorientiert aufgebaut sein.

## Elemente des ISMS

Für den Aufbau und den Betrieb eines ISMS ist die Unterstützung des Top-Managements unabdingbar. Meist wird das Management Commitment durch eine Security Policy deutlich zum Ausdruck gebracht. In dieser sind auch die Grundzüge des ISMS mit Organisation, Prozessen und zugehörigen Verantwortlichkeiten definiert. Häufig wird zudem eine Dokumenten-Hierarchie eingeführt.

Die Sicherheitsrichtlinien definieren dabei die grundlegenden Sicherheitsanforderungen des Unternehmens, die dann in den Sicherheitskonzepten sowohl technisch als auch organisatorisch konkretisiert werden. Zur Realisierung eines kontinuierlichen Verbesserungsprozesses werden interne Audits und sogenannte „Management Reviews“ eingeführt. Durch regelmäßige interne Audits wird kontrolliert, ob

die umgesetzten Maßnahmen des ISMS greifen und ein angemessenes Sicherheitsniveau gewährleisten. Interne Audits können sich dabei auf das gesamte ISMS beziehen oder auch nur auf Teile davon. Das Management des Unternehmens wiederum kontrolliert die Funktionsfähigkeit des ISMS insgesamt aus Managementsicht. Insbesondere wird beurteilt, ob die Sicherheitsziele und das angestrebte Sicherheitsniveau im Einklang stehen mit den Geschäftszielen des Unternehmens (Business Alignment). Zur Durchführung des Management Reviews lässt sich die Unternehmensführung durch den für das ISMS Verantwortlichen einen Sicherheitsbericht vorlegen, der insbesondere die wesentlichen Risiken, weitere Kennzahlen bezüglich Informationssicherheit (den Reifegrad von Prozessen wie Change Management etc.), die umgesetzten Maßnahmen sowie Vorhaben ausweist. Das Management prüft diesen Bericht, akzeptiert Risiken ausdrücklich oder ordnet weitere Verbesserungen an. Zudem stellt

das Management für die Aufgaben des ISMS die nötigen Ressourcen (Budget, Mitarbeiter) bereit. Um risikobasiert arbeiten zu können, muss ein Risikomanagement etabliert werden, durch das in einem definierten Vorgehen Risiken identifiziert, bewertet, behandelt und kontrolliert werden. Auf der Grundlage der Risikoanalyse können dann Maßnahmen, beispielsweise zur Risikoreduktion oder -vermeidung, identifiziert und priorisiert werden. Diese Maßnahmen erfüllen die im ISO 27001 Standard geforderten Controls und sollen der Gewährleistung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit dienen.

## Controls des ISO 27001

Die Zugriffssteuerung mit Benutzer- und Rechtevergabe spielt hierbei eine zentrale Rolle bei der Gewährleistung der Informationssicherheit. Dies wird in Abbildung 1 dadurch wiedergegeben, dass das Control A.11 mit den Controls A.8 bis A.10 und A.12 in

ISMS Requirements (Chapter 4.8)			
A.5 – Security Policy			
A.6 – Organization of Information Security			
A.7 – Asset Management			
A.8 – Human Resources Security	A.9 – Physical and Environment Security	A.10 – Communication and Operations Management	A.12 – Information Systems acquisition, development and maintenance
A.11 – Access Control			
A.13 – Information Security Incident Management			
A.14 – Business Continuity Management			
A.15 – Compliance			

Abbildung 1: Controls des ISO 27001

wechselseitiger Beziehung steht (siehe Pfeile).

### Gewährleistung der Schutzziele

Die klassischen Schutzziele der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Häufig werden auch zusätzlich die Schutzziele Nachvollziehbarkeit und Authentizität gesehen. Es stand nie zur Diskussion, dass Verfügbarkeit ein Merkmal von Sicherheit ist. Aufgrund der zunehmenden Wirtschaftskriminalität im Bereich der Informationstechnologie gewinnen in letzter Zeit aber gerade die Merkmale Vertraulichkeit, Integrität, Authentizität und Nachvollziehbarkeit immer mehr an Bedeutung und werden deshalb in diesem Artikel vorrangig behandelt.

Die Integrität von Informationen zu schützen, ist eine große Herausforderung. Wesentlicher Bestandteil der notwendigen Maßnahmen ist die technische Unterstützung des Controls „A.11“ und hier insbesondere die Themen „User Registrierung“, „Rechte-Management“ sowie „Passwort-Management“ aus dem Teilbereich „A.11.2 User Access Management“, um nicht autorisierten Zugriff zu vermeiden und Berechtigungen nach dem Minimalprinzip zu vergeben. Die technische Ausprägung dieses Prinzips ist etwa durch ein Identity Management, Single Sign-on oder eventuell starke Authentisierung gegeben. Unterstützend hierzu ist auch eine passive Maßnahme – die Protokollierung – erforderlich, die Bestandteil des Controls „A.15“ ist. Hiermit erreicht man die Nachvollziehbarkeit bei Integritätsverletzungen und hebt somit die Hemmschwelle, Information vorsätzlich zu manipulieren.

Um bei einer Integritätsverletzung die ursprünglichen Daten wiederherstellen zu können, ist ein Archivierungskonzept erforderlich, das den fachlichen Workflow berücksichtigt. Die Erkennung der Integritätsverletzung kann mithilfe des Archivs und entsprechenden automatischen Prüfprozessen erfolgen, aber auch durch digitale Signatur.

Die Vertraulichkeit von Informationen – wir sprechen aktuell von Data

Leakage Prevention oder Information Leakage Prevention – benötigt als grundlegende Voraussetzung ebenfalls eine Umsetzung des Controls „A.11“ (siehe Integrität) und sollte darüber hinaus in Abhängigkeit des Bedarfs weitere technische Maßnahmen berücksichtigen:

- Software zur Prüfung von Content an Schnittstellen wie Netzwerkübergängen und Schnittstellen zu mobilen Datenträgern (DLP/ILP Software, A.12.5.4, A.11.2.2)
- Information Rights Management (A.12.5.4, A.11.2.2)
- Verschlüsselung der Informationen, sowohl auf dem Kommunikationskanal (A.10.8.4) als auf den Datenspeichern (A15.1.4, A.11.2.2)

Oracle unterstützt die Anforderung der Controls aus ISO 27001 sowohl mit selbstständigen Produkten als auch mit sogenannten „Optionen“ und „Features“ zu diesen Oracle-Produkten. Dies wird im Folgenden detaillierter dargestellt.

### Benutzer- und Rechte-Management-Prozess

Das User Access Management (A.11.2) wird im Wesentlichen mit dem Oracle Identity Management (IDM) technisch unterstützt. Oracle versteht darunter auch Komponenten wie Single Sign-on (A.11.2.3), Passwort-Synchronisierung (A.11.2.3), Zertifikatsverwaltung und -ausstellung (A.12.3.2) für starke Authentisierung (A.11.2.3), Federation Services (A.11.2.1-3) sowie Provisionierungs- und Authentisierungsschnittstellen zu anderen Systemen. Weitere Bestandteile sind ein Workflow-System, um den Beantragungsprozess von Accounts und Berechtigungen – angepasst an die Belange des Unternehmens – auf elektronischem Weg zu unterstützen, sowie die Protokollierung des Prozesses, um die Nachvollziehbarkeit sicherzustellen, die in Control A.11.2.4 gefordert ist. Diese Workflow-Komponente unterstützt ganz wesentlich darin, ein funktionierendes Identity Management im Unternehmen zu etablieren, so dass zum Beispiel unbe-

nutzte Accounts (sogenannte „orphan accounts“) erst gar nicht entstehen. Natürlich unterstützt Oracle eine Anbindung an HR-Systeme, um eine redundante Datenhaltung zu vermeiden.

### Authentizität

Identitätsdiebstahl wird zu einer wesentlichen Herausforderung in der heutigen vernetzten Welt. Eigene Begriffe für den Identitätsdiebstahl wie „Phishing“ und „Shoulder Surfing“ werden geprägt. Es ist wohl unbestritten, dass User-Id und Passwort als Authentisierungsmethode für den Zugang zu Daten mit höchsten Anforderungen an Vertraulichkeit und Integrität nicht ausreichen. Auch hier wird man mit dem Einsatz von Mechanismen der Oracle-Advanced-Security-Option im Bereich der Datenbank unterstützt. Alle gängigen Authentisierungsmethoden können damit eingebunden werden und so ist etwa der Einsatz einer zertifikatsbasierten Anmeldung an der Oracle Datenbank problemlos möglich. Bei Web-Applikationen ist der Einsatz von SSL und beidseitiger Authentisierung mit Zertifikaten in einfacher Weise möglich, da das Oracle IDM ein Zertifikatsmanagement enthält.

Sind jedoch User-Id und Passwort aufgrund der Anforderungen ausreichend, so kann eine Passwort-Policy bei allen Oracle-Produkten konfiguriert beziehungsweise durch eigene Module ergänzt werden. Der Mitarbeiter kann damit nicht mehr gegen bestehende Passwort-Policies verstoßen, die gemäß Control A.11.3.1 festzulegen und durch die Anwender zu beachten sind. Am Beispiel der Oracle Datenbank wird die Passwort-Policy durch Konfiguration erzwungen (siehe Abbildung 3). Hierzu ist die Prüfung der Passwort-Policy mit dem Script UTLPLDMP.SQL anzulegen.

Die Passwort-Policy wird an das Oracle-Profil „<name>“ gebunden und damit für Benutzer sichergestellt, die dieses Profil zugewiesen bekommen. Für unterschiedliche Zwecke beziehungsweise Benutzer können verschiedene Profile angelegt sein. Dies ist zu beachten beim Einsatz von sogenann-

Parameter	Wert	Beschreibung
SEC_CASE_SENSITIVE_LOGON	TRUE	Passwörter sind casesensitiv
SEC_MAX_FAILED_LOGIN_ATTEMPTS	3	Anzahl der fehlgeschlagenen Anmeldungen bis der Account beim Zugriff über OCI gesperrt wird
FAILED_LOGIN_ATTEMPTS	3	Anzahl der fehlgeschlagenen Anmeldungen bis der Account gesperrt wird
PASSWORD_GRACE_TIME	7	Grace Period für ablaufende Passwörter. Der Account wird nach Ablauf gesperrt
PASSWORD_LIFE_TIME	180	Gültigkeitszeitraum für Passwörter
PASSWORD_LOCK_TIME	UNLIMITED	Gesperrte Accounts müssen vom Administrator zurückgesetzt werden
PASSWORD_REUSE_MAX	10	Ein Passwort kann frühestens nach 10 Änderungen wiederverwendet werden, jedoch nicht vor PASSWORD_REUSE_TIME
PASSWORD_REUSE_TIME	30	Ein Passwort kann frühestens nach 30 Tagen wiederverwendet werden. Es muss jedoch auch die Beschränkung PASSWORD_REUSE_MAX berücksichtigt werden

Abbildung 3: Passwort-Policy durch Konfiguration

ten „technischen Accounts“, die von Applikationsservern, automatisch gestarteten Scripts etc. benutzt werden. Dazu ein Beispiel für das Anlegen eines Profils:

```
CREATE PROFILE pw_pol LIMIT
  FAILED_LOGIN_ATTEMPTS 3
  PASSWORD_LOCK_TIME 30
  PASSWORD_LIFE_TIME 180;
ALTER USER <username> PROFILE
pw_pol;
```

Bei Bedarf können weitere Funktionen hinzugefügt werden. Dann ist die Funktion vergleichbar dem Script UTL-PWDMG.SQL anzulegen und dem gewünschten Profil zuzuweisen. Auch dazu ein Beispiel:

```
ALTER PROFILE pw_pol LIMIT
  PASSWORD_VERIFY_FUNCTION ve-
rify_function_pw_pol;
```

### Access Control auf Applikationen und Informationen

Für die Umsetzung der Anforderungen aus Control A.11.6 (Application and Information Access Control) gibt es zahlreiche Varianten in Abhängigkeit der Zugriffsebene und der qualitativen Anforderungen des jeweiligen Unternehmens.

Applikationen: Oracle IDM stellt sicher, dass ausschließlich autorisierte Benutzer auf die Applikationen zugreifen können, sofern sie an das Oracle IDM angebunden sind. Bei Einsatz des Oracle WebLogic Portals lässt sich der Zugriff auf die Applikationen über Portalrollen steuern und in einer SOA stehen die üblichen Features für die Zugriffssteuerung auf Web Services zur Verfügung.

Informationen: Auf Betriebssystemebene können die Daten der Datenbank mithilfe der Oracle Transparent Data Encryption verschlüsselt werden, somit wird auch der Zugriff auf dieser Ebene unterbunden. Selbst wenn eine Festplatte einmal nicht gemäß der Vorgaben des Benutzers bei der Entsorgung zerstört wird, bleibt die Vertraulichkeit der Daten gewahrt – insbesondere wenn man die Schlüssel für die Verschlüsselung in einem sogenannten „Hardware Security Module“ (HSM) sicher aufbewahrt. Sollten dennoch Daten abhanden kommen, haben die Betriebssystem-Administratoren gute Argumente, dass der Benutzer es nicht war. Denn wer die Daten nicht kennt, kann sie auch nicht weitergeben.

Auf Datenbank-Ebene lässt sich mit Oracle Database Vault der Zugriff auf fachliche Daten auf die fachlichen Benutzer einschränken. Damit reduziert man in Zeiten von Outsourcing, Cloud

Computing, Remote Support, Remote Administration etc. den Zugriff auf Informationen von Personen, die einem bekannt sind und die den Zugriff auch wirklich benötigen.

Manchmal ist die Anforderung komplexer, als es mit der üblichen Vergabe von Berechtigungen über Rollen und Gruppen möglich ist. Auch hier bietet Oracle beim Betrieb von Datenbanken Unterstützung. Mit Virtual Private Database und Label Security stehen Mechanismen zur Verfügung, mit denen man den Zugriff auf klassifizierte Daten (geheim, vertraulich, intern, öffentlich) einfach verwalten kann. Es ist somit möglich, dass logisch zusammengehörende Daten in einer Tabelle verbleiben können und trotzdem der Zugriff für unterschiedliche Personen in Abhängigkeit der Klassifizierung geregelt ist.

Sollen Informationen in Form von Dokumenten unabhängig vom Ablageort und dem Kommunikationsweg in Bezug auf Vertraulichkeit und Integrität geschützt werden, kann dies mit dem Oracle Information Rights Management (IRM) erfolgen, auch wenn man keine Oracle Datenbank im Einsatz hat. Oracle IRM ermöglicht, die Vertraulichkeit der Dokumente auch außerhalb der Datenbank durchzusetzen und dies auch über Unternehmensgrenzen hinweg, falls man Partner in die Plattform integriert.

### Access Control auf Betriebssystem-Ebene

Das oben erwähnte Oracle Identity Management unterstützt auch Anforderungen aus dem Control A.11.5 (Operating System Access Control), da es Konnektoren zu üblichen Betriebssystemen gibt. Dies ist besonders hervorzuheben, da gerade der Zugriff bei Servern auf Betriebssystemebene mit umfangreichen Berechtigungen einhergeht und ein zeitnahes Management der Accounts wichtig ist.

### Access Control auf Netzwerk-Ebene

Selbst Anforderungen aus dem Control A.11.4.1 (Network Access Control) können durch Funktionen von Oracle unterstützt und ergänzt werden. Im

einfachsten Fall lässt sich der Listener der Oracle Datenbank einschränken, so dass er nur Zugriffe von bestimmten IP-Adressen erlaubt. Eine ebenfalls einfache, jedoch flexiblere Lösung ist hier der Einsatz von Logon Triggern und Secure Application Roles. Die Anmeldung eines technischen Accounts kann man mit einem Logon Trigger überwachen und auswerten. Kommt die Anmeldung von einem bekannten Rechner (zum Beispiel dem Applikationsserver) und Programm, werden die benötigten Berechtigungen über die Secure Application Role zugeordnet, andernfalls nicht.

### Kommunikation

Eine sichere Kommunikation beim Zugriff auf die Datenbank mit Oracle-Protokollen gemäß Control „A.10“ (Communication and Operations Management) lässt sich mit Oracle Advanced Security sicherstellen. Es beinhaltet unter anderem die Verschlüsselung des Kommunikationskanals mit Secure Socket Layer (SSL). Damit stellt man sicher, dass die Daten im Netzwerk nicht abgehört werden können und einem gleich hochwertigem Schutz unterliegen, wie es im Umfeld von Web-Applikationen bereits „State of the Art“ ist und auch vom Oracle WebLogic Server unterstützt wird.

### Entwicklung und Qualitätssicherung

Zu den Anforderungen gemäß Control „A.12“ (Information Systems Acquisition, Development and Maintenance) hat Oracle umfangreiche Funktionen im Angebot. Entwickler bekommen einen Satz fertiger Bibliotheken und Module an die Hand, um einfach sicherheitsrelevante Anforderungen in Applikationen zu implementieren. Die Security Developer Tools liefern Unterstützung (A.12.3) für Kryptografie, Public Key Infrastructure, Web Service Security, SAML, Federation sowie Content Management. Der Aufwand für die Entwickler in die Einarbeitung von sicherheitsrelevanten Programmmodulen reduziert sich somit auf ein Minimum. Für die Qualitätssicherung der Software-Entwicklung sind unbedingt

geeignete Tests und Reviews (siehe A.10.3.1, A.10.3.2, A12.2.1, A12.2.4, A12.5.2) durchzuführen. Tests würden dann die Produktion am besten simulieren, wenn Produktiv-Daten eingesetzt werden könnten. Dies ist aber nicht ratsam, da Produktiv-Daten häufig personenbezogene oder andere sehr sensitive Daten enthalten, die nur von berechtigten Person eingesehen werden dürfen, jedoch sicherlich nicht von Administratoren und Entwicklern, die auf die Test- und Qualitätssicherungs-Umgebungen meist mit sehr hohen Privilegien zugreifen. Häufig ist die Passwort-Richtlinie für diese Umgebungen aufgeweicht und manchmal stehen die Rechner nicht einmal im Rechenzentrum. Um dennoch mit Daten, die den Produktiv-Daten entsprechen, testen zu können und gleichwohl die Vertraulichkeit sicherstellen zu können, müssen die Produktiv-Daten anonymisiert beziehungsweise pseudonymisiert werden. An dieser Stelle greift Oracle Data Masking. Es ist äußerst flexibel und kann die gleichen Regeln bedienen wie die Applikation. Das heißt, dass beispielsweise beim Austausch der Adresse darauf geachtet wird, dass die neue Adresse aus der gleichen Tarif-Region stammt, dass das Alter in der Spanne des Tarifs bleibt etc. Somit kann der Konflikt der widersprüchlichen Anforderungen bezüglich Tests mit Produktiv-Daten einerseits und Schutz der Vertraulichkeit enorm reduziert, wenn nicht sogar beseitigt werden.

Ein weiteres Problem bei der Entwicklung oder Änderung von Systemen stellen gesicherte Performance-Aussagen dar. Oracle Real Application Testing liefert mit einem überschaubaren Aufwand konkrete Performance-Zahlen der Datenbank vorab für geplante Änderungen (Major Upgrades, Aktivierung von Optionen und Features). Das grundsätzliche Vorgehen für die Ermittlung der Performance-Zahlen ist:

- Aufzeichnen der üblichen Aktivitäten im produktiven System mit Real Application Testing
- Replay der Aktivitäten in einem Testsystem, um den Performance-Unterschied zwischen Produktion-

und Testsystem zu ermitteln, falls etwa unterschiedliche Hardware zum Einsatz kommt

- Aktivierung der gewünschten Option oder des gewünschten Features im Testsystem
- Replay der aufgezeichneten Aktivitäten im modifizierten Testsystem
- Auswertung der Performance-Daten und Hochrechnung auf das Produktionssystem

Damit werden nicht nur die Anforderungen gemäß Control „A.12.5.2“ erfüllt, sondern auch Unsicherheiten beim Betrieb vorab ausgeräumt und somit ungeplante Ausfallzeiten und Störungen vermieden. Das wiederum deckt auch Anforderungen gemäß „A.10.3.2“ ab. Zudem können Web-Applikationen mit der Oracle Application Testing Suite bei Veränderungen der Applikation mit einem definierten Test-Set in der Qualitätssicherungs-Umgebung umfangreich vor der Produktivsetzung getestet werden, ohne dass personelle Ressourcen aus dem Fachbereich für die Regeltests benötigt werden. Dies macht eine Umsetzung der Controls „A.10.3.2“ und „A.12.5.2“ erst praktikabel.

### Auditing

Im Sinne des Unternehmens kann eine ungewollte Manipulation der Daten durch autorisierte Benutzer erfolgen. Dagegen müssen reaktive Maßnahmen implementiert sein. Was bei ERP-Systemen im Sinne des Controls „A.15“ (Compliance) üblich ist, wird bei Datenbanken oft versäumt beziehungsweise fälschlicherweise als nicht notwendig betrachtet. Eine der wichtigsten Maßnahmen ist, eine geeignete Protokollierung auf den zu überwachenden Systemen zu implementieren.

Oracle stellt zahlreiche Möglichkeiten für eine angemessene Protokollierung zur Verfügung. Voraussetzung hierfür ist natürlich, dass entsprechende Maßnahmen wie personalisierte Accounts, auch in der Administration, umgesetzt sind. Im Standard-Umfang kann die Protokollierung für den Superuser „SYS“ generell aktiviert werden und natürlich auch für weitere Benutzer, indem zum Beispiel die Zugriffe



auf Datenbank-Objekte oder die Verwendung von Systemprivilegien überwacht werden.

Anforderungen gemäß den Controls „A.10.10.1“ und „A.10.10.4“ sind damit problemlos möglich. Je nach Infrastruktur und Organisation des Unternehmens und für eine wirksame und überschaubare Umsetzung der Controls „A.10.10.3“ und „A.15.2.1“ ist früher oder später der Einsatz von Oracle Audit Vault ratsam. Damit besteht die Möglichkeit, zentral die Konfiguration der Protokollierung zu verteilen, durchzusetzen und die Ergebnisse auszuwerten. Organisatorische Voraussetzung hierfür ist, dass im Rahmen des Information Security Management Systems (ISMS) ein Bereich definiert wurde, der für die Security-Administration zuständig ist. Dies unterstützt auch die Anforderung des Controls „A.15.3.2“, dem Schutz der Audit-Tools, insbesondere vor Missbrauch.

Besteht die Anforderung an revidierbare Protokollierung, ist Oracle

Total Recall das Mittel der Wahl. Es protokolliert alle Änderungen der definierten Datenbankobjekte in der Datenbank so, dass sie selbst von Administratoren nicht mehr manipuliert werden können. Für die Protokollierung kann eine Löschrfrist definiert werden, nach der sie automatisch gelöscht wird, also genau so, wie es auch gesetzliche Regelungen fordern. Oracle Total Recall unterstützt dabei aber auch bei einer ganzen Reihe von Anforderungen aus dem ISO 27001:

- Die Anforderungen aus „A.10.10“ bezüglich Audit und Protokollierung lassen sich wesentlich besser umsetzen
- Die Überprüfung der Integrität von Informationen gemäß „A.12.2.3“ erhält eine sichere Grundlage
- Anforderungen in Bezug auf Schutz wichtiger Daten gemäß „A.15.1.3“ können überprüft werden

## Fazit

Ein Management der Informationssicherheit ist mit einem geeigneten Rahmen, wie ihn der ISO-27001-Standard vorgibt, wirtschaftlich realisierbar. Gerade bei der Umsetzung vieler Controls des ISO 27001 wird man effizient durch Oracle-Produkte und deren Sicherheits-Features unterstützt. In manchen Fällen wie dem Identity-Management ist der Einsatz eines Tools unvermeidlich, um Anforderungen auch von Wirtschaftsprüfern bezüglich der Nachvollziehbarkeit von Rechten einzelner Benutzer genau belegen zu können.

## Kontakt:

Dr. Thomas Störtkuhl

stortkuhl@secaron.de

Hans Wagner

wagner@secaron.de

## MT AG managing technology

### Enabling the Adaptive Enterprise



Die MT AG unterstützt ihre Kunden mit modernsten Methoden, Technologien und Verfahren bei der Implementierung des „Adaptive Enterprise“. Schwerpunkte sind dabei die agile und wirtschaftliche Realisierung neuer, IT-gestützter Geschäftsprozesse zur Verbesserung der Wertschöpfung, Transparenz und Sicherheit im Unternehmen.

Als Business Innovation und Transformation Partner bietet die MT AG umfassende IT-Beratung und -Dienstleistung für Großunternehmen und Mittelstand. Dabei vereint die MT AG herstellerunabhängige Expertise in den marktführenden Technologien wie IBM, Microsoft, Oracle, SAP und OpenSource mit fundiertem Themen- und Lösungs-Know-how in den Kerndisziplinen des Adaptive Enterprise unter einem Dach.

Besuchen Sie uns auf der DOAG vom  
17. – 19. November 2010, Stand-Nr. 330  
oder bei unseren Vorträgen.

**ORACLE** Platinum  
Partner

MT AG | Balcke-Dürr-Allee 9 | 40882 Ratingen | Tel. +49 (0) 2102 309 61-0 | Fax +49 (0) 2102 309 61-10 | info@mt-ag.com | www.mt-ag.com

# Von der Geschäftsprozess-Analyse zur Prozess-Ausführung

Evgenia Rosa, ORACLE Deutschland B.V. & Co KG

**Mit der neuen Oracle BPM Suite 11g bekommen Anwender ein innovatives BPM-Produkt, mit dem Geschäftsprozesse in BPMN 2.0 modelliert und nativ in einer BPMN-Laufzeitumgebung ausgeführt werden können. Der Artikel zeigt, wie sich die neue Suite in die bereits bestehenden Oracle-Produkte zur Geschäftsprozess-Modellierung und -Ausführung einfügt.**

Für die Geschäftsprozess-Modellierung, -Analyse und -Ausführung stellt Oracle seinen Kunden die Oracle Business Process Analysis Suite (Oracle BPA Suite) und die Oracle SOA Suite schon seit einiger Zeit zur Verfügung. Diese Produkte haben sich bereits in vielen Projekten zur Gestaltung flexibler Prozessabläufe und Unterstützung der Zusammenarbeit zwischen Fach- und IT-Abteilungen vielfältig bewährt. Nun nähert sich Oracle mit Oracle BPM Suite 11g der Lösung des viel besprochenen Business-IT-Gaps aus einer weiteren Perspektive.

## Prozess-Architektur mit der BPA Suite aufbauen und mit der SOA Suite ausführen

Die BPA Suite, die auf einer OEM-Version der IDS Scheer ARIS-Plattform basiert, dient der fachlichen Modellierung, Simulation, Analyse und Optimierung der Geschäftsprozesse. Das primäre Ziel dabei ist die Prozess-Dokumentation. Für die Ausführung der Prozesse kommt die SOA Suite zum Tragen, wobei die in der BPA definierten Modelle aus einer Prozessnotation (BPMN, EPK) mithilfe der spezifischen Erweiterungen in eine ausführbare Sprache (BPEL) transformiert werden.

Durch die Integration dieser beiden Werkzeuge werden Fach- und IT-Abteilungen in ihrer Zusammenarbeit unterstützt. Folgende Rahmenbedingungen sind hierbei gegeben:

1. Auf der fachlichen Seite wird ein – meist unternehmensweites – BPM-Vorhaben angestrebt, dem die Abbildung der Prozess-Architektur (Business Process Architecture) beziehungsweise der Unternehmens-

Architektur (Enterprise Architecture) zugrunde liegt. Dazu gehören:

- Modellierung der strategischen Aspekte der Unternehmens-Architektur wie Ziele, Erfolgsfaktoren, Marktsegmente
- Modellierung der Prozesse und Prozesshierarchien (Ist- und Soll-Zustände)
- Modellierung der in die Prozesse involvierten Artefakte wie Daten, Rollen, IT-Systeme und Services
- Modellierung der Organisationsstrukturen des Unternehmens und der IT-Landschaften
- Auswertungen (Reports) der wichtigen Unternehmenskennzahlen und der Abhängigkeiten zwischen Prozessen, IT-Systemen und Rollen
- Unternehmensweite Kommunikation der Prozesse durch rollenbasierten Zugriff auf Prozessmodelle.

Diese Ziele werden mit dem Einsatz der Oracle BPA Suite erreicht.

2. Die als Ergebnis des BPM-Vorhabens optimierten Soll-Prozesse werden in einer SOA umgesetzt und durch den Einsatz einer SOA-Plattform, wie der Oracle SOA Suite, automatisiert. Um diese Automatisierung der Prozessmodelle optimal zu unterstützen, hat Oracle die BPA und die SOA Suite – mit einem auf einem Repository basierten Ansatz – integriert. Dabei ist neben der Generierung der ausführbaren BPEL-Gerüste aus Prozessmodellen auch der sogenannte „Roundtrip“ möglich (mehr dazu siehe DOAG Business News 2/2008).

Auch wenn die Integration der beiden Produkte die Überführung der Prozessmodelle in die Ausführung weitgehend erleichtert, müssen die Anwender sich hier einigen Herausforderungen stellen. Nicht alle Prozessmodelle sind direkt nach BPEL überführbar, da die Prozessnotationen wie EPK und BPMN einige Modellierungselemente wie zum Beispiel „Rücksprünge“ beinhalten, die im BPEL nicht abbildbar sind. Das heißt, die zur Ausführung bestimmten fachlichen Modelle müssen zuerst durch einen IT-versierten Prozessarchitekten entsprechend bearbeitet werden, wobei sie dadurch an ihrer fachliche Aussagekraft und der Verständlichkeit für den Fachanwender verlieren können.

## Schnell und effektiv Prozessabläufe automatisieren

Während beim Einsatz der Oracle BPA Suite die Abbildung der Prozess-beziehungsweise der Unternehmens-Architektur im Vordergrund steht, fokussiert sich die BPM Suite 11g (siehe Artikel auf Seite 42 in diesem Heft) auf die eigentliche Automatisierung der Prozess-Abläufe, ohne dass eine detaillierte Erfassung der Prozess-Architektur, Organisationseinheiten, Daten und IT-Systeme notwendig ist. Dies ist meist der Fall, wenn die Soll-Prozesse bereits bekannt sind oder es sich um lokale Prozesse auf der Abteilungsebene oder in einem mittelständischen Unternehmen handelt.

Für diesen Anwendungsfall bietet die BPM Suite 11g einen wichtigen Vorteil: Die Fach- und IT-Anwender arbeiten am gleichen Modell in unterschiedlichen, jeweils für sie geeigneten Sichten, ohne dass eine Transformation zwischen dem Prozessmodell

# Houston, wir haben ein Problem!

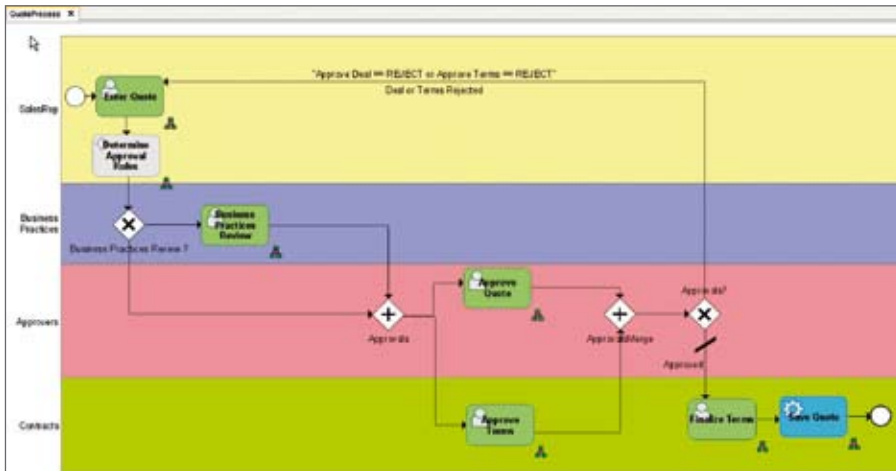


Abbildung 1: Sales Quote Prozess in Oracle BPA Business Architect

und der Ausführungsrepräsentation des Prozesses notwendig ist. Die Fachanwender modellieren mit BPMN im BPM Studio (basierend auf JDeveloper) oder im Web-basierten Process Composer, und IT-Entwickler verfeinern das gleiche Modell mit technischen Details. Anschließend können die BPMN-Prozesse nativ (ohne vorherige Transformation in eine andere Sprache) in einer BPMN-Ablauf-Umgebung ausgeführt werden. Die direkte Ausführung der Prozessmodelle wurde mit der neuen BPMN-2.0-Spezifikation möglich. Diese Version des Standards beinhaltet – im Gegensatz zu früheren Versionen – neben der grafischen Notation auch ein Metamodell und die dazugehörige

XML-basierte Repräsentation, die eine Grundlage für die Interpretation und die Ausführbarkeit durch entsprechende Werkzeuge darstellen.

Durch direkte Ausführung der BPMN-Modelle erübrigen sich die oben beschriebenen Nachteile, die bei der Transformation der BPMN-Modelle nach BPEL entstehen können. Anmerkung der Autorin: Nach dem heutigen Stand ist der BPMN-2.0-Standard noch nicht final verabschiedet.

### BPA Suite und BPM Suite 11g ergänzen sich

Damit ein Unternehmen die Vorteile der beiden oben dargestellten BPM-

## ...und wir die Lösung!

IT im Alarmzustand! Fachbereiche rufen nach neuen und besseren IT-Services. Governance, Risikomanagement & Compliance sind auf der Tagesordnung. Und das IT-Budget steht auf dem Prüfstand.

Zeit, mit einem verlässlichen Partner zu sprechen, der mit Ihnen gemeinsam wirtschaftliche Lösungen entwickelt. Höchste Zeit, mit PROMATIS zu sprechen!

PROMATIS verbindet intelligente Geschäftsprozesse mit modernen Oracle Technologien und Applikationen:

- Oracle E-Business Suite und CRM On Demand
- Oracle Accelerate Mittelstandslösungen
- Universal Content Management, WebCenter, Beehive
- Business Intelligence und Data Warehouse
- BPM, Oracle SOA und Application Integration (AIA)
- Bewährte Projekt-Vorgehensmodelle und Best Practice-Prozesse

Profitieren Sie von der PROMATIS Lösungskompetenz und unserer internationalen Erfahrung. Sprechen wir darüber!

## PROMATIS

Knowledge Powered Business Processes

PROMATIS software GmbH  
Tel.: +49 7243 2179-0 · Fax: +49 7243 2179-99  
www.promatis.de · hq@promatis.de  
Ettlingen/Baden · Hamburg · Berlin

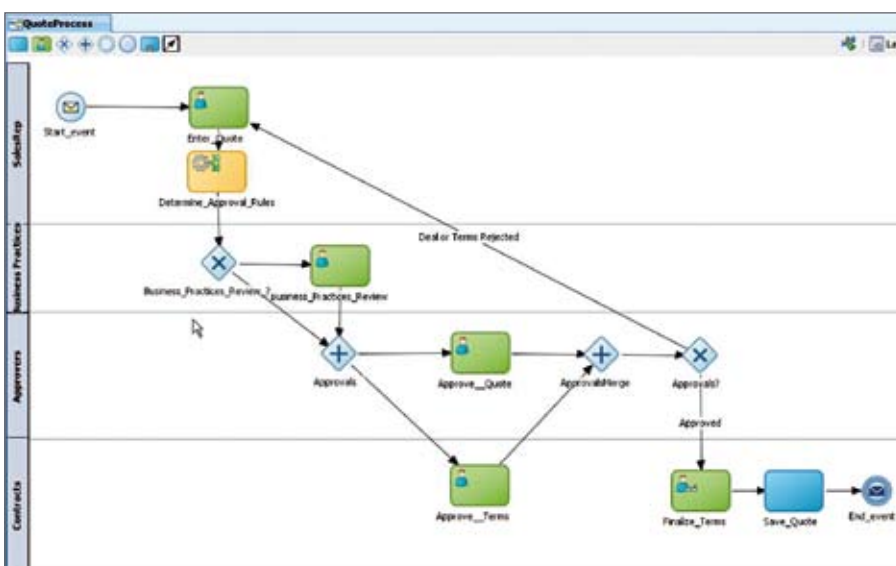


Abbildung 2: Sales Quote Prozess, importiert in Oracle BPM Studio

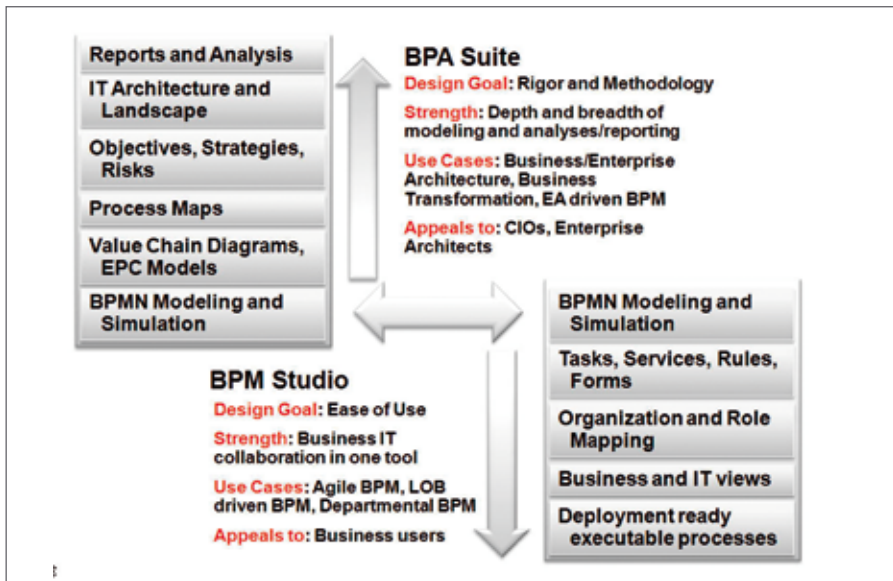


Abbildung 3: Gegenüberstellung BPA Suite und BPM Studio 11g

Ansätze nutzen kann, also neben der anspruchsvollen Modellierung aller wichtigen Unternehmensaspekte auch die native BPMN-Ausführung, arbeitet Oracle an der Integration der BPA und BPM 11g Suite. Zum heutigen Zeitpunkt ist diese Integration bereits teilweise verfügbar: Die mit der BPA Suite modellierten BPMN-Prozesse können in das BPM Studio 11g importiert und in der BPMN-Engine ausgeführt werden. Nachfolgend ist das Vorgehen beschrieben.

Das BPMN-Modell im Oracle BPA Business Architect wird wie gewohnt an die IT-Abteilung durch die „Share Blueprint with IT“-Funktionalität übergeben. Dabei ist ein Prozess-Blueprint im BPA-Repository angelegt. Nun kann der IT-Entwickler sich aus dem JDeveloper heraus durch die Verbindung zum BPA-Repository entweder ein SOA-Projekt mit einem BPEL-Prozess anlegen oder – und das ist neu – ein BPM-Projekt mit einem BPMN-Prozess erzeugen lassen. In beiden Fällen entsteht ein SCA-konformes Composite, das den Prozess entweder als eine BPEL- oder als eine BPMN-SCA-Komponente enthält. Nun kann der BPMN-Prozess im BPM Studio (beziehungsweise im BPEL Designer) mit IT-Details angereichert und implementiert werden.

Die Roundtrip-Funktionalität zwischen der BPA und der BPM Suite, so wie sie heute zwischen der BPA und SOA Suite existiert, ist für die nachfol-

genden Versionen der beiden Produkte geplant. Abbildung 1 zeigt einen BPMN-Prozess in der BPA Suite, Abbildung 2 den gleichen Prozess nach dem Import in das BPM Studio.

#### Der Anwender hat die Wahl

Je nach Anwendungsfall und den Anforderungen in einem BPM-Projekt können nun Oracle-Anwender zwischen mehreren Möglichkeiten wählen:

- Die BPA Suite für die anspruchsvolle Modellierung und den Aufbau der Prozess- beziehungsweise der Unternehmens-Architekturen.
- Die BPA Suite und die SOA Suite, um die modellierten Prozesse mit BPEL zu automatisieren.
- Die BPM Suite für die BPMN-Modellierung und native BPMN-Ausführung. Dabei steht vielmehr die eigentliche Prozess-Ausführung und weniger die Erfassung der unternehmensweiten Geschäftsprozess-Architektur im Vordergrund.
- Die BPA Suite und die BPM Suite, falls beide Aspekte und sowohl die anspruchsvolle Modellierung der Unternehmens-Architektur als auch die native Ausführung der BPMN-Prozesse wichtig sind.

Da die BPM Suite auf der SOA Suite basiert, wobei sowohl die BPMN-Run-time als auch die BPEL-Run-time in einem BPM-Server angesiedelt sind, bietet sich für Oracle-Kunden ein weiterer Vorteil: Für die Ausführung der Prozesse kann sowohl der BPMN- als auch der BPEL- Standard genutzt beziehungsweise kombiniert werden. Abbildung 3 zeigt die Schwerpunkte und Einsatz-Szenarien für die BPA- und BPM-Modellierungswerkzeuge.

#### Fazit

Die effektive Zusammenarbeit zwischen Fach- und IT-Abteilungen ist die Voraussetzung für die optimale Umsetzung der flexiblen Geschäftsprozesse. Oracle bietet hierfür die Unterstützung mit der Auswahl mehrerer BPM-Werkzeuge für die Modellierung und die Ausführung: BPA Suite, SOA Suite und BPM Suite. Diese Produkte können je nach Anwendungsfall entweder einzeln oder in Kombination eingesetzt werden und so optimal die projektspezifischen Anforderungen erfüllen. Die Unternehmen haben die Wahl, die am besten geeigneten BPM-Werkzeuge und Technologien für sich auszusuchen, und können dabei von deren enger Integration profitieren.

#### Abkürzungen:

BPMN	Business Process Modeling Notation
EPK	Ereignis-Prozess-Ketten
BPEL	Business Process Execution Language

#### Kontakt:

Evgenia Rosa  
evgenia.rosa@oracle.com

# Oracle Virtual Assembly Builder

Marcus Schröder, ORACLE Deutschland B.V. & Co KG

**Der Artikel beschreibt die Arbeitsweise des Oracle Virtual Assembly Builders (OVAB). Dieser ist seit 1. Mai 2010 verfügbar und vereinfacht das Erstellen von Oracle Applikations-Infrastrukturen und die Bereitstellung auf einer Oracle VM.**

Für die Erstellung von lauffähigen Templates auf der Oracle VM existieren verschiedene Vorgehensweisen:

- Verwendung eines von Oracle vorgefertigten Templates inklusive aller benötigten Software-Komponenten (Bezugsquelle: <http://edelivery.oracle.com>)
- Installation der gewünschten Umgebung auf einer physischen oder virtuellen Umgebung und Erstellen eines Templates mit dem Oracle Template Builder
- Automatische Ermittlung einer bestehenden System-Umgebung, Aufteilung in Basis-Komponenten, Zusammenstellung einer neuen Umgebung und Deployment auf eine Oracle VM durch den Virtual Assembly Builder

Im Folgenden sind die Erstellung und das Deployment eines Assemblys durch den Oracle Virtual Assembly Builder (OVAB) beschrieben. Alle Arbeitsschritte werden bis auf eine Ausnahme wahlweise über eine grafische Benutzeroberfläche (GUI) oder ein Command Line Interface (CLI) durchgeführt. Die Ausnahme ist das Erstellen des Assemblys (Schritt 2), da dieser Schritt eine grafische Modellierung beinhaltet.

Der gesamte Prozess besteht aus sechs Einzelschritten.

## Introspection/Ermittlung der Konfiguration des Quell-Systems

In der Introspection wird das gewünschte System einschließlich der Konfigurationsdaten und installierten Schemata/Applikationen ermittelt. Diese Informationen sind als Metadaten gespeichert und enthalten den gesamten Aufbau der ermittelten Umgebung. Dazu ein Beispiel: Ein System

besteht aus einer Datenbank mit einem WebLogic Server und einer Web-Tier-Komponente. Die Introspection/Ermittlung des Quell-Systems liest die Installations-Information und Metadaten aus den einzelnen Quell-System-Komponenten aus und speichert sie im Assembly Builder Repository ab. Anschließend stehen die System-Komponenten, zum Beispiel Datenbank oder WebLogic Server, zur Modellierung im Assembly Builder bereit.

In diesem Arbeitsschritt erfolgt die Ermittlung des Quell-Systems. Der Assembly Builder ermöglicht im aktuellen Release (11.1.1.2.0) die Introspection der folgenden Oracle-Produkte:

- Oracle DB 11g R1 Single Instance (nicht mit ASM)
- Oracle WebLogic Server 10.3.x
- Oracle WebServer 11g
- Oracle WebCache 11g

Der Arbeitsschritt umfasst das Abbilden des ursprünglichen „\$ORACLE\_HOME“. Dabei werden alle enthaltenen Datenbank-Schemata und WebLogic-Applikationen einschließlich Konfigurationen ermittelt und als Meta-Informationen abgespeichert. Pro Introspection wird jeweils eine Oracle-Komponenten-Konfiguration bestimmt. Die Ermittlung der Konfigurationen erfolgt „remote“ oder „lokal“, das heißt, entweder per SSH-Verbindung und lokales Absetzen von Befehlen oder durch ein Kopieren eines Introspection-Agenten auf das Quell-System und eine entfernte Ausführung. Erfahrungsgemäß wird empfohlen, die Introspection Remote auf das gewünschte Objekt durchzuführen, da im Falle von Fehlern diese ansonsten erst nach dem Übertragen auf das lokale Repository erkannt werden.

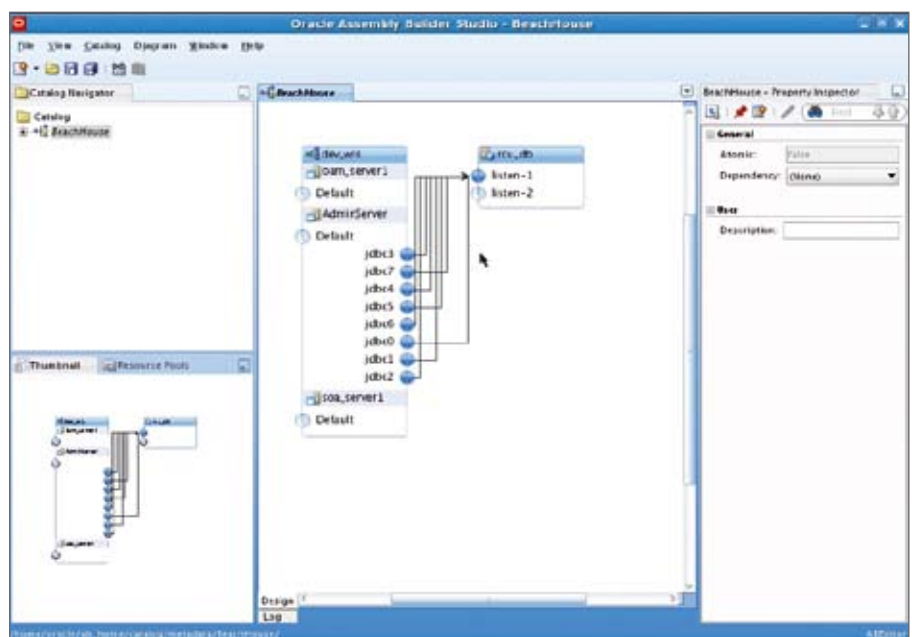


Abbildung 1: Introspection einer WebLogic-Server-Instanz

## Create Assembly/ Erstellen des Assemblys

Die Applikations-Komponenten (Appliances) werden in diesem Arbeitsschritt zu einer neuen Applikations-Umgebung (Assembly) kombiniert. Ein Beispiel: Aus der gewonnenen Datenbank und WebLogic Appliance wird eine neue Umgebung mit mehreren Datenbanken/WebLogic Servern und Anbindungen an externe Datenquellen modelliert.

Das Erstellen eines Assemblys ist ein rein grafischer Arbeitsschritt. Die gewonnenen Appliances werden zu einer neuen Umgebung des sogenannten „Assemblys“ kombiniert. Diese Kombination wird durch „Drag & Drop“ der einzelnen Appliances und anschließender Verbindung untereinander durchgeführt. Diese Verbindungen unterstützen die gängigen Protokolle wie HTTP, JDBC etc.

Zur Anbindung externer Ressourcen, die nicht direkt zum Assembly gehören, wird ein Platzhalter erzeugt, in dem die gewünschten Verbindungs-Parameter angegeben werden. Dieser Platzhalter wird „Externe Ressource“ genannt und unterstützt ebenfalls eine Reihe von gängigen Protokollen.

## Build Template

Die im ersten Schritt ermittelten Konfigurationen der einzelnen Komponenten wie Datenbank und WebLogic Server sowie Meta-Konfigurationen aus dem zweiten Schritt (Erstellen des Assemblys) werden in einem Arbeitsschritt zu einem deploybaren Assembly kombiniert.

In diesem Arbeitsschritt werden die Appliances jeweils auf ein vorinstalliertes System-Image installiert und konfiguriert. Dieses Standard-System-Image ist im Assembly-Builder-Verzeichnis abgelegt und entspricht einer Oracle Enterprise-Linux-5.3 32-Bit-Installation. Ausnahme: Für WebLogic Server besteht die Auswahlmöglichkeit zwischen dem 32-Bit-OEL-5.3-System-Image und einem Image der JRockit Virtual Edition (JRVE). Die JRVE ist als Java Virtual Machine ohne Betriebssystem direkt auf dem Hypervisor der

Oracle VM lauffähig und wirkt sich somit sehr sparsam auf die Ressourcen aus. Das Resultat dieses Arbeitsschritts ist ein Assembly, das alle Applikations-Komponenten, System Images und Verbindungs-Metadaten (zu den Appliances untereinander und externen Ressourcen) enthält.

Tipp: Da das Assembly viel Speicherplatz benötigt, sollte man ausreichend Platz vorrätig halten. Als Richtwert gilt folgende Formel: Appliance (ca. 500 MByte) + System Image (ca. 1000 MByte) \* Anzahl der Systemkomponenten = benötigter Plattenplatz.

## Erstellen Deployment-Plan

Ein Assembly kann mit oder ohne Deployment-Plan registriert/deployed werden. Der Deployment-Plan ermöglicht das Definieren von Parametern auf ein bereits existierendes Assembly, um eine maximale Flexibilität zu bieten und im Nachgang Konfigurationen in einem existierenden Assembly zu ändern.

Diese Parameter sind IP-Adresse, CPU- und Memory-Ressourcen, Skalierungsfaktoren etc. Der Deployment-Plan wird bei der Registrierung des Templates beziehungsweise beim Deployment explizit angegeben. Das Auswerten der im Deployment-Plan angegebenen Parameter wird während des Deployments auf der Oracle VM durchgeführt, dieser Vorgang heißt „Late Binding“. Pro Registrierung/Deployment kann jeweils nur ein De-

ployment-Plan pro Assembly angegeben sein. Wird kein Deployment-Plan angegeben beziehungsweise ist der Deployment-Plan aufgrund falscher Parameter ungültig (etwa durch nicht vorhandene IP) wird das Assembly mit Standard-Einstellungen registriert, deployed und gestartet.

## Register Template

Während dieses Arbeitsschrittes wird das generierte Assembly auf den dafür vorgesehenen Server Pool der Oracle VM kopiert. Beim Registrieren des Templates auf dem OVM Manager ist es erforderlich, den Ressourcen-Pool des Ziel-Systems anzugeben, inklusive der dazugehörigen Maschine. Beim Registrierungs-Vorgang wird das Assembly im OVM-Pool erstellt.

## Deploy Assembly

Im letzten Schritt werden aus dem Assembly Builder eine Instanz des Assemblys auf der Oracle Virtual Machine erstellt und alle vorhandenen Komponenten in der korrekten Reihenfolge gestartet. Anschließend wird das Assembly Template auf der Oracle VM instanziiert und in der korrekten Reihenfolge in Gang gesetzt. Die Steuerung der Instanzierung (Starten) und die Steuerung des gesamten Lebenszyklus' des Assemblys (Erstellen, Herunterfahren, Verwerfen) können aus dem Oracle VM Manager durchgeführt werden, es

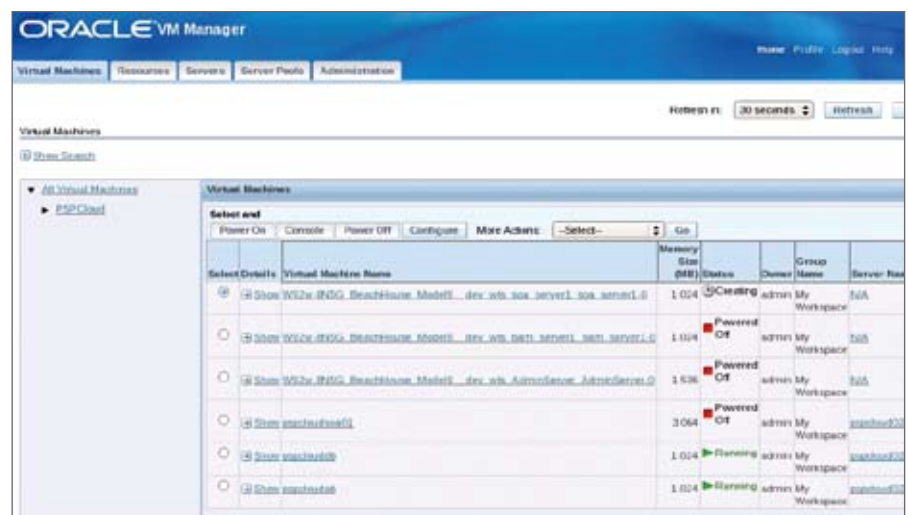


Abbildung 2: Erstellen eines Assemblys mit einer externen Datenbank-Ressource

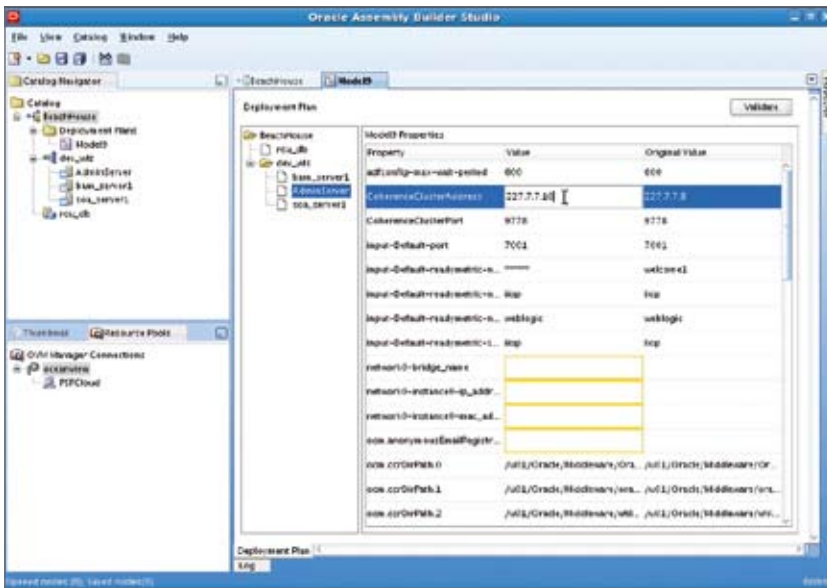


Abbildung 3: Eintragen von Deployment-Plan-Parametern (Coherence Cluster IP)

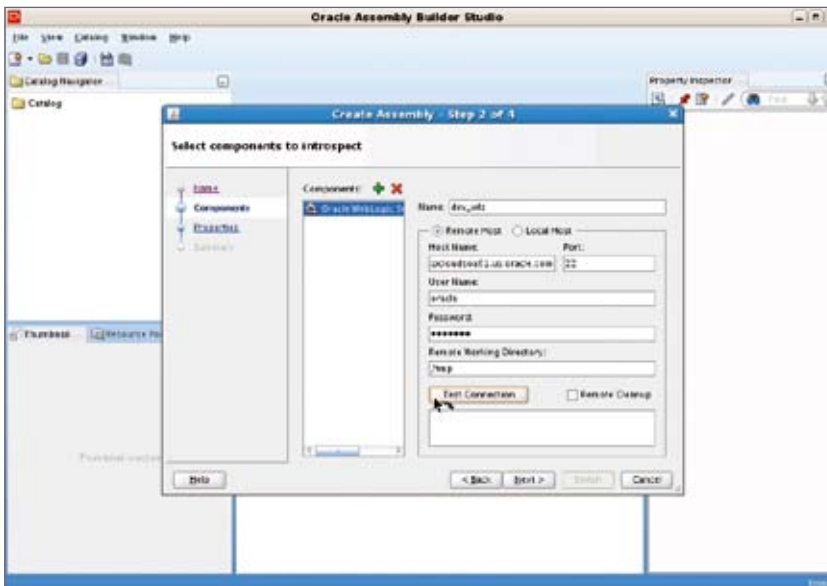


Abbildung 4: Das Assembly wird auf dem Oracle VM bereitgestellt und automatisch gestartet

ist aber empfehlenswert, dieses durch die Assembly Builder GUI bzw. besser durch das Assembly Builder Command Line Interface (CLI) zu steuern.

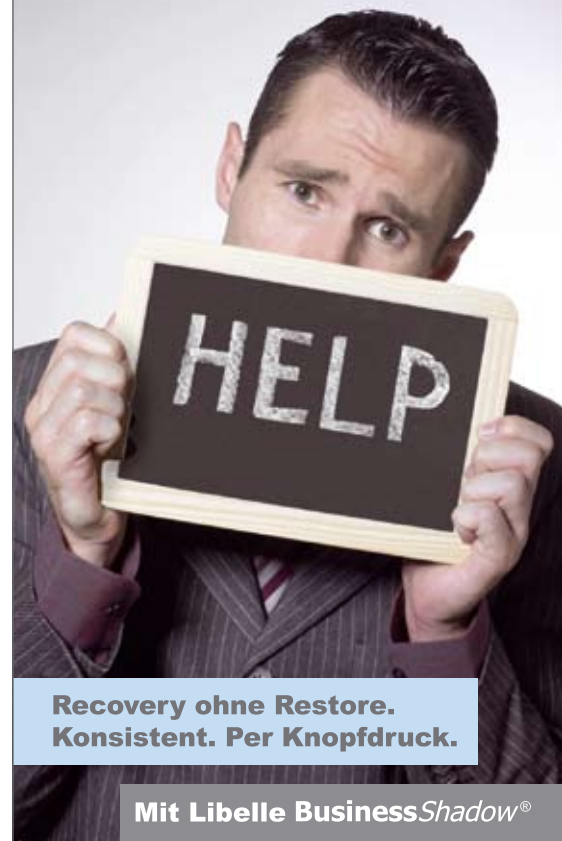
## Fazit

Der Oracle Virtual Assembly Builder ermöglicht das schnelle und fehlerfreie Bereitstellen von einfachen und komplexen Oracle Applikations-Komponenten. Die Zeitersparnis, Flexibilität und Wiederverwendbarkeit gegenüber einer manuellen Erstellung eines Templates ist ein gewichtiges Argument für den Einsatz des Assembly Builders.

Ein zentrales Einsatzgebiet des Oracle Virtual Assembly Builders ist die Modellierung und Bereitstellung von System-Instanzen innerhalb einer Cloud-Computing-Umgebung für eine private/public PaaS. Durch die flexible Arbeitsweise kann beispielsweise der Cloud-Administrator mittels GUI neue Assemblies modellieren, die anschließend durch das Assembly Builder Command Line Interface aus einem Self Service Portal des Cloud-Anbieters automatisiert bereitgestellt werden.

### Kontakt:

Marcus Schröder  
marcus.schroeder@oracle.com



**Recovery ohne Restore.  
Konsistent. Per Knopfdruck.**

Mit Libelle BusinessShadow®

Datenverluste und Systemstillstände lassen sich nicht immer vermeiden. Gut, wenn Sie dann eine Lösung haben, mit der Sie Ihre Daten schnell, einfach und vor allem konsistent wieder parat haben – ohne manuelles Recovery oder Snapshots. Dafür auf Knopfdruck.

Zudem sind Ihre Datenbanken, Filesysteme und Applikationen durch zeitversetzte Spiegelung sowohl bei physikalischen als auch logischen Fehlern (z.B. Datenkorruptionen) abgesichert.

Schaffen Sie sich jetzt Spielräume für Verfügbarkeit und Disastervorsorge mit Libelle **BusinessShadow®**!

### Profitieren Sie durch:

- Einfache Integration der Spiegellösung
- Systemübergreifende Datenkonsistenz
- Kürzeste Wiederherstellungszeiten
- Automatisierte System-Umschaltung
- Absolute Entfernungsunabhängigkeit
- Einfachste Bedienbarkeit
- Eine Lösung für heterogene Landschaften

**Neu: Libelle Web Academy**  
Spannende HA-/DR-Themen  
in 30 Minuten.

[www.libelle.com/webacademy](http://www.libelle.com/webacademy)



**Libelle**

**ORACLE** Gold Partner

### Libelle AG

Gewerbestr. 42 • 70565 Stuttgart, Germany  
T +49 711 / 78335-0 • F +49 711 / 78335-148  
[www.libelle.com](http://www.libelle.com) • [sales@libelle.com](mailto:sales@libelle.com)

# Neu: Oracle BPM Suite 11g

Gert Schüßler, ORACLE Deutschland B.V. & Co KG

Die Oracle BPM Suite 11g ist eine neue Entwicklung im Bereich des Prozess-Managements. Das neue Release ist die konsequente Weiterentwicklung der BPM Suite 10g, die auf dem Release AquaLogic BPM von BEA basiert. Die Oracle BPM Suite 11g enthält Tools für die Entwicklung und die Laufzeitumgebung für organisations- und systemübergreifenden Prozesse und unterstützt das Konzept des Business Process Managements (BPM), bei dem die Prozesse in einem fortwährenden Zyklus analysiert, entwickelt, beobachtet und verbessert werden.

Die Arbeitsweise in Unternehmen wird heute sehr stark durch Geschäftsprozesse geprägt, die schnell verändert werden müssen, da sich die Anforderungen stetig ändern. Diese Prozesse wurden früher durch Workflow Management Systeme (WMS) abgebildet, die hauptsächlich für Prozesse mit starker Beteiligung von Personen konzipiert waren. Heute bildet man solche Prozesse über Prozess-Management-Systeme ab, die auf Standards basieren und über standardisierte Schnittstellen zu den unterschiedlichsten Systemen verfügen. Viele Prozesse laufen heute nicht mehr nur in einer Applikation ab, sondern sie müssen applikations- und teilweise unternehmensübergreifend konzipiert und realisiert werden. Außerdem können Prozesse in diesen neuen Systemen sehr schnell und einfach angepasst werden, um rasch auf neue Anforderungen zu reagieren.

Die Oracle BPM Suite 11g umfasst folgende Produkte:

- Oracle BPM Studio
- Oracle Process Composer
- Oracle Process Workspace
- Oracle Business Activity Monitoring (BAM)
- Oracle BPEL Process Manager
- Oracle Business Rules

## Modellierung mit BPMN 2.0

Die Modellierung der Prozesse wird mit der Business Process Modeling Notation (BPMN) Version 2.0 durchgeführt. Diese Notation wird von der Object Management Group (<http://www.bpmn.org/>) spezifiziert und wird immer mehr zum Standard bei der Modellierung von Geschäftsprozessen. Die BPMN ist eine grafische Notation und deshalb auch

für Business-Analysten und Endanwender leicht lesbar (siehe Abbildung 1). Modelliert werden folgende Elemente:

- **Activities**  
Wie manuelle Aufgabe (User Task) oder Aufruf eines (Web-) Services
- **Events**  
Wie Start, End, Timer, Error Event
- **Gateways**  
Wie Exclusive Gateway (XOR), entspricht einer if-Abfrage oder einem Case Statement in Programmiersprachen
- **Connections**  
Verbindungen zwischen den einzelnen Elementen eines Prozesses, um den Prozessfluss festzulegen (Flow)
- **Artifacts**  
Wie Anmerkung innerhalb des Prozesses
- **Swimlanes**  
Wie Abbildung der Organisationsstruktur mit den Abteilungen, denen bestimmte Aufgaben zufallen

## Process Composer

Für die Modellierung gibt es Oberflächen für IT- und Business-Analysten. Der „Process Composer“ ist eine Web-Oberfläche, mit der Business-Analysten arbeiten. Dieser kann auch Endanwendern zur Verfügung gestellt werden, damit sie beispielsweise die definierten Prozesse noch einmal auf ihre Richtigkeit überprüfen oder sich später ein Bild über den gesamten Prozess abrufen können, in den sie involviert sind. Im Process Composer wird bei der Definition und Darstellung der Prozesse ebenfalls mit der BPMN 2.0 gearbeitet.

## BPM Studio

Das BPM Studio ist als Werkzeug für den IT-Entwickler und im Oracle JDeveloper integriert. Hier werden nicht nur die Prozessabläufe in BPMN 2.0 modelliert, sondern auch die technischen Details definiert, zum Beispiel,

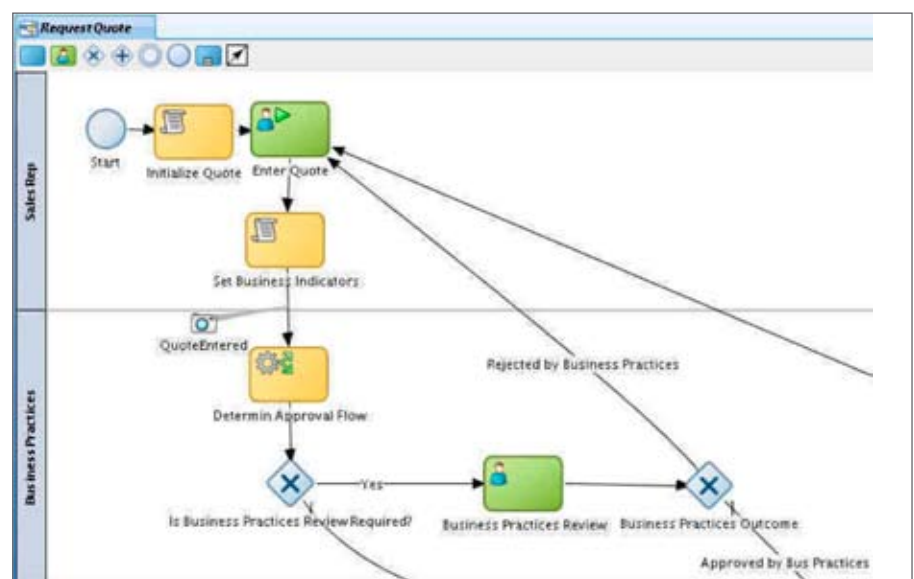


Abbildung 1: Beispiel Genehmigungsprozess



welche Datenstrukturen und Variablen benutzt werden oder welcher Web-Service aufgerufen wird. Die BPM Suite ist in die Service Component Architecture (SCA) integriert, die Oracle bereits mit der SOA Suite 11g unterstützt (siehe Abbildung 2). Der Vorteil ist, dass weitere Komponenten wie BPEL-Prozesse und Business-Rules integriert werden und Zugriffe auf unterschiedliche Datenquellen über Adapter (Database, File, FTP Adapter etc.) realisiert sind.

### MDS Repository

Die Entwicklung der Prozesse kann mit beiden Werkzeugen – BPM Studio oder Process Composer – beginnen. Die grundlegenden Schritte für die Prozesse werden normalerweise von Business-Analysten definiert, die mit dem Process Composer arbeiten. Die Prozessinformationen werden zwischen dem Business-Analysten und dem IT-Entwickler über ein gemeinsames zentrales Repository (MDS) ausgetauscht, so dass eine enge Zusammenarbeit zwischen IT und Analysten sichergestellt ist.

Über den JDeveloper können auch Prozess-Templates im Repository abgelegt werden, die im Process Composer die Grundlage für neue Prozesse bilden. Damit können beispielsweise Analysten schnell neue Prozesse imple-

mentieren, die nur an einigen Punkten modifiziert werden müssen.

### Simulation

Vor der Implementierung kann man die Prozesse durch eine Simulation im BPM Studio auf Schwachstellen oder Engpässe im Prozessablauf untersuchen. Die gesammelten Statistiken, etwa über Laufzeiten oder Kosten, ermöglichen einen Einblick in den Prozessablauf, so dass die Prozesse bereits vor der Implementierung geändert und verbessert werden können.

### Process Workspace

Der Process Workspace ist eine Web-Anwendung, in der die Aufgaben (User Tasks), die im Prozessverlauf an Personen oder Gruppen verteilt werden, zur Bearbeitung angezeigt sind (siehe Abbildung 3). Der Process Workspace verfügt über zusätzliche Funktionalitäten wie das Delegieren von Aufgaben oder die Zuweisung einer Aufgabe an eine andere Person oder Gruppe, die somit im Prozessdesign nicht mehr berücksichtigt werden müssen. Eine Aufgabe muss abgeschlossen werden, damit der Prozess weiterlaufen kann. Für jede Aufgabe gibt es „1...n“ Antwortmöglichkeiten wie „Genehmigung“ oder

„Ablehnung“. Für jede Aufgabe wird der Inhalt der Aufgabe in Masken angezeigt, die mit dem Oracle ADF (Application Development Framework) generiert und weiter angepasst werden können. In der BPM Suite 11g kommt ebenfalls das Konzept der Human Task aus der SOA Suite 11g zum Einsatz.

### Business Activity Monitoring

Oracle Business Activity Monitoring (BAM) überwacht online die laufenden Prozesse. Es werden Kennzahlen (KPIs, SLAs, etc.) gesammelt, die zum Beispiel Informationen über die gesamte Laufzeit eines Prozesses oder über Engpässe im Prozessablauf liefern (siehe Abbildung 4). Der Vorteil ist, dass die Daten fast in Echtzeit, das heißt innerhalb weniger Sekunden, gesammelt und ausgewertet werden, so dass man Probleme im Prozessablauf sofort beheben kann. Die gesammelten Informationen werden in Dashboards und Reports in Web Browsern und Portalen dargestellt.

### Fazit

Die Oracle BPM Suite bietet umfassende Möglichkeiten zur Definition von flexiblen Prozessen, bei denen sowohl die Einbeziehung von Personen als auch die Integration von unterschiedlichen

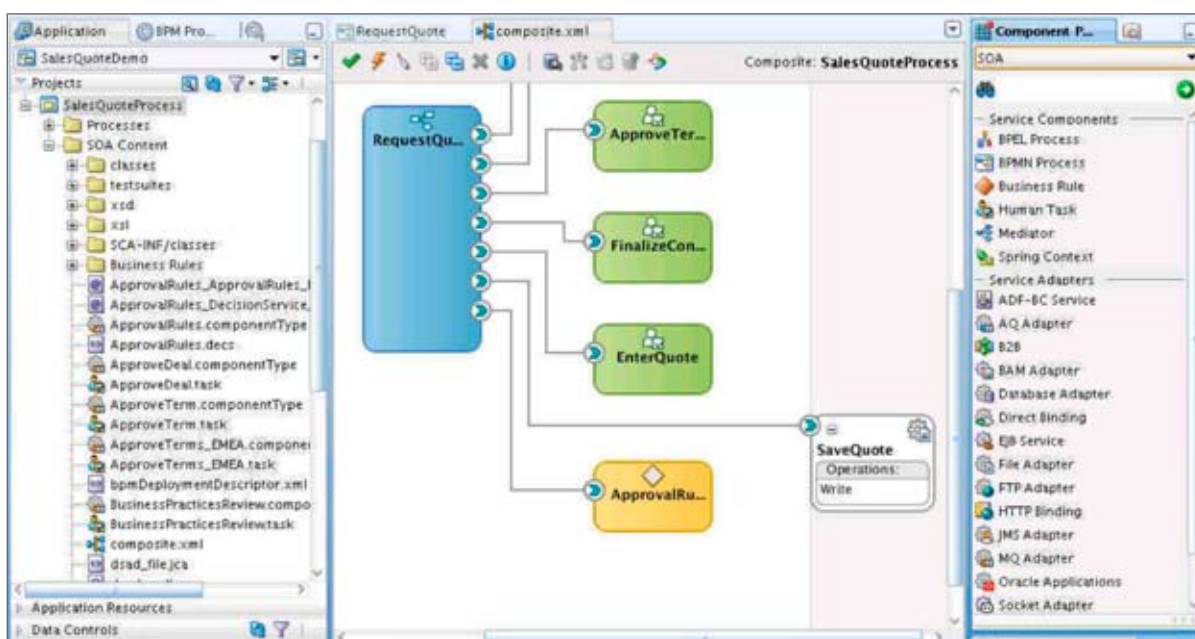


Abbildung 2: Service Component Architecture im JDeveloper

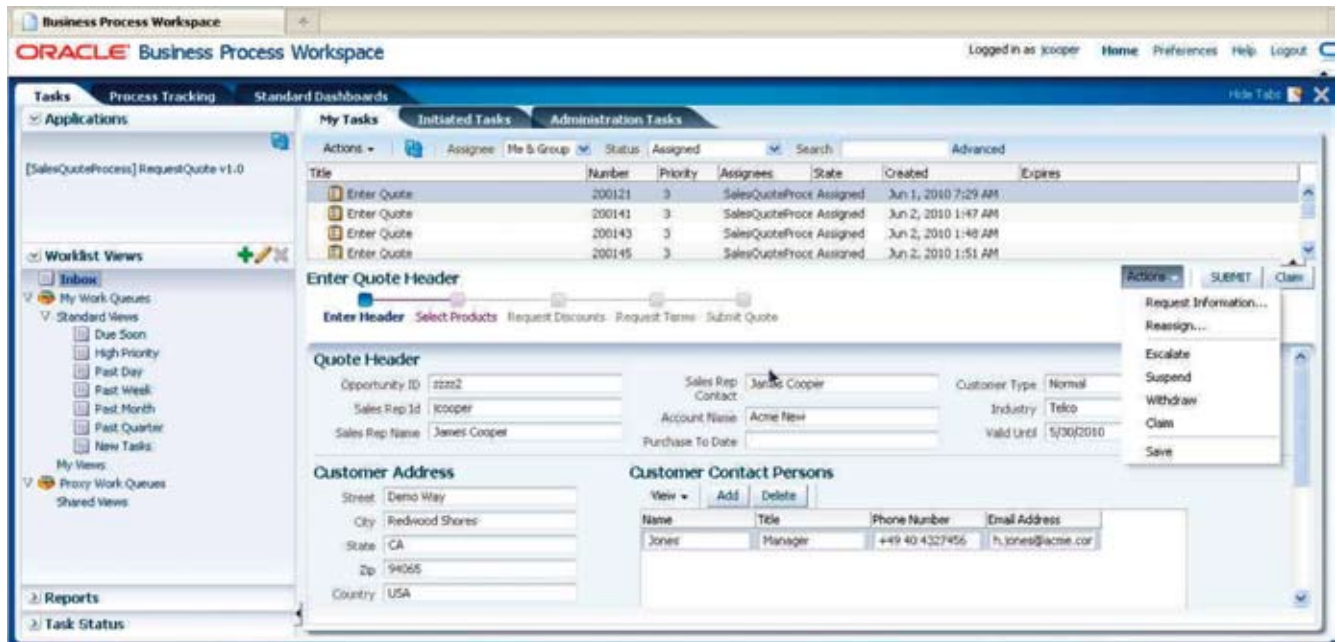


Abbildung 3: Business Process Workspace



Abbildung 4: Oracle BAM Dashboard

Systemen möglich sind. Unterschiedliche Umgebungen für IT-Entwickler und Business-Analysten fördern die Zusammenarbeit und Kommunikation zwischen den an der Entwicklung beteiligten Personen. Eine Simulation ermöglicht die Verbesserung der Prozesse bereits vor der Implementierung. Die Online-Überwachung durch Oracle BAM gibt Auskunft über die laufenden Prozesse. Diese Informationen dienen dann ebenfalls dazu, die bestehenden Prozesse zu verbessern. Mit diesen Funktionen und Möglichkeiten unterstützt die Oracle BPM Suite 11g die Methode des Business Process Managements und damit den gesamten Lebenszyklus von Prozessen.

**Kontakt:**

Gert Schüssler  
gert.schuessler@oracle.com

**Impressum**

**Herausgeber:**  
DOAG Deutsche ORACLE-  
Anwendergruppe e.V.  
Tempelhofer Weg 64, 12347 Berlin  
Tel.: 0700 11 36 24 38  
www.doag.org

**Verlag:**  
DOAG Dienstleistungen GmbH  
Fried Saacke, Geschäftsführer  
info@doag-dienstleistungen.de

**Chefredakteur (VisdP):**  
Wolfgang Taschner,  
redaktion@doag.org

**Chefin von Dienst (CvD):**  
Carmen Al-Youssef,  
office@doag.org

**Gestaltung und Satz:**  
Claudia Wagner,  
DOAG Dienstleistungen GmbH

**Anzeigen:**  
CrossMarketteam  
Ralf Rutkat, Doris Budwill  
www.crossmarketteam.de

Mediadaten und Preise unter:  
www.doag.org/publikationen/

**Druck:**  
adame Advertising and Media  
GmbH Berlin  
www.adame.de

# Exklusiv für Sie: Die COMPUTERWOCHE-Abo-Pakete Noch nicht abonniert? Jetzt aber los!



- ✓ **Mehr erfahren, viel sparen:**  
Erhalten Sie geballtes Fachwissen im Kombi-Paket zum sensationell günstigen Preis
- ✓ **Versandkostenfrei:** Druckfrisch und top-aktuell auf Ihrem Schreibtisch
- ✓ **Vorsprung durch Wissen:**  
Fundiertes Know-how von Experten exklusiv im Abo

✓ Großer Preisvorteil im Kombiabo!  
✓ Exklusiver Premium-Content online!

**Schnell sein lohnt sich:**  
Jetzt bestellen und aus einer Vielzahl von Prämien wählen!  
(Prämienbeispiel: Handy LG GB210)

**Bestellhotline:**  
0180 5 72 7252-276\*  
(\*aus dem dt. Festnetz nur 0,14 € pro Minute, Mobilfunkpreise max. 0,42 € pro Minute)

Alles rund um die Abo-Pakete Ihrer COMPUTERWOCHE finden Sie unter

[www.computerwoche.de/aboshop](http://www.computerwoche.de/aboshop)

# Virtualisierung 2.0 mit Oracle VM

Björn Bröhl, OPITZ CONSULTING GmbH

**Vor dem Hintergrund anhaltenden Kostendrucks und des verstärkten Interesses an Green IT ist Server-Virtualisierung nach wie vor eines der wichtigsten aktuellen IT-Themen.**

Der Anspruch der Kunden hat sich gewandelt. Während in der Vergangenheit vorrangig Test- und Entwicklungsumgebungen virtualisiert wurden und Virtualisierung als Hilfsmittel für Server-Konsolidierung angesehen wurde, steht die IT heute vor wesentlich komplexeren Herausforderungen: Kunden verlangen nach kompletten Lösungen, die sich einfach integrieren und kosteneffizient betreiben lassen. Auf Infrastruktur-Ebene versprechen dies die Virtualisierung 2.0 und der Übergang zu Cloud-Computing-Betriebsmodellen.

Oracle bietet mit Oracle VM eine Lösung zur Server-Virtualisierung an, die für die Virtualisierung von unternehmenskritischen Anwendungen gebaut wurde.

Doch die Oracle-Produktstrategie geht weit über die eigentliche Virtualisierung hinaus: Im Gegensatz zu anderen Herstellern, die nur einzelne Komponenten des Software-Stacks anbieten, fokussiert Oracle auf einen kompletten, funktionierenden Software-Stack. Aus Sicht von Oracle kann nur so eine optimale Bereitstellung der IT-Services mit minimalem Integrations- und Wartungsaufwand gewährleistet werden. Wichtige Komponenten sind hier:

- Grid-Computing, basierend auf der Kombination aus Server-Splitting (mittels Oracle VM) und Server-Pooling (mittels Real Application Cluster)
- Integriertes Management über alle Ebenen des Software-Stacks (Enterprise Manager Grid Control)
- Ein Ansprechpartner für den Support des gesamten Software-Stacks

## Fundamentaler Baustein für eine neue RZ-Generation

Die Virtualisierung in der Generation 2.0 umfasst nicht nur eine virtualisier-

te Infrastruktur. Der Anspruch besteht heute darin, eine einfache, agile, administrierbare und kosteneffiziente IT-Infrastruktur zu implementieren und zu erhalten. Dies kann aus Sicht von Oracle nur dann gelingen, wenn sämtliche Layer im Software-Stack integriert und einheitlich – durch Management-Tools und Support-Services – verwaltet und gewartet werden können.

Als führender Anbieter von Middleware, Datenbanken und Applikationen verfügt Oracle über eine einzigartige Ausgangssituation, um IT-Anwendungen gemäß dem Anspruch von Virtualisierung 2.0 anzubieten. Der Kundenmehrwert entsteht dabei über den gesamten Lebenszyklus, vom initialen Deployment und Provisioning bis zum Management und Support.

Auch wenn Oracle VM nur ein Bestandteil des gesamten Software-Stacks ist, kommt diesem Layer eine fundamentale Rolle zu. Oracle hat im vergangenen Jahr erhebliche Ressourcen in die Entwicklung von Oracle VM wie auch in die Unterstützung der Xen-Community, die den zugrundeliegenden Hypervisor entwickelt, investiert. Darüber hinaus wurde der Hersteller Virtual Iron akquiriert, dessen Virtualisierungsprodukte sich insbesondere durch einfache Bedienbarkeit und ein breites Set an Funktionalitäten auszeichnen.

Die neue Generation von Oracle VM ist somit leistungsfähiger denn je. Im Bereich Ressourcen- und Kapazitätsmanagement wird es beispielsweise möglich sein, anhand der tatsächlichen Ist-Auslastung virtuelle Maschinen konsolidieren zu lassen – automatisiert, ohne manuellen Eingriff des Administrators. Damit stellt Oracle Anwendern mit Oracle VM eine vollständige und effiziente Virtualisierungslösung für den Betrieb und das Management des Rechenzentrums zur Verfügung.

## Grid-basierte Virtualisierung und Oracle VM

Oracle ist der einzige Hersteller, der die Technologien der Server-Virtualisierung über physikalische Systeme hinweg (sogenanntes „Clustering“) mit der Virtualisierung innerhalb eines Systems – zur Aufteilung des Systems – komplementär verbindet.

Datenbank- und Middleware-Cluster können so aus physikalischen und virtuellen Knoten gebaut werden oder aus einer Kombination von beiden. Produktseitig ergibt sich damit eine Kombination aus Oracle Real Application Cluster und Oracle VM.

Kunden wie beispielsweise die University of Massachusetts setzen auf exakt diese Kombination. Sie erschließen sich damit die Vorteile einer noch konsequenteren Server-Konsolidierung: Durch das Pooling der Ressourcen können die Systeme je nach aktueller Auslastung der RAC-Datenbank oder einer anderen Oracle-Anwendung zur Verfügung gestellt werden. Es ist auch möglich, einen Server mit mehreren CPUs mittels Hard-Partitioning aufzuteilen und somit nur einzelne CPUs des Servers für RAC zu lizenzieren. Zwar bedeutet dies eine Einschränkung der

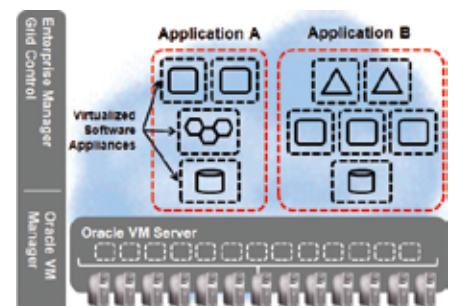


Abbildung 1: Oracle kombiniert die Virtualisierung über physikalische Instanzen hinweg und innerhalb von einzelnen physikalischen Ressourcen

gewünschten Flexibilität in der Systemnutzung – allerdings zugunsten einer optimierten Lizenzierung.

Der Zeitaufwand für das Provisionieren neuer Anwendungen umfasst das Server-Deployment sowie die Installation und Konfiguration der Software. Durch Einsatz von Oracle VM lassen sich beide Phasen verkürzen, denn mittels der VM-Templates stehen vorkonfigurierte, direkt lauffähige virtuelle Maschinen zur Verfügung, so dass man beispielsweise RAC-Knoten einfach und direkt starten kann.

Schließlich lassen sich mit Oracle VM auch virtuelle RACs aufsetzen, also ein Cluster mit mehreren virtuellen Knoten auf einem einzelnen Server. Während diese Konfiguration für eine Produktivumgebung ungeeignet ist, kann sie dennoch für Test- und Demozwecke oder für eine Entwicklungsumgebung wertvoll sein. Nicht zuletzt ist Oracle VM die einzige Virtualisierungslösung für Oracle RAC auf x86- / x86-64-Hardware, die von Oracle zertifiziert und von Seiten des Supports vollständig abgedeckt wird.

### Ganzheitliches Management des Software-Stacks

Oracle VM Manager bietet sämtliche Basisfunktionalitäten, um den Lebenszyklus einer virtuellen Maschine abzubilden. Viele Oracle-Kunden haben jedoch Management-Bedürfnisse, die weit darüber hinausgehen. Deshalb gibt es ein Oracle VM Management Pack für den Oracle Enterprise Manager 10g.

Die Vorteile für das System-Management sind:

- *Automatisiertes Patchen*  
Das Patchen des Betriebssystems und anderer Oracle-Software-Komponenten innerhalb der virtuellen Maschinen ist ohne manuellen Eingriff möglich.
- *Performance sichtbar machen*  
Mittels Monitoring des Zustands von Applikationen, Infrastruktur-Komponenten und Business-Services werden die Performance der virtuellen Infrastruktur und die Applikationsperformance sichtbar. Diese Informationen ermöglichen es dem Administrator, die physikalischen Server- und Storage-Ressourcen den virtuellen Gästen individuell zuzuordnen – anhand von Applikationsbedürfnissen und Geschäftsprioritäten.
- *Daten sammeln*  
Der Oracle Enterprise Manager sammelt Performance- und Verfügbarkeitsdaten, wie die CPU- und Memory-Auslastung oder den Platten- und Netzwerk-Durchsatz, von Oracle VM Servern und den virtuellen Gästen.
- *Komponenten inventarisieren*  
Im Bereich Configuration Management wird automatisch ein Inventar an virtualisierten Infrastrukturkomponenten in einem zentralen Repository geführt
- *IT-Compliance einhalten*  
Der Policy Manager hilft bei der kontinuierlichen Einhaltung von IT-Compliance.
- *Weniger Aufwand durch Automatisierung und Standardisierung*  
Ein automatisierter Lebenszyklus der virtuellen Maschinen reduziert

den Aufwand, neue Betriebssystem- oder Applikationsumgebungen zur Verfügung zu stellen und sorgt für Standardisierung, indem bereits bestehende Konfigurationen geklont werden.

- *Geringere Ausfallzeiten*  
Die Ausfallzeiten von Applikationen werden reduziert, indem der Application Service automatisiert im laufenden Betrieb auf andere physikalische Ressourcen im Serverpool verlagert wird.

Fazit: Oracle-Anwender profitieren von einem einheitlichen Management-Tool für den gesamten Stack – von der Applikation bis zur virtuellen Infrastruktur.

### Best Practices

„Den Weg“ zum Next Generation Data Center gibt es nicht. Vielmehr müssen verschiedene Anforderungen an das Rechenzentrum überprüft und in Einklang gebracht werden. Im nachfolgenden Abschnitt sind mögliche Ansprüche und die angewandten Lösungsszenarien beschrieben. Alle genannten Anforderungen beruhen auf Kunden-Erwartungen und wurden bereits durch Oracle Technologie gelöst.

Spricht man heute mit Kunden, RZ-Leitern oder IT-Verantwortlichen darüber, welche Anforderungen sie an den Betrieb der Systeme und Anwendungen haben, so werden folgende Punkte am häufigsten genannt:

- Flexibilität in der Reaktion auf neue Anforderungen
- Erfüllung und Überwachung von Compliance-Anforderungen
- Senkung der Betriebskosten

Darüber hinaus werden natürlich noch weitere Anforderungen genannt, auf die dieser Artikel nicht explizit eingeht.

### Flexibilität

In vielen Fällen ist die IT nur Erfüllungsgehilfe und reagiert mehr oder weniger schnell auf neue Anforderungen. So müssen zum Beispiel neue Systeme, Datenbanken oder Anwendungen (beispielsweise mit Middleware)

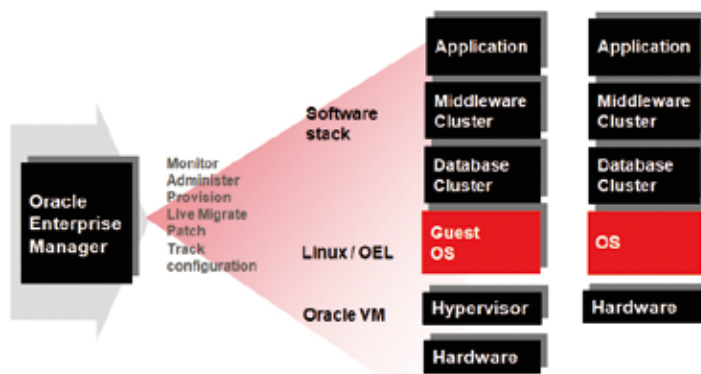


Abbildung 2: Das Oracle VM Management Pack ermöglicht einen ganzheitlichen Ansatz für die Verwaltung von System-Ressourcen

zur Verfügung gestellt werden. Ein anderes Beispiel ist die Bereitstellung von Testsystemen. Diese zeichnet aus, dass sie nur eine gewisse Zeit (während der Testphase) verfügbar sein müssen.

Dazu ein Projektbeispiel: Ein Kunde wollte die Bereitstellungszeit von neuen Systemen drastisch verkürzen. Bisher wurden fünf bis zehn Arbeitstage benötigt, um ein neues Oracle Datenbank-System aufzusetzen. Der Kunde setzte bisher zwar schon Virtualisierung ein – allerdings nicht für Oracle-Systeme.

Durch die Einführung von Oracle VM konnte er die Zeiten für das Deployment neuer Systeme auf wenige Minuten reduzieren. Dies ist durch die Option möglich, bestehende virtuelle Server zu klonen oder aus Templates zu erzeugen. Um Templates virtueller Maschinen nutzen zu können, gibt es verschiedene Möglichkeiten zur Auswahl. Die einfachste Variante ist der Einsatz bereits komplett fertiger Templates von Oracle. Auf der Website <http://edelivery.oracle.com/oraclevm> stehen verschiedene zur Verfügung, bestehend aus Betriebssystem (Oracle Enterprise Linux) und weiterer, bereits fertig installierter Oracle Software (Weblogic Server, Datenbank, Siebel etc.). Diese muss man lediglich herunterladen und in Oracle VM registrieren.

Ist die gewünschte Konfiguration noch nicht als Template vorhanden

oder soll andere Software innerhalb eines Templates zur Verfügung stehen, bietet der Oracle VM Template Builder eine Möglichkeit zur Erstellung und Konfiguration von Templates.

**Verfügbarkeit**

Besondere Ansprüche an das Rechenzentrum stellen auch Anwendungen, die hochverfügbar betrieben werden müssen. Benötigt werden für solche Anwendungen meist verschiedene Backend-Systeme (Datenbank, Middleware etc.). Außerdem muss man für jede dieser Komponenten eigene HA-Konfigurationen implementieren und betreiben.

Auch dazu ein Projektbeispiel: Ein Automobil-Zulieferer betreibt eine Anwendung zur Produktionsplanung und -steuerung. Da die Produktion in mehreren Schichten erfolgt, muss diese Anwendung hochverfügbar betrieben werden. In Betrieb befinden sich hierzu eine Datenbank als Real Application Cluster (RAC) und zwei Middleware-Server als Aktiv-Aktiv-Cluster. Insgesamt sind vier dedizierte Server und ein Storage-System im Einsatz.

Um die beschriebene Umgebung zu optimieren, wurde Oracle VM auf zwei neuen Servern installiert und für die Kompensation eines möglichen Serverausfalls wurde Oracle VM als Clus-

ter konfiguriert. Dazu konnte man das bestehende Storage des Kunden weiter verwenden. Mit Oracle VM wurden vier virtuelle Server eingerichtet – zwei als Basis für die RAC-Datenbank und zwei weitere als Basis der Middleware. Neben der reinen Konsolidierung (Einsparung von Hardware-Ressourcen) war auch die Verfügbarkeit sichergestellt. Darüber hinaus besitzt der Kunde nun eine Umgebung, die über entsprechende Kapazitäten verfügt, um weitere virtuelle Systeme und damit auch weitere Anwendungen und Datenbanken zu betreiben.

**Betriebskosten und Einhaltung von Compliance-Regeln**

In den beiden beschriebenen Beispielen wurden primär Anforderungen an die Flexibilität und Verfügbarkeit gestellt. In größeren Rechenzentren kommt in der Regel noch dazu, dass diese Anforderungen für eine größere Anzahl von Systemen gelten und dadurch ein besonderes Augenmerk auf das Management der großen Umgebung gelegt wird. Zusätzlich existieren in vielen Fällen Compliance-Regeln, die eingehalten und überwacht werden müssen. Dazu ein Beispiel: Ein Unternehmen im Pharma-Umfeld betreibt über tausend Oracle Datenbanken. Dazu sind über zweihundert Server-Systeme im Einsatz, auf denen jeweils mehrere getrennte Oracle Homes (ein Oracle Home je Datenbank) installiert sind. Um diese Umgebung administrieren und überwachen zu können, wird Oracle Grid Control verwendet. In solch einer großen Umgebung sind ständig Systeme abzulösen oder neu zu implementieren.

Parallel zu den bestehenden Systemen wird eine Farm von Oracle VM-Servern installiert. Diese sind alle als Cluster konfiguriert, um den Ausfall der VM-Server zu kompensieren. Damit die Implementierung von neuen Systemen zukünftig einfacher wird, soll primär mit Templates von virtuellen Servern gearbeitet werden. Oracle Grid Control administriert und überwacht auch diese neue Umgebung. Dies ermöglicht den Administratoren die Verwendung eines Tools sowohl für die alten als auch für die neuen Systeme. Dabei

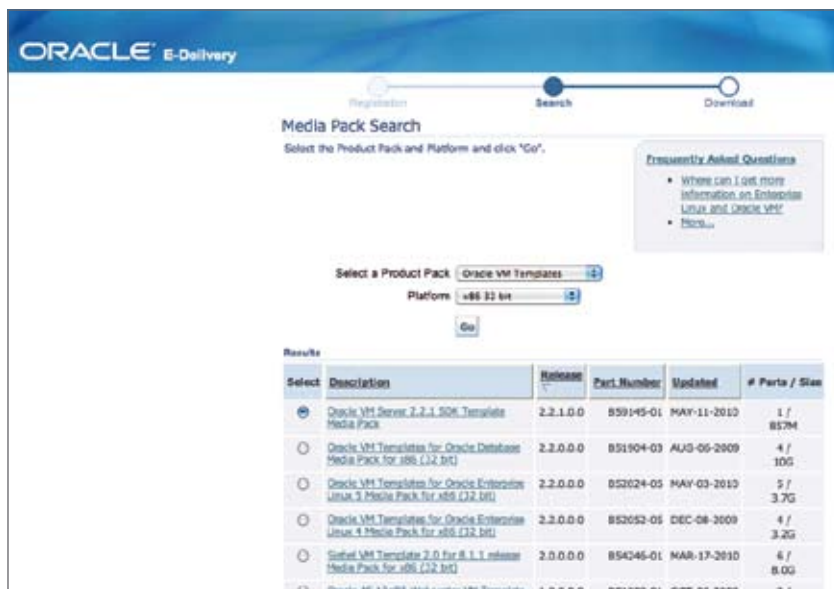


Abbildung 3: Screenshot der Oracle Website mit verschiedenen Templates von virtuellen Servern

ist es egal, ob diese virtualisiert oder auf physikalischer Hardware betrieben werden. Auch die Überwachung und Einhaltung definierter Compliance-Regeln ist durch die Integration in Grid Control kein Problem. Alle Änderungen an der Konfiguration werden hier erfasst und sind somit nachvollziehbar.

**Fazit**

Bevor man daran geht, wie beschrieben eine einfache, agile, administrierbare und kosteneffiziente IT-Infrastruktur zu implementieren, sollte man verschiedene Faktoren berücksichtigen:

- Als Erstes gilt es zu beachten, ein valides und realisierungsfähiges Konzept für die gesamte Infrastruktur und die Dienste (Datenbanken, Middleware, Anwendungen etc.) zu erstellen.
- Der besondere Vorteil einer Lösung mit Oracle VM und weiteren Oracle-Komponenten besteht darin, dass

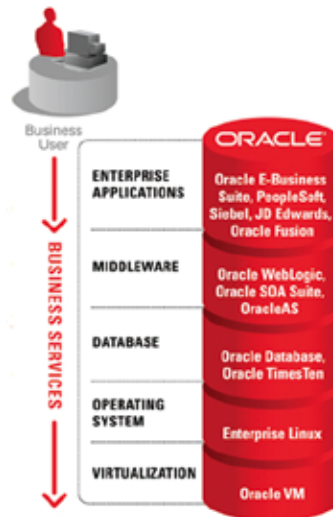


Abbildung 4: Reduzierung des Technologie-Stacks zur Optimierung der Kompatibilität, Stabilität und Kosten

- Oracle diese als einziger Hersteller für alle Schichten liefern kann.
- Kommen Virtualisierungstechnologie, Betriebssystem, Datenbank,

Middleware und Oracle Grid Control für die Überwachung und Administration aus einer Hand, sichert dies ein optimales Maß an Kompatibilität und Stabilität.

- Gleichzeitig sorgt dieser Umstand für die Optimierung der Kosten (etwa durch spezielle Lizenzvorteile auf Basis von Oracle VM) und die Sicherstellung des bestmöglichen Supports – nicht von unterschiedlichen Herstellern, sondern aus einer Hand.

Nach Erstellung des Konzepts sollten eine Ressourcen-Planung und die Dimensionierung der Infrastruktur erfolgen. Damit ist aus unserer Sicht der Grundstein für das Datacenter gelegt. Da die Umsetzung schrittweise vollzogen werden kann, muss der Weg zum Next Generation Data Center also gar nicht steinig sein.

**Kontakt:**

Björn Bröhl

bjoern.broehl@opitz-consulting.com



## Technology for success

Wir unterstützen Ihren Erfolg mit der Konzeption und dem Aufbau Ihrer Datenbankanwendungen, sowie deren technischem Support.

Wir von der Krug & Partner GmbH bestehen aus einem hoch motivierten Team von Oraclespezialisten. Regelmäßige Schulungen halten unsere Fachkräfte immer auf dem aktuellsten Stand der Technik.

- **Datenbanken**  
Datenbank-Installation & -Konfiguration  
Administration & Wartung  
Backup/Recovery  
Health-Check
- **Projekte**  
Gewerblicher Rechtsschutz (IP)  
Automotive Medien- & Energiewirtschaft
- **Application Server Systeme**  
JDeveloper Forms & Reports  
PL/SQL (CMSDK, OEM, Disco...) u.v.m.
- **Lizenzierung**  
Beratung & Analyse des Lizenzstatus  
Lizenzierung



# Das Business ist nicht nur online – Erfahrungen mit der Oracle Database Lite im Außendienst

Volker Ricke, POINT. Consulting GmbH

Die mobile Datenbank-Plattform Oracle Database Lite ist ein effizientes Werkzeug zum Austausch von Informationen zwischen einer Oracle Datenbank und mobilen Endgeräten. Im Oracle Portfolio tritt sie allerdings nicht sehr stark in Erscheinung. Ist es daher eine Mutprobe, Oracle Lite in einem strategischen Außendienstprojekt einzusetzen? Erfahrungen aus mobilen Projekten beantworten diese Frage und zeigen Stärken und Schwächen der „leichten“ Oracle Datenbank auf.

Für ein bekanntes Unternehmen aus der Konsumgüter-Branche ist der Außendienst von elementarer Bedeutung gegenüber dem Wettbewerb. Frühzeitig begann er mit der Entwicklung eines Marketing-Außendienst-Systems für die Betreuung der Verkaufsstellen – der Begriff „Customer Relationship Management“ (CRM) hatte sich zu diesem Zeitpunkt noch gar nicht eingebürgert. Ein Konsumenten-Kontaktpflegesystem und eine Datenbank für die Unterstützung der Marketing-Aktivitäten in Hotels, Restaurants und Cafés wurden durch unterschiedliche Dienstleister beigesteuert (siehe Abbildung 1).

Eine Vielzahl von Technologien fand hier bis 2003 Verwendung:

- C++ Anwendung auf Windows PC, Datenbank und Replikation über Lotus Notes, Schnittstellen über Flat Files zum IBM-Großrechner und zur Oracle Datenbank
- C++ Anwendung auf Pocket PC (Windows CE), Microsoft SQL Server und SQL-Server-Mobile-Edition-Datenbank, keine Schnittstellen zur zentralen Oracle Datenbank
- Von einer Fachabteilung direkt beauftragte Microsoft Access-Anwendung auf Windows Notebooks

Im Zuge einer anstehenden Konsolidierung der IT-Systeme – Oracle war als zentrale Datenbank-Plattform vorgesehen – wurden auch die Außendienst-

Systeme auf Schwächen untersucht. Insbesondere folgende Punkte fielen dabei auf:

- Wartungs- und supportintensive Schnittstellen zwischen den Lotus-Notes-Server-Repliken und der zentralen Oracle Datenbank
- Medienbruch durch die unterschiedlichen Datenstrukturen in Lotus Notes und der relationalen Oracle Datenbank
- Insellösung Microsoft SQL Server ohne Anbindung an die zentralen Auswertungs- und Planungslösungen
- Fachlich und technisch bereits mit fünf Benutzern überforderte Access-Lösung mit vielen Problemen beim Datenaustausch

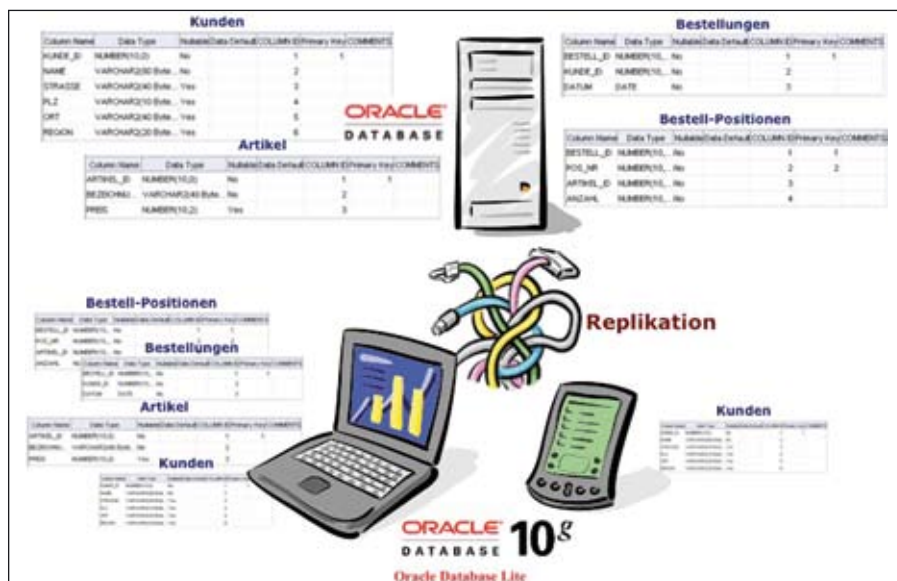


Abbildung 1: Daten mobil

Nach einer erfolgreichen Teststellung fiel die Entscheidung, zukünftig Oracle Database Lite für alle mobilen Systeme zu nutzen. Von der Lösung wurden einige Vorteile erwartet:

- Eine standardisierte Replikationsplattform erleichtert die Zentralisierung des Application Supports für alle mobilen Systeme und reduziert die Kosten für Entwicklung und Infrastruktur
- Oracle Lite unterstützt mit demselben Replikationsmodell die verwendeten Client-Plattformen MS Windows und Windows CE
- Die Datenbanken sämtlicher zentraler OLTP- und OLAP-Anwendungen werden im Zuge der Großrechner-



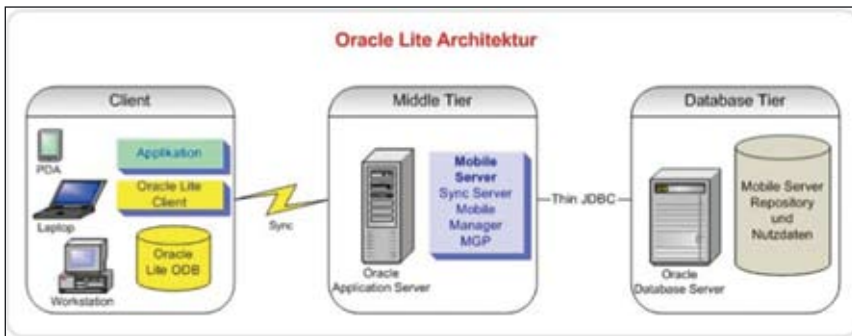


Abbildung 2: Die Architektur

Ablösung auf Oracle migriert, so dass mit einer Oracle-internen Replikation auf weitere Schnittstellen verzichtet werden kann

- Auch die Daten der bisherigen Insel-lösungen werden direkt in der zentralen Datenbank auswertbar sein
- Alle mobilen Systeme können die Stammdaten gemeinsam verwenden

Als Pilot-Projekt wurde 2003 die Pocket-PC-Lösung auf Oracle 9i Lite umgestellt. Gleichzeitig hat man die Lösung auch für Windows-Notebooks verfügbar gemacht. 2005 und 2006 wurden das Marketing Außendienstsystem von der Lotus-Notes-Datenbasis auf die nun verfügbare Version Oracle 10g R2 Lite umgestellt sowie die bisherige Access-Lösung durch eine Neuentwicklung unter Microsoft .Net und Oracle Lite abgelöst. Nachdem der Pocket PC nicht mehr gefragt war, hat man 2006 auch das Konsumenten-Kontaktpflege-System auf eine Laptop-gerechte Oberfläche umgestellt. Somit sind seit 2006 drei Außendienst-Systeme mit der Oracle Lite Datenbank im Einsatz:

- 160 Snapshots, 220 User, 100.000 bis 350.000 Datensätze pro Client
- 90 Snapshots, 50 User, ca. 450.000 Datensätze pro Client
- 32 Snapshots, 60 User, ca. 11.000 Datensätze pro Client

Die Anwender replizieren mindestens täglich und benötigen für den Austausch von rund 500 geänderten Datensätzen pro Sync zwischen fünf und dreißig Sekunden. Nach Bewältigen einiger Anlaufprobleme entstand eine stabile Replikationsumgebung.

**Was ist Oracle Lite?**

Oracle Lite macht Daten aus einer Oracle Datenbank offline auf unterschiedlichen mobilen Endgeräten verfügbar (Windows, Windows Mobile, Symbian, Linux sowie in der im Februar 2010 eingeführten Version 10.3.0.3 auch SQLite Clients wie Blackberry). Oracle Lite besteht aus einem Replikations- und Administrationsserver („Mobile Server“), einem Datenbank-Repository und dem Client.

Varianten wie „Web-To-Go“ (online und offline lauffähige Java Web-Anwendungen) und „Branch Office“ (netzwerkfähige Oracle Lite Datenbank für Zweigstellensysteme wie Kassenterminals) ergänzen die reine Client-Datenbank. Für einige Plattformen ist auch ein Device Manager enthalten, über den administrative Zugriffe auf die Clients möglich sind. Der Oracle Lite Client ist auf dem Desktop nur wenige Megabyte groß, die Datenbank

selber wird automatisch bei der ersten Replikation eines Clients erstellt und ist administrationsfrei.

Zum Aufsetzen der Replikation steht ein Development Kit zur Verfügung, das aus grafischen Werkzeugen und einem Java API besteht. Die Abläufe für das Erstellen der Replikationsobjekte sind immer gleich – unabhängig davon, ob die Zielplattform eine Telematik-Box unter Embedded Linux oder ein Windows Notebook ist. Struktur und Datenmenge der Snapshots werden als SQL-Statement formuliert. Das SQL kann Bind Variablen enthalten, mit deren Hilfe die Datenauswahl dem einzelnen Benutzer angepasst werden kann.

Der Austausch der client- und serverseitigen Änderungen erfolgt über In- und Out-Queues, was die erforderliche Online-Zeit reduziert. Die eigentliche Verarbeitung der Queue-Tabellen – also das Einspielen der von den Clients gesendeten Daten in der zentralen Datenbank und das Bereitstellen der serverseitigen Änderungen in den Out Queues – erfolgt in einem asynchronen Prozess, dem „Message Generator & Processor“ (MGP).

Die Clients kommunizieren ausschließlich mit dem Replikationsserver und bauen keine direkte Verbindung zur zentralen Datenbank auf. Die Replikation kann manuell durch den Anwender oder per Sync API über die Anwendung initiiert werden. Seit Version 10g R3 Lite können Snapshots automatisch im Hintergrund aktualisiert wer-

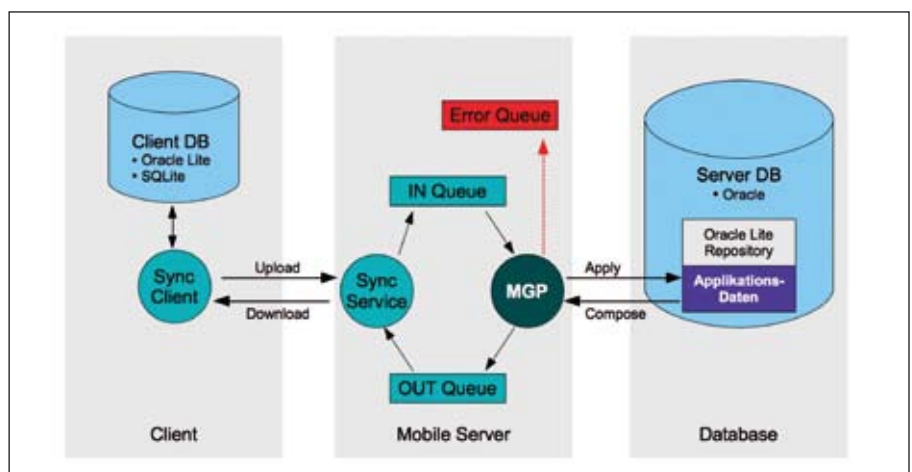


Abbildung 3: Asynchrone Oracle Lite Replikation

den, sobald eine Verbindung zum Mobile Server aufgebaut ist.

### Warum keine Online-Lösung?

Der Außendienst des Unternehmens ist in ganz Deutschland und Österreich unterwegs. Der Einsatz einer reinen Online-Lösung wäre riskant, Punkte wie die mangelhafte Mobilfunkabdeckung in einigen Regionen oder eine schlechte Übertragungsrate durch überlastete Funkzellen sprechen auch heute noch für eine Offline-Lösung mit Replikation. Je nach Umfeld kann sich in anderen Projekten aber auch eine Online-Lösung empfehlen, die gegenüber einer Replikationslösung mit aktuelleren Daten und weniger Konfliktpotential punkten kann. Als Kompromiss bietet sich eine Lösung an, die je nach Verfügbarkeit auf Online-Daten oder die lokale Replik zugreift.

### Erfahrungen mit Oracle Lite

Gegenüber dem eher unspektakulären Piloten boten die Folgeprojekte größere Herausforderungen. Nachfolgend einige Projekt-Erfahrungen:

- *Gute Admin-Werkzeuge*  
Vieles hat sich seit Version 10g R2 für den Administrator getan. Gab es in 9i nur eine rudimentäre Verwaltungsoberfläche, in der nicht viel mehr möglich war, als mobile Benutzer anzulegen und mit ihren Datenteilmengen-Parametern für eine Anwendung zu berechtigen, gibt es nun sehr umfangreiche Monitoring- und Administrationsfunktionen. Ob die Synchronisations-Historie detailliert angezeigt, die Error Queue bereinigt und nachverarbeitet, eine Parameter-Änderung auf einem Client durchgeführt oder ein umfangreiches Tuning vorgenommen werden soll – der Mobile Manager bietet viele praxisgerechte Funktionen.
- *Schwaches Developer Kit*  
Bei dem Unternehmen lag der Fokus auf den Programmiersprachen C# und PL/SQL. Auf den Einsatz von Java sollte verzichtet werden. Normalerweise kein Problem, da Oracle

Lite ja grafische Tools zum Aufbau der Replikationsobjekte bereitstellt. Aus heutiger Sicht lohnt sich die Einarbeitung in das Oracle Lite Java API. Weder der Packaging Wizard aus der Version 9i (maschinelle Benennung der Objekte erschwert das Monitoring, Probleme mit der Verwendung der gleichen Basistabelle in Snapshots zweier Projekte), noch die in 10g R2 neu eingeführte Mobile Database Workbench (arbeitet direkt im Repository, keine Versionierung möglich, fehlerhaftes Deployment, Fehlen jeglicher Sortierung im GUI) arbeiten zuverlässig und intuitiv. Die Mobile Database Workbench (MDW) ist immerhin ganz gut für den Einstieg geeignet, um die Struktur der Oracle Lite Replikation zu verstehen. Oracle tut sich aber keinen Gefallen damit, ausgerechnet die Werkzeuge, die der Entwickler als erstes zu sehen bekommt, so schwach auszuführen. In den Projekten wurden die Objekte mit der MDW aufgebaut, die Migration von Schema-Änderungen erfolgte direkt per MDW im Ziel-Repository.

- *Einstellungen*  
Im Auslieferungszustand scheint Oracle Lite nur für kleinere Systeme ausgelegt zu sein. Es mussten einige Parameter auf dem Client, dem Mobile Server und dem Application Server angepasst werden, um eine stabile Replikation zu gewährleisten.
- *Schema-Evolution*  
Zu den Weiterentwicklungen der Systeme nach ihrem Rollout gehörten auch Datenbank-Änderungen. In einer Replikationsumgebung können Tabellenänderungen kritisch werden. Oracle empfiehlt, vor Änderungen an Oracle Lite Snapshots die entsprechenden Objekte zu löschen und neu anzulegen. In der Praxis hat sich diese Vorgehensweise bewährt: für Read-Only Snapshots wird der Empfehlung gefolgt – die Clients können hier keine offenen Änderungen haben. Bei änderbaren Snapshots klappt das Hinzufügen neuer Spalten auch über ein rei-

nes Ändern der Replikationsobjekte, so dass der Client noch die Chance hat, offene Änderungen zu replizieren, bevor er die Tabellen-Erweiterung erhält.

- *Performance*  
Viele Punkte sind bei der Gestaltung der Snapshot Queries zu beachten. Diese werden nicht nur während der Replikation, sondern insbesondere auch durch den MGP beim Verteilen der zentralen Änderungen auf die Out Queues der jeweils betroffenen Clients ausgeführt. Die Art und Weise der Einbindung des SQLs in die MGP-Abfragen kann über Templates optimiert werden, diese können aber natürlich ein bereits langsames Snapshot SQL nicht beschleunigen. Manchmal half nur ein gezieltes Denormalisieren.
- *Änderungsprotokoll*  
Oracle Lite arbeitet mit „dirty records“ – per Trigger werden alle Zeilen der Basistabellen markiert, auf die DML abgesetzt wurde, unabhängig davon, ob bei Updates relevante Änderungen vorgenommen wurden. Es sollten an die Clients aber nur die tatsächlichen Änderungen übertragen werden. Insbesondere für Schnittstellen hieß es daher, Updates nur bei inhaltlichen Änderungen vorzunehmen, ein Merge konnte nicht verwendet werden.
- *Konflikte*  
Wenn Datensätze gleichzeitig auf Client- und Serverseite geändert werden, zieht die Konflikt-Auflösung. Standardmäßig lassen sich in Oracle Lite die Regelwerke „Client siegt“ oder „Server siegt“ einstellen. Reicht das nicht aus, kann man per PL/SQL eigene Konfliktauflösungen einbinden.
- *Verteilte Sequences*  
Eine wichtige Neuerung war in Version 10g R2 das Modell verteilter Sequences. Es können Fenstergrößen definiert werden, aus denen die Clients überschneidungsfreie Werte ziehen können, per Schwellwert wird der Grenzwert definiert, ab dem bei

## Probleme mit Ihren Geschäftsprozessen?



Sprechen Sie uns an - wir optimieren Ihre IT!

### Strategieberatung

Mit optimierten Geschäftsprozessen und cleveren IT-Strategien die Zukunft aktiv gestalten. Wir zeigen Ihnen wie!

### Projektmanagement

Von der Vision bis zur Einführung: GPM zertifizierte Projektleiter garantieren Projektmanagement auf höchstem Niveau.

### Technologie

Das Beste aus beiden Welten mit Oracle und Open Source. Richtungsweisende Internet Applications mit Adobe Flex, ADF, APEX und Grails.

Erleben Sie uns live auf der DOAG Konferenz + Ausstellung  
16. - 19. November - Nürnberg

Profitieren Sie von unserem Oracle Know-how in den neuen esentri Workshops:

APEX Einsteiger	2 Tage
APEX Allrounder	1 Tag
APEX Champion	2 Tage

Nutzen Sie auch den individuellen IT-Fitness Workshop und erfahren Sie, welche Potenziale in Ihrer IT stecken.

# esentri

Stephanienstr. 36  
76133 Karlsruhe  
Tel. 0721 / 7540 7530  
Fax 0721 / 7540 7539  
www.esentri.com  
info@esentri.com

der nächsten Replikation ein neues Window generiert wird. Überschneidungen zur Sequence auf dem Server lassen sich ausschließen, indem eine Seite lediglich gerade, die andere ungerade Werte erhält.

- **Client-Installation**

Den personalisierten Oracle Lite Client soll der Anwender selber vom Mobile Server herunterladen und auf seinem Gerät installieren. Bis Version 10g R2 klappte das aber nicht ohne Administrator-Rechte. Auch eine Einbindung in die Software-Verteilungsmechanismen des Unternehmens ist wegen der Personalisierung nicht möglich, eine allgemeine MSI-Installer-Routine musste erstellt werden. Seit Version 10g R3 ist die Client-Installation aber auch mit eingeschränkten Rechten möglich.

- **Oracle Lite Datenbank**

Oracle Lite basiert auf einer eigenen Code-Basis und ist keine abgespeckte Version der Oracle Datenbank. Stored Procedures sind in Java, nicht aber in PL/SQL möglich, der Optimizer ist regelbasiert, die SQL-Syntax ist an die des Oracle Servers angelehnt, aber nicht mit ihr identisch. Viele standardmäßige Oracle Single Row Functions stehen aber auch in Oracle Lite zur Verfügung.

- **Mobile Device Manager**

War die Basis-Installation des Oracle Lite Clients auf dem Windows Notebook erfolgreich, ist der Device Manager eine echte Hilfe. Es lassen sich Oracle Lite Patches per Software-Update einspielen sowie zur Änderung von Parametern Kommandos verteilen.

- **Daten-Teilmengen über Abo-Tabelle**

Die Mimik, welcher Außendienstler welche Daten zu bekommen hat, kann in den Projekten komplex werden. Aus Performance- und Wartungsgründen sollte sich diese Komplexität aber nicht in den Snapshot Queries niederschlagen. Eine Abo-Tabelle mit der Zuordnung von Daten-IDs zu den Clients

wurde daher erstellt und mit zentraler Logik gepflegt. Per Subselect in den Snapshot Queries werden die Daten für die User gefiltert. Nach Änderung einer Zuordnung untersucht der Oracle Lite MGP auch die abhängigen Tabellen und generiert Änderungssätze in den Queue-Tabellen. Voraussetzung hierfür ist, dass die Abo-Tabelle ebenfalls mit in die Replikation aufgenommen ist.

- **Fehlverhalten**

Der Upload geänderter Daten eines Clients wird als eine Transaktion betrachtet. Können die Änderungen nicht in die zentrale Datenbank eingespielt werden, wandert die gesamte Transaktion in die Error Queue und wartet auf ihre Korrektur. Für den Außendienstmitarbeiter verwirrend ist jedoch, dass seine Daten bei der nächsten Replikation auf den Stand des Servers zurückgesetzt sind. Wurden die Daten in der Error Queue in der Zwischenzeit noch nicht korrigiert und nachverarbeitet, fehlen dem Client die vorher erfassten Daten. Um das zu vermeiden, wurden Up- und Download intelligenter gesteuert. Der Download erfolgt erst dann, wenn die Error Queue leer ist. Das Sync API bietet für jeden Sync-Schritt eigene Methoden an.

### Fazit

Oracle Lite ist keine Schonkost, dafür sind das Produkt zu komplex und seine Möglichkeiten zu umfangreich. Wer plant, Daten aus einer Oracle Datenbank auf mobilen Geräten verfügbar zu machen, sollte die Einbindung von Oracle Lite in Betracht ziehen. In der Design- und Implementierungsphase sind einige Punkte zu beachten, die große Auswirkungen auf die Stabilität und die Performance des Systems haben können. Als Belohnung für eine gut aufgesetzte Umgebung winkt eine stabile Replikations-Plattform für die gängigsten mobilen Endgeräte.

### Kontakt:

Volker Ricke  
volker.ricke@point-gmbh.com

# 2 RAC or not 2 RAC?

Rainier Kaczmarczyk, OPITZ CONSULTING München GmbH

**Oracles Real Application Cluster (RAC) bietet viele Vorteile hinsichtlich Verfügbarkeit und Skalierbarkeit – aber auch Nachteile, was die Komplexität und insbesondere die Lizenzkosten betrifft. In einem Beispielprojekt stand die Frage im Raum, ob nicht auch ein anderer Weg zum Ziel führen könnte. Zusammengefasst: „Ich habe eine Lösung. Nur passt sie auch zum meinem Problem?“**

Aufgabe des Projekts war, Flugbewegungsdaten, die mittels Radar erfasst worden sind, in einer Oracle Datenbank abzuspeichern. Die Ansprüche an die Verfügbarkeit lagen im Bereich von weniger als einer Sekunde Ausfallzeit und damit sehr hoch – schließlich war das vorliegende System für die Sicherheit des Flugverkehrs von einiger Relevanz. Pro Radarsystem waren allerdings weniger als zehn Arbeitsplätze vorgesehen.

RAC schien dem Team des Autors in diesem Fall die erste Wahl zu sein. Zumindest, wenn es den allgemeinen Aussagen über RAC uneingeschränkt Glau-

ben schenken konnte (siehe Abbildung 1). Doch leider hat es die Erfahrung gemacht, dass für den Betrieb eines RACs deutlich mehr Fachwissen benötigt wird als gemeinhin angenommen.

Ebenfalls gegen den Einsatz von RAC sprach, dass die Möglichkeiten der Administration der dezentralen Systeme vor Ort stark eingeschränkt waren. Sie sollte vorzugsweise im Tower des Flughafens und hier möglichst wartungsfrei erfolgen. Aus diesem Grund wurde ein robusteres System als RAC gewünscht. Auch hätte ein RAC bei Ausfall der gemeinsam genutzten Platten keinen ausreichenden Schutz geboten.

Oracle Data Guard und Oracle Streams kamen für dieses Projekt aus Kostengründen nicht in Frage, da das RAC-System als Standard Edition lizenziert werden kann, die beiden erstgenannten Optionen aber nur in der Enterprise Edition zur Verfügung stehen. Grob gesehen kostet eine Datenbank in der Enterprise Edition mindestens das Dreifache einer Standard Edition, eine Standard Edition One sogar nur die Hälfte der Standard Edition.

In dem Beispielprojekt bot sich ein Replikationsmechanismus als Lösung an. Da die beiden Rechnersysteme in diesem Fall nur eine Netzwerkverbin-

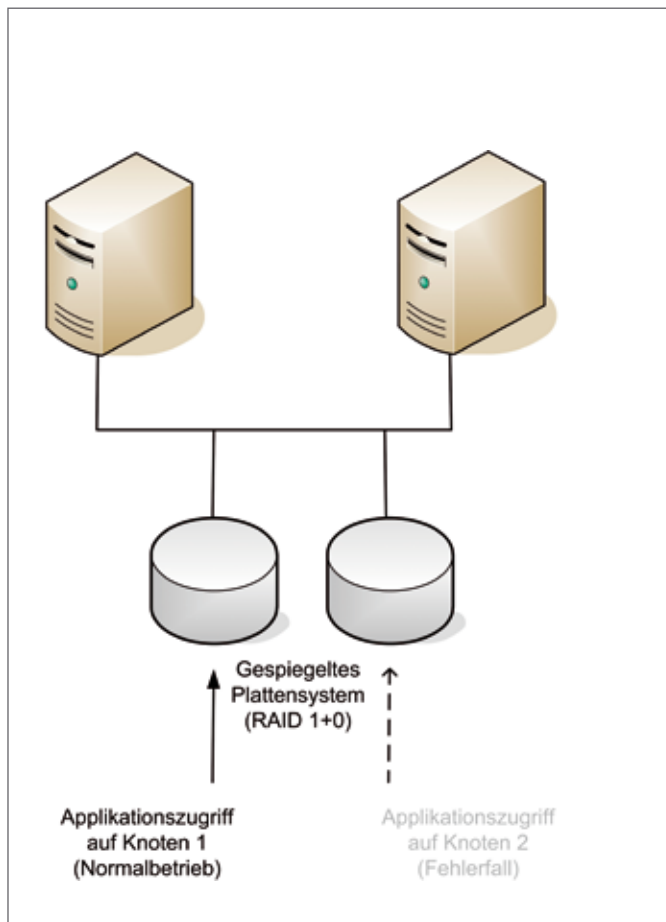


Abbildung 1: Klassisches RAC-Layout

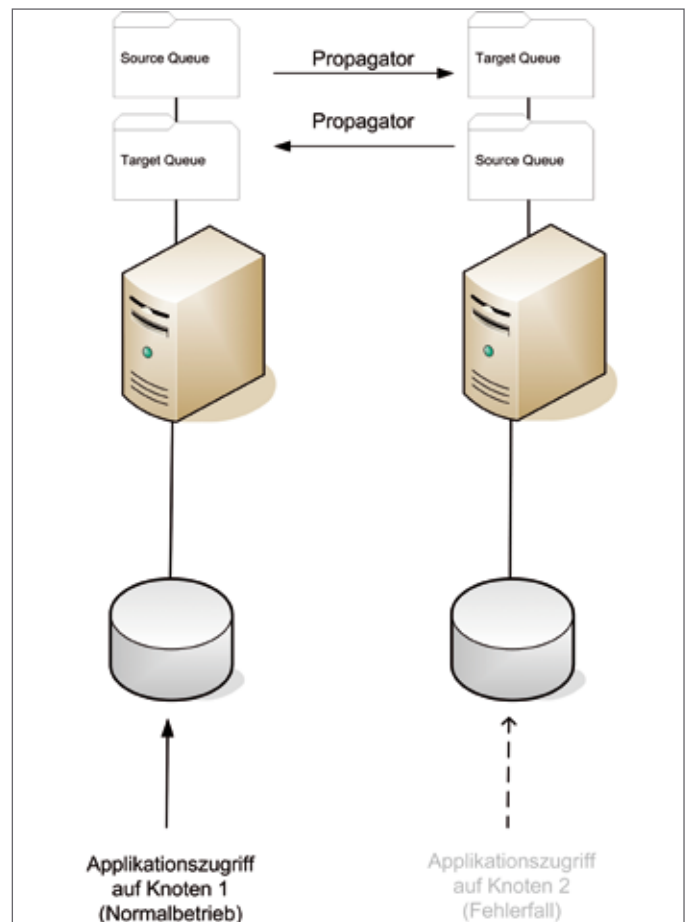


Abbildung 2: Replikation mit Advanced Queuing (AQ)

derung benötigten, konnten sie zudem ohne Aufwand räumlich getrennt betrieben werden, was die Sicherheit erhöhte. Realisiert wurde die Replikation mit Advanced Queuing (AQ).

Glücklicherweise war es möglich, die Datenbank-Anwendung entsprechend anzupassen. Nach einem Insert, Update oder Delete in der Datenbank (also einer DDL-Operation) auf dem Primärsystem wurde dieselbe DDL-Operation in die Source Queue des Primärsystems gestellt. Im nächsten Schritt übertrug der Propagator den Befehl automatisch innerhalb weniger Zehntelsekunden in die Target Queue des Sekundärsystems. Anmerkung: Der Propagator ist ein spezieller Prozess des Oracle Advanced-Queuing-Systems, der die Daten vollautomatisch von

der Source Queue in die Target Queue transferiert.

In der Target Queue wurde der Befehl in einem Endlosprozess ausgelesen und mittels „execute immediate“ ausgeführt. Um die Daten-Konsistenz auch im Fehlerfall (Sekundärsystem ist aktiv) zu gewährleisten, wurde dieser Mechanismus symmetrisch ausgelegt, wie Abbildung 2 zeigt.

Doch auch diese Architektur besitzt eine Achillesferse: Ein Datensatz, der bereits im Primärsystem vorhanden ist, wird vom Propagator nicht mehr übertragen, wenn das Primärsystem in diesem Moment abstürzt. Der Verlust einiger weniger Datensätze war bei dem vorliegenden System allerdings tolerabel und stand in unserem Projekt nicht im Widerspruch zur ge-

forderten Sicherheit des Flugverkehrs. Zudem geht der Datensatz in so einem Fall auch nicht komplett verloren, da Advanced Queuing die Persistenz bei einem Wiederanlauf des abgestürzten Systems gewährleistet.

Mithilfe von Advanced Queuing (AQ) wurde somit ein hochverfügbares und sehr robustes System aufgebaut. Auch bezüglich der Kosten bot das gewählte Vorgehen erhebliche Vorteile: Da Advanced Queuing in der Standard Edition One verfügbar ist, konnten die Lizenzkosten, im Vergleich zur ursprünglich vorgesehenen Standard Edition, halbiert werden.

**Kontakt:**

Rainier Kaczmarczyk  
rainier.kaczmarczyk  
@opitz-consulting.com

## Oracle 11g – das umfassende Handbuch

gelesen von Björn Bröhl



Auf über 700 Seiten wird nahezu alles vermittelt, was man über die Oracle Datenbank 11g wissen sollte – zumindest bis zum Release 1. Das Buch gliedert sich in fünf Teile: „Installation, Architektur und Infrastruktur“, „Einführung in die Oracle Datenbank-Administration“, „Erweiterte Datenbank-Administration“, „Data Warehouse“ und „Hochverfügbarkeit“. Die ersten Kapitel widmen sich den Grundlagen für die Installation und Konfigura-

tion von Oracle Datenbanken. In zweiten Teil gibt es eine Einführung in die Oracle Datenbank-Administration. Hier werden insbesondere die Backup- und Recovery-Features von 11g beschrieben, außerdem wird auf Aspekte zur Sicherheit von Datenbanken eingegangen. Im Teil „Erweiterte Datenbank-Administration“ geht es unter anderem um die XML-Funktionalitäten, Oracle Grid Control, Tuning, Real Application Testing und ASM.

Ein eigener Teil beschäftigt sich mit den Möglichkeiten, die Oracle 11g für den Einsatz als Data Warehouse bietet: von der Planung und dem Aufbau eines Projektes über die Beschreibungen der Tools (wie zum Beispiel den Warehouse Builder) bis zur Administration. Zuletzt werden Hochverfügbarkeits-Funktionalitäten wie Dataguard und Real Application Cluster sowie deren neue Features in Oracle 11g erklärt.

**Fazit**

Zu jedem neuen Oracle Release erscheinen Nachschlagewerke wie dieses, in

denen für Einsteiger und Fortgeschrittene die Funktionalitäten vorgestellt werden und nebenbei auch noch einmal auf die Grundlagen eingegangen wird. Normalerweise tue ich mich mit diesen Bänden schwer und bevorzuge eher Bücher mit einer klaren Ausrichtung, zum Beispiel nur zu den neuen Funktionalitäten eines Release. In diesem Fall gelingt dem Autor der Spagat zwischen den Grundlagen und den neuen Funktionalitäten für Einsteiger und Profis jedoch gut. Ein Buch, das ich nur weiterempfehlen kann.

Titel:	Oracle 11g – das umfassende Handbuch
Autor:	Lutz Fröhlich
Sprache:	Deutsch
Umfang:	784 Seiten
Preis:	69,95 Euro
ISBN:	3-8266-5913-9

**Kontakt:**

Björn Bröhl  
bjoern.broehl@opitz-consulting.com

# Oracle meets MS SQL Server – Zugriff von Oracle auf das Fremdsystem

Vladimir Poliakov, AREVA NP GmbH

Sind Sie ein Oracle DBA oder Entwickler? Läuft Ihre Datenbank auf Linux, aber Ihre Kunden oder Lieferanten arbeiten mit dem MS SQL Server auf Windows? Möchten Sie das Datentransfer-Verfahren und den Zugriff auf Fremdsysteme vereinfachen? Dann wären Oracle Heterogeneous Services eine mögliche Lösung.



Abbildung 1: Server-Landschaft

Oracle Heterogeneous Services [1] sind ein Bestandteil des Oracle Datenbank-Servers und wurden entwickelt, um auf die Daten in Fremdsystemen ohne großen Aufwand über eine ODBC-Schnittstelle zugreifen zu können. Der Artikel zeigt anhand eines Beispiels aus der Praxis, wie man von der Oracle Datenbank die Daten aus einer MS SQL Datenbank lesen beziehungsweise in diese schreiben kann (siehe Abbildung 1).

Die Kommunikation zwischen Oracle Datenbank und MS SQL Server erfolgt über ODBC-Schnittstelle und Oracle Heterogeneous Agent, der vom Listener gestartet wird. Nach der Listener-Konfigurierung wird der Database Link zur MS SQL Datenbank erstellt, damit die Daten mit Oracle SQL-Mitteln bearbeitet werden können.

## Konfigurieren einer ODBC-Verbindung

Wie schon gesagt, erfolgt die Kommunikation zwischen der Oracle Daten-

```
#
# HS init parameters
#
HS_FDS_CONNECT_INFO = TESTHS
HS_FDS_TRACE_LEVEL = OFF
```

Listing 1: Konfigurationsdatei des Oracle Heterogeneous Agents

bank und MS SQL Server über Oracle Heterogeneous Agent, der seinerseits die ODBC-Schnittstelle verwendet. Deswegen wurden erst auf einem separaten Server B (siehe Abbildung 1) die ODBC-Treiber installiert und danach eine ODBC-System-DSN zum MS SQL Server eingerichtet und getestet (siehe Abbildung 2).

Da die Oracle Heterogeneous Services ein Bestandteil des Datenbank-Servers sind, muss man auf dem Server B entsprechende Oracle-Software ohne irgendeine Datenbank-Instanz installieren. Danach befindet sich die Konfigurationsbeispieldatei im Verzeichnis „\$ORACLE\_HOME\hs\admin\“ und heißt „inithsodbc.ora“. Für den Agent im Beispiel wurde noch der Name der Datei im Format „init<DNSODBC>.ora“ angepasst, wobei „DNSODBC“ mit dem ODBC-System-DSN-Namen übereinstimmen muss (siehe Abbildung 2). Der Inhalt der Konfigurationsdatei ist in Listing 1 dargestellt.

## Konfigurieren des Oracle Listeners

Nachdem der Oracle Heterogeneous Agent konfiguriert worden ist, wird die Konfigurationsdatei des Oracle Listeners entsprechend angepasst (siehe Listing 2). Wichtig ist, dass der Listener auf dem gleichen Server läuft, auf dem der

```
LISTENER =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)
      (HOST = <Server_B_Name>)(PORT =
        <Server_B_Listenerport>))
    )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (ORACLE_HOME = <Pfad_zum_
        ORACLE_HOME_auf_dem_Server_B>)
      (SID_NAME = <ODBC_Name_
        Abbildung_2>)
      (PROGRAM = HSODBC)
    )
  )
```

Listing 2: Konfigurationsdatei des Oracle Listeners

```
TESTHS_SERVER_B =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)
      (HOST = <Server_B_Name>)
      (PORT = <listenerport_on_
        Server_B>)
    )
    (CONNECT_DATA = (SID = <SID_
      NAME_LISTENER.ORA_Listing_2>))
    (HS=OK)
  )
```

Listing 3: Ausschnitt aus der TNSNAMES.ORA-Datei

Oracle Heterogeneous Agent gestartet werden soll. In unserem Beispiel ist das der Server B (siehe Abbildung 1).

### Konfigurieren der TNSNAME.ORA-Datei

Der letzte Schritt vor dem Erstellen des Database-Links ist das Konfigurieren der „TNSNAMES.ORA“. Diese Datei liegt auf dem Datenbank-Server, in unserem Beispiel Server A (siehe Abbildung 1). Sie wird, wie in Listing 3 gezeigt, angepasst. Der Eintrag (HS=OK) bezeichnet die Heterogeneous-Service-Verbindung. Sollte etwas nicht stimmen, kann man das Protokollieren der Zugriffe (HS\_FDS\_TRACE\_LEVEL = ON in Listing 1) aktivieren. Die Trace-Dateien findet man dann auf dem Server B (siehe Listing 1) im Verzeichnis „\$ORACLE\_HOME\hs\trace\“.

### Erstellen des Database-Links

Nachdem Oracle Heterogeneous Services, Listener und TNSNAMES.ORA-Datei

konfiguriert sind, können der Database-Link erstellt und die Verbindung zum MS SQL Server aus SQL\*Plus getestet werden (siehe Listing 4).

```
CREATE DATABASE LINK „TESTHS_
DBLINK“ CONNECT TO „<userna-
me>“ IDENTIFIED BY „<password>“
USING ‚TESTHS_SERVER_B‘;

SELECT count(*) FROM table_
name@TESTHS_DBLINK;
```

Listing 4: Erstellen des Database-Links und Test der Verbindung

### Fazit

Oracle Heterogeneous Services vereinfachen die Kommunikation zwischen Oracle und Fremdsystemen via ODBC-Schnittstelle. Anstelle des MS SQL Servers können auch eine Excel-Datei oder eine MS Access Datenbank [2] verknüpft sein. Somit ist dieses Verfahren eine Alternative zum SQL\*Loader (etwa beim Transfer der Daten).

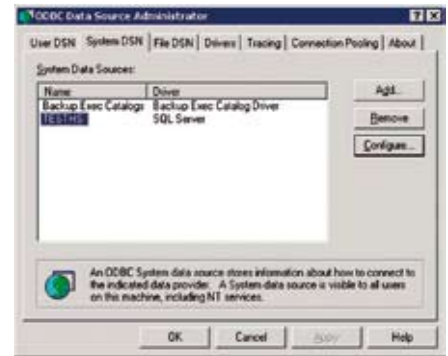


Abbildung 2: Einrichten der ODBC-System-DSN

### Referenzen

- [1] Oracle Dokumentation zu Oracle Heterogeneous Services: [http://download.oracle.com/docs/cd/E11882\\_01/appdev.112/e10492/toc.htm](http://download.oracle.com/docs/cd/E11882_01/appdev.112/e10492/toc.htm)
- [2] Heterogeneous Connectivity: <http://www.muniqsoft.de/tipps/monatstipps/jahr-2004/januar-2004.htm>

### Kontakt:

Vladimir Poliakov  
vladimir.poliakov@areva.com





## Oracle Senior Consultant

### Ihre Aufgaben

- Administration, Konfiguration und Support von komplexen Datenbanklösungen
- Monitoring bestehender DB-Systeme
- Backup/Recovery- und Hochverfügbarkeitslösungen
- Migrationen
- Referententätigkeit im Seminarumfeld

### Ihre Qualifikationen

- Sehr gute Oracle-Kenntnisse (Unix/Windows)
- Gute Unix-/Windows-Kenntnisse
- Mindestens 5 Jahre Erfahrung in der Administration von Oracle Datenbanklösungen
- Perfektes Deutsch in Wort und Schrift
- Uneingeschränkte Reisebereitschaft innerhalb Deutschlands

### Das zeichnet ORDIX aus

- Interessante Projekte bei namhaften Kunden
- Breites persönliches Aufgabenspektrum
- Ausgeprägtes, internes Know-how-Netzwerk
- Stetige Weiterbildung, persönliche Förderung
- Attraktive Vergütung, Firmen-PKW
- Soziale Absicherung

### Interesse?

Dann senden Sie Ihre Bewerbung mit Angabe Ihrer Gehaltsvorstellung und dem gewünschten Einstellungstermin an:

ORDIX AG | Christoph Lafeld | Westernmauer 12 - 16 | 33098 Paderborn  
Tel.: 05251/1063-0  
personal@ordix.de

**Weitere Infos unter [www.ordix.de](http://www.ordix.de)**

# Eine Oracle Konzern-Lizenz – Fluch oder Segen?

Christian Grave, Sören Reimers, ProLicense GmbH

**Dieser Artikel zeigt dem Leser die Aspekte des Unlimited License Agreements (ULA), einer Form der Oracle Konzern-Lizenz. Im Vordergrund stehen die Motivationen sowohl von Oracle als auch der Kunden, eine solche Lizenz abzuschließen. Das soll Unternehmen bei der Entscheidungsfindung für oder wider diese Vertragsform helfen.**

CIOs und IT-Einkäufer fordern immer wieder flexiblere Lizenzmodelle von Oracle, die sich der IT-Strategie anpassen, die Kostenstruktur optimieren und Sicherheit hinsichtlich Compliance bieten. Insbesondere im Rahmen der Virtualisierung von Servern tut Oracle sich schwer, ein bedarfsgerechtes Modell anzubieten.

Grundsätzlich basieren die von Oracle angebotenen Lizenzmodelle auf dem Prinzip, dass die Anzahl der Anwender oder Prozessoren ermittelt und ein bestimmter Rabattsatz für das einzukaufende Lizenzvolumen verhandelt wird. Als Lösung für das Thema „Virtualisierung“ und auch als Modell zur nachhaltigen Kostenreduktion wird häufig das Unlimited License Agreement (ULA) als Konzern-Lizenzmodell angeboten.

Die ersten ULAs, die 2006 in Deutschland abgeschlossen wurden, sind bereits ausgelaufen oder stehen kurz davor. Die Kunden fragen sich zu Recht, ob die damalige Entscheidung im Rückblick betrachtet die richtige war. Zudem muss entschieden werden,

ob die ULA verlängert wird oder der Lizenzbedarf zukünftig wieder auf Projektbasis gedeckt werden soll.

## Wie definiert sich eine ULA?

Die ULA ist der Erwerb eines Bundles ausgewählter Produkte zum festen Preis. Für die Produkte erhält der Kunde, vereinfacht ausgedrückt, zudem eine unbegrenzte Nutzungserlaubnis für einen definierten Zeitraum. Nachfolgend die wichtigsten Parameter, die bei Abschluss einer ULA geklärt sein sollten:

- Wie sieht der Lizenzbedarf für die kommenden Jahre tatsächlich aus?
- Welche Produkte sollten in die ULA aufgenommen und lizenziert werden? (Datenbank EE, Optionen, Application Server, HR, CRM etc.)
- Für welchen Zeitraum wird die ULA abgeschlossen, das heißt, wie lange sollen die lizenzierten Produkte unbegrenzt installiert und genutzt werden? Die meisten Verträge haben eine Laufzeit von zwei bis maximal fünf Jahren.

- Welche IT-Budgets werden belastet? Welche Unternehmensbereiche profitieren von dem Vertrag? Typischerweise wird die Nutzung auf Mehrheitsbeteiligungen oder auf eine festgelegte Liste von Unternehmensgesellschaften begrenzt.
- Sind Merger, Akquisitionen oder Carve Outs geplant? Die ULA gibt hier Regelungen vor, die sich auf die Lizenzierung im Rahmen der Laufzeit auswirken.

## Warum bietet Oracle die ULA als Lizenzform an?

Nach Gesprächen mit einer Vielzahl von Oracle-Kunden, die bereits eine ULA abgeschlossen haben oder sich gerade in der Entscheidungsphase befinden, sind die Autoren der Ansicht, dass es für Oracle sieben Hauptmotivationen gibt (siehe Abbildung 1).

Die ULA wird oft als Lösung für die im Rahmen einer Virtualisierungsstrategie entstehenden Lizenzierungsprobleme angepriesen. Als Hauptmotivation sehen die Autoren aber die Sicherung des für die ULA vertraglich vereinbarten Support-Preises. Für diesen zukünftig gesicherten und margenträchtigen Support-Umsatz ist Oracle meist bereit, ein preislich attraktives ULA-Angebot zu unterbreiten, da der gesamte Support-Umsatz des Kunden auch über die Laufzeit der ULA hinaus gesichert bleibt.

Die Kunden verknüpfen mit dem Abschluss einer ULA neben dem sicherlich oft attraktiven Preismodell weitere Aspekte (siehe Abbildung 2).

## Wem wird eine ULA angeboten?

Typischerweise werden ULA-Verhandlungen von Oracle initiiert, wenn der

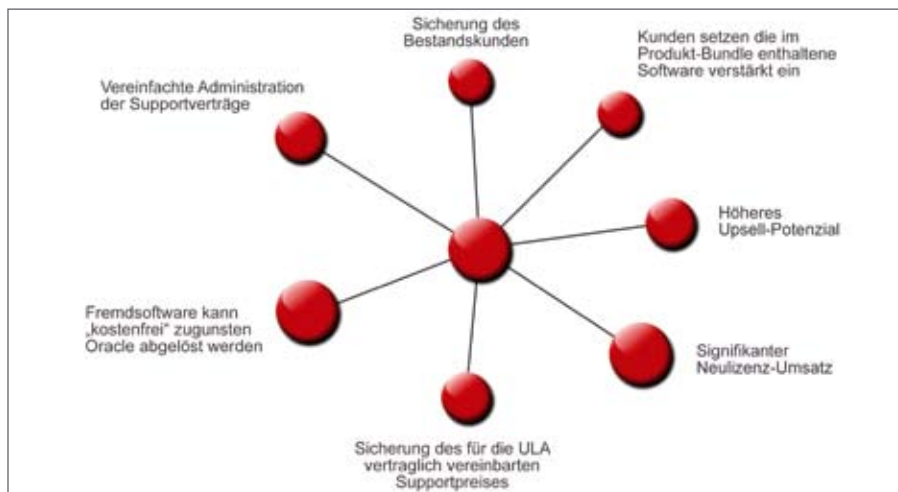


Abbildung 1: Oracles Hauptmotivationen zum Abschluss einer ULA



Kunde eine längere Vertragshistorie hat und einen erheblichen Lizenzvertragsbestand vorweisen kann. Diesen gilt es aus Sicht von Oracle für die Zukunft zu sichern. Oft ergibt sich das Gespräch zu einer ULA auch im Anschluss an ein Audit, im Rahmen einer Virtualisierungsstrategie des Kunden oder durch einen signifikanten Lizenzbedarf, der als Initialsumme genutzt werden kann.

Im Rahmen eines Audits können sich sehr konkrete Zahlen ergeben. Es ist teilweise aber auch sehr schwierig, alle Systeme richtig zu vermessen. Sollte sich eine Unterlizenzierung herausgestellt haben oder sich zumindest konkret andeuten, kann die ULA eine gute Möglichkeit sein, die kritische Situation der Non-Compliance zu heilen und einen Zustand mit Compliance-Sicherheit für die kommenden Jahre zu schaffen.

Sollte kein Audit durch Oracle erfolgt sein, ist der Verhandlungsspielraum des Kunden wesentlich größer, da er das Thema „Non-Compliance“ nicht konkret zu befürchten hat. Aber auch im Rahmen einer solchen Verhandlung sollte dem Kunden bewusst sein, das sich bei der Analyse des Lizenzbestands gegebenenfalls eine Unterlizenzierung herausstellen kann.

Anhand der historischen Lizenzbeschaffungen und der eventuell bestehenden Unterlizenzierung wird Oracle dann gemeinsam mit dem Kunden ein Wachstums-Szenario erstellen, auf dessen Grundlage die ULA-Preisfindung stattfindet. Hier lassen sich durch ein wenig Geschick und Gespür oft sehr gute Preiskonditionen verhandeln.

### Wie wird die ULA kalkuliert?

Beim Abschluss der ULA werden sämtliche im Bestand des Kunden befindlichen Lizenzen umgewandelt. Sie dienen lediglich als Kalkulationsbasis für die ULA. Von dieser Basis ausgehend werden die zusätzlichen Lizenzen verhandelt, um auf den für die ULA notwendigen Auftragswert zu kommen. Die Nutzungsrechte an den originären Lizenzen erlöschen. Stattdessen erhält der Kunde mindestens für die betreffenden Produkte und die vereinbarte Laufzeit ein unbegrenztes Nutzungsrecht.

Die Supportkosten, die für den umgewandelten Lizenzbestand ursprünglich gezahlt wurden, werden in den ULA-Vertrag eingerollt und sind somit auch weiterhin zu zahlen. Hinzu kommen der Preis für die zusätzlichen Lizenzen und der dazugehörige Supportbetrag. Sollte der Kunde im Zeitraum bis zwei Jahre vor dem ULA-Vertragsschluss Support für Produkte gekündigt haben, die jetzt in die ULA aufgenommen werden sollen, so werden diese wiedereingesetzt und ebenfalls eingerollt.

Bei der ULA-Rechnungsstellung ergeben sich damit drei Werte:

1. ULA-Lizenzpreis (einmalig)
2. ULA-Supportpreis – Standard ist 22 Prozent des verhandelten Lizenzpreises (pro Jahr)
3. Supportpreis für die „eingerollten“ Lizenzen (pro Jahr)

### Was geschieht zum Ende der ULA-Laufzeit?

Spätestens ein Monat vor dem Ablauftermin ist vom Kunden die Anzahl von installierten und genutzten Lizenzen an Oracle zu übermitteln und zu bestätigen. Dies erfolgt regelmäßig durch das Ausfüllen eines sogenannten „Oracle Server-Worksheets“. Die gezahlten und bestätigten Lizenzen werden dem Kunden zum Ende der Laufzeit festgeschrieben und gelten als lizenziert. Das unlimitierte Nutzungsrecht erlischt automatisch. Die Gesamt-Supportkosten bleiben (mit Ausnahme der jährlichen Erhöhung von typischerweise maxi-

mal 4 Prozent) konstant; es ist dabei egal, ob der Kunde nur 50 Prozent der ursprünglich geschätzten Lizenzmenge installiert oder die Schätzung um ein Vielfaches überschritten hat. Zusätzliche Lizenzgebühren fallen hierbei nicht an, werden aber auch nicht bei Unterschreitung der ursprünglich geschätzten Lizenzmenge erstattet.

### Fazit

Eine gut verhandelte ULA kann für Unternehmen viele Vorteile bieten. Meist lässt sich preislich ein sehr attraktives Modell mit Oracle verhandeln und durch das unlimitierte Nutzungsrecht weiteres Einsparpotenzial realisieren. Dem Kunden sollte aber vor der Unterschrift auch die Tragweite des Vertragsinhalts bewusst sein. Er bindet sich sehr stark an Oracle. Alle vormalig existierenden Einzelverträge sind durch den Abschluss der ULA in einen Vertrag konsolidiert und ersetzt worden. Somit ist die Kündigung von einzelnen, nicht mehr benötigten oder überbewerteten Lizenzen wesentlich erschwert. Sollte der Kunde einen Teil der Lizenzen kündigen und dadurch Support einsparen wollen, so ist dies nicht mehr möglich, ohne dass der Support für alle anderen im Vertrag befindlichen Lizenzen neu kalkuliert wird.

### Kontakt:

Christian Grave  
christian.grave@prolicense.de  
Sören Reimers  
soeren.reimers@prolicense.de

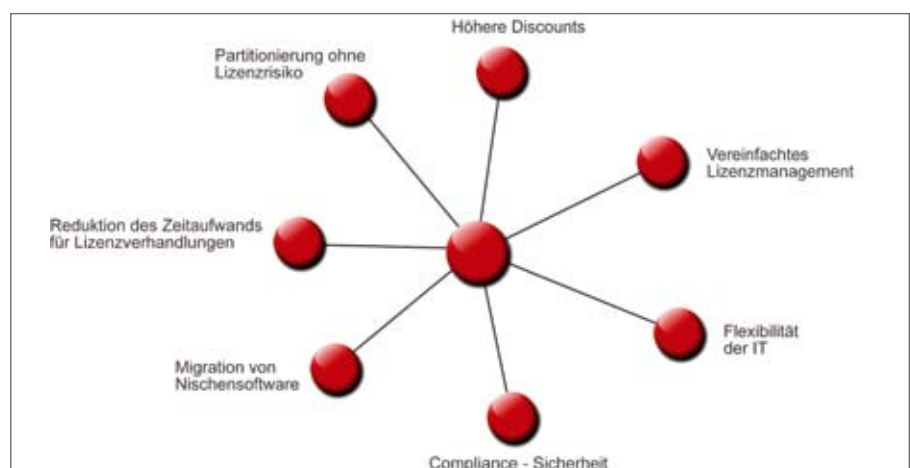


Abbildung 2: Hauptmotivationen von Kunden zum Abschluss einer ULA



# Das Treffen der Oracle-Community

16. – 18. November 2010 in Nürnberg: **DOAG 2010** Konferenz + Ausstellung



400 Fachvorträge • Keynotes bekannter Manager • Ausstellung • Networking

[www.doag2010.org](http://www.doag2010.org)

# Oracle Web-Portale barrierefrei anpassen: <https://recht.nrw.de>

Frank Christian Hoffmann, Logica Deutschland GmbH

Web-Portale können schon nach wenigen Jahren veralten. Der Informationsgehalt ist zwar nach wie vor gegeben, aber Aufbau und Layout sind nicht mehr zeitgemäß. Oft wurde in der Vergangenheit auch nicht an die Zugänglichkeit für Menschen mit Behinderungen gedacht oder es kamen HTML-Techniken wie Frames zum Einsatz, die für viele Anzeigegeräte zu unbefriedigenden Darstellungen führen.

Das Innenministerium NRW entschied sich, ein erfolgreiches Oracle-Bürgerportal nach zehn Jahren komplett neu zu gestalten und die Webseiten nach den Kriterien der WCAG 2.0 barrierefrei anzupassen. Das Portal wurde wie auch schon die Vorgängerversion komplett mit Tools und Technologien von Oracle entwickelt und beinhaltet die Sammlung aller geltenden Normen des Landes NRW.

## Projektphase1: Layout

Das Projekt fing mit der Analyse des bestehenden Portals an. Eine Kommunikationsagentur führte eine IST-Analyse des Portals durch und erkannte eine Reihe von Stärken, Schwächen und Chancen. Als Stärken wurden erkannt:

- Aktualität des Angebots (Texte werden direkt eingestellt)
- Umfang (Gesetze, Verordnungen und Erlasse); einzigartiges Angebot
- Schnelle Prozesse (die schlanken Prozesse ermöglichen eine schnelle Bearbeitung und Publikation der Inhalte)

Als Schwächen wurden angesehen:

- keine klare Struktur der Inhalte
- keine klare Nutzerführung durch das Angebot
- sehr lange Klickpfade zu den Inhalten (bis zu fünf Klicks)
- keine Trennung zwischen Navigation und Inhalten
- keine variablen Schriftgrößen
- Redundante Navigation (Reiter oben und Links auf der Seite)
- Wording nicht eindeutig (zum Beispiel Startseite und Einstiegsseite)

Als neue Chancen wurden definiert:

- Das Portal soll besser (klarer, strukturierter) über Rechtstexte informieren
- Ein neues Portal soll helfen, die Qualität des Angebotes zu vermitteln
- Wachsende Nutzerzahlen können dazu beitragen, mit dem Portal zum führenden Rechtsportal in NRW zu wachsen

Neben einem aussagekräftigen Logo sollte das neue Portal auch mit einem Claim (Behauptung, Anspruch) den Inhalt griffiger beschreiben. Dafür wurde „bestens informiert“ gewählt, weil dieser Begriff die Qualität und den Umfang des Angebots sowie die Ausrichtung des neuen Portals wiedergibt:

- Auf <https://recht.nrw.de> findet man alle Gesetzestexte des Landes NRW (Gesetze, Verordnungen, Erlasse)
- Die Texte sind schnell nach Beschluss nur hier online verfügbar
- Das ganze Angebot wird direkt vom Verfasser eingestellt

Auf Basis dieser Ziele wurde ein Layout entwickelt und mit dem Kunden abgestimmt.

## Der mühsame Weg zur Erstellung von barrierefreien Webseiten

Webseiten werden barrierefrei entwickelt, um ihre Inhalte für alle Menschen mit oder ohne Behinderungen zugänglich zu machen. Die Richtlinien zur barrierefreien Webentwicklung werden von dem WWW-Konsortium (W3C) unter dem Begriff „Web Content Accessibility Guidelines“ (WCAG) zusammengefasst. Für Deutschland

sind die WCAG-Gestaltungsrichtlinien in einer Verordnung unter der Abkürzung BITV (Barrierefreie Informationstechnik Verordnung) in einer Anlage übersetzt und zusammengefasst. Nähere Informationen dazu gibt es über folgende Webseiten:

- WCAG 2.0 Originalquelle: <http://www.w3.org/TR/WCAG20/>
- WCAG 2.0 nach Konformitätsstufe: <http://2bweb.de/wcag20/index.html>
- Seite mit vielen Tipps und Tricks: <http://www.barrierefreies-webdesign.de/>
- Übersetzung der WCAG-Richtlinien: <http://www.einfach-fuer-alle.de/artikel/bitv/>

Im Projekt sollten die Webseiten nach den neuen Richtlinien (Version 2.0) der WCAG entwickelt werden. Weiterhin wurde die Konformitätsstufe (A) gewählt. Das bedeutete für das HTML-Design, dass folgende Grundvoraussetzungen zu beachten sind:

- Skalierbarkeit der Schrift bis 200 Prozent (beispielsweise Arial 12, 14, 16, 20, 24)
- Konformität der Darstellung zu allen Bildschirmauflösungen ab 800 \* 600 Pixel
- Alle Grafiken müssen mindestens ein Kontrastverhältnis von 1:4 haben
- Validierung der Seiten mit dem W3C-Validator ([validator.w3.org](http://validator.w3.org))
- Kompatibilität zu allen verbreiteten Browsern wie Internet Explorer 6, 7 und 8 sowie Firefox 1.3 und 2
- Navigationsleisten als Listen
- Hervorhebung von Links durch Roll-over oder Tastatur
- Komplette Tastatursteuerung

- Beschreibung aller Bilder, Felder, Listen und Tabellen
- Vermeidung verschachtelter Tabellen
- Aufbau der Webseite mit Struktur und Formaten (H1, H2 etc.)
- Einfache Sprache in den Verlinkungen (wie „Alle Gesetze“)

Mit dem bekannten OWA-Package von Oracle gab es Probleme und es mussten einige Anpassungen vorgenommen werden. Für eine fehlerfreie Validierung des HTML-Textes waren viele HTML-Tags anders auszugeben. Das OWA-Package verursacht zudem einen Schwung von W3-Konformitätsverletzungen.

Da nahezu alle Layout- und Format-einstellungen über ein Cascading Style-sheet (CSS) gesteuert werden, wurde ein Package entwickelt, das der Laufzeit entsprechend die richtigen Formatierungen für alle Browser liefert. Eine große Herausforderung war, die Grafiken gemeinsam mit den Schriftgrößen zu skalieren. Mit dem (+) / (-)-Button kann die Schriftgröße in dem neuen Portal um 50 beziehungsweise 100 Prozent vergrößert werden. Es wurden Positionen und Größen der Grafiken dynamisch zur Laufzeit berechnet und dargestellt – dafür ist PL/SQL sehr gut geeignet. Mit JAVA-Skript wäre das extrem aufwändig geworden. Dadurch, dass Grafiken und Dokumente komplett in der Datenbank lagen, konnten viele dynamische Abfragen erstellt werden.

Es gibt eine Webseite, mit der man auf W3C-Konformität überprüfen kann. Dazu wird einfach der Quelltext einer gewünschten HTML-Seite markiert, kopiert und in „validator.w3.org“ kopiert. Das Ergebnis der Konformität erscheint detailliert auf der Webseite.

Das Kontrastverhalten lässt sich mit einem Browser-Plug-in prüfen (zum Beispiel WCAG Contrast Checker). Die Struktur der Seiten kann man gut mit Firebug (Firefox-Plug-in) und die Konformität mit dem Internet Explorer recht praktisch mit dem IE-TESTER prüfen. Sehr zu empfehlen ist das Browser-Plug-in „WEB Developer“ – dieses Tool erlaubt eine Vielzahl nützlicher Prüfungen auf Bildschirm-Formate, Cookie-Werte, Klassen-Informationen, Struktur sowie Ein- und Ausblenden verschiedener Elemente. Ein großes



Abbildung 1: Alte Webseite



Abbildung 2: Neue, barrierefreie Webseite

Problem ist bei Firefox, dass der Browser schon bei einem Fehler im CSS die Webseite zweimal lädt. Besonders bei Abrechnungssystemen könnte das zu unerwünschten Effekten führen.

Aufwändig erwiesen sich die CSS-Programmierung, die Darstellung von Menüs in Listen sowie die Abbildung verschachtelter Tabellen (mehrere Tabellen ineinander) durch CSS-Formatierungen. Hier waren viele manuelle Anpassungen erforderlich. Immer wieder waren auch Validierungsfehler zu beheben und kleinere Adaptionen für die verschiedenen Browserversionen durchzuführen. Im Laufe des Projekts

entstanden Frameworks, die dann wiederverwendet werden konnten.

Jede Webseite wurde als Prozedur entwickelt, die jeweils die Style- und Header-Informationen aus dem Style-Package integriert. Die Suche in den Überschriften und dem Volltext (erweiterte Suche) nutzt die FUZZY-Funktion von Oracle Text. Um Phishing-Versuche zu unterbinden, werden nur Buchstaben und wenige Sonderzeichen für die Abfrage erlaubt. Als guter Kompromiss erwies sich eine Gewichtung von etwa 70, um aus knapp 13.000 Dokumenten eine vernünftige Schärfe zu bekommen, zum Beispiel die Abfrage

nach „Polizei“, „Poolizei“ und „Pooolei“. Das Wort „Polizei“ führt zu dem gleichen Ergebnis wie das fehlerhaft geschriebene Wort „Poolizei“. Ein weiterer Fehler wie „Pooolei“ wird nicht mehr toleriert. Die Fuzzy-Suche sollte anhand wichtiger Schlüsselbegriffe geprüft und der Schärfegrad entsprechend dem Wunschergebnis eingestellt werden.

Eine Variable wandert durch alle Prozeduren und definiert die Schriftgröße. Mit deren Auswahl kann auch die richtige Grafik angezeigt werden.

```
<input type="image"
src="br_get.img?p_id='|| to_
char(550+sg) || ' " alt="Suche
starten" class="btn_suche"/>';
```

Das Package „br\_get.img“ lädt die Grafik, wobei je nach Schriftgröße eine andere Grafik geladen wird. Im Projekt wurde auch ein Framework entwickelt,

um beliebige SQL-Abfragen in barrierefreien HTML-Tabellen oder Excel-Ausgaben anzuzeigen. Vorher geschachtelte Tabellen wurden durch CSS-Formatierungen neu entwickelt. Navigationsleisten, die als Tabellen erstellt wurden, werden jetzt in Listen ausgegeben.

#### Fazit

MOD\_PL/SQL ist gut geeignet, um barrierefreie, dynamische Webseiten zu entwickeln, die auf Oracle Datenbanken zugreifen. Für barrierefreie Webseiten ist eine Reihe von Anpassungen erforderlich, die sich aufwändig, aber gut realisieren lassen – Standard-CMS-Systeme oder auch die Oracle Apex-Seiten sind nicht barrierefrei und erfüllen viele Kriterien nicht.

Die Einhaltung aller WCAG-Richtlinien ist kaum möglich. Daher erfüllen

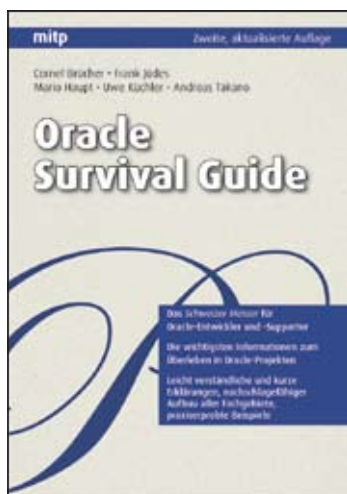
gute Webseiten maximal 90 Prozent beziehungsweise sehr gute Webseiten 95 Prozent der Kriterien. Mit dem Wort „barrierefrei“ sollte daher in Angeboten vorsichtig umgegangen werden. Der Autor empfiehlt, exakt zu definieren, welche Konformitätsstufe erwartet wird und welche Alt-Dokumente übernommen werden müssen. Es ist einfacher, ein Portal und dessen gesamten Inhalt neu zu erstellen. Die Vorteile von MOD\_PL/SQL-Seiten sind die gute Lesbarkeit des Programmcodes, die mühelose Einbindung von Inhalten und Struktur und die Möglichkeit, Zeichen und Styles so auszugeben, wie sie von der WCAG-2.0-Richtlinie gefordert werden. Die knapp 800.000 Pagehits im ersten Monat konnten mühelos abgearbeitet werden.

#### Kontakt:

Frank Christian Hoffmann  
frank.hoffmann@logica.com

## Oracle Survival Guide

gelesen von Björn Bröhl



Alles Wesentliche von VI über Unix, LDAP bis SQL und PL/SQL in einem Buch? Auf knapp 390 Seiten findet sich tatsächlich einiges, was den Untertitel „Die wichtigsten Informationen zum Überleben in Oracle Projekten“ verdient.

Den Anfang machen einige Kapitel zu SQL und PL/SQL. Hier sind die wichtigsten Grundlagen rund um diese Sprachen sehr gut verständlich beschrieben. Gerade für Einsteiger sind dies wichtige

Kapitel, die sich auch gut als Nachschlagewerk eignen. In den nachfolgenden Kapiteln werden wichtige Werkzeuge wie der SQL\*Loader oder Export/Import (bzw. Datapump) erklärt. Weitere Kapitel beschäftigen sich mit der Installation und dem Troubleshooting unter Windows und Linux.

Besonders spannend ist das sehr umfangreiche Kapitel „Wie sag ich’s dem Orakel?“ Hier wird für verschiedene Sprachen (C++, Java, C#, PHP, Perl etc.) erläutert, wie die Anbindung an eine Oracle Datenbank funktioniert und somit geklärt, wie letztendlich auf die Datenbank und deren Inhalte zugegriffen werden kann. Allgemeine Kapitel über VI, Unix, XML, Tipps und Tricks sowie die Oracle-/LDAP-Anbindung runden das Buch als Universalwerkzeug ab.

#### Fazit

Die Autoren haben sich der Herausforderung gestellt, einen „Survival Gui-

de“ für Oracle Datenbank-Projekte zu schreiben. Sicherlich mussten sie an der einen oder anderen Stelle Abstriche machen, beispielsweise bei der Auswahl der vorgestellten Tools. Alles in allem sind die dargestellten Inhalte jedoch sehr ausgewogen und das Buch ist sowohl für Einsteiger als auch für erfahrene Anwender als Nachschlagewerk zu empfehlen.

**Titel:** Oracle Survival Guide  
**Autoren:** Cornel Brücher, Frank Jüdes, Mario Haupt, Uwe Kuchler, Andreas Takano  
**Verlag:** MITP  
**Sprache:** Deutsch  
**Umfang:** 386 Seiten  
**Preis:** 29,95 Euro  
**ISBN:** 3-8266-5098-0

#### Kontakt:

Björn Bröhl  
bjoern.broehl@opitz-consulting.com

# Datengetriebene Applikationen

Hans Niedermeier, PRO-Software GmbH

**Um Applikationen zu entwickeln, benötigt man vielerlei Spezialwissen. Bei kleineren bis mittelgroßen Projekten erwartet man vom Entwickler, dass er sowohl die betriebswirtschaftlichen Anforderungen in Prozesse umsetzen als auch das Datenbankdesign durchführen und letztlich die Programme – meist mit einem hohen Anteil für die grafische Präsentation- erstellen kann. Die GUI-Programmierung war schon immer, aber noch verstärkt in der letzten Dekade, von schnellen Änderungszyklen betroffen. Die Aneignung dieses Spezialwissens erfordert verhältnismäßig viel Zeit und ist zudem einer kurzen Halbwertszeit unterworfen.**

Ein hoher Prozentsatz der GUI-Objekte einer Anwendung besteht normalerweise aus Standard-Funktionalitäten wie einfachen Formularen, Tabellen, Charts oder Buttons.

Rollen-basierte Ansteuerung der GUI-Objekte wird meistens gefordert, bedeutet aber zusätzliche Programmier-Arbeit für die entsprechende Infrastruktur. Wird noch sprachabhängige Darstellung benötigt, treibt dies den Zeitaufwand für jedes Projekt erheblich in die Höhe.

All diese Fakten bewegten den Autor, ein System für „datengetriebene“ (datadriven) Anwendungen zu erstellen. Basis ist ein Repository, in dem alle GUI-Objekte einer Anwendung definiert werden können, inklusive aller nötigen Aufrufe an die Datenbank-Select-Statements. PL/SQL-Code und Package-Aufrufe seien als die wichtigsten genannt.

Das Repository (REPOS) liegt im Schema einer Oracle Datenbank. Fast alle unter dem Label „datadriven“ veröffentlichten Applikationswerkzeuge verstehen darunter, aus unzähligen XML-Dateien Code zu generieren, der innerhalb der zugrundeliegenden Sprach-beziehungsweise Script-Schicht eingebettet ist. Diese Art müsste man „datadriven“ Code-Generierung nennen, weil als Ergebnis viele Sourcen entstehen, welche später kompiliert und gepflegt sein wollen.

Was hier vorgestellt wird, ist „datadriven“ im eigentlichen Sinn! Es existiert nur ein Programm, basierend auf einer Source, die das erledigt und darstellt, was von außen – sprich von dem wohl strukturierten Repository – kommt; die Informationen aus dem

Repository werden interpretiert und nicht kompiliert. Zur Runtime des Programms steht für jede Anwendung eine speicheroptimierte Form der internen Kontrollstrukturen als Set von Dateien zur Verfügung.

Bei Auswahl einer Anwendung wird dieses Set in den Speicher geladen, im weiteren Verlauf sind weder Zugriffe auf das Dateisystem noch auf das REPOS erforderlich. Um damit grafische Anwendungen zu entwickeln/definieren, ist keinerlei

Spezialwissen über GUI-Programmierung (wie Forms, Apex J2EE, JAVA, .NET etc.) ist notwendig. Man kann sich beim Bau der Oberflächen mit dem „Was“ beschäftigen, anstatt sich mit dem „Wie“ herumschlagen zu müssen. Es reichen das Wissen über die Anwendungsdatenbank, die Beherrschung von SQL beziehungsweise PL/SQL und der Überblick darüber, was den Tabs an vorgefertigten GUI-Objekten (Formularen, Tabellen, Charts, Buttons etc.) angeboten wird.

Den größten Nutzungswert und die beste Produktivität beim Definieren der „datadriven-GUI“ wird erreicht, wenn die Applikationsdaten in einer Oracle Datenbank liegen und die Betriebswirtschaft der Anwendung auch in Oracle PL/SQL implementiert ist, da in diesem Programm viele nur in Oracle vorhandenen Features angesprochen werden. Liegen die Applikationsdaten in einer Nicht-Oracle Datenbank, dann kann man Eigenschaften wie „Nutzung von Packages“ nicht beziehungsweise nur mit Anpassungsaufwand nutzen.

Der Kurzname für das System beziehungsweise Programm lautet „DAP5“.

- Datadriven (im engeren Sinne auch databasedriven)
- Application
- 5 weil es über Eigenschaften von Systemen der 4th Generation hinausgeht

4-GL erzeugt normalerweise Code für jedes benötigte Objekt (Programm, Maske, Fenster). DAP5 kann man im Vorfeld anpassen, kompilieren und es dann für viele zu schaffende Anwendungen benutzen.

## DAP5 und das Programmierwerkzeug

In der Planungsphase wurde überlegt, mit welcher Sprache das Programm am besten zu realisieren ist und auf welchen Plattformen es lauffähig sein soll. Die Wahl für das Implementierungswerkzeug fiel auf XDEV2 (siehe [www.xdev-software.de](http://www.xdev-software.de)). Der Leistungsumfang von XDEV2 (Enterprise Version 2.5, nun 2.6 im Einsatz) ermöglicht weitgehende Plattform-Unabhängigkeit:

- Fat-Client-Programm
- Windows, Unix, Mac
- Browser-Webstart PHP oder JSP-Scripts
- Browser Applet PHP oder JSP-Scripts

XDEV2 war in den Anfängen eine RAD-Workbench auf Java-Basis, bewegt sich aber derzeit deutlich in Richtung bekannter Java-Paradigmen. Mit XDEV3 (für Mitte 2010 angekündigt) wird höchste Flexibilität bezüglich des Java-Codes erreicht. Exportierter Code aus XDEV kann „1:1“, zum Beispiel nach Eclipse, übernommen werden.

**Eigenschaften von XDEV**

Für den Autor war es äußerst wichtig, nicht erst die kompletten JavaOO-Programmiertechniken erlernen zu müssen. Nach einer relativ kurzen Einarbeitungszeit war es möglich, ein tragfähiges Konzept für die anspruchsvolle Aufgabe zu entwerfen.

Das in XDEV angebotene Persistenz-Feature der „Virtuellen Tabellen“ (siehe [http://www.xdev-software.de/downloads/doku/xdev2\\_6/alpha/XDEV%20Manual.html?topic.htm](http://www.xdev-software.de/downloads/doku/xdev2_6/alpha/XDEV%20Manual.html?topic.htm)) und der auf diesen virtuellen Tabellen basierenden Methoden machten es möglich, mit einem Datenbank-zentrierten Ansatz die REPOS-Informationen geschickt und performant aufbereiten zu können. Persistenz siehe [http://de.wikipedia.org/wiki/Java\\_Persistence\\_API](http://de.wikipedia.org/wiki/Java_Persistence_API).

**Basis-Layout**

In der derzeit vorliegenden Prototyp-Implementierung wurde eine sechszellige Aufteilung des (bisher einzigen) Fensters verwendet. LOGO, IMMA und PRES sind derzeit fix programmiert. Die Bereiche „ACTB“, „NAVT“ und „TABX“ werden zu 100 Prozent aus dem Repository gesteuert. Das Basis-Design könnte in unterschiedlichsten Varianten, orientiert an speziellen Kundenwünschen, implementiert werden. Momentan ist die Fensteraufteilung innerhalb der Zellen fixiert. Denkbar ist, diese Objekte freier, größenverstellbar und verschiebbarer (scrollbar) zu definieren.

LOGO	IMMA
PRES	ACTB
NAVT	TABX

Abbildung 1: Anordnung der Zellen

Die blau markierten Zellen (siehe Abbildung 1) werden zu 100 Prozent aus dem REPOS bedient. Die Zelle PRES ist vordefiniert, der Inhalt bestimmt sich aus den Rollenzuordnungen.

**Kurzbeschreibung der Bereiche (Zellen)**

LOGO = LOGO-Area, um ein Bild zu platzieren (beliebiges Firmen-Logo)



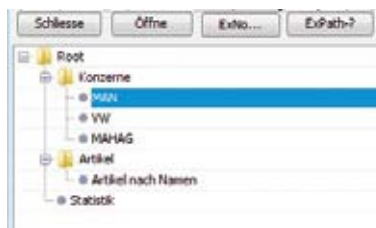
IMMA = IMMEDIATEActions ist für Anmeldung fest programmiert. Hilfe, Sprachauswahl und sonstige Spontaninformationen können dort abgerufen werden.



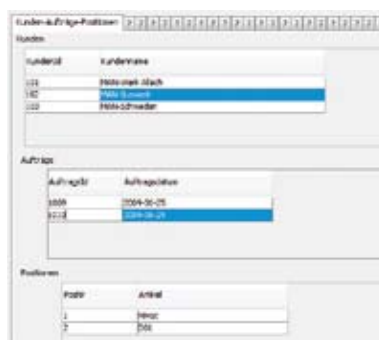
PRES = PRESelection dient zur Auswahl einer Applikation, zu welcher der angemeldete Benutzer berechtigt ist. Dieser Bereich ist ebenfalls fest programmiert, berücksichtigt aber schon die für den angemeldeten Anwender zugelassenen Applikationen.

ID	Application	xdev_datasource	purpose
613	AG1	ORAA1	Demo
612	AG2	ORAA1	Demo-2
614	AZ2	ORAA1	Test-Auftragsb...

NAVT = NAVigationTree ist der Kern der Anwendung – ein höchst flexibler Navigationsbaum (TreeContol). Aufgrund dessen Flexibilität wurde auf die Nutzung einer Menübar verzichtet.



TABX = TABpanes X Tabs sind vordefiniert und ausprogrammiert. Zu einem ausgewählten Knoten des NAVT werden die dazugehörigen Tabs mit Daten gefüllt und stehen zur Anzeige beziehungsweise Verarbeitung dieser zur Verfügung. In den Tabs sind viele Varianten und Kombinationen aus Formularen und Tabellen-Objekten realisiert. Es können auch Push-Buttons in den Tabs aktiviert werden.



ACTB = ACTIONButtons zur Definition der im Kontext zu (NAVT) und (TABX) verfügbaren Push-Buttons. Ein Mapping der dahinter liegenden Funktionalität auf vordefinierte und aktivierbare Buttons innerhalb der TAB-Bereiche ist möglich – somit stehen die Buttons optisch näher an den GUI-Objekten, in deren Kontext die Buttons wirken sollen.



Die technische Bezeichnung der Bereiche wird deshalb hier veröffentlicht, weil in diversen Beispielen (teils eigene Dokumente) und in der Folge darauf verwiesen wird. Auch die Zellen „LOGO“, „IMMA“ und „PRES“ könnten in Zukunft aus dem REPOS definiert werden. Diese Implementierung ist derzeit jedoch zweitrangig.

**Das Repository (REPOS)**

Das Repository liegt auf einem Schema einer Oracle Datenbank. Es besteht derzeit aus rund dreißig Tabellen, aus fast ebenso vielen Views und einem Set von Oracle-Stored-Objects. Das zentrale Package ist das REPOS-API (siehe unten), ausschließlich darüber werden Applikationen in das REPOS eingespeist.

Bei herkömmlicher Programmierung von GUIs stehen die Bezugnahmen auf Anwendungs-DB-Objekte (Tables, Columns, Prozeduren) im entstehenden Programmcode. Bei DAP5 wird alles Anwendungs-DB-Spezifische im REPOS hinterlegt. Die wichtigsten Tabellen von REPOS sind:

- Applikationen
- Strukturen – jede Struktur ist einem Objekt-Typ und einer Vater-Struktur zugeordnet, außer bei Roots
- Objekte wie im Navigationsbaum (NAVT), Tabs (TABX), Buttons (ACTB) und andere – jede Struktur gehört zu einem Objekttyp
- Aktionen sind mit Strukturen verbunden wie „Lesen Daten“, „Ausführen Button-Aktionen“ etc.

- Calls beinhalten die Codezeilen zur Ausführung von Aktionen wie Select-Statements, PL/SQL-Code, Package-Aufrufe, Systemaufrufe, gegebenenfalls Web-Adressen etc.
- Parameter dienen dem dynamischen Mapping von Platzhaltern innerhalb der Calls (Selects, PL/SQL-Aufrufe, Package-Aufrufe, Systemaufrufe, DLL-Aufrufe)
- Display beinhaltet und gruppiert die anzuzeigenden Items
- DisplayItems beschreiben einzelne Anzeigefelder (Beschriftung)
- Attribute nehmen weitere Informationen auf, welche über die DisplayItems zu legen sind (zur Breite in Bytes), zusätzliche Eigenschaften wie „Farbe“ sind möglich
- Sprachen
- Rollen
- Berechtigungen
- und diverse andere zur Feinspezifikation

### Das REPOS-API

Das REPOS-API besteht aus einem Oracle-Package, mit dessen Prozeduren man das REPOS füllt. Die Aufrufe an das API sind absichtlich so geschaffen, dass der Bezug zum gewünschten GUI-Objekt sichtbar und real ist. Listing 1 zeigt ein kleines Beispiel (verkürzte Form der API-Aufrufe „dap\_pac.dap\_prc...“). Dies sind die Aufrufe an das REPOS-API, eingebettet in einen PL/SQL-Block, siehe Listing 1.

Jeder dieser REPOS-API-Aufrufe schreibt „1-n“ Datensätze in verschiedene REPOS-Tabellen, je nach Aufruf. Die Verteil-Logik ist technisch bedingt und soll vorerst hier außen vor bleiben. Die Aufrufe 1.0 bis 9.2 haben zur Folge, dass die Anwendung „A01“ zwar klein, aber ablauffähig im REPOS steht.

Abbildung 2 ist ein ausgewählter Ausschnitt, der die in dem Beispiel definierte Anwendung in Aktion zeigt:

- Die ausgewählte Anwendung A01
- Den Navigationsbaum mit allen Knoten – statische (Konzerne, Artikel, Statistik) wie dynamische (MAN, VW, MAHAG)
- Den Tab mit der Master-Detail-Detail-Darstellung von „Kunden“,

```
(1.0) ..cr_app(,A01', 'ORAA1', 'Demo-Auftragsabwicklung', 1);
(2.0) ..cr_constant (,NAVT', null, 'KON', 'Konzerne');
(3.0) ..cr_sql
      (,NAVT', 'KON', 'KONS', 0,
        ,Select id      TextId      ,|| chr(10) ||
          ,      ,konzern TextF01   '|| chr(10) ||
          ' from Konzerne');
(3.1) ..cr_displayitem ('KONS', 2);
(4.0) ..cr_sql
      ('TABX', 'KONS', 'KUNX11X', 11,
        ,Select id      Textid      ,|| chr(10) ||
          ,      ,kon_id  TextF01    ,|| chr(10) ||
          ,      ,name1   TextF02    ,|| chr(10) ||
          ' from Kunden
          , where kon_id = <KON_ID>');
(4.1) ..cr_param (,KUNX11X', '<KON_ID>', ,NAVT', -1, 1, null);
(4.2) ..cr_displayitem ('KUNX11X', -1, 'Kunden-Aufträge-Positionen');
(4.3) ..cr_displayitem ('KUNX11X', 0, 'Kunden');
(4.4) ..cr_displayitem ('KUNX11X', 1, 'KundenId');
      ..cr_displayitem ('KUNX11X', 3, 'Kundenname');
(4.5) ..cr_attribute (,KUNX11X', 1, 'BYTES', '10');
      ..cr_attribute (,KUNX11X', 3, 'BYTES', '30');
(5.0) ..cr_sql
      (,TABY', ,KUNX11X', 'KUNX11Y', 11,
        ,Select id      TextId      ,|| chr(10) ||
          ,      ,adatum TextF01    ,|| chr(10) ||
          ' from Auftraege
          , where kun_id = <KUN_ID>');
      ..cr_param (,KUNX11Y', '<KUN_ID>', ,TABX', 11, 1, ,X');
      ..cr_displayitem (,KUNX11Y', 0, 'Aufträge');
      ..cr_displayitem (,KUNX11Y', 1, 'AuftragsId');
      ..cr_displayitem (,KUNX11Y', 2, 'Auftragsdatum');
      ..cr_attribute (,KUNX11Y', 1, 'BYTES', '10');
      ..cr_attribute (,KUNX11Y', 2, 'BYTES', '20');
(6.0) ..cr_sql
      (,TABZ', ,KUNX11Y', 'KUNX11Z', 11,
        ,Select p.posnr TextId      ,|| chr(10) ||
          ,      ,p.auf_id TextF01   ,|| chr(10) ||
          ,      ,a.artnr  TextF02   ,|| chr(10) ||
          , from Aufpos p, artikel a ,|| chr(10) ||
          , where p.art_id = a.id    ,|| chr(10) ||
          ' and p.auf_id = <AUF_ID> ');
      ..cr_param (,KUNX11Z', '<AUF_ID>', ,TABY', 11, 1, ,Y');
      ..cr_displayitem (,KUNX11Z', 0, 'Positionen');
      ..cr_displayitem (,KUNX11Z', 1, 'PosNr');
      ..cr_displayitem (,KUNX11Z', 3, 'Artikel');
      ..cr_attribute (,KUNX11Z', 1, 'BYTES', '10');
      ..cr_attribute (,KUNX11Z', 3, 'BYTES', '20');
(7.0) ..cr_button ('ACTB', 'KUNX11X', 'KUNDE_UPD1', 'Ändere Kunden-
name'
                  , 'Tooltip ändern Kundenname');
(8.0) ..cr_callplsql ('ACTB', 'KUNDE_UPD1', 'KUNDE_UPD1_C',
'DECLARE
  vKunId number(8) := <KUN_ID>;
BEGIN
  update kunden
  , set name1 = , '<KUN_NAME>' ,
  , where id = vKunId;
  , commit;
,END;');
      ..cr_param (,KUNDE_UPD1_C', '<KUN_ID>', ,TABX', 11, 1,
,X');
      ..cr_param (,KUNDE_UPD1_C', '<KUN_NAME>', ,TABX', 11, 3,
,X');
(9.0) ..cr_constant (,NAVT', null, 'ART', 'Artikel');
(9.1) ..cr_constant ('NAVT', 'ART', 'ARTNAME', 'Artikel nach Namen');
(9.2) ..cr_constant (,NAVT', null, 'STA', 'Statistik');
--
```

Listing 1



<b>CR_APP</b>		Erzeugen einer Applikation
* APPL	A01	Kurzname der Applikation
* DATASOURCE	ORAA1	Datenquelle (dahinter liegt Connect)
* NAME	Test-Auftrag-01	Langname der Anwendung
* LANGUA_ID	1	Default-Sprache der Anwendung
<b>CR_CONSTANT</b>		Erzeuge eine festen Knoten im TREE
* OBJECT	NAVT	GUI-Objekt-Bezug
* PARENT	Null	Wenn ein neuer Root-Eintrag im Tree
.....	Name	des Vaterknotens
* STRUCTUE	Name	des neuen Knotens
* DISPLAY	Konzerne	Der neue Knoten zeigt „Konzerne“
<b>CR_SQL</b>		Erzeuge dynamischen Knoten (TAB)
* OBJECT	NAVT TABX(Y,Z) LOVT	GUI-Objekt-Bezug Select für TABnn Block X Select für eine Werteliste
* PARENT	Name	des Vaterknotens
* STRUCTURE	Name	des neuen Knotens
* ELEMENT	Nummer	0, bei NAVT, nn bei TABnn
* CALL	Select .... where abc = <XXX>	Frei definierbares Select-Statement bei Bedarf mit Platzhalter <XXX>
<b>CR_PARAM</b>		Mapped zu Parametern die Daten
* STRUCTURE	Name	des aktuellen Knotens
* PARAM	<XXX>	Platzhalter
* OBJECT	NAVT TABX(Y,Z)	NAVT, TABX, ... und andere
* LEVEL	-1	Im NAVT einen Level zurück
* COLNO	2	Davon die 2. Spalte
* REF	null	(könnte auch PROG-Variable sein)
<b>CR_DISPLAYITEM</b>		Erzeuge ein Anzeige-Item
* STRUCTURE	Name	des Knotens, zu dem das Item gehört
* COLNO	-1,0,1-n	Spaltennummer des Knoten-Selects
* ITEM	Kunden	Spaltenbeschriftung bei Table-Objekt
<b>CR_ATTRIBUTE</b>		Weitere Attribute zu Items definieren
* STRUCTURE	Name	des Knotens, zu dem das Item gehört
* COLNO	1,..,n	Spaltennummer des Knoten-Selects
* ATTRIBUTE	BYTES	Definiert ein Attribut BYTES (Länge)
* VALUE	1,..n	Länge in Bytes (Breite der Spalte)
<b>CR_BUTTON</b>		Erzeuge einen Button
* OBJECT	ACTB	GUI-Bezug, wo Button platziert wird
* PARENT	Name	des Knotens, wo Button definiert wird
* STRUCTURE	Name	Name der Button-Struktur
* TEXT	Ändere	Beschriftung des Buttons
* TOOLTIP	Ändere Kundenname	Test für den Tooltip
<b>CR_CALLPLSQL</b>		PL/SQL-Block ausführen
* OBJECT	ACTB	GUI-Bezug, wo Call platziert wird
* PARENT	Name	des Buttons, wo Call definiert wird
* STRUCTURE	Name	Name der CALL-Struktur
* TEXT	BEGIN.....END;	PL/SQL-Block
Weitere Procs des		API ohne Detailbeschreibung
<b>CR_DEL_APPX</b>	Löschen APP	Entfernt alle Daten einer APP
<b>CR_CALLPROC</b>	Ruft Package-Proc	Mit Parameter-Rücknahme und Ausw.
<b>CR_CALL_SEQ</b>	Kann weitere Calls	Zum Basis-Call hinzufügen (Refresh)
<b>CR_LOVMAP</b>	Mappen Zeilenwerte	einer Werteliste in die Base-Table
<b>CR_MDIA</b>	Definiert Schritte von	Modalem Dialog
<b>CR_SQL_REPEAT</b>	Kann einen Knoten	mit Kindern rekursiv vervielfältigen
<b>CR_REF</b>	Erstellt Referenzen	Beziehungen von Appl-1 zu Appl-2
<b>CR_CMD / DLL</b>	Systemaufrufe	Kommando-Ebene oder DLL-Module

„Auftraege“ und „Positionen“ des ausgewählten Konzerns „MAN“, jeweils mit den gewünschten Beschriftungen und Spalteninhalten

- Dem Push-Button „Ändere Kundenname“

### Beschreibung der Schichten

Man kann den Weg der REPOS-Informationen in DAP5 wie folgt beschreiben:

- S1  
Das REPOS enthält die Metadaten der Anwendung.
- S2-1  
Das Programm liest bei Auswahl einer Applikation die beschreibenden Daten aus dem REPOS ein und füllt die internen virtuellen Tabellen (#VT) inklusive ausgefeilter Pointer, um schnelle Wege innerhalb dieser Kontrollstrukturen zu ermöglichen. Anschließend werden die aufgebauten Kontrollstrukturen aus den #VT-Tabellen auf das Dateisystem geschrieben (als Deploy-Objekte).
- S2-2  
Im Produktiv-Betrieb entfällt die Schicht S2-1, anstelle dessen werden die einmal aufgebauten Kontrollstrukturen aus dem Dateisystem in die #VT zurückgelesen.
- S3  
Durch Interaktion primär auf den Navigationsbaum und sekundär auf den zugeordneten Tabs und Button-Bereichen wird die auszuführende Programmlogik identifiziert (Event-gesteuert).
- S4  
Die identifizierten Teile der Kontrollstrukturen werden ausgeführt durch Aufrufe an das XDEV-Framework und darunterliegend auch an die Datenbank.
- S5  
Das XDEV-Framework bedient sich des SPRING-Frameworks.

In einer Produktiv-Umgebung muss das datenbankgestützte REPOS nicht vorhanden sein – es genügt das Einlesen der #VTs in Schicht S2-2. Die Inter-

Tabelle 1: API-Aufrufe mit Parametern

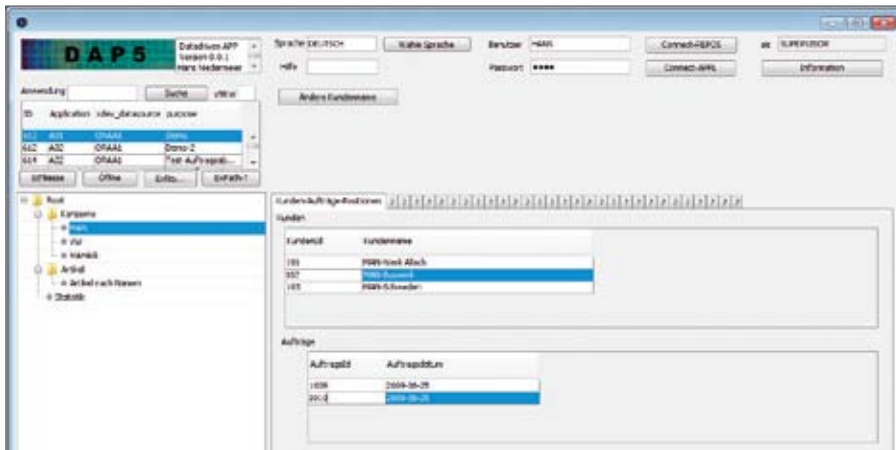


Abbildung 2: Alles auf einen Blick

pretation der Anwendung läuft somit innerhalb der optimierten Kontrollstrukturen ab, die wiederum auf die Methodenaufrufe an das XDEV-Framework abgestimmt sind.

## Übersicht über die Leistungsmerkmale

Die Leistungsfähigkeit des Programms einschließlich des REPOS definiert sich über drei Gruppen von Eigenschaften. Ohne alle Punkte aufzulisten, sei dazu angemerkt:

### 1. Features

Derzeit ist ein Satz von Features implementiert, der über das REPOS definiert und abgerufen werden kann. Neben den Möglichkeiten, wie im einfachen Beispiel demonstriert, zählen dazu:

- Aufrufe von Packages, Auswertung des Return-Codes und Weiterleitung an definierbaren modalen Dialog
- Definierbare Refresh-Aktionen, die nach ausgeführtem DML nötig sind
- Update/Delete Row-Level-Security, also optimistisches Locking
- Rollenkonzept
- Mehrsprachigkeit
- ein ORA-API, welches aus den Tabellen und Views eines Applikationschemas Statements generiert, die mit geringer Nachbearbeitung für unterschiedlichste Zwecke verwendet werden können
- In einer weiteren Entwicklungsstufe wird dieses API erweitert, um aus vorgefertigten PL/SQL-Templates

sogar Packages für die Geschäftslogik vorgenerieren zu können

- Ein zentrales, datenbankgestütztes, ebenfalls mehrsprachiges Meldungssystem (Logging)

### 2. Realisierte Tab-Objekte

In den realisierten Tab-GUI-Objekten (XDEV-TabPanes) verbirgt sich eine Fülle von Möglichkeiten, Applikationsdaten darstellen, eingeben, ändern und löschen zu können. Von einfachen Formularen, Charts und Tabledarstellungen, die jeweils in einem Tab platziert sind, reicht die Palette der vorgefertigten GUI-Objekte bis zu einer dreistufigen Master-Detail-Detail-Präsentation (siehe Beispiel „Kunden“, „Auftraege“, „Positionen“) mit vollständiger Synchronisation, wie man es auch von SQL-Forms gewohnt ist. Es gibt auch Mischformen von Table-Objekten und Formularen.

Anzumerken ist, dass die Synchronisation mehrerer Table-Objekte auf eine neutrale Art implementiert ist. Es spielt keine Rolle, welche Daten in den GUI-Objekten dargestellt werden – es zählt einzig und allein der Platzhalter-Parameter.

Darüber hinaus synchronisieren sich Inhalte von einem Tab(1) auf einen Tab(2), sobald innerhalb des Tab(2) ein Parameter in den Tab(1) zeigt.

Die Synchronisationslogik wird ausschließlich innerhalb der virtuellen XDEV-Tabellen (#VT) abgewickelt. In einem Tab mit drei Blöcken hat jeder Block eine vordefinierte #VT, in welcher die Daten eines Selects abgelegt werden.

Änderungen von Feldern auf einem GUI-Objekt schlagen sich ohne Zutun sofort in der zugrundeliegenden #VT nieder. XDEV bietet zwar Methoden an, dass Änderungen in GUI-Objekten über die #VT auch sofort in der DB wirksam werden. Dieses Feature wird nicht benutzt, einzig und allein definierte Calls unter Buttons (PLSQL oder Package-Proc) stoßen die entsprechenden Insert-, Update- oder Delete-Operationen an. Dabei werden auch Transaktionen unterstützt.

Gezielte Refresh-Aufrufe nach ausgeführten Button-Aktionen können ebenfalls im REPOS hinterlegt werden. Derzeit noch nicht möglich ist die Benutzung von Radio-Buttons und Checkboxes über das REPOS.

### 3. Infrastruktur

Da alles Applikations-Spezifische aus dem Programm herausgelöst und in das REPOS verlagert wurde, bot sich ein Weg an, den Entwicklungsprozess durch einige, natürlich REPOS-definierte Anwendungen zu unterstützen. Aus diesem Grund sind mehrere REPOS-Applikationen im Bau. Diese werden über das API definiert und stellen die GUI-basierte Workbench des REPOS dar:

- Build-Applikation für Entwickler, welche das Definieren, Ändern und Klonen von Anwendungen grafisch und generisch unterstützt. Diese Applikation nutzt intern das REPOS-API, pro definierter Anwendung kann eine Aufrufdatei reverse generiert werden.
- Translate-Applikation, um bei REPOS-Anwendungen die sprachabhängigen Texte wie Button- oder Spaltenbeschriftungen übersetzen, einstellen und kontrollieren zu können
- User-Applikation für Verwaltung von Benutzern, Rollen und Zuordnung zu Anwendungen. Hinweis: Eine in einer schon bestehenden Anwendungsdatenbank vorliegende Userverwaltung kann natürlich verwendet/integriert werden
- Analyze-Applikation, die 100 Prozent durchgängige Verwendungsnachweise von Tabellen+Columns beziehungsweise auch Stored Ob-

jects in Applikationen aufzeigen kann

- Deploy-Applikation, mit der man Anwendungen aus dem REPOS aufbereiten und verteilen kann, so dass zum Beispiel in einem Produktiv-System/Webserver die REPOS-Daten einer Anwendung speichernah aufbereitet in verschlüsselten Dateien vorliegen

Das angepeilte Ziel, 100 Prozent „data-driven“ zu sein, ist erreicht. Folglich ist es nicht erforderlich, dass das kompilierte und ausgelieferte Programm auch nur eine einzige Tabelle der Applikationsdatenbank einer Anwendung kennen muss und deren Aufbau im Kompilat (JAR) des Programms enthalten ist.

### Hybrid-Anwendungen

Nun gibt es jedoch oft Spezialwünsche an GUIs, die den Rahmen von „data-driven“ sprengen würden. Werden zukünftig neue Features definiert und implementiert, sollte dies möglichst mit dem derzeitigen Stand des Repositories erfolgen, indem man neue Objekt-Typen definiert und in DAP5 die damit beabsichtigte Funktionalität umsetzt. Ein ständiges Aufbohren des Repositories, selbst zur Umsetzung neuer GUI-Wünsche, wäre sehr schnell kontraproduktiv. Für spezielle und ausgefallene GUI-Wünsche kann man auf XDEV selbst zurückgreifen.

Wie schon im DAP5-Prototyp implementiert, kann man speziell angefertigte TABS mit den gewünschten, fest programmierten Eigenschaften erstellen und diese genauso den Knoten des Navigationsbaumes zuordnen – die Sprachschicht des REPOS kann auch benutzt werden, ebenso die Basis-Selcts für die darin angezeigten Objekte.

Nur beim Hybrid-Betrieb für eine Anwendung muss man die angesprochenen DB-Objekte in einem Entwicklungsschema zur Verfügung haben, weil XDEV deren Aufbau zur Referenzierung in Methodenaufrufen und zur Kompilierung benötigt.

In diesem Falle werden durch Assistenten die vorliegenden DB-Objekte

zur Auswahl und Konfiguration angeboten, so dass durch wenige eventbezogene Codezeilen die Datenbank-TableRows in abgeleitete virtuelle Tabellen transportiert werden und von dort auf die GUI-Objekte verteilt werden.

XDEV2 mit dem grafischen Daten-Modeller, dem GUI-Designer und dem Code-Editor bietet von sich aus schon hervorragende Eigenschaften, um Java-Anwendungen zügig entwickeln zu können. Alles was Java bietet, kann genutzt werden.

### Weitere geplante Features

Momentan sind die Insert-, Update- und Delete-Aktionen (Button-bezogen) nur satzweise möglich. Wie in Oracle SQL Forms enthalten, sollte jedoch eine Multi-Row-Verarbeitung, ausgehend von Multi-Row-GUI-Objekten, möglich sein – dies ist als weiteres DAP5-Feature geplant.

XDEV2 bietet einfach zu bedienende Methoden, um Tabellen (intern in virtuellen XDEV-Tabellen abgebildet) im CSV-Format ausgeben zu können. Dieses Feature wird zukünftig auch angeboten, aber nur über zu definierende Buttons, welche dem Rollenkonzept unterworfen sind. Es ist geplant, diese im CSV-Format auszugeben, allerdings nach Namenskonventionen und mit Hinweis auf vorgefertigte Excel-Sheets, welche das erzeugte CSV-File als INPUT erkennen und durch Makro-Aktivierung eine sofortige Formatierung und Pivotisierung innerhalb Excel erfolgen lassen.

E-Mail-Generierung kann auf ähnliche Art im Programm angebunden werden. Obendrein gibt es noch sehr viele Features, die man per XDEV2 und dem REPOS in den Anwendungen zur Verfügung stellen kann. Die Protokollierung von sensiblen Aktionen ist ebenfalls angedacht.

Um einen gewissen Grad an Applikations-Sicherheit zu gewährleisten, wird es Mechanismen zur Sicherung gegen unerlaubtes Ändern, Verschieben und Austauschen von REPOS-Inhalten und REPOS-Dateien geben. Die Konsistenz zwischen REPOS und ausgelagerten REPOS-Dateien muss auf alle Fälle abgesichert werden.

Durch die Neugestaltung der XDEV3-Workbench soll es noch leichter möglich sein, speziell angefertigte Java-Bausteine (Beans usw.) zu integrieren – dieses Thema wurde bisher noch nicht behandelt, bietet aber sicher interessante Möglichkeiten. Mit der ebenfalls angekündigten AJAX-Implementierung in XDEV3 eröffnen sich unter Umständen weitere Aspekte, um das „Look&Feel“ beim Betrieb unter einem Browser zu verbessern – allerdings sei angemerkt, dass der Fokus von DAP5 mehr auf der Verarbeitung von Daten liegt (mit vielen Eigenschaften aus der Oracle-Forms-Welt), als auf der schicken Präsentation im Intranet/Web.

### Fazit

Unter der Annahme, dass die GUI-Entwicklung meist wesentlich mehr als 50 Prozent der Gesamtprojektkosten in Anspruch nimmt, bietet DAP5 die Chance, durch die Nutzung der vorgefertigten Bausteine einen wesentlichen Teil davon einsparen zu können. Würden anstelle der „vorgefertigten Bausteine“ die GUI-Objekte individuell programmiert, müsste man für jedes der Objekte den Code erstellen, testen und verwalten, was viel an Zeit und Budget kostet – auch dann noch, wenn die Entwickler RAD-Tools verwenden.

Als Entscheidungskriterien, um über „datadriven“ und DAP5 nachzudenken, seien zwei wesentliche genannt:

- Können in einem Projekt mit DAP5 mehr als 90 Prozent der GUI-Objekte mit vorgefertigten Bausteinen realisiert werden?
- Ist anzunehmen, dass nach Fertigstellung des GUI überdurchschnittlich viel Änderungsbedarf und Erweiterungen zu erwarten sind?

Werden beide Fragen mit „Ja“ beantwortet, bietet die Philosophie des „datadriven“ eine Alternative – DAP5 ist eine Lösung innerhalb dieser Philosophie.

### Kontakt:

Hans Niedermeier  
hans\_niedermeier@t-online.de

# Tipps und Tricks aus Gerds Fundgrube

## Heute: Tipps zur IDE

Gerd Volberg, OPITZ CONSULTING GmbH

**Diesmal gibt es ausnahmsweise kein Code-Beispiel, sondern ein paar Tipps zum effizienteren Arbeiten mit der IDE.**

Abbildung 1 zeigt die beste Anordnung von Objekt-Navigator, Property-Palette, Layout-Editor und PL/SQL-Editor. Objekt-Navigator und Property-Palette sind überschneidungsfrei direkt nebeneinander angeordnet. In Abbildung 2 liegen Layout- und PL/SQL-Editor übereinander und nehmen den Raum ein, den der Objekt-Navigator frei lässt.

### Canvas-Platzierung

Masken, in denen viele Canvases existieren, bereiten häufig Probleme, weil jeder Canvas beim Öffnen des Layout-Editors an einer anderen Stelle positioniert wird. Möchte man nun alle Canvases im gleichen Bereich der IDE anzeigen, wie in Abbildung 1 beschrie-

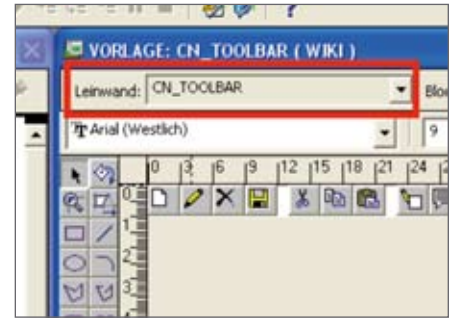


Abbildung 3: Bulk-Changes von Canvas-Position und -Größe

ben, müsste man dies für jeden Canvas einzeln tun und das Ganze würde in erhebliche Arbeit ausarten. Es geht auch einfacher: Nachdem der erste Canvas optimal positioniert wurde, werden alle weiteren mit dem List-Item „Leinwand“ ausgewählt und die Maske anschließend gespeichert. Von jetzt an werden diese Canvases an der gleichen Position und in derselben Größe angezeigt (siehe Abbildung 3).

### Mehrfaches Erzeugen von Objekten

Benötigt man in einer Canvas mehrere Buttons, Items oder andere GUI-Elemente, klickt man mit der Maus einfach doppelt auf das entsprechende Icon in der Werkzeugleiste. Dieses Icon bekommt dann zur Bestätigung eine kleine rote Stecknadel. Von nun an kann man im Layout-Editor beliebig viele Buttons nacheinander anlegen (siehe Abbildung 4).

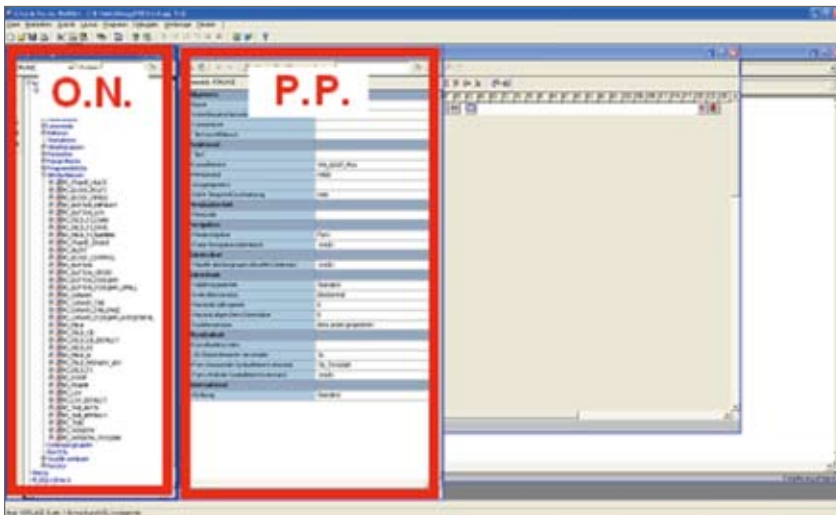


Abbildung 1: Platzierung von Objekt-Navigator und Property-Palette

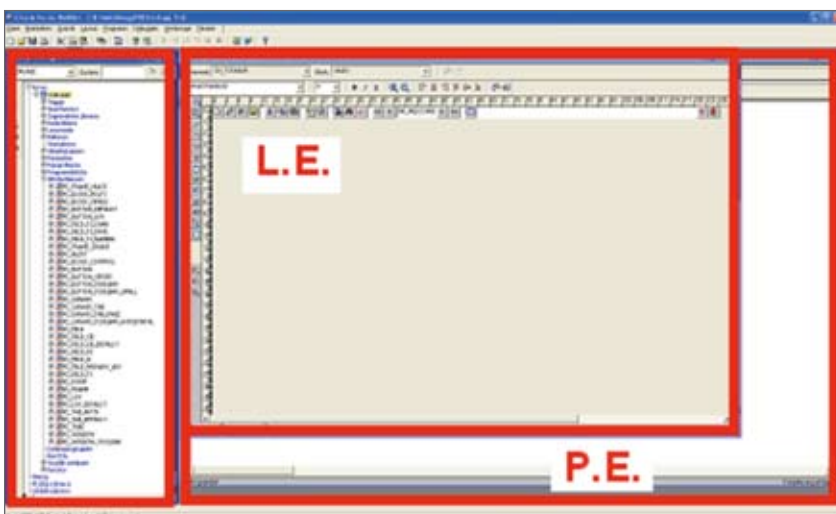


Abbildung 2: Platzierung des Layout- und des PL/SQL-Editors

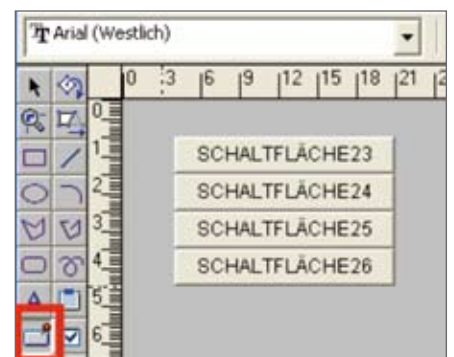


Abbildung 4: Mehrfaches Erzeugen von Objekten

**Kontakt:**  
Gerd Volberg  
talk2gerd.blogspot.com

19. - 20. Oktober 2010  
Meistersingerhalle Nürnberg

**database pro**  
powerdays

2 Konferenztage zu

# Datenbanken in der Cloud

Für Leser der  
**DOAG News**  
**€100,-**  
Ermäßigung auf  
die Teilnahme  
(€ 399,- statt € 499,- zzgl. MwSt.)  
Ihr Anmeldecode:  
**DBPD10DOAG**

19. Oktober 2010

**SQL Azure**

**„Database as a Service“  
in der Microsoft-Welt**

Content-Manager und Moderator:  
**Markus Eilers**, Geschäftsführer, runtime software GmbH

- SQL-Azure-Projekte aufsetzen, verwalten, mit der richtigen Architektur einbinden
- Die richtigen Architekturmuster zur Skalierbarkeit und Performancesteigerung
- Sicherheit garantieren mit Datenverschlüsselung und Zugriffskontrolle

20. Oktober 2010

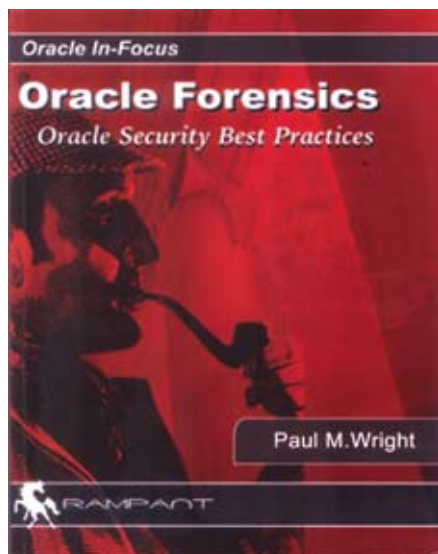
**SimpleDB, CouchDB & Co.**

**NoSQL und Map-Reduce für  
Ihre Anwendung**

Content-Manager und Moderator:  
**Prof. Dr. Stefan Edlich**, Beuth Hochschule für Technik Berlin

- Grundlagen: Jenseits der SQL-Server - Datenbanken für das Web 2.0
- Replikation und Persistenzstrategien für Cloud-Datenbanken
- Zukunftssicher - Skalieren von nichtrelationalen Datenbanken

Information und Anmeldung: **www.databasepro-powerdays.de**



# Oracle Forensics Oracle Security Best Practices

gelesen von Franz Hüll

Beim ersten Durchblättern fällt auf, dass das Buch im Mai 2007 erschienen ist und die Liste der Oracle Versionen bei der Version 10 Schluss zu Ende ist. So viel sei schon vorweggenommen, dass sich die darauf gründende Skepsis beim Lesen des Buches nicht bestätigt hat.

In der Einleitung beschreibt der Autor, Paul M. Wright, seine Zielgruppe und gibt auch gleich den praktischen Hinweis, dass erfahrene Leser zwei sehr kurze Einführungskapitel überspringen können.

Zu Beginn werden typische Sicherheitsprobleme beschrieben, die an unterschiedlichen Stellen in der Architektur (Client side, Application Server, Netzwerk, Datenbank etc.) auftreten können.

Danach leitet der Autor zu typischen Angriffen über und beschreibt im Detail, wie diese aufgebaut sind und ablaufen können. Hier wird das Buch seinem Titel „Forensik“ gerecht. Es wird gezeigt, welche Spuren ein Angreifer hinterlässt, wenn er unerfahren ist und wie ein erfahrener Angreifer Spuren verwischen kann. Es werden aber auch die Gegenmaßnahmen aufgezeigt, die den Versuch des Angreifers seine Spuren zu entfernen ins Leere laufen lassen bzw. erschweren.

Ein wichtiges Kapitel beschäftigt sich mit den Maßnahmen, die zu ergreifen sind, nachdem ein Angriff erkannt wurde. Eine der wichtigsten ist

die Sicherstellung der Angriffsspuren für spätere Untersuchungen. Es wird erläutert, wo sich entsprechende Daten befinden können und wie diese sicher aufzubewahren sind. Das sind natürlich alle Arten von Logfiles, es können aber auch Speicherinhalte oder Daten in der Datenbank bzw. auf Betriebssystemebene sein. Die Spuren können flüchtig oder irgendwo auf Platte fest abgespeichert vorliegen.

Dabei werden auch verschiedene Tools wie z.B. BBED (Block Browser and Editor) aber auch Oracle Features wie Flashback mit einbezogen. Das zeigt, dass sich der Autor spätestens in diesen Kapiteln an den erfahrenen Leser wendet.

So geht Paul Wright immer mehr in die Tiefe und die im Kapitel 6 aufgeführten forensischen Szenarien sind sehr informativ und spannend zu lesen.

Im letzten Viertel des Buches gibt Paul Wright noch eine ganze Reihe von Hinweisen und Anleitungen zu verschiedenen Aspekten rund um die Sicherheit von Datenbanken. Er zeigt an ein paar Beispielen, wie die Suche nach Sicherheitslücken durchgeführt werden kann, er widmet sich der Frage, wie die Datenbankversion und der Patchstatus zu ermitteln ist und er befasst sich ausführlich mit Checksummen, die dazu verwendet werden, Veränderungen an Datenbank-Objekten zu erkennen.

## Fazit

Insgesamt ist das Buch gut und flüssig zu lesen und liefert eine Vielzahl von Informationen. Dass das Buch nicht hochaktuell ist, ist nur ein kleiner Nachteil. Insgesamt gesehen ist das Buch, da es alle wesentlichen Aspekte zum Thema Oracle Forensik ausführlich behandelt, sehr informativ und für den Leser, der sich mit Forensik beschäftigt sicher sehr nützlich.

Über das ganze Buch verteilt findet der Leser viele Hinweise auf weiterführende Literatur und zu anderen Quellen im Internet.

Titel:	Oracle Forensics Oracle Security Best Practices
Autor:	Paul M. Wright
Umfang:	320 Seiten
Verlag:	Rampant Tech Pr (Mai 2010)
Sprache:	Englisch
ISBN-10:	0977671526
ISBN-13:	978-0977671526

**Kontakt:**  
Franz Hüll  
securityfragen@doag.org

# Humane Nutzung der Informationstechnologie – mehr Lebensqualität durch IT!



## 1. Kongress der Integrata-Stiftung

14. Oktober 2010 im Radisson Blu Hotel Karlsruhe

### Parallele Sessions

- **Bildung:**  
Lernen und IT  
Moderation Prof. Dr. Andreas Oberweis, KIT
- **Kommunikation:**  
Social Media und die Verantwortung der IT  
Moderation Prof. em. Dr. Rolf Pfeiffer, Hochschule Reutlingen
- **Gesundheit:**  
Prävention und Heilung unterstützt von der IT  
Moderation Dipl.-Inf. Waltraud Dehning, Branta Expert Net Consulting GmbH

### Hochkarätige Keynote Speaker

Keynote Gesellschaft  
Prof. Dr. Andreas Meier,  
Universität Fribourg (CH)

Keynote Wirtschaft  
Wolfgang Braun,  
Meta Mergers & Acquisitions

Keynote Wissenschaft  
Prof. Dr. Dr. Hermann Maurer,  
TU Graz (A)

Informationen und Anmeldung unter [www.doag.org/events/khnit](http://www.doag.org/events/khnit)

[www.integrata-stiftung.de](http://www.integrata-stiftung.de)

## DOAG-Vorstand beschließt die jährliche Vergabe des Ehrenpreises „DOAG-Botschafter“

Die DOAG wird künftig jedes Jahr zwei Preise vergeben: DOAG-Botschafter im Bereich Technologie und DOAG-Applications-Botschafter im Bereich Business Applications. Die Ehrung erhält diejenige Person, die sich in den Medien der DOAG durch hohes Engagement und große Kompetenz ausgezeichnet hat. Zu den Medien zählen DOAG News, DOAG Business News, SIGs, Regios, Expertenseminare, Konferenzen und die Internet-Plattform. Vorschlagsrecht haben alle DOAG-Mitglieder, die Entscheidung trifft ein DOAG-Gremium aus Vorstandsmitgliedern und Beiräten. Die vorgeschlagenen Personen dürfen nicht dem Vorstand und dem Beirat der DOAG angehören, müssen aber nicht DOAG-Mitglied sein. Die Preise werden im Rahmen der DOAG 2010 Konferenz beziehungsweise der DOAG 2011 Applications überreicht.

Unter [www.doag.org/go/botschafter](http://www.doag.org/go/botschafter) ist eine Seite eingerichtet, auf der DOAG-Mitglieder bis 30. September 2010 ihre Vorschläge für den DOAG Botschafter 2010 einreichen können.

## Die DOAG entwickelt sich gut!



Dr. Dietmar Neugebauer  
Vorstandsvorsitzender

Basierend auf den guten Zahlen in 2008 hat die DOAG auch das Geschäftsjahr 2009 erfolgreich beendet: Sowohl der Verein als auch die Tochtergesellschaft

DOAG Dienstleistungen GmbH haben jeweils mit einem guten positiven Ergebnis abgeschlossen.

Das Engagement der Mitarbeiterinnen und Mitarbeiter der DOAG, der vielen aktiven Mitglieder, Beiräte und Vorstände wirkt sich positiv aus. Der Verein kann, basierend auf den guten Zahlen, kraftvoll an die neuen Herausforderungen herangehen, die die Community vor sich hat. Durch den Zukauf von Sun durch Oracle kommen viele neue Aufgaben auf die DOAG zu. Das sind zum einen softwaretechnische Themen wie Java, MySQL, das Betriebssystem Solaris sowie weitere Open-Source-Lösungen und zum anderen die Hardware-Produkte. Ziel ist es, auch künftig die Interessen aller deutschen Oracle-Anwender zu vertreten. Ich bin überzeugt, dass wir mit unseren vielen Mitgliedern und guten Mitarbeiterinnen und Mitarbeitern diese Herausforderungen meistern werden.

Der Finanzbericht 2009 steht unter [www.doag.org/go/finanzbericht](http://www.doag.org/go/finanzbericht) zum Download bereit.

### Kontakt:

Dr. Dietmar Neugebauer  
[dietmar.neugebauer@doag.org](mailto:dietmar.neugebauer@doag.org)

## Start der eigenständigen SIG Java



Andreas Badelt  
Leiter der SIG Java

Am 29. April 2010 ging in Nürnberg die neue Special Interest Group Java an den Start. Die Veranstaltung zum Thema „Rapid Application Development mit Java“ war gleich eine doppelte Kooperation: zum einen mit der SIG Development, aus der die SIG Java ausgegründet wurde und zum anderen

mit der Java User Group (JUG) Nürnberg im Rahmen des neuen Interessenverbands der Java User Groups e.V. (iJUG) – dem auch die DOAG angehört ([www.ijug.eu](http://www.ijug.eu)).

Das Interesse an der Veranstaltung war erfreulich groß, es konnten mehr als 50 Teilnehmer begrüßt werden – die bislang größte Teilnehmerzahl für ein SIG-Treffen mit Java-Themen, abgesehen von der DOAG-Konferenz. Dies ist sicher der erhöhten Aufmerksamkeit für Java durch die Übernahme von Sun durch Oracle sowie der neuen Kooperation innerhalb des iJUGs zu verdanken. Zudem stieß die umfangreiche Agenda auf reges Interesse, was sich im Laufe der Veranstaltung bestätigte.

Nach kurzer Begrüßung durch die Organisatoren (Christian Schwitala für die SIG Development, Andreas Badelt für die SIG Java sowie Oliver Szymanski für die JUG Nürnberg und als Vorstand des iJUGs) ging es dann auch gleich los. Die ersten beiden Vorträge hielt Markus Stiegler von der XDEV Software Corporation: Zunächst führte er in das Thema ein, indem er die Frage beantwortete, was Rapid Application Development eigentlich bedeutet – nämlich nicht nur Tools, sondern auch eine Methode zur Anforderungsspezifikation und zur Risiko-Minimierung in Software-Projekten mittels Prototypen. Dann ging er auf die Vor- und Nachteile dieser Vorgehensweise ein. Am Beginn stand die Erkenntnis, dass in Software-Projekten häufig keine ausgearbeiteten Lastenhefte mehr als Basis dienen und dass dies häufig auch gar nicht möglich ist, weil den Auftraggebern die Kenntnisse dazu fehlen. Dies wurde von den Zuhörern bestätigt. Unter anderem war zu hören, dass selbst Behörden inzwischen vielfach nach dem Motto vorgehen: „Wir wissen zwar noch nicht genau, was wir wollen, aber wann es fertig sein und was es kosten soll.“ Zu großer Erheiterung trug auch die Erkenntnis eines Teilnehmers bei, dass „Telepathie auch ein Teil von Software-Entwicklung ist“.

Um nun die fehlende Spezifikation zu ersetzen, bietet es sich an, „Rapid GUI Prototyping“ zu betreiben, um mit dem Kunden die funktionalen Anfor-



derungen (die ja in der Regel anhand der GUI sichtbar werden) durchgehen und festlegen zu können. Ein weiterer Vorteil ist, dass mit dem Prototypen Anforderer und Management erst einmal „beruhigt“ werden können, die sonst in der Regel lange auf erste sichtbare Ergebnisse warten müssten. Gleichzeitig zeigte Markus Stiegler aber auch wieder den Nachteil auf: dass ein fertiger Prototyp nämlich häufig zu der Frage des Kunden führt, warum die Implementierung denn noch so lange dauern werde – es sei doch eigentlich schon alles fertig. So wie dieses wurden viele Details des Prototypings in ihren Vor- und Nachteilen vorgestellt und rege diskutiert. Die Folien dazu sind natürlich – wie auch für die anderen Vorträge – für DOAG-Mitglieder und andere Teilnehmer auf dem DOAG-Server verfügbar.

#### XDEV

Nach dieser Einführung ins Thema stellte Markus Stiegler die eigene Software XDEV vor. „Was macht Java so schwierig?“, war die einleitende Frage, die er damit beantwortete, dass 4GL-Entwicklern der Umstieg auf reine Objektorientierung in der Regel sehr schwer fällt und eine längere Zeit benötigt. Das XDEV-Framework verspricht hier nun Abhilfe, indem es diesen Entwicklern ermöglicht, Java-Applikationen so zu entwickeln, wie sie es von jeher gewohnt sind, mit einfach zu bedienenden, aber Feature-reichen Tools zur GUI-Erstellung und der Wizard-getriebenen Implementierung aller nötigen Logik, um die GUI mit den Datenquellen zu verknüpfen. Auch browsergestützte Applikationen werden hier unterstützt, was über Applets realisiert ist. Den pauschalen Bedenken in vielen Firmen gegen Applets trat Markus Stiegler entgegen: „Im Zusammenhang mit JavaFX hat auch noch niemand den Einsatz von Applets diskutiert ... Applets sind sicher und optimal.“ Trotzdem wird es im Lauf des Jahres auch eine XDEV-Version mit Ajax-Integration geben, um hier den Markt zu erweitern, auch wenn dies rein technisch wenig Sinn ergibt.

Das Lizenzmodell von XDEV sieht eine freie Version für kleinere Projek-

te vor, ab einer gewissen Größe müssen dann Entwicklungslizenzen (keine Runtime-Lizenzen) erworben werden. Die aktuelle Version 2 von XDEV ist eher für GUI-Entwickler und Java-Anfänger geeignet, ab der demnächst verfügbaren Version 3 sollen aber auch „Hardcore-Java-Entwickler“ gewonnen werden. Durch die Umstellung der Entwicklungs-Umgebung auf Eclipse, mit den GUI-/RAD-Tools als Aufsatz, sollen dann beide Welten kombiniert werden: detaillierte Kontrolle über den Code, umfangreiche Tool-Unterstützung für die Core-Java-Entwicklung sowie die RAD-Features von XDEV.

#### Datengetriebene Applikationen

Den nächsten Vortrag hielt Hans Niedermeier über „Datengetriebene Applikationen“. Der Referent zeigte hier ein von ihm selbst geschriebenes Framework. Die Motivation dafür bestand zum einen aus der Erkenntnis, dass die Applikationsentwicklung viel Spezialwissen vom Entwickler erfordert, das gerade bei der GUI-Entwicklung einer geringen Halbwertszeit unterliegt. Zum anderen aus der Tatsache, dass GUIs raschen Änderungen unterliegen, aber zu einem sehr großen Teil aus Standard-Funktionalitäten bestehen. Aus dieser Motivation heraus entwickelte Hans Niedermeier ein Framework, das den gesamten Aufbau einer Anwendung (Zusammensetzung, Zugriffsrechte, Menüs, Datenbankzugriffe etc.) in einem Repository hält und daraus automatisch eine entsprechende Applikation aufbaut. Mithilfe der zuvor vorgestellten Plattform XDEV wird aus den Metadaten zur Laufzeit(!) eine Anwendung aufgebaut. Auf diese Art und Weise ist auch ein in Java wenig erfahrener Entwickler in der Lage, eine Web-Anwendung zu erstellen. Hans Niedermeier skizzierte kurz die Möglichkeiten des Systems und betonte, dass er es weiterentwickeln wird.

#### JavaFX

Der Vortrag von Peter Doschkinow (noch: Sun Deutschland) hatte JavaFX als Thema. JavaFX ist zwar (noch) nicht direkt dem Bereich RAD zuzuordnen. Dennoch war dieser Vortrag

eingepflanzt worden, da diese Technologie das Potential hat, in Zukunft einen großen Beitrag zur RAD-Entwicklung in Java zu leisten.

Zunächst ordnete Peter Doschkinow JavaFX gegenüber der Konkurrenz (Flash, Silverlight) ein und betonte dabei, dass diese zurzeit noch großen Vorsprung habe, JavaFX jedoch allein schon durch die enorme Verbreitung von Java Unterstützung erfahre. Momentan sei die Technologie aber noch jung und nicht vollständig ausgereift, was sich unter anderem an den großen Sprüngen zwischen Releases zeige (aktuelle Version seit April 2010: 1.3) – teilweise entstehen bei Upgrades noch Inkompatibilitäten. Ein aktuelles Manko sei auch, dass es keine eingebaute Unterstützung für Client-Server-Synchronisation gebe. Aber der Plan sehe vor, JavaFX um dieses und andere Features zu erweitern, sobald die Grundlagen komplett funktionieren. So ist beispielsweise an eine Integration in JSF / ADF gedacht. Auch die Beschleunigung von JavaFX-Applikationen durch gezielte Hardware-Unterstützung ist geplant, dazu finden derzeit Verhandlungen mit Herstellern statt. Speziell zum Stichwort „RAD“ verwies der Referent auf den neuen JavaFX Composer, der bereits als Plugin für NetBeans 6.8 / 6.9 beta verfügbar ist und das einfache Zusammenbauen von Oberflächen per Drag&Drop ermöglicht. Hiermit wurde bereits ein wichtiger Schritt vollzogen, auch wenn das Tool sicher noch nicht ausgereift ist.

Zwischendurch demonstrierte Peter Doschkinow anhand einer kleinen Vorführung das Potential von JavaFX, wenn es um die Erstellung von Rich Internet Applications geht – die sowohl im Browser als auch auf mobilen Clients laufen.

#### Rapid Web Application Development

Der Vortrag über „Rapid Web Application Development mit Grails und Oracle“ sollte eigentlich von Robert Szilinski gehalten werden – dieser war jedoch kurzfristig verhindert. Einer wohl ziemlich seltenen Konstellation war es aber zu verdanken, dass der Vortrag kurzfristig von seinem Bruder Frank übernommen wurde, der eben-

falls für die Firma esentri consulting GmbH arbeitet. Zunächst gab er einen kurzen Überblick über die Entstehungsgeschichte von Groovy und dem darauf basierenden Open-Source-Framework Grails, das nach dem Kauf von SpringSource nun zu vmware gehört. Danach zeigte Frank Szilinski anhand von Beispielen eindrucksvoll, wie einfach sich mit Grails Applikationen erstellen lassen – zum einen durch die gegenüber Java prägnante und produktive Sprache, zum anderen durch die Prinzipien des Frameworks, wie „Convention over Configuration“ oder „Scaffolding“ (das Erzeugen eines Applikationsgerüsts). Auch die große Menge an Plugins und deren einfache Austauschbarkeit wurde erwähnt. Inzwischen, so der Referent, wird Grails auch bei Oracle wahrgenommen, eine Unterstützung in ADF ist jedenfalls geplant.

Der große Haken ist derzeit noch die Performance – verglichen mit einer Java-Applikation ist Grails noch 5- bis 15-mal langsamer. Dies liege jedoch nicht an Grails selber, sondern an Groovy, das noch einiges an Performance-Steigerungen vertragen könne. Verbesserungen seien aber in Planung, insbesondere die verbesserte Unterstützung dynamischer Sprachen durch die JVM (Java 7) dürfte hier einiges bewirken. Eine Frage kann man aber wohl bereits positiv beantworten, nämlich ob Grails „Enterprise Ready“ sei: Es gibt schon einige „große“ Seiten mit Millionen von Nutzern beziehungsweise mindestens einer Million Zugriffen pro Monat, die auf Grails basieren.

### Oracle Application Development Framework

Der nachfolgende Vortrag drehte sich um das Oracle Application Development Framework (ADF) und wurde von Jürgen Menge (Oracle) gehalten. Die Hauptmotivation für ADF ist laut Menge „die Unmenge an Standards, die ein (Java-)Entwickler heute kennen muss. Es bleibt keine Zeit mehr für die Entwickler, sich einzuarbeiten.“ Das Ziel, das Oracle mit ADF erreichen wolle, sei daher eine Entwicklungsplattform, die auf offenen Standards basiert und komplett ist, die aber von technischen Details abstrahiert und

eine hohe Produktivität ermöglicht. Die Entwickler sollen fachliche Anforderungen umsetzen, ohne sich um die Details zu kümmern. Dies führte zu der Frage eines Teilnehmers: „Wie produktiv ist ein ADF-Entwickler – hat sich hier seit den Zeiten von UIX vor einigen Jahren viel getan gegenüber 4GL-Umgebungen wie Forms?“ Die Frage sei schwierig zu beantworten, so der Referent, aber dann wagte er doch eine Aussage: „Bei gleicher Aufgabenstellung ist ein Forms-Entwickler heute in der Regel immer noch produktiver, aber ADF holt stark auf.“

Die Stärken, die ADF heute gegenüber den meisten anderen Frameworks auszeichnen, sind unter anderem die Möglichkeiten der Transaktionssteuerung, Session-Verwaltung, das durchgängige Sicherheitskonzept, Templates und Skinning sowie die Browser-Unabhängigkeit. Ein weiterer wichtiger Punkt von ADF ist die Unabhängigkeit von View und Model (EJB, ADF Business Components, Web Services etc.) durch das Data Binding (JSR-227, der „leider immer noch nicht verabschiedet“ wurde). Auch auf JSR-127, die von Oracle stark unterstützen „Java Server Faces“ und die speziell für ADF entwickelten Ergänzungen (ADF Faces) ging der Vortrag ein. Ein weiteres Detail aus dem Vortrag sei hier noch vermerkt: Die neueste ADF-Version enthält eine MS Excel-Integration.

### Erfahrungsbericht über die Migration

Der letzte Vortrag des Tages wurde von Oliver Zandner und Björn Christoph Fischer zum Thema „Single Sourcing in Java – Desktop-Anwendung & Web-Applikation aus einer Quelle“ gehalten. Es war ein Erfahrungsbericht über die Migration einer über viele Jahre gewachsenen, auf Oracle Forms basierenden Standard-Software in die Java-Welt. Zunächst wurden die spezifischen Anforderungen an die existierende beziehungsweise die neu zu schaffende Labor-Software „Lisa“ vorgestellt, wie Wiederverwendung des vorhandenen PL/SQL-Codes, „pessimistic locking“, um versehentliche parallele Änderungen von vornherein auszuschließen, sowie hoher Bedienungskomfort. Ein

weiteres wichtiges Ziel war, die in die Java-Welt migrierte Anwendung sowohl für Rich Clients als auch für (mobile) Web Clients zur Verfügung zu stellen. Um nun nicht die Applikation zweimal zu entwickeln, wurde versucht, den gemeinsamen Code-Anteil für beide Varianten soweit wie möglich auszudehnen.

Nach einigem Experimentieren mit verschiedenen Technologien, so die Referenten, wurde dann die ideale Voraussetzung dafür gefunden: Die Eclipse „Rich Client Platform“ (RCP) in Kombination mit dem Ajax-basierten „Rap Widget Toolkit“ (RWT). Die Applikation wird mit RCP für Rich Clients entwickelt. Für die browserbasierten Clients wird dann das in RCP enthaltene „Standard Widget Toolkit“ (SWT) durch das API-kompatible RWT ersetzt.

Im weiteren Verlauf des Vortrags wurde dann gezeigt, wo die Grenzen des Ansatzes liegen, beziehungsweise wie damit umgegangen werden kann, weil beispielsweise innerhalb des Browsers „Key Bindings“ oder „Mouse Tracking“ fehlen. Fazit: Es gibt ein paar kleinere Nachteile, insbesondere für die Web Clients, aber die Code-Wiederverwendung liegt typischerweise zwischen 90 und 95 Prozent.

### Fazit

Die Veranstaltung wurde durch eine Abschlussdiskussion abgerundet, in der die Teilnehmer noch einmal Fragen an alle Referenten stellen oder auch untereinander diskutieren konnten. Das Feedback der Teilnehmer war sehr positiv, so dass die DOAG sich in der Gründung einer eigenen SIG Java bestätigt fühlte. Das nächste Treffen der SIG Java findet am 9. September in München statt. Das Thema: Java Enterprise Edition (JEE) 6. Dazu werden noch Referenten gesucht. Für alle Fragen, Themenvorschläge, Vortragsangebote etc. ist die E-Mail-Adresse sig-java@doag.org eingerichtet.

### Kontakt:

Andreas Badelt  
sig-java@doag.org



Michael Pfautz  
Leiter der SIG Database

## SIG Database für Einsteiger

Das Zustandekommen dieses Termins war die Kombination einer außergewöhnlichen Diskussion der DOAG-Aktiven anlässlich der Beiratssitzung 2010 und des Feedbacks einiger Teilnehmer und Mitglieder aus vorherigen Veranstaltungen. Warum immer nur in den Tiefen der Oracle-Prozesse wühlen und nicht mal einfache und leichte Kost für die vielen Oracle-Beginner bringen? Das Fazit dieser Diskussion hatte diese Veranstaltung zum Ergebnis.

Ganz spontan hat sich hier Johannes Ahrends von Quest Software bereit erklärt, der bereits eine ähnliche Veranstaltung im Rahmen eines einwöchigen Seminars an der Hochschule zusammen mit seinem Kollegen Thomas Klughardt gehalten hat. Beiden Referenten nochmals ein herzliches Dankeschön für die spontane Zusage und gut vorbereitete Veranstaltung.

Bemerkenswert für diese SIG war die rege Teilnahme aus dem gesamten Bundesgebiet. Bei wunderschönem Wetter startete die Veranstaltung pünktlich mit vollständig anwesender Teilnehmerschaft. Dies war bereits die erste Besonderheit bei dieser SIG.

Die beiden Referenten führten gekonnt und routiniert durch das Tagesprogramm. Im Rahmen der einzelnen Vorträge wurden durch Fragen und gezielte Rückfragen die Teilnehmer sehr gut mit einbezogen, was sich auch in der sonst nicht so angetroffenen regen Diskussion zwischen Teilnehmern und Referenten widerspiegelte. Sogar die Pausen wurden ausgiebig genutzt, um im Teilnehmerkreis und mit den

Referenten einige Themen und Punkte noch tiefergehend zu besprechen beziehungsweise zu diskutieren.

Eine Einführung in die einzelnen Oracle Datenbank-Produkte (Standard, Enterprise, Personal und Express) mit den verfügbaren Features und Funktionen war der Startschuss in einen für viele interessanten und informativen Tag. Hier wurden sehr viele Fragen seitens der Teilnehmer über die Zusatzoptionen und deren Verwendung und Lizenzierung gestellt.

Die Referenten vermittelten die Basis der Datenbank-Software, angefangen von Aufbau und Struktur über die Prozesse bis hin zum Netzwerk. Auch hier kamen aus dem Teilnehmerkreis immer wieder viele Fragen über generelle Funktionsweisen und Abläufe sowie über Zusammenhänge der einzelnen Oracle-Prozesse und deren Abhängigkeiten. Dies ist eine generelle Problematik, die auch als weiteres Thema (beispielsweise „Was passiert mit meinem SELECT in der Datenbank?“) in den Feedback-Bögen genannt wurde.

Mit den Themen „Installation und Konfiguration“ und „Backup und Recovery“ sowie Anmerkungen zu den Tools wurden die Teilnehmer aufgrund der Fülle mit Folien und Informationen überschüttet. Details können die Teilnehmer aus den Folien auf dem DOAG-Server nochmals einsehen. Bei so vielen Themen war dieser interessante Tag für viele Teilnehmer viel zu kurz, die meisten hätten lieber zwei Tage dafür aufgewendet.

Bemerkenswert war auch das Feedback der Teilnehmer: Die vielen Themenvorschläge, Anregungen und Wünsche (PL/SQL mit Versionskontrolle, Apex, Migration und Upgrade, Patching, DB-Monitoring per SNMP, Schnittstelle zu Java etc.) werden natürlich alle ausgewertet und für die Planung der nächsten Termine genutzt, um noch mehr interessante Themen und Veranstaltungen für die DOAG-Mitglieder ins Leben rufen zu können. Überlegungen für die gewünschte Wiederholung einer solchen Veranstaltung werden ebenfalls geführt.

Der Organisator und Vorstand Michael Pfautz bedankt sich bei allen

Teilnehmern und den Referenten für die so aktive Teilnahme und das hervorragende Feedback und wünscht allen noch viele weitere so muntere und informative DOAG-Treffen wie dieses. Schreiben Sie uns, falls Sie weitere Themenwünsche oder Anregungen zur SIG Database haben, und welche Themen Sie aktuell interessieren.

### Kontakt:

Michael Pfautz  
sig-database@doag.org



Christian Schwitalla  
Leiter der SIG Development

## Treffen der SIG Development zum Thema „DB-Programmierung“ in Hamburg

Datenbank-Programmierung gehört zu den Kernthemen der SIG Development und ist daher regelmäßig ein Schwerpunktthema. Bei komplexen, datenintensiven Anwendungen steht vor allem die Datenbank-Schicht im Fokus der Entwickler. Nach wie vor fällt hier – und weniger in der GUI-Schicht – die Entscheidung über den Projekterfolg.

Im ersten Vortrag „Bäume und Mengenlehre – neue Features mit connect by, analytical functions – citius, altius, fortius (und simplicius)“ berichtete Helmut Skarka, pDv Technische Automation + Systeme GmbH, über seine Erfahrungen mit dem Einsatz von Analytical Functions in komplexen SQL-Abfragen. Obwohl sie seit der Datenbank-Version 8XXX zur Verfügung stehen, werden die Analytical Functions immer noch kaum eingesetzt, abgesehen von reinen Data-Warehouse-Anwendungen.

Zu Unrecht, wie der Referent meint. Analytical Functions erweitern den SQL-Sprachumfang und führen häufig zu dramatischen Verbesserungen der Performance. Als Beispiel wurden unter anderem ORDER BY SYBLINGS oder LAG() bzw. LEAD() genannt. In zahlreichen Beispielen aus dem Projekt-Alltag wurde die Mächtigkeit der Analytical Function veranschaulicht.

Carsten Czarski und Ulrike Schwinn von Oracle Deutschland hielten die beiden nächsten Vorträge. Zunächst konzentrierten die sich beim Thema „Oracle11g aus Entwicklersicht“ auf ausgewählte Features, die für Datenbank-Entwickler sehr nützlich sein können, aber häufig einen zu kleinen Bekanntheitsgrad haben. Das in der Datenbank-Version 11g neu eingeführte Oracle File System bietet eine einfache Schnittstelle, wenn es darum geht, Dateien in eine Datenbank-Tabelle aufzunehmen. Nach entsprechender Konfiguration reicht es dann, die betroffenen Dateien einfach in ein Verzeichnis im File-System zu kopieren. Es wurden noch weitere Features präsentiert wie Image Watermarking, Recursive WITH-Klausel, SQL PIVOT, virtuelle Spalten, Result Cache, Invisible Indexes, Fine Grained Dependency Tracking oder das direkte Ansprechen von Sequences.

Im zweiten Vortrag „PL/SQL Packages nutzen – Zeit und Aufwand sparen“ kamen ein paar ausgesuchte Datenbank-Packages zur Sprache:

- DBMS\_REDEFINITION
- DBMS\_METADATA
- DBMS\_DATAPUMP
- DBMS\_ASSERT

Diese Packages bieten zahlreiche nützliche Funktionen, die für den Projekt-Alltag wertvoll, aber häufig nicht bekannt sind, und daher nicht eingesetzt werden.

Als weiterer Referent präsentierte Hans Niedermeier, PRO-Software GmbH, den Vortrag „Datengetriebene Anwendungen definieren, ohne eine GUI-Sprache benutzen zu müssen“. Darin stellt er eine selbst geschriebene Entwicklungsumgebung für einfache, datenzentrierte Anwendungen vor. Der Ansatz hierbei ist: die Anwendungs-

entwicklung erfolgt zu 100 Prozent deklarativ. Die Informationen über den Aufbau einer Anwendung werden in einem DB-Repository gespeichert und daraus Java-Anwendungen generiert. Dabei wird das Framework XDEV2 der Firma XDEV Software Corp ([www.xdev-software.de](http://www.xdev-software.de)) genutzt. Die Stärke einer solchen Entwicklung ist eine extrem kurze Einarbeitungsphase. Der Nachteil: Man kann nur bestimmte, recht einfach aufgebaute Anwendungen auf diese Art erstellen, beispielsweise Pflegemaschinen für Stammdaten. Hans Niedermeier ist jedoch der Meinung, dass es in dem Bereich einen ernst zu nehmenden Markt für Entwicklungssysteme gibt, die auch ohne kostspielige Schulungen schnell einsetzbar sind. Die Entwicklungsumgebung wird noch weiter ausgebaut. Im Anschluss fand eine rege Diskussion darüber statt.

In den letzten beiden Vorträgen wurde die Architektur der IT-Landschaft der Berenberg Bank vorgestellt. Darin spielt die Oracle Datenbank nicht nur die Rolle des Datenspeichers – sie beherbergt auch die Geschäftslogik für die gesamte heterogene IT-Landschaft. In dem Vortrag „Geschäftslogik in der Datenbank – Architektur und objektorientierte PL/SQL-Programmierung“ präsentierte Andriy Terletsky die Überlegungen, die zu der Entstehung einer solchen Architektur geführt haben. Der Nachteil der Abhängigkeit von einem Software-Hersteller wird laut Referent dadurch mehr als ausgeglichen, dass die Geschäftslogik nur einmal entwickelt werden muss. Nicht nur für die Daten, auch für die Geschäftsregeln (Datenverarbeitungs- und Datenerfassungslogik) stellt die Oracle Datenbank den Single Point of Truth. Zentrale Rolle spielen hierbei die PL/SQL-Object-Types. Datenspeicherung erfolgt jedoch konventionell in relationalen Tabellen. Die Object Type Tables haben sich als unflexibel erwiesen, wenn es um die Schema-Evolution geht. Die jeweiligen Kernbereiche (Handelssystem, Backoffice, DWH und Kundenbereich) wurden in eigenständigen DB-Instanzen implementiert. Dies bietet eine hohe Flexibilität. Die Kommunikation zwischen

den DB-Instanzen erfolgt mit Hilfe von Oracle Streams.

Im nächsten Vortrag „Geschäftslogik in der Datenbank – Best Practice“ stellten Tobias Kreidel und Nis Nagel weitere Details vor: VPD, Rule Manager, PL/PDF, Import von Massendaten, Anbindung externer Systeme (auch COBOL-Anwendungen) sowie asynchrone Prozesse mit AQ. Der zweite Vortrag hat den Eindruck weiter verfestigt, dass die Berenberg Bank über eine interessante und anspruchsvolle IT-Landschaft verfügt. Sie ist stark Oracle-zentriert und nutzt intensiv Features der Datenbank.

An dieser Stelle vielen Dank an alle Referenten für ihre interessanten Vorträge! Das nächste Treffen der SIG Development findet in Form einer Doppel-SIG statt: am 7. Oktober in Berlin (<http://mydoag.doag.org/termine/termine.php?tid=347207>) und am 8. Oktober in München (<http://mydoag.doag.org/termine/termine.php?tid=347205>). Das Thema lautet: „Apex Total“. Das Treffen in München wird gemeinsam mit der Deutschen Application Express Community ([www.oracle.com/global/de/community/index.html](http://www.oracle.com/global/de/community/index.html)) organisiert. Themenvorschläge für weitere Treffen der SIG Development sind jederzeit willkommen.

#### Kontakt:

Christian Schwitalla  
sig-development@doag.org



Christian Trieb  
stellv. Vorstandsvorsitzender

## Internationales

Anfang Mai trafen sich die Vertreter der Oracle-Anwendergruppen aus EMEA zum Austausch und Kennen-

lernen in Budapest. Es waren Vertreter von 22 Usergroups anwesend, so dass es viele Informationen aus den einzelnen Ländern gab. Die DOAG war durch den stellvertretenden Vorsitzenden Christian Trieb vor Ort. Viele Anwendergruppen führen Veranstaltungen für ihre Mitglieder durch, bei denen es für Referenten aus Deutschland durchaus die Möglichkeit gibt, dort eine Präsentation zu halten. Anfragen bitte an christian.trieb@doag.org. Hier kann ein Kontakt zu anderen Oracle-Anwendergruppen hergestellt werden.

Auch Oracle war in Budapest mit Repräsentanten vertreten. So stellten Andrew Sutherland, Senior Vice President Middleware Business, und Chris Baker, Senior Vice President Core Technology Business, die Möglichkeiten von Oracle Cloud Computing vor. Karsten Roigk, Vice President Applications Strategy & Sales Support, präsentierte Neuigkeiten zur Strategie im Bereich Fusion Applications. Massimo Vogesi, Senior Director References, zeigte das Oracle Customer Reference Program. Bob Vangeel, EMEA Vice President Customer Advocacy, stellte aktuelle Informationen zum Oracle Support vor. Insbesondere wurde eine zukünftige Erweiterung von My ORACLE Support präsentiert, der Upgrade Advisor – ein Tool, das die Anwender bei der Durchführung von Upgrades sinnvoll unterstützen soll.

Mary Lou Dopart, Senior Director User Group Management, sprach über die wachsende Bedeutung der Anwendergruppen für Oracle, auch unter der Berücksichtigung, dass mit der Übernahme von Sun die Anzahl der Oracle-Anwendergruppen weltweit auf rund 900 gestiegen ist.

Das Treffen war diesmal stark durch den Austausch der Anwendergruppenvertreter untereinander geprägt. Dies gilt es in Zukunft noch auszubauen.

#### **Kontakt:**

Christian Trieb  
christian.trieb@doag.org



*Franz Hüll  
Leiter der Regionalgruppe Südbayern /  
München*

## DOAG-Regionaltreffen in München

### **April 2010**

Passend zum Schwerpunkt dieser DOAG News ging es beim Regiotreffen im April um die Sicherheit von Datenbanken und Web-Applikationen. Der erste Vortrag von Ralf Reinhardt (SecureNet GmbH) stellte sehr detailliert die Gefahren dar, die den Daten in der Datenbank drohen, wenn die Weboberfläche nicht sicher implementiert ist. Techniken wie XML-Injection, Cross-Site Scripting und SQL-Injection wurden anhand von Beispielen erläutert. Der Referent gab auch wertvolle Hinweise für Entwickler, um solche Schwachstellen zu vermeiden.

Der zweite Vortrag des Abends, gehalten von Alexander Kornbrust, Red Database-Security-GmbH, bestand aus zwei Abschnitten. Im ersten gab der Referent einen Überblick über die aktuelle Lage zur Datenbank-Sicherheit, inklusive des kurz vor dem Regiotreffen veröffentlichten Critical Patch Update (April-CPU). Der zweite Teil befasste sich mit der Verwendung von Triggern (Logon-, DDL- und Error-Trigger), um einen besseren Schutz der Datenbank zu erreichen. Als kleine Hilfe, wenn die Trigger implementiert werden sollen, stellt der Referent auf dem DOAG-Server auch Beispiel-Skripte zum Download zur Verfügung.

### **Mai 2010**

Im Mai trafen wir uns wieder einmal in der Hauptverwaltung von Oracle. Zum zweiten Mal stand der Einkaufskorb von Larry Ellison auf dem Prüfstand.

Diesmal wurde ein besonders großes Paket in diesem Einkaufskorb beleuchtet; Michael Künzner von Oracle Deutschland referierte über den Erwerb von Sun Microsystems (Schwerpunkt: Oracle Database Machine / Exadata). Als Zweites wurde dann noch über GoldenGate gesprochen.

Im Anschluss daran gab es eine Präsentation mit dem Titel „Systematische Migration vom Oracle Application Server zum WebLogic Server“, Referent war Dr. Georg Molter von der Zühlke Engineering GmbH. In seiner ausführlichen und mit vielen Details angereicherten Präsentation brachte er den Teilnehmern das Thema nahe.

Nach den Vorträgen war die Regiogruppe wieder einmal bei Oracle zu Gast und wurde mit einem leckeren Buffet verwöhnt. Vielen Dank an dieser Stelle an den Hausherrn.

### **Juni 2010**

Das dritte Treffen im Quartal begann mit einem Vortrag von Martin Decker von ora-solutions.net. Er konzentrierte sich auf Neuerungen zu Data Guard in 11g, Release 1 und Release 2. Zur Einstimmung aber gab es erst mal eine kurze Einführung in Data Guard. Damit war der Boden bereitet für die anschließende Besprechung der neuen Features. So konnten sich auch die Zuhörer, die Data Guard noch nicht so gut kannten, ein sehr gutes Bild machen. Abgerundet wurde das Ganze durch einige Demos.

Nach der Pause, in der es Butterbrez'n gab, sprach Martin Schlichenmayer von Oracle Deutschland über „BAM – Business Activity Monitoring in 11g“. In gewohnt lockerer Art und Weise begann der Referent seinen Vortrag und nutzte gleich als Erstes die Tafel des Hörsaals, um mit Kreide die ersten Bilder und Übersichten zu malen. Nach einer ganzen Reihe von grundlegenden Zusammenhängen wurde anhand von mitgebrachten Beispielen „Activity Monitoring“ live gezeigt.

Die Vorträge gaben den Zuhörern einen sehr guten und informativen Überblick über die jeweils angesprochenen Themenbereiche. Es gab teilweise sehr anregende Diskussionen. An alle Referenten ein herzlicher Dank

für die Zeit, die sie aufgewendet haben, um ihren Vortrag vorzubereiten und auf dem DOAG-Regionaltreffen zu präsentieren. Wenn Sie Themenwünsche haben, die Sie bei einem der nächsten Regio-Treffen behandelt sehen möchten sollten, dann schicken Sie bitte eine Mail an [regiomuenchen@doag.org](mailto:regiomuenchen@doag.org). Wir nehmen Ihre Anregungen gerne auf. Die Vorträge liegen auf dem DOAG-Server für Mitglieder bereit. Sie sind auch über die Referenten verfügbar.

**Kontakt:**

Franz Hüll  
 Andreas Ströbel  
[regio-muenchen@doag.org](mailto:regio-muenchen@doag.org)



*Ralf Kölling  
 DOAG-Vorstand und verantwortlich für IT- und Internet-Strategie*

**Die DOAG und Web 2.0**

**Herr Kölling, Sie sind im Vorstand für IT- und Internet-Strategie zuständig. Wie ist die DOAG im Web 2.0 unterwegs?**

Wir sind inzwischen in vielen sozialen Netzwerken aktiv. In Xing, LinkedIn und OracleMix gibt es jeweils DOAG-Gruppen, in denen sich unsere Mitglieder vernetzen können. Wir beginnen mit einem Blog und die DOAG twittert mittlerweile auch.

**Können Sie Näheres zum DOAG-Blog sagen?**

Vor Kurzem haben wir den DOAG Oracle Blog Aggregator DOBA ( <http://blog.doag.org/> ) aufgebaut. Ziel ist es, alle uns bekannten deutschsprachigen

Blogs mit Oracle-Bezug über eine Webseite erreichbar zu machen, wobei wir den Fokus auf techniklastige Blogs setzen.

**Gibt es auch eigene Beiträge?**

Bisher noch nicht; diese sind aber möglich und auch vorgesehen. Jeder, der gerne ab und zu Beiträge zur Oracle-Technologie veröffentlichen möchte, aber kein eigenes Blog betreibt, kann sich über eine E-Mail an [webmaster@doag.org](mailto:webmaster@doag.org) als Autor registrieren lassen und Beiträge veröffentlichen.

**Und was passiert bei Twitter?**

Bei Twitter ist die DOAG mit zwei Accounts vertreten. Unter dem Namen DOAGeV ( [www.twitter.com/doagev](http://www.twitter.com/doagev) ) werden Informationen über Termine sowie Neuigkeiten aus der DOAG und der Oracle-Welt veröffentlicht. Außerdem gibt es ab sofort aktuelle Informationen über die DOAG 2010 Konferenz ( [www.twitter.com/doagkonferenz](http://www.twitter.com/doagkonferenz) ), der größten deutschsprachigen Oracle-Anwenderkonferenz. Es ist geplant, während der Konferenz mit diesem User auch Echtzeit-Informationen über Änderungen im Konferenzprogramm und sonstige Ereignisse zu verbreiten.

**Wie kann man die DOAG-Beiträge am besten finden?**

Die DOAG kennzeichnet ihre Tweets mit sogenannten „Hashtags“, damit sie über die Twitter-Suchfunktion einfach zu finden sind. Wir benutzen bisher folgende Schlagworte:

- #doagev      Alle DOAG-relevanten Tweets
- #doagnews    Hinweise auf neue News-Artikel
- #doagtermin   Informationen über neue Termine
- #doag2010    Alle Tweets, die die DOAG Konferenz betreffen

**Kontakt:**

Ralf Kölling  
[ralf.koelling@doag.org](mailto:ralf.koelling@doag.org)

**Unsere Inserenten**

IDG Kommunikations Media AG <a href="http://www.idg.de">www.idg.de</a>	Seite 45
Neue Mediengesellschaft Ulm mbH <a href="http://www.databasepro.de">www.databasepro.de</a>	Seite 71
esentri consulting GmbH <a href="http://www.esentri.com">www.esentri.com</a>	Seite 53
exensio GmbH <a href="http://www.exensio.de">www.exensio.de</a>	Seite 17
Hunkler GmbH & Co. KG <a href="http://www.hunkler.de">www.hunkler.de</a>	Seite 3
Integrata Stiftung <a href="http://www.integrata-stiftung.de">www.integrata-stiftung.de</a>	Seite 73
Krug & Partner <a href="http://www.krug-und-partner.de">www.krug-und-partner.de</a>	Seite 49
Libelle AG <a href="http://www.libelle.com">www.libelle.com</a>	Seite 41
MT AG <a href="http://www.mt-ag.com">www.mt-ag.com</a>	Seite 35
MuniQsoft GmbH <a href="http://www.muniqsoft.de">www.muniqsoft.de</a>	Seite 21
OPITZ CONSULTING GmbH <a href="http://www.opitz-consulting.de">www.opitz-consulting.de</a>	U 2
ORACLE Deutschland GmbH <a href="http://www.oracle.com">www.oracle.com</a>	U 3
ORDIX AG <a href="http://www.ordix.de">www.ordix.de</a>	Seite 57
PROMATIS software GmbH <a href="http://www.promatis.de">www.promatis.de</a>	Seite 37
Retarus messaging services <a href="http://www.retarus.com">www.retarus.com</a>	Seite 11
Trivadis GmbH <a href="http://www.trivadis.com">www.trivadis.com</a>	U 4

## Wir begrüßen unsere neuen Mitglieder

### Firmenmitglieder

Matthias Klein, T-Systems International GmbH  
 Walter Hoff, T-Systems International GmbH  
 Martin Hoffmann, T-Systems International GmbH  
 Roland Schulte, T-Systems International GmbH  
 Hendrik Bergheim, DGUV  
 Rossen Rachev, DGUV  
 Jürgen Stobinski, AVANCIS GmbH & Co. KG  
 Dr. Jörg Baumbach, AVANCIS GmbH & Co. KG  
 Lars Volland, AVANCIS GmbH & Co. KG  
 Raymond J. Tuleweit, Quasar EDV-Informationsges. mbH  
 Sebastian Bolz, Immobilien Scout GmbH  
 Thorsten Becker, Immobilien Scout GmbH  
 Dierk Bachmann, Immobilien Scout GmbH  
 Linda Waldner, gkv informatik  
 Detlef Willmann, Kalorimeta AG & Co. KG  
 Harald Kelm, Kalorimeta AG & Co. KG  
 Holger Linge, Kalorimeta AG & Co. KG  
 Björn Soininen, AM GmbH  
 Raphael Steinmetz, motiondrive AG  
 Michael Arnold, motiondrive AG  
 Thomas Fachtan, motiondrive AG  
 Oliver Herges, HighValue IT Consulting GmbH  
 Jens Gogoll, HighValue IT Consulting GmbH  
 Frank Grabner, HighValue IT Consulting GmbH  
 Dr. Reinhold Thurner, Metasafe GmbH  
 Thomas Heine, Trivadis GmbH  
 Meik Truschkowski, Nobilia Werke Stickling GmbH & Co. KG  
 Fred Johannsen, Deutsche Bank AG  
 Andreas Lehberger, infoscore Forderungsmanagement GmbH  
 Uwe Höll, infoscore Forderungsmanagement GmbH  
 Andreas Schrempp, infoscore Forderungsmanagement GmbH  
 Stephan Pfeiffer, HOYER GmbH

### Persönliche Mitglieder

Markus Mandl  
 Dennis Honecker  
 Frank Christian Hoffmann  
 Frank Christian Herrmann  
 Tobias Bühlmann  
 Carlotta Schröder  
 Peter Sechser  
 Reza Morshedian  
 Romeo Pirelli  
 Markus Wingert  
 Sven Eversmeier  
 Klaus Bethke  
 Michael Rahms  
 Georg Egger

### Vorschau auf die nächste Ausgabe

Das Schwerpunkt-Thema der Ausgabe Q4/2010 lautet: **„Datenbank 11g R2“**

Gesucht sind Beiträge zu folgenden Themen:

- Vorstellung / Darstellung neuer 11g R2-Features
- Backup & Recovery, Best Practices, Erfahrungsberichte
- Performance-Tuning in 11g R2, Tipps und Tricks
- Installation und Migration auf 11g R2, Erfahrungsberichte oder Best Practices
- Datenbank 11g R2 und Grid Control 11g
- Datenbank Security und Compliance in 11g R2
- Cluster Infrastructure, Best Practices, Tipps und Tricks
- Hochverfügbarkeit (RAC, Data Guard) mit 11g R2
- Erfahrungsberichte mit Exadata
- Spezialthemen wie Spatial, Java in der Datenbank etc.

- Oracle VM und Datenbanken, Virtualisierung & Performance
- Configuration Manager und My Oracle Support

Darüber hinaus finden Sie wie in jeder Ausgabe:

- Fachartikel aus dem Bereich „Entwicklung“
- Best Practice im Umgang mit den Oracle-Produkten
- Aktuelle Informationen über Veranstaltungen der DOAG
- Neues von Oracle

Redaktionsschluss ist am **27. August 2010**

Die Ausgabe Q4/2010 erscheint am **29. Oktober 2010**



02.09.2010  
**SIG Database**  
 „Oracle Enterprise Manager“ 11gR1 Workshop  
 Michael Pfautz, Christian Trieb  
 sig-database@doag.org

07.09.2010  
**Regionaltreffen NRW**  
 Dierk Lenz, Stefan Kinnen, Hildgund von  
 Alten-Krämer  
 regio-nrw@doag.org

07.09.2010  
**Regionaltreffen Jena/Thüringen**  
 Jörg Hildebrandt  
 regio-thueringe@doag.org

08.09.2010  
**Regionaltreffen Berlin Brandenburg**  
 DataWarehousing  
 Michel Keemers  
 regio-bb@doag.org

09.09.2010  
**SIG Java**  
 Java Enterprise Edition 6 (JEE 6)  
 Andreas Badelt  
 sig-development@doag.org

09.09.2010  
**Regionaltreffen Dresden/Sachsen**  
 Kostenfreie Oracle-Produkte, Logging bei  
 Oracle und MySQL  
 Helmut Marten  
 regio-sachsen@doag.org

13.09.2010  
**Regionaltreffen Osnabrück/Bielefeld/  
 Münster**  
 Andreas Kother, Klaus Günther  
 regio-osnabrueck@doag.org

14.09.2010  
**SIG Oracle Spatial**  
 Tipps & Tricks zum Tuning von Spatial-Abfra-  
 gen in Oracle  
 Kushtrim Krasniqi  
 sig-spatial@doag.org

14.09.2010  
**SIG Fusion Middleware**  
 Perry Pakull  
 sig-middleware@doag.org  
 14.09.2010  
**Regionaltreffen Hamburg/Nord**  
 Stefan Thielebein  
 regio-nord@doag.org

15.09.2010  
**Workshop SIG Oracle Spatial**  
 APEX und Oracle MAPS Spatial  
 Kushtrim Krasniqi  
 sig-spatial@doag.org

15.09.2010  
**SIG Primavera: Gründungsveranstaltung**  
 Christian Körner, Sebastian Hunke  
 sig-primavera@doag.org

16.09.2010  
**SIG Security Datensicherheit**  
 Frank Stöcker  
 sig-security@doag.org

21.09.2010  
**Regionaltreffen Nürnberg/Franken**  
 Jürgen Häffner, Daniel Saraci  
 regio-franken@doag.org

22.09.2010 – 23.09.2010  
**DOAG Berliner Expertenseminare**  
 Oracle 11g Performance Forecast & Oracle  
 11g Performance Firefighting  
 mit Lutz Fröhlich  
 DOAG Geschäftsstelle  
 office@doag.org

27.09.2010  
**SIG E-Business Suite in Cooperation  
 mit OAG**  
 Back to Growth - Are your Oracle Applications  
 Ready for Takeoff?  
 Frank Schönthaler  
 sig-ebusiness@doag.org

27.09.2010  
**Regio München/Südbayern**  
 Franz Hüll, Andreas Ströbel  
 regio-muenchen@doag.org



04.10.2010 - 05.10.2010  
**DOAG Berliner Expertenseminare**  
 Oracle – sichere Planung und sichere Imple-  
 mentierung kritischer Oracle-Umgebungen  
 mit Dierk Lenz und Günter Unbescheid  
 DOAG Geschäftsstelle  
 office@doag.org

05.10.2010  
**Regionaltreffen Bremen**  
 Ralf Kölling  
 regio-bremen@doag.org

12.10.2010  
**SIG BPM**  
 BPM - Matchwinner für Software-Projekte  
 Sebastian Graf  
 sig-bpm@doag.org

12.10.2010  
**SIG Database**  
 Real Application  
 Michael Pfautz, Christian Trieb  
 sig-database@doag.org

13.10.2010 - 14.10.2010  
**DOAG Berliner Expertenseminare**  
 Advanced APEX I & Advanced APEX II  
 mit Marco Patzwahl  
 DOAG Geschäftsstelle  
 office@doag.org

14.10.2010  
**Regionaltreffen Stuttgart**  
 Jens-Uwe Petersen  
 regio-stuttgart@doag.org

20.10.2010  
**SIG SOA**  
 Fokus auf Integration. Alles rund um SOA,  
 SOA Suite, AIA, Testing  
 Torsten Winterberg, Hajo Normann  
 sig-soa@doag.org

26.10.2010  
**Regionaltreffen Hamburg/Nord**  
 Stefan Thielebein  
 regio-nord@doag.org

26.10.2010  
**Regionaltreffen Freiburg/Südbaden**  
 Andreas Flubacher  
 regio-freiburg@doag.org

27.10.2010  
**Regionaltreffen NRW**  
 Dierk Lenz, Stefan Kinnen, Hildgund von  
 Alten-Krämer  
 regio-nrw@doag.org

29.10.2010  
**SIG JD Edwards**  
 Kasi Färcher-Haag  
 sig-jde@doag.org

29.10.2010  
**SIG CRM**  
 Detlef Kubusch  
 sig-crm@doag.org



16.11.2010 - 18.11.2010  
**DOAG 2010 Konferenz + Ausstellung**  
 23. Deutsche ORACLE-Anwenderkonferenz  
 office@doag.org

Weitere, aktuelle Informationen finden Sie  
 unter [www.doag.org/termine](http://www.doag.org/termine)