Hochverfügbarkeit und K-Fall-Absicherung mit Engineered Systems

Hartmut Streppel, Andris Perkons
Oracle Deutschland B.V. & Co. KG
München, Düsseldorf

Schlüsselworte
Hochverfügbarkeit, Disaster Recovery, Engineered Systems, Stretched Cluster, K-Fall-Absicherung

Einleitung
Der Alptraum eines jeden RZ-Verantwortlichen ist, dass eine Katastrophe Teile des RZs lahmlegt. Eine solche Katastrophe könnte auch „nur“ eine Datenkorruption in einer unternehmenskritischen Datenbank sein. Der Traum dieser RZ-Verantwortlichen ist, dass auf Knopfdruck Katastrophen überwunden werden und komplette Anwendungs-Stacks den Anwendern innerhalb kürzester Zeit und ohne Datenverlust wieder zur Verfügung gestellt werden. Wie solche Szenarien im Zusammenhang mit Oracles Engineered Systems, speziell mit dem SPARC SuperCluster T4-4 aussehen, soll dieser Beitrag beschreiben.

Hochverfügbarkeit (HA) und K-Fall-Absicherung (DR) mit Oracles Engineered Systems

Unsere Beobachtungen in den letzten Jahren haben gezeigt, dass typische Deployments von unternehmenskritischen Anwendungen in Deutschland (und Nordeuropa) anders als in anderen Teilen der Welt betrieben werden: als Metro-Cluster über mehrere Rechenzentren verteilt, auch Campus- oder „stretched“ Cluster genannt. In anderen Teilen der Welt werden eher lokale Cluster in Verbindung mit DR-Lösungen genutzt, die dann in entfernten RZs betrieben werden.

Ein HA- und DR-Konzept auf der Basis von Oracles Engineered System entspricht den Lösungen in anderen Teilen der Welt, aber nicht dem typischen, deutschen Deployment. Diese konzeptionellen Unterschiede führen immer wieder zu heftigen Diskussionen über den wahren Weg zu einer sehr hohen Verfügbarkeit und einer möglichst abgesetzten Disaster Recovery Lösung.

Traditionell werden in Deutschland Hochverfügbarkeitslösungen als sog. Metro- - oder stretched – Cluster implementiert, bei denen die redundanten Komponenten auf getrennte Rechenzentren oder Brandabschnitte verteilt werden. Damit soll neben den typischen Einzelfehlern (z.B. Rechnerausfall) auch der Ausfall eines kompletten RZs abgesichert werden, was oft als der typische und wahrscheinlichste Fall einer Katastrophe betrachtet wird.

Dabei werden allerdings drei Dinge verkannt:

a) Datenkorruption, die nur durch ein Zurückspielen von Backup-Bändern wieder behoben werden kann, ist sicherlich eine größere Katastrophe als ein RZ-Ausfall. Bei den heutigen Datenmengen werden dabei sicherlich alle in den SLAs gültigen Unterbrechungszeiten überschritten.

b) ein RZ-Ausfall wird nur dann sicher von einer Hochverfügbarkeitssoftware als solcher erkannt, wenn er tatsächlich einfach ist, d.h. z.B. durch einen kompletten Stromausfall verursacht wurde. Tritt dagegen eine wirkliche Katastrophe ein, z.B. durch einen Wassereinbruch an mehreren Stellen, der sukzessive unterschiedliche Komponenten des RZ lahmlegt, ist fraglich, ob dies per Software eindeutig diagnostiziert und darauf richtig und schnell reagiert werden kann.

c) RZ-Ausfälle sind gar nicht so wahrscheinlich (außer dort, wo man weiß, dass die Stromversorgung sehr instabil ist), und Datenkorruption (s.o) oder fehlgeschlagene Patchaktionen, die zu nicht mehr startbaren Clustern führen, sind wahrscheinlicher als der angenommene Totalausfall eines RZ.

Für solche Fehlerfälle hilft nur eine Disaster Recovery Umgebung, die als weitestgehend unabhängige Konfiguration aufgesetzt und betrieben wird. Unabhängig heißt, dass weder Netz, noch SAN noch Cluster mit der ausgefallenen Umgebung geteilt werden. Und es ist ein Mechanismus notwendig, der automatisch alle notwendigen Aktionen durchführt, um ein ausgefallenes System den Kunden wieder zur Verfügung zu stellen. Dies bedeutet aber nicht, dass dieser Mechanismus auch automatisch ausgelöst wird. Es ist allgemeine Überzeugung, dass in K-Fällen durch einen wohldefinierten Entscheidungsprozess weitere Aktionen angestoßen werden.

Hochverfügbarkeit und Disaster Recovery mit dem SPARC SuperCluster T4-4

Engineered Systems (ES) von Oracle, z.B. Exadata und SPARC SuperCluster sind hoch integrierte Systeme, die Server, Storage und Netzinfrastruktur in einem Rack enthalten. Typische Einzelfehler werden durch Redundanz in der Hardwarekonfiguration und Hochverfügbarkeitsmechanismen in der Software maskiert. In der Regel werden Anwendungen und Verbindungen zu Client-Systemen durch solche Fehler nicht beeinträchtigt. Im Folgenden werden wir uns ausschließlich dem SPARC SuperCluster T4-4 (SSC) widmen.

Um Vorsorge zu treffen gegen Katastrophen, wird eine zusätzliche, möglichst getrennte Umgebung benötigt, die im K-Fall aktiviert werden kann – möglichst schnell und möglichst ohne Datenverlust. Die Trennung von lokaler Hochverfügbarkeit und Disaster Recovery über RZ-Grenzen hinweg entspricht der Maximum Availability Architecture (MAA), die Oracles Blaupause für diese Themen ist. (http://www.oracle.com/technetwork/database/features/availability/maa-096107.html)

Für beide Fälle, Hochverfügbarkeit und DR, stehen bewährte Produkte zur Verfügung:

- Hochverfügbarkeit in einem SPARC SuperCluster u.a. Oracle Clusterware für das DB-Layer und Oracle Solaris Cluster für die Anwendungsdomains

- Disaster Recovery mittels Oracle Data Guard für die Datenbank und Oracle Solaris Cluster Geographic Edition für Anwendungen und Daten, die nicht in der Datenbank liegen.

Beide Cluster-Produkte überwachen ihre Anwendungen und reagieren bei typischen Einzelfehlern mit entsprechenden korrigierenden Aktionen, um die Anwendung am Leben zu erhalten.

Bei Doppelfehlern, z.B. totaler Stromausfall oder Ausfall mehrerer Serversysteme, müssen alle Komponenten eines Anwendungsstacks auf ein zweites SSC, das typischerweise in einem entfernten RZ steht, geschwenkt werden. Hierzu stehen zum einen Oracle Data Guard zur Verfügung, um Redo-Daten von der produktiven Datenbank zu einer Schattendatenbank im entfernten SSC zu transportieren. Dieser Transport kann auf unterschiedliche Art konfiguriert werden, um den Sicherheits- und Performance-Anforderungen der Anwendung gerecht zu werden. Ist die Entfernung zwischen den beiden RZs zu groß, wird typischerweise eine asynchrone Replikation konfiguriert. Mit entsprechendem Aufwand, z.B. mehrere „Zwischen-“Standorte, zu denen zunächst synchron repliziert werden kann, kann eine erhebliche Verringerung des für asynchrone Replikation typischen Risikos erreicht werden.

Zum anderen wird die Oracle Solaris Cluster (OSC) Geographic Edition genutzt, um sog. Protection Groups, d.h. Cluster Ressourcegruppen mitsamt ihrer replizierten Daten zwischen Clustern in den beiden RZs zu schwenken. Die OSC Geographic Edition ist in der Lage, Oracle Solaris Cluster

Ressource Gruppen zu überwachen, zu schwenken, zu starten und zu stoppen, aber auch die dazugehörigen Datenreplikation, z.B. zwischen zwei ZFS Storage Appliances zu überwachen, aber auch zu schwenken. Diese Integration verschiedenster Technologien, von der IP-Adresse über Zpools und Anwendungskomponenten bis hin zur Datenreplikation, nimmt gerade in Stresssituationen, z.B. während der „Bekämpfung“ einer Katastrophe, die Bürde der Beherrschung der Komplexität eines Schwenks vom verantwortlichen Administrator.

Ein Proof of Concept mit SPARC SuperCluster T4-4

Marketingaussagen sind schön, Produktdokumentation ist besser, ein Proof of Concept ist am besten. Also versuchten wir, ein komplexes Setup aus zwei SSCs mit mehreren Domains und den oben genannten Produkten aufzubauen und verschiedene Fehlerfälle durchzuspielen. Wir entschieden uns, eine Architektur aus zwei Engineered Systems durch eine funktional sehr ähnliche mit zwei kleinen T4 Systemen nachzubauen. Hierbei bildeten 4 Domains innerhalb eines T4 Systems je zwei Domains in unterschiedlichen Servern eines SSC ab. Jeweils 2 Domains, die in einem echten SSC in verschiedenen Servern konfiguriert würden, wurden geclustert, um einmal Oracle RAC zu implementieren und ein anderes Mal hochverfügbare SAP Central Services mit dem HA Netweaver Agenten für Oracle Solaris Cluster. Die Konfiguration, die wir damit abbildeten, entspricht funktional zwei Knoten in einem SSC wie in Abb. 1 dargestellt. Node 1 und Node 2 wären Bestandteil eines SSC.

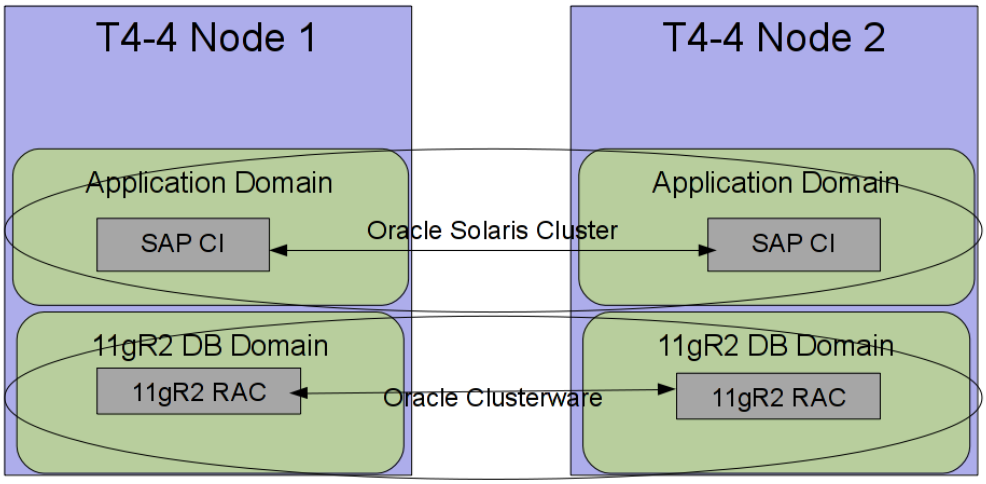

Abb. 1: SSC Setup mit Oracle RAC und HA Netweaver Agenten für Oracle Solaris Cluster

Hochverfügbarkeit innerhalb eines SSC

Innerhalb eines SSC garantiert die voll redundante Hardware-Architektur in Verbindung mit der eingesetzten Cluster-Software, dass alle typischen Einzelfehler schnell und sicher abgefedert werden – mit nur minimalem Einfluss auf die Anwendungen und ihre Verbindungen zu externen Client-Systemen. Nicht-typische Einzelfehler sind z.B. Datenkorruption, administrative Fehler mit schweren Folgen, logische Datenbankfehler, nicht bootbare Cluster und Probleme mit Softwareversionen, die identisch auf allen entsprechenden Komponenten eines Systems eingespielt sind, z.B. Platten-Firmware. Bei all diesen Fehlern hilft ein lokales Cluster nur bedingt weiter.

Bei logischen Fehlern kann u.U. mittels Flashback Technologie auf eine Version der Daten zurückgesprungen werden, in der der Fehler noch nicht aufgetreten war.

In den anderen Fällen und natürlich auch bei Doppelfehlern muss eine Katastrophe festgestellt und entsprechende Recovery Maßnahmen müssen eingeleitet werden.

Es ist offensichtlich, dass in all den genannten Fällen ein Metrocluster keine zusätzliche Sicherheit bieten würde. Ein entferntes zweites System mit aktuellen Daten, auf das schnell und sicher umgeschaltet werden kann, sorgt dafür, dass all diese Fehlersituationen überstanden werden können.

Disaster Recovery Lösung zwischen SSCs in unterschiedlichen Rechenzentren

Um eine weitestgehende Trennung der DR Umgebung von der Produktionsumgebung zu erreichen, ist es sinnvoll, nur IP-Verbindungen zwischen den Systemen zu nutzen. Kein gemeinsames SAN, keine gekoppelten Netze, keine Cluster über große Entfernungen. Man kann sogar noch weiter gehen und fordern, dass andere Software-Versionen am DR-Standort eingesetzt werden sollten oder sogar andere Technologien. Es hat Fälle gegeben, in denen identische und fehlerhafte Firmware Versionen an mehreren Standorten zu zeitgleichen Ausfällen aller Komponenten führte, die mit dieser Version betrieben wurden und somit trotz angenommener Redundanz ein Totalausfall die Folge war.

Oracle Data Guard repliziert Redo-Daten über IP, und auch die meisten storage-basierten Replikationstechnologien unterstützen dies, z.B. die Replikation der ZFSSA. Ob mit Data Guard synchron oder asynchron repliziert wird, ist zunächst einmal eine Entscheidung, die auf der Basis des Redo-Aufkommens und der Latenz zwischen den RZs getroffen wird. Sollte nur eine asynchrone Replikation möglich sein, um die geforderte Performance der DB zu gewährleisten, kann durch geeignete zusätzliche Komponenten (mehrere lokale Schattendatenbanken) das Risiko gesenkt werden, dass es bei einer Katastrophe zu Datenverlust kommt.

Die ZFSSA unterstützt nur asynchrone Replikation, d.h. darf es auch bei den auf der ZFSSA gespeicherten Daten im schlimmsten Fehlerfall keinen Datenverlust geben, sollten die Daten in der – hoffentlich – synchron replizierten Datenbank abgelegt werden.

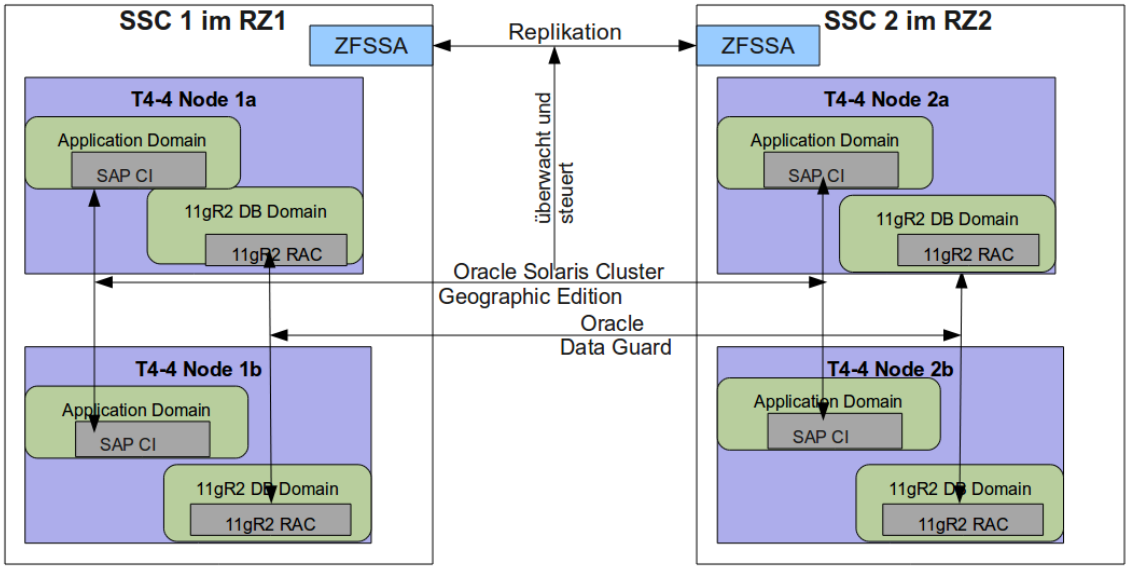

Abb. 2: Disaster Recovery Konfiguration zwischen zwei SSC mit Oracle Data Guard und Oracle Solaris Cluster Geographic Edition

Mit Hilfe der OSC Geographic Edition wird die Cluster Ressource Gruppe, die die SAP SCS Ressourcen enthält, zusammen mit einer ZFSSA „replication component“ in eine sog. Protection

Group zusammengefasst. Diese Protection Group ist die Einheit, die nun zwischen RZs und zwischen Clustern geschwenkt werden kann. Dabei sorgen die Automatismen der OSC Geographic Edition dafür, dass

- eine solche Protection Group zu jedem Zeitpunkt nur auf einem der beiden Cluster aktiv ist
- die Cluster Ressourcegruppe auf den richtigen Knoten gestoppt, bzw. gestartet wird
- die Cluster überwacht und bei Fehlern Alarme ausgelöst werden und
- bei einem Schwenk die Replikationsrichtung der ZFSSA umgekehrt wird.

Der wesentliche Vorteil dieser Lösung ist, dass alle diese Schritte automatisiert ablaufen, und ein Administrator nur(!) den – imaginären – roten Knopf drücken muss, damit ein Schwenk ausgelöst wird. Wie bei K-Fall-Lösungen Standard, wird ein Schwenk nicht automatisch ausgelöst, sondern muss manuell, nach einem Entscheidungsprozess, ausgelöst werden.

Orchestrierung des Switchovers zwischen RZs

Der Traum der RZ-Leitung ist sicherlich, im K-Fall eine vollautomatische Übernahme kompletter Anwendungsstacks zu erreichen. Das ist aus mehreren Gründen unrealistisch:

- eine vollständige Business Continuity Lösung umfasst eine Menge nichttechnischer Systeme und Abläufe und kann nicht automatisiert werden
- bestimmte Subsysteme, z.B. das Netzwerk, besitzen ihre eigenen Disaster Recovery Mechanismen, die nur sehr schwer in einen Automatismus integriert werden können
- die für einen kompletten Anwendungsstack verwendete SW ist in der Regel so heterogen, dass es keine Software gibt, die alle Aspekte berücksichtigen könnte.

Aber es ist schon viel gewonnen, wenn die Anwendungs-Ebenen, die auf einer oder zumindest identischen Plattformen laufen, einheitlich und zusammenhängend geschwenkt werden können.

In dem hier beschriebenen POC soll also nun durch ein Kommando sowohl die DB als auch die Protection Group für die SAP SCS geschwenkt werden. Ein einfaches Shellskript, dessen entscheidende drei Zeilen die folgenden sind:

```
ssh $SAPCI_runs_on /usr/cluster/bin/geopg switchover -f \
               -m "$SAPCI_target_primary" "$SAP_PG" &
su - oracle -c "dgmgrl sys/<passw>@$DB_TARGET_PRIMARY\
               \"switchover to $DB_TARGET_PRIMARY\""
ssh $DB_SECONDARY_HOST /usr/tmp/do_start.sh
```

schwenkt zunächst im Hintergrund die Protection Group, führt dann im Vordergrund mit Hilfe des Data Guard Brokers den Rollentausch der DB aus, um zuletzt die ehemals primäre DB mit Hilfe eines lokalen Skripts neu zu starten. Natürlich muss das vollständige Skript die richtigen Namen evaluieren, Variable setzen, parametrisiert werden, um z.B. einen pro-aktiven Switch, bei dem die aktive Umgebung sauber gestoppt wird, von einem reaktiven, bei dem die ehemals aktive Seite mehr oder weniger ignoriert wird, zu unterscheiden. Und zuletzt muss das Skript auch noch eine umfassende Fehlerbehandlung implementieren.

Um ein Gefühl für die Dauer solcher Schwenkoperationen zu bekommen, haben wir mehrere Fehlersituationen simuliert und dann die Zeiten gemessen, die bis zur Erreichbarkeit der DB und der

SAP SCS vergingen. Alle Tests wurden ohne Last durchgeführt, da wir zunächst einmal die Funktionalität des Ansatzes nachweisen wollten. Alle kombinierten Schwenks zwischen den Clustern in den beiden RZs waren in weniger als einer Minute vollständig durchgeführt.

Auswirkungen auf den kompletten Anwendungsstack

Interessant ist aber nicht nur die Zeit, bis eine Anwendung nach einem Fehler wieder verfügbar ist, sondern auch, welche Auswirkungen ein Schwenk auf andere Layer der Anwendung hat. In unserem Beispiel laufen nur die Datenbank und die SAP SCS auf den von uns betrachteten SPARC SuperCluster Systemen. SAP Application Server und die Benutzerschnittstelle sapgui laufen auf anderen Systemen. Die Kommunikation zwischen den einzelnen Systemen ist in Abb. 3 dargestellt.

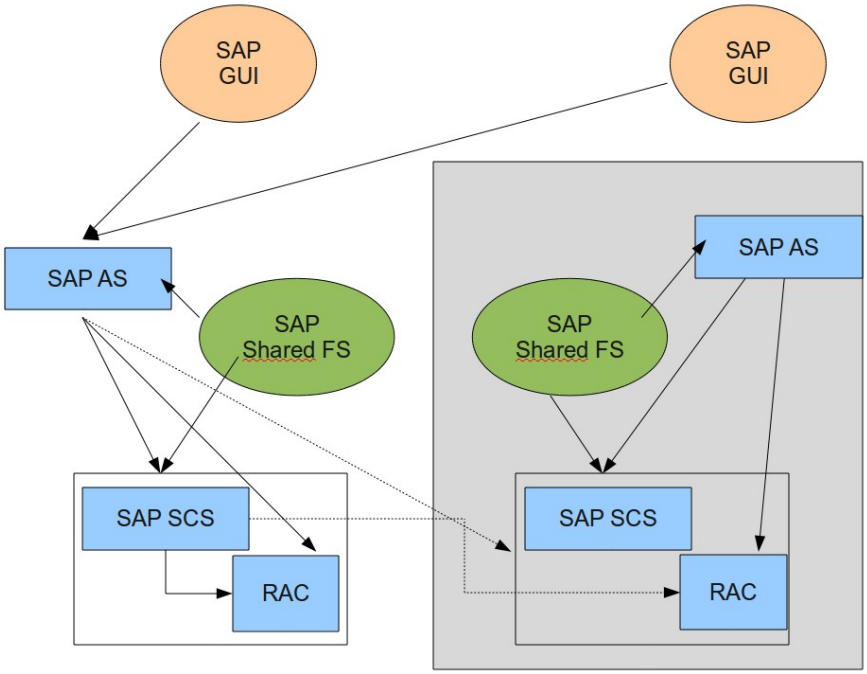

Abb. 3: Kommunikationsbeziehungen eines SAP Stacks

Die interessanten Fragen sind also:

- führt ein lokaler Schwenk der SAP SCS innerhalb eines Clusters zu einer merkbaren Unterbrechung bei der Arbeit mit der SAP GUI?
- Führt der Ausfall eines DB-Knoten, der eine RAC-Instanz beherbergt, zu einer merkbaren Unterbrechung bei der Arbeit mit dem SAP Application Server? Muss am Application Server manuell eingegriffen werden?
- Führt ein Schwenk der Datenbank auf das Ausweichsystem zu einer merkbaren Unterbrechung?
- Was sind die Folgen eines Schwenks der SAP shared Dateisysteme auf das Replikationssystem?

Zusammenfassend kann gesagt werden, dass die meisten Fehlersituationen keinerlei oder nur sehr kurze Auswirkungen auf das Gesamtsystem haben. Kritisch wird es immer dann, wenn sich IP-

Adressen von Diensten ändern. Dies kann z.B. dann notwendig sein, wenn im Ausweich-RZ ein separates IP-Netz betrieben wird.

Zusammenfassung

Unsere Tests haben gezeigt, dass mit bewährten Standard-Technologien wie Oracle Data Guard und Oracle Solaris Cluster Geographic Edition komplette und komplexe Anwendungsstacks, die innerhalb eines SPARC SuperClusters laufen, sicher und schnell auf ein anderes SSC in einem Ausweich-RZ geschwenkt werden können. Die Umschaltzeiten sind so kurz, dass die durch sie bedingten Serviceunterbrechungszeiten kein Grund sein dürften, auch für bestimmte administrative Aufgaben an Produktionssystemen keinen Schwenk eines kompletten Stacks durchzuführen.
Für die Weiterführung unternehmenskritischer Aufgaben im K-Fall sind diese Technologien erste Wahl.

Kontaktadressen:

Hartmut Streppel
ORACLE Deutschland B.V. & Co. KG
Riesstrasse 25
D-80992 München

Telefon: +49 (0) 89-1430-2588
E-Mail Hartmut.Streppel@oracle.com
Internet: www.oracle.com

Andris Perkons
ORACLE Deutschland B.V. & Co. KG
Hamborner Straße 51
D-40472 Düsseldorf

Telefon: +49 (0) 211-74839 -791
E-Mail Andris.Perkons@oracle.com
Internet: www.oracle.com