

E-Commerce-Anwendungen bilden heute in vielen Unternehmen wichtige Business-Prozesse ab und tragen wesentlich zum Unternehmenserfolg bei. So sind zum Beispiel Online-Handel, Online-Banking oder die unkomplizierte Informationsgewinnung im Zeitalter des Internets nicht mehr wegzudenken.

End-to-End-Monitoring für E-Commerce-Anwendungen mit dem Oracle Enterprise Manager 12c

Jens Zwer, ORACLE Deutschland B.V. & Co. KG

Oracle kann mit dem Produkt Real User Experience Insight (RUEI) in Echtzeit die Verfügbarkeit und Antwortzeiten aller Anwender und deren Transaktionen monitoren und „end-to-end“ analysieren (siehe Abbildung 1). Mit RUEI ist es möglich, ein aktives und ein passives Monitoring aufzubauen:

Aktives Monitoring

Hier werden bestimmte kritische Transaktionen definiert und diese dann durch einen PC oder Server in zeitlich definierten Intervallen ausgeführt. Dadurch sind ein „24*7“-Monitoring und historische Performance-Analysen möglich. Ein Nachteil dieser Mess-Methodik ist die Überwachung von schrei-

benden Transaktionen wie Kaufen und Bezahlen eines Produkts oder die Veränderung von Datensätzen, da in einem produktiven System gemessen wird und somit diese Art von Transaktionen gar nicht oder nur mit erhöhtem Aufwand (Dummy Accounts) überwacht werden können.

Passives Monitoring

Hier fungiert RUEI als klassischer Netzwerk-Sniffer. Ein oder mehrere RUEI-Server werden vor den Web-Servern implementiert und verarbeiten „real-time“ den ein- und ausgehenden Web-Traffic. Durch diesen Mess-Ansatz ist man in der Lage, die wirkliche Enduser-Performance inklusive Netzwerk-Anteil

zu ermitteln, egal wo in der Welt der User tätig ist, da zu jeder Transaktion ebenfalls die aktuelle Netzwerk-Bandbreite bekannt ist. Da nur der kopierte Datenstrom verarbeitet wird, entsteht kein zusätzlicher Overhead für das System. Ebenfalls sind keine Änderungen an den zu überwachenden Anwendungen nötig, wodurch eine sehr schnelle Implementierung innerhalb weniger Tage möglich ist. SSL-geschützter Traffic lässt sich auch überwachen, ohne dabei den Datenschutz zu umgehen, da alle schützenswerten Daten mittels der sogenannten „Binding-Funktion“ nicht aufgezeichnet werden. Aus diesem Grund ist RUEI auch bei Online-Händlern, Online-Banken oder Tele-

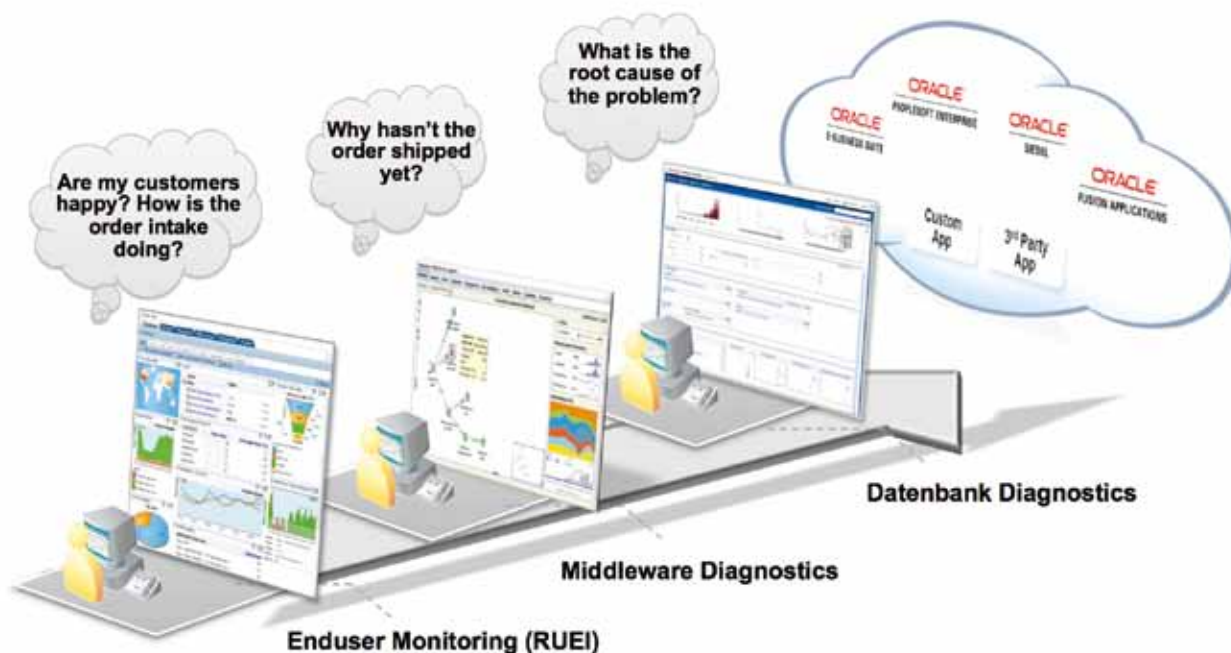


Abbildung 1: Überblick Oracle End-to-End-Monitoring

kommunikations-Unternehmen im Einsatz.

Daraus ergeben sich folgende Vorteile:

- **End-to-End-Performance-Monitoring vom End-User bis zur Datenbank**
Durch die direkte Integration von RUEI mit weiteren Monitoring-Plug-ins wie Java-, Business-Transaction- und Datenbank-Diagnostic kann in kürzester Zeit die Ursache für Performance-Probleme analysiert werden (siehe Abbildung 2).
- **Plattformunabhängiger Einsatz für alle webbasierten Anwendungen**
Da die Mess-Methodik auf dem Netzwerk-Level aufsetzt, lassen sich alle webbasierten Anwendungen überwachen. Die eingesetzte Hardware, Infrastruktur, Middleware oder Datenbank spielen dabei keine Rolle, sodass ein plattformunabhängiger Einsatz möglich ist. Neben sämtlichen Web-Anwendungen gibt es speziellen Support für Oracle-Anwendungen wie Siebel, Peoplesoft, E-Business Suite, iFlex, Fusion Applications oder auf Basis von Forms und ADF entwickelte Applikationen.
- **Priorisierung und Eingrenzung von Problemen**

Da sämtliche User und alle Transaktionen in Realtime überwacht werden, lassen sich auftretende Probleme sofort lokalisieren und priorisieren, etwa nach Anzahl der betroffenen User, Wichtigkeit der Applikation oder kritischen Business-Transaktionen. Zusätzlich ist sofort erkennbar, ob die Probleme in der Anwendung selbst oder in der zugrunde liegenden Infrastruktur begründet sind.

- **Informationsgewinnung für alle IT- und Unternehmens-Bereiche**
Der typische Einsatz dieser Monitoring-Lösung obliegt der IT-Abteilung und ist insbesondere für Mitarbeiter im Helpdesk, Support, Entwicklung, Qualitätssicherung und operativen Betrieb gedacht. Darüber hinaus werden aber auch sehr wichtige Kennzahlen und Informationen über den End-User für die Bereiche „Marketing“ und „Vertrieb“ geliefert. So können beispielsweise abgebrochene Transaktionen oder funktionale Fehler getrackt werden, um mögliche Umsatz-Einbußen frühzeitig zu erkennen und entgegenwirken zu können.
- **Datenschutz und Compliance-Überwachung**

Da sämtliche User, Transaktionen und Anfragen an die Anwendung überwacht werden, sind Hackerangriffe (Botnet-/Fraud-Attacken) oder ungewöhnliche, atypische Anfragen von Robotern oder nicht zugriffsberechtigten IP-Adressen identifizierbar. In diesem Fall sind sofort Gegenmaßnahmen möglich, um die Daten und das System zu schützen.

Die Architektur

Für die Anwendung einer Netzwerk-Protokoll-Analyse (NPA) ist ein nicht-invasiver Architektur-Ansatz erforderlich. Der Vorteil besteht darin, dass es keine Performance-Auswirkungen auf die Anwendung gibt und die Anwendungs-Architektur nicht verändert werden muss. Auch bei Updates beziehungsweise Upgrades der Anwendung kommt es zu keiner Änderung, die eine Rückwirkung auf das implementierte Anwendungs-System hat.

Die Basis-Architektur von RUEI besteht aus drei Kern-Komponenten:

- **Data Collection**
Die Sammlung von Monitoring-Daten aus dem Netzwerk. Hierbei kommen zwei Verfahren zum Einsatz, die Verwendung eines Switch-Spiegel-Ports oder eines Test Access Points (TAP). Ein Netzwerk-TAP dient dazu, den Datenverkehr eines Netzwerks zu Analyse-Zwecken auszulesen. Es hat normalerweise mindestens drei Ports – A und B für die Netzwerk-Anschlüsse und einen Monitoring-Port. Für die Sammlung von Monitoring-Informationen wird grundsätzlich ein TAP empfohlen, da dieser auch bei einer hohen Netzwerk-Auslastung zuverlässig alle Netzwerk-Daten ausliest. Bei der Verwendung eines Switch-Spiegel-Ports kann es passieren, dass bei hoher Auslastung des Switch nicht alle durchlaufenden Daten an den Port weitergegeben werden.
- **Data Processing**
Diese Komponente verarbeitet die „Roh“-Daten der Netzwerk-Informationen zu auswertbaren OLAP-Daten. Die so gewonnenen Daten werden nach der Verarbeitung persistent in einer Oracle-Datenbank gespeichert.



Abbildung 2: Frei konfigurierbares RUEI-Dashboard mit Realtime-Daten

Da bei der Netzwerk-Protokoll-Analyse sehr viele Daten verarbeitet und auch (zwischen-)gespeichert werden müssen, ist das Vorhalten von ausreichendem Speicherplatz im Disk-System und der Datenbank Voraussetzung. Für das Disk-System wird ein Minimum von 400 GB HDD empfohlen. Die Dimensionierung der Datenbank ist abhängig von der Art der Daten und der Aufbewahrungsdauer. Die Art der Daten beschreibt die Unterscheidung zwischen Zugriffsinformationen und detaillierten Informationen über Fehler (wie ein HTTP xxx Fehler). Als Richtwert für Konfigurations-Informationen und gespeicherte Netzwerk-Informationen kann ebenfalls eine Datenbank-Größe von 400 GB geplant werden. Da das Speichern von Netzwerk-Daten auf der Festplatte einen gewissen Daten-Durchsatz voraussetzt (mindestens 70 MB/s), ist von der Verwendung eines NFS-Device dringend abgeraten.

- **Data Presentation**

Die Präsentations-Schicht wird für die Analyse und das Reporting der gewonnenen Informationen verwendet. Der Zugriff auf diese Daten ist browserbasiert und kann somit unabhängig von jedem Arbeitsplatz erfolgen, der Web-Zugriff auf den Reporting-Server hat. Die angezeigten Informationen geben Aufschluss über die technischen Abläufe der Applikation wie Durchlaufzeiten, Antwortzeiten, Fehler, SLAs etc. Hinzu kommen auch fachliche Informationen wie regionale Zuweisung der Anfragen, Unterteilung der Anfragen in Informationen, Kauf-Entscheidung etc. Die gewonnenen Daten lassen sich im RUEI-System bis zur Retention-Periode aufbewahren oder in ein externes System zur Analyse exportieren. Eine weitere Funktion ist das Reporting der Informationen. Die enthaltenen Daten werden aufbereitet und den interessierten Abteilungen bereitgestellt.

Im Grunde ist dies der klassische Ansatz einer Monitoring-Lösung. Die verwendeten Komponenten sind in die drei Installations-Teilprodukte „Collector“, „Processing Engine“ und „Reporter“ aufgeteilt. Der Collector sammelt den Netzwerk-Verkehr und überträgt ihn an den Reporter. Dieser ist in der Lage, die Daten von mehreren Collectors zu verarbeiten. Der Reporter verarbeitet die empfangenen Daten und speichert diese in einer Oracle-Datenbank. Zusätzliche Informationen wie KPIs, SLAs, Umgebungs-Informationen etc. sind in der Konfigurations-Datenbank gespeichert. Die Processing Engine ist eine optionale Einheit, um in einer hochausgelasteten Umgebung den Reporter zu entlasten. Sie besitzt eine eigene lokale Datenbank, in der die aktuell verarbeiteten Daten zwischengespeichert sind. Nach deren Verarbeitung werden sie an den Reporter übertragen. Die Processing Engine hat damit die Funktion einer Skalierungseinheit.



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

- **Application Server Systeme**

JDeveloper Forms & Reports
PL/SQL (CMSDK, OEM, Disco...) u.v.m.

- **Projekte**

Gewerblicher Rechtsschutz (IP)
Automotive Medien- & Energiewirtschaft

- **Lizenzierung**

Beratung & Analyse des Lizenzstatus
Lizenzierung



Krug & Partner GmbH ◦ Treitschkestr. 3 ◦ D-69115 Heidelberg
Telefon: +49 (0) 62 21/60 79 0 ◦ Telefax: +49 (0) 62 21/60 79 60

E-Mail: info@krug-und-partner.de
www.krug-und-partner.de



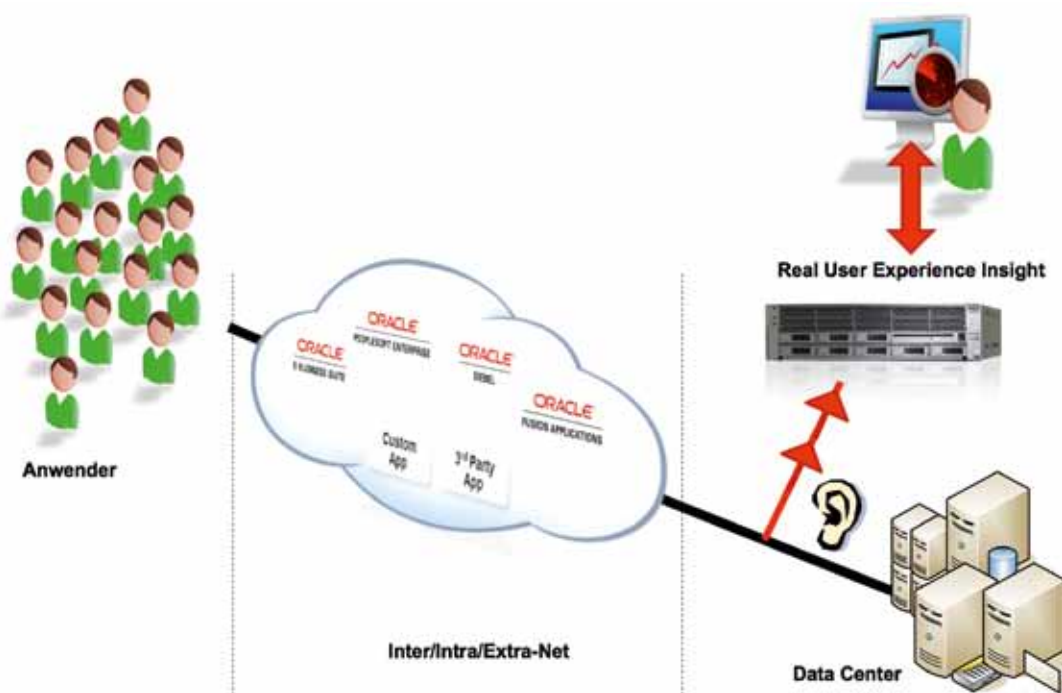


Abbildung 3: Passives Monitoring durch dedizierten Mess-Server

Bezogen auf die drei genannten Komponenten kann die geplante Architektur je nach Skalierbarkeits-Anforderungen unterschiedlich implementiert sein. Es existieren folgende drei Basis-Best-Practice-Implementierungen:

- **Single Server**
Bei geringem und mittlerem Netzwerk-Verkehr ist diese Implementierungsart empfohlen. Collector, Reporter und Data Processing werden auf einer Box installiert. Die verwendete(n) Datenbank(en) für Konfigurations- und Monitoring-Daten können auch auf dieser Box installiert sein. Es wird jedoch empfohlen, für die Datenbank einen separaten Server zu verwenden, da der I/O des verwendeten Servers ansonsten zu groß wird und das System nicht alle Netzwerk-Daten verarbeiten kann.
- **Multiple Collector**
Diese Implementierungsart ist für einen höheren Netzwerk-Verkehr (siehe Abbildung 3). Dabei sind die Komponenten zwar auf einer Box installiert, bekommen jedoch aus anderen Systemen zusätzliche Rohdaten von externen Collectors geliefert. Der Vorteil sind die Möglichkeiten,

ein verbessertes Security-System zu implementieren. Durch die Verwendung mehrerer Collectors können diese auch außerhalb des Reporter-Netzwerks implementiert sein. Somit bleibt das Kernsystem innerhalb der sicheren Zone und die Reporter können in „unsicheren“ Netzwerken Monitoring-Daten sammeln.

- **Drei Tier**
Bei sehr hohem Netzwerkverkehr ist diese Implementierungsart zu empfehlen. Die Trennung der Komponenten auf separate Hardware ermöglicht eine praktisch unbegrenzte Skalierung. In dieser Architektur kann es zu einer beliebigen Kombination in der Anzahl und Verteilung von Collectors und Processing Engines kommen.

Failover

Monitoring ist kritisch – wenn die Überwachungssysteme ausfallen, sind viele Unternehmen „im Blindflug“ unterwegs. Aus diesem Grund ist die Konfiguration hochverfügbarer Monitoring-Systeme immens wichtig.

RUEI bietet die Möglichkeit, die Komponenten nach dem Aktive-Passiv-Prinzip hochverfügbar auszulegen. In dieser Konfiguration sind die

Komponenten mittels Heartbeat verbunden. Wenn dieser für das passive System nicht mehr erreichbar ist, schwenkt der Datenverkehr automatisch vom Collector zum Failover-System über. Der Administrator muss anschließend auf das ehemals aktive System manuell zurückschwenken.

Naming Pages und Web-Services

Ist RUEI installiert und das System konfiguriert, wird die zu überwachende Umgebung ermittelt. Hierzu ist es wichtig, das dahinterliegende Konzept zu verstehen. RUEI identifiziert anhand des Netzwerk-Verkehrs die aufgerufenen Webseiten beziehungsweise Web-Services und stellt sie in einen Kontext zu einer Applikation beziehungsweise zu einem Service. Dazu ist es nötig, die Applikationen/Services mit den Domänen-Namen, XPath-Ausdrücken oder URL-Strukturen zu definieren und zuzuordnen.

Diese Konfiguration erfordert einen gewissen manuellen Aufwand. Der Benutzer definiert in einem ersten Schritt die zu überwachende Domäne (wie oracle.com), deren URL (wie /technology) und die URL-Argumente. Dieser Filter wird mit einem eindeutigen und in RUEI einmaligen Service-/Applikations-

Namen versehen. Nachfolgend kann der Benutzer einige Automatismen nutzen, um die Zuordnung der dazugehörigen Naming Pages/Web Services zu erstellen. Dazu eine beispielhafte Auflistung der Naming-Pages-Automatismen:

- **Page Tagging**
Die Seiten werden durch (HTML-) Tags unterschieden
- **Client Request**
Die Seiten werden anhand der URL-Struktur ermittelt
- **Server Response**
Die Seiten werden auf Basis der Xpath-Ausdrücke identifiziert
- **Manual**
Alle Seiten werden manuell definiert

Die Filtermöglichkeiten der verschiedenen Automatismen sind sehr detailliert und ermöglichen die weitgehend automatische Ermittlung der Applikations-/Service-Struktur einer Umgebung (siehe Abbildung 4).

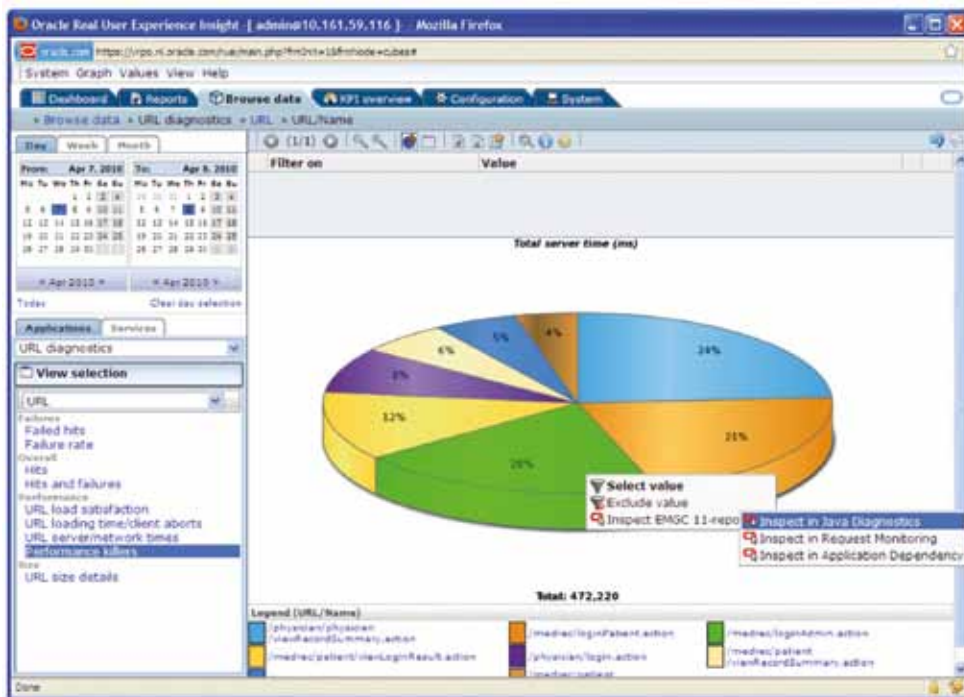


Abbildung 4: Direkter Drilldown bei Server-Problemen in die integrierte „Java & Datenbank“-Diagnostic

Einsatzbeispiel und Projekt-Erfahrungen

Die Herausforderungen bei einer großen deutschen Investment-Bank waren:

- Wesentliche vertriebliche Geschäftsprozesse werden über derzeit 14 webbasierte Applikationen mit rund drei Millionen Nutzern in Internet und Intranet abgewickelt
- Durch Outsourcing von Hardware- und Netzwerk-Leistungen an unterschiedliche Service-Provider ließen sich Performance-Probleme nicht immer eindeutig lokalisieren
- Bedarf nach einem End-to-End-Monitoring-Werkzeug, das die Einhaltung von Vorgaben überwacht und bei Problemen automatisch die Verantwortlichen benachrichtigt
- Kritische Applikationen bzw. Komponenten mit hohem Nutzungsgrad sollten gezielt optimiert werden

Der Einsatz von Real User Experience Insight führte zu folgender Situation:

- Leistungsfähigkeit und Verfügbarkeit der Vertriebskanal-Systeme werden aus Sicht einzelner Nutzer überwacht

- Durchgängige Überwachung relevanter Mess- und Schwellenwerte der internen und externen Geschäftsprozesse über den kompletten produktiven Betrieb
- Kontinuierliches Performance-Monitoring für die rund 1,5 Millionen Sessions mit ca. 13 bis 14 Millionen Hits pro Tag
- Eindeutige Identifizierung eventuell auftretender Fehler auf Server-, Applikations- oder Netzwerk-Seite, erheblich vereinfachte Lokalisierung von Fehlerursachen
- Automatische Alarmmeldung beim Überschreiten vorgegebener Werte für Antwortzeiten beziehungsweise bei Fehlerhäufungen aufgrund von Nichtverfügbarkeit von Seiten
- Keinerlei Beeinträchtigung der Systemleistung durch das Monitoring mit Oracle Real User Experience Insight, keinerlei Änderung an den Applikationen zur Einführung erforderlich

Fazit

Durch den Einsatz von RUEI ist ein umfassendes End-to-End-Monitoring für webbasierte Anwendungen möglich.

Dies stellt die Verfügbarkeit, Performance und Funktionalität besonders von kritischen E-Commerce-Plattformen sicher. Die Implementierung ist ohne großen Aufwand und ohne Änderung der Applikationen oder Infrastruktur realisierbar. Der Einsatz ist nicht auf Oracle-Systeme oder -Technologien beschränkt, sondern funktioniert für alle auf HTTP, HTTPS oder Web-Services kommunizierenden Anwendungen. Weitere Informationen stehen unter <http://www.oracle.com/technetwork/oem/app-performance-mgmt/index.html> im Internet.

Jens Zwer
jens.zwer@oracle.com

