WebLogic Server/SOA Diagnostic Frameworks für Entwickler und Administratoren

Natascha Schönfeld/Maria Salzberger
Oracle Customer Support
Oracle Corporation
München

Schlüsselworte
Fehleranalyse, Fehlerdiagnose, Oracle Support Interaktion, Oracle Fusion Middleware, WebLogic Server, SOA Suite, Diagnostic, WLDF, DFW, RDA, Tracing, ODL.

Einleitung

Um Ausfallzeiten in Fusion Middleware Umgebungen zu minimieren, ist es notwendig auftretende Probleme möglichst schnell zu lokalisieren, zu klassifizieren und zu lösen. Durch die steigende Komplexität der Systemumgebungen, wie zum Beispiel Fusion Applications oder Application Integration Architecture (AIA), kann der Problemlösungsprozess mehrere Zyklen zur Sammlung der fehlerrelevanten Information erfordern. Die Bestimmung des genaueren Fehler-Kontexts kann oft erst nach der iterativen Analyse von zusätzlichen Debug- oder Trace Daten erfolgen. Dafür ist es extrem wichtig, alle relevanten Systemdaten zeitnah analysieren zu können.

Die schnelle Lösung eines Problems ist meistens von der Genauigkeit und der Relevanz der zur Verfügung stehenden Informationen abhängig. Zu diesem Zweck bietet Oracle Fusion Middleware verschiedene Frameworks (Infrastrukturkomponenten) und Werkzeuge, welche das automatische Aufzeichnen von fehlerrelevanten Systeminformationen für diagnostische Zwecke auf Weblogic Server- oder SOA-Ebene unterstützen.

Diagnostic Frameworks - Prinzipien

Abgeleitet von den o.g. Anforderungen unterstützt das Framework zur Diagnose und Fehleranalyse folgende Prinzipien:

Flexibilität: Die Menge und die Art der diagnostischen Information ist konfigurierbar, so dass die Art der gesammelten Analyseinformation an die Art des Problems angepasst und abhängig vom Fehlerbild vordefiniert werden kann.

Integration: Alle Fusion Middleware Komponenten nutzen einheitliche Schnittstellen um diagnostische Information in einem gemeinsamen Repository abzulegen. Für die Bearbeitung des Fehlerarchivs (Repository) werden ebenfalls die gleichen Werkzeugen zur Paketierung und Analyse genutzt.

Zeitnahe Erfassung*:* Sowohl auf Systemebene (WebLogic Domäne / WebLogic Server), als auch auf Applikations/Komponenten Ebene, kann diagnostische Information unmittelbar beim Auftreten eines Fehlers automatisiert gesammelt werden.

Incident – Definition eines „Vorfalls“ im Diagnostic Framework

Jedes Problem, das in Form eines Fehlercodes für eine Serverkomponente manifestiert wird, kann die Erstellung eines Incidents antriggern. Ein Incident erhält eine eindeutige Idenfifikationsnummer und wird damit in ein ‚Fehlerarchiv‘ eingetragen. Zu einem Problem können mehrere Incidents registriert werden.

Die Informationssammlung zu einem Incident wird manuell oder automatisch ausgeführt. Dies geschieht mithilfe von Diagnostic Dumps. Das Ergebnis der Ausführung von Diagnostic Dumps ist die Erstellung von Dateien mit spezifischen Infomationen, welche den Zustand bzw. das Abbild der Laufzeitumgebung wiedergeben. Man unterscheidet zwischen System Dumps (z.B. Thread Dumps, Log Dateien, Flight Recordings) und Applikations- bzw Komponenten Dumps (etwa für die soa-infra Applikation). Diese sind z.B. Konfigurationsdateien von BPEL PM, Mediator, Human Workflow oder spezielle Artefakte wie etwa der WSDL Cache oder der Audit Trail.

Ein Überblick über die Tools für Fusion Middleware Komponenten, die zu diagnostischen Zwecken in SOA Suite Umgebungen genutzt werden, zeigt *Abbildung 1*.

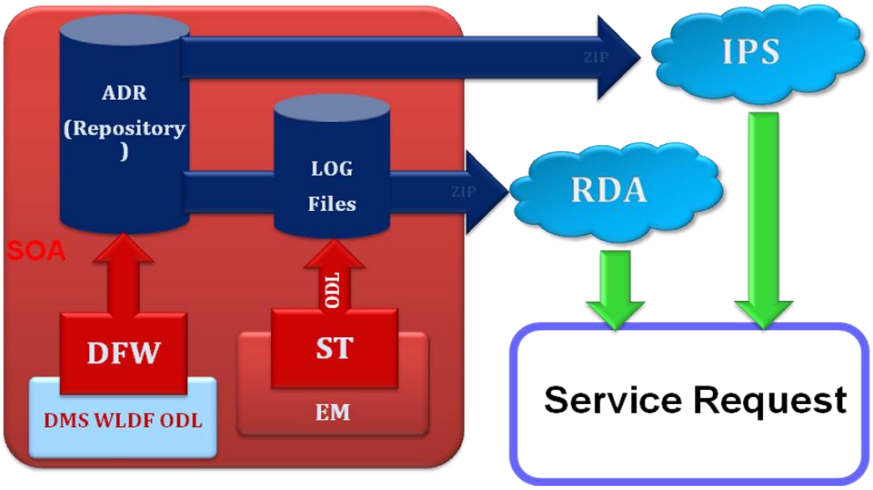

Abb. 1: Überblick über die Diagnostic Tools für Fusion Middleware und SOA

Information sammeln und validieren – die Rolle von ODL, DMS und WLDF

Als Informationsquellen für die Generierung eines Incidents werden Protokolldateien und Sensoren verwendet, welche den Lebenszyklus des Servers oder einer Serverkomponente begleiten. Folgende Infrastrukturkomponenten dienen als Informationsquellen:

DMS (Dynamic Monitoring Service)

Oracle Dynamic Monitoring Service (DMS) bietet eine gemeinsame Schnittstelle zu allen Middleware Komponenten in Form von Sensoren und MBeans. Es erstellt Laufzeitstatistiken (z.B. Anzahl Requests, Free Heap Size, Processing Time usw.). Jede Applikation bzw. Komponente implementiert eine Anzahl von Sensoren bzw. MBeans, welche Statistiken verschiedener Laufzeitparameter sammeln. Ein Administrator kann die Werte mit Hilfe von administrativen Werkzeugen wie WLST , Fusion Middleware Control oder DMS Spy abfragen, um kritische Schwellenwerte festzulegen, die zur Generierung von Incidents führen müssen.

ODL (Oracle Diagnostic Logging)

Oracle Diagnostic Logging (ODL) ist die wichtigste Logging Komponente von Oracle Fusion Middleware. Komponenten und Services nutzen das ODL Protokollformat um eigene Laufzeit-Informationen in die Diagnostic Logdateien des Servers zu schreiben. Das ODL Format definiert welche Pflichtattribute eine Applikation bzw. eine Komponente protokollieren soll und in welcher Reihenfolge. Pflichtattribute sind z.B COMPONENT ID (Module wie oracle.mds), Zeitstempel, MSG_ID, ECID (Execution Context Id) usw. Das ODL Format erleichtert die Filterung der Werte dieser Attribute zu diagnostischen Zwecken. Der Detaillierungsgrad der Protokollierung kann u. A. über die Fusion Middleware Control im Enterprise Manager definiert werden.

Selective Tracing (ST)

Das Selective Tracing umfasst eine Reihe von Funktionen, welche es Adminstratoren und Entwicklern erlauben, Detaillierungsstufen in den Protokollierungsdateien auf ein Composite, eine Applikation oder einen Benutzer zeitlich einzuschränken und die Erstellung eines Incidents manuell mittels Fusion Middleware Control zu veranlassen . Der Anwender benutzt die Fusion Middleware Control oder WLST, um eine Protokollierungssitzung (Session) zu starten und zu stoppen. Der Anwender kann optional einen eindeutigen Identifikator (TRACE_ID) festlegen, welcher additiv zu den anderen ODL Formatattributen mitprotokolliert wird. Damit können während der Fehleranalyse die Protokolldateien auf die TRACE_ID selektiv gefiltert werden. Selective Tracing ist verfügbar ab Version 11.1.1.5 (11gR1 PS4).

WLDF (WebLogic Diagnostic Framework)

WLDF ist das Diagnose-Framework von WebLogic Server. Es existiert seit WebLogic Server Version 9 und besteht aus einer Reihe von Diensten, welche zur Laufzeit das Serververhalten und den Ressourcenverbrauch überwachen und diagnostische Informationen über das Innenleben des Servers sammeln.

Zusätzlich bietet WLDF ein umfangreiches Regelwerk zur Klassifizierung von Fehlersituationen, welche das Sammeln von diagnostischen Informationen erfordern. Zur Formulierung von Bedingungen für die Regeln dienen sowohl Laufzeitwerte, die Server- MBeans zur Verfügung stellen, als auch Protokollinformationen in den WebLogic Server Logs (nicht Diagnostic Logs). Ein Beispiel für eine Regel-Bedingung ist das Vorkommen einer bestimmten Fehlernummer oder die Unterschreitung eines umgebungsspezifischen Schwellenwerts, z.B FreeHeapSize. Bedingungen können mittels logischer Operatoren verknüpft werden.

Treffen alle Bedingungen für eine Regel zu, verwendet WLDF Benachrichtigungen (‚Notifications'), um die Informationssammlung über unterschiedliche Wege (Email, JMS, JMX, Diagnostic Dumps, SNMP Traps) in Form von Thread Dumps, diagnostic Images oder JRockit Flight Recordings zur Verfügung zu stellen. Wichtig ist, dass WLDF ausschliesslich Systemdaten, nicht applikationsrelevante Daten sammelt.

Administratoren können Überwachungspunkte (Watches) in der WebLogic Administrationskonsole oder mittels WLST aufsetzen , die an eine oder mehrere Bedingungen geknüpft sind. Administratoren können auch Überwachungspunkte nach Bedarf aktivieren und zurücksetzen oder zu einem oder mehreren Benachrichtigungstypen (Notifications) zuordnen.

Ab 11gR1 PS5 (11.1.1.6) werden drei Überwachungspunkte (Stuck Threads, Deadlocks und unhandled Exceptions) schon bei der Erstellung einer Domäne aufgesetzt, welche eine ‚out-of-the-

box‘ WLDF Notification (‘FMWDFW-notification') nutzen, um in diesen Fehlersituationen System Dumps zu erzeugen.

Incidents generieren und katalogisieren – die Rolle von DFW

ODL, DMS und WLDF zeichnen Laufzeitinformationen auf, aber generieren selbst keine Incidents. Diese Aufgabe übernimmt das DFW – das Oracle Diagnostic Framework.

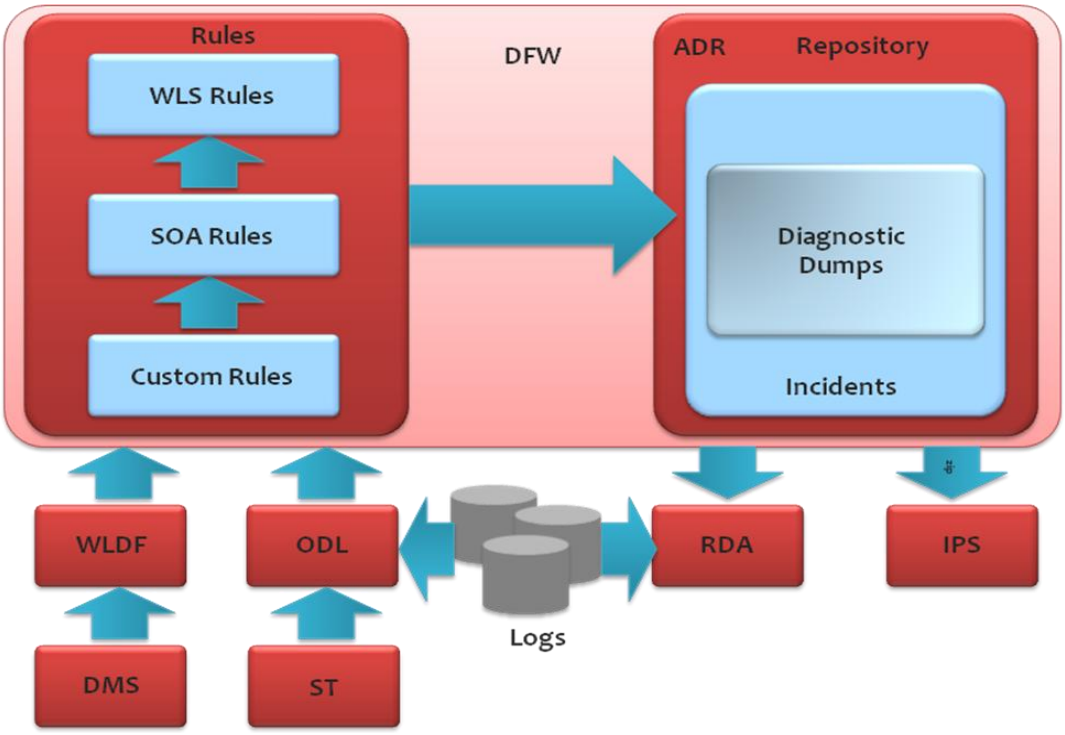

Abb. 2: Architektur von Oracle Diagnostic Framework (DFW)

DFW (Oracle Diagnostic Framework)

Das DFW ist die Kernkomponente der Diagnostic Frameworks in Fusion Middleware. Es ist zuständig für:

- Die Generierung von Incidents.

- Die Registrierung und die automatische Ausführung von applikationsspezifischen Diagnostic Dumps.

- Die Katalogisierung und Zuordnung der diagnostischen Informationen zu einem Incident.

Wie in in *Abbildung 2* dargestellt , ist DFW durch sein Regelwerk nahtlos mit ODL, WLDF und DMS integriert. Das DFW Regelwerk hat die Form einer XML Datei und wird als Betandteil einer Applikation oder Komponente installiert, z.B für SOA als Teil der Fabric Bibliotheken . Ein Beispiel wird in *Abbildung 3* dargestellt.

```
<?xml version="1.0" encoding="UTF-8"?>
<diagnosticRules xmlns="http://www.oracle.com/DFW/DiagnosticsFrameworkRules"
xmlns:xs="http://www.w3.org/2001/XMLSchema-instance">
    <logDetectionConditions>
        <condition messageSeverity="ERROR" messageId="SOA-21537"/>
    </logDetectionConditions>
    <processingRules>
        <rule name="WLDF Watch Rule Timeout">
            <ruleCondition>
                <condition name="MESSAGE_ID" value="SOA-1234" operator="EQ"/>
            </ruleCondition>
            <ruleActions>
                <dumpAction name="soa.composite.trail">
                    <argument name="ecid" value="ECID" valueType="Fact" mandatory="true"/>
                </dumpAction>
            </ruleActions>
        </rule>
    </processingRules>
    <defaultActions>
        <dumpAction name="soa.composite">
            <argument name="compositeName" value="composite_name"/>
        </dumpAction>
        <dumpAction name="soa.wsdl">
            <argument name="compositeName" value="composite_name"/>
        </dumpAction>
    </defaultActions>
</diagnosticRules>
```

Abb. 3: DFW Regelwerk

In diesem Regelwerk wird festgelegt:

LogDetectionConditions: Bedingungen, die sich auf das Vorkommen eines bestimmten Fehlercodes oder irgendeines Fehlers einer SOA Komponente (z.B BPEL) in den Diagnostic Logs beziehen. In diesem Zusammenhang werden die Attributwerte des ODL Protokollformats genutzt, um diese Bedingung zu validieren.

Processing Rules: Diese Angabe stellt die Verbindung zwischen WLDF und DFW her. **<rule>** referenziert einen WLDF Überwachungspunkt und <**ruleActions**> definieren die spezifischen SOA Diagnostic Dumps, die erstellt werden sollen. Diese werden **zusätzlich** zu den System Dumps generiert.

Aus diesem Grund kann die automatische Ausführung einer Reihe von SOA-spezifischen Diagnostic Dumps ausschließlich in dem DFW-Regelwerk als Aktion definiert werden, um SOA-Kontextinformationen zur erhalten. Folgende SOA Suite spezifische Diagnostic Dumps sind ab 11gR1 PS5 (11.1.1.6) verfügbar:

- *soa.config: MDS Konfigurationsdateien für alle SOA Engines.*
- *soa.composite: Information über Composite und Artefakte z.B Laufzeit Engine Properties.*
- *soa.wsdl: WSDL Artefakte aus dem Runtime WSDL- und Schema Cache*
- *soa.edn: EDN Konfigurationsinformation für das Event System.*
- *soa.db: Metadaten und Information zur SOA Infrastructure Datenbank.*

- soa.env: Umgebungsvariablen für SOA.

- soa.composite.trail: Audit Trail Information für eine bestimmte ECID., die die Ausführung eines Requests durch alle beteiligten Komponenten der SOA Infrastruktur eindeutig identifiziert.

In Ausnahmesituationen (‚Race-Conditions') kann das DFW-Regelwerk durch zusätzliche Regeln erweitert werden um ein bestimmtes Problem zu analysieren, das nicht gezielt reproduziert werden kann. In diesem Fall wird Oracle Support eine XML-Datei (custom-rules.xml) zur Verfügung stellen, die auf Domänen- oder Server-Ebene kopiert werden soll, um abhängig von der Fehlersituation, die Generierung von zusätzlichen Incidents zu veranlassen. DWF wird in diesem Fall ALLE festgelegten Regeln (Rules in custom-rules.xml, Applikationsregeln von soa-infra und WLDF Regeln) berücksichtigen.

Das DFW registriert Incidents und veranlasst die Ausführung von Diagnostic Dumps, welche eine Reihe von Dateien mit diagnostischem Inhalt im **ADR (Automatic Diagnostics Repository)** physikalisch ablegen**.** ADR ist ein Filesystem Repository zur Speicherung, Katalogisierung und Archivierung von Diagnostic Dumps per Incident. Ein ADR Repository existiert für jeden Server innerhalb einer SOA Domäne. Die ADR Verzeichnisstruktur wird in *Abbildung 4* gezeigt.

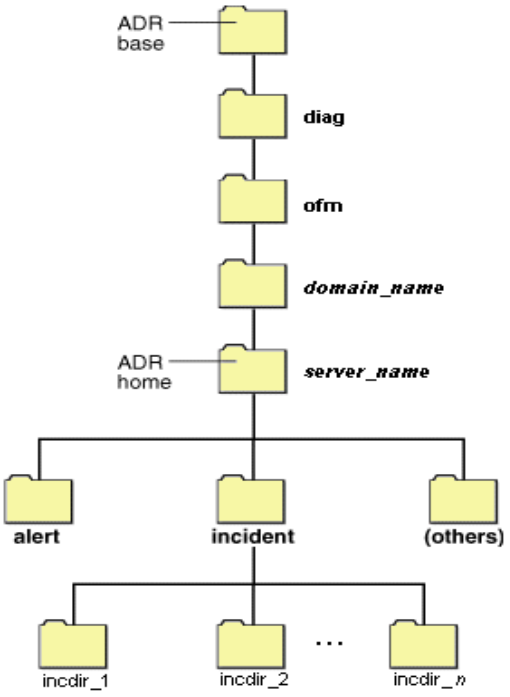

Abb. 4: ADR Verzeichnisstruktur

Das DFW veranlasst die Ausführung von Diagnostic Dumps asynchron. Somit hat seine Interaktion mit anderen Systemkomponenten keine negative Auswirkungen auf die Systemleistung. Das default Memory Footprint ist 512K.

Das DWF bietet eigene MBeans zu Konfigurations- bzw Administrationszwecken, welche mittels Fusion Middleware Control oder WLST zugänglich sind. Zu den Admisnistrationsaufgaben gehören u.a die Festlegung der maximalen Anzahl von Incidents zu einem Problem (FloodControlEnabled), das Aktivieren oder Deaktivieren der Incident Generierung (IncidentCreationEnabled), das Ein- bzw.

Ausschalten des Logfilters (LogDetectionEnabled) oder die Verwaltung von Incidents im ADR. Auf diesem Weg können Diagnostic Dumps für registrierte Incidents manuell erzeugt werden oder der Inhalt der Dumps abgefragt werden.

Bearbeitung von Incidents – IPS, ADRCI und RDA

Incident-Daten können manuell mit den gleichen Tools bearbeitet und analysiert werden, welche schon mit Oracle Database 11gR1 benutzt werden (IPS, ADRCI).

Diese Tools dienen zur Generierung von Paketen, die Diagnostic Dumps für einen bestimmten Incident beinhalten.

ADRCI (Automatic Diagnostics Repository Command Interpreter):

Ein Kommandozeilen Werkzeug zur manuellen Bearbeitung von Daten im Diagnostic Repository ADR. Es kann u.a. genutzt werden, um **IPS (Incident Packaging System)** Kommandos zu verwenden, um Pakete zur erstellen. Diese enthalten die Diagnostic Dumps die zu einem Incident gehören. Mithilfe von ADRCI können auch Inhalte des Diagnostic Repository (ADR) gelöscht werden.

RDA (Remote Diagnostic Agent):

RDA ist ein Tool zur Sammlung von Konfigurations- und Laufzeitdaten. Es stellt verschiedene Module für Fusion Middleware Produkte zur Verfügung, die eine umfassende Sammlung (Collection) von Informationen erstellen. RDA kann auf explizierte Anfrage Collections aus schon vorhandenen diagnostischen Daten erstellen.

In einer RDA-Collection für WebLogic Server oder SOA sind automatisch die Informationen zu den letzten 10 Incidents enthalten. Mit RDA erzeugte Collections können zu einem Service Request hochgeladen werden um sicherzustellen, dass relevante Konfigurations- und Laufzeitinformation zur Verfügung steht.

Anwendungsfälle –Wann kann ich welches Framework nutzen?

Insbesondere DFW und WLDF sind konzipiert um das System zu überwachen und die zeitnahe Aufzeichnung von Systeminformation in Ausnahmesituationen zu automatisieren. Die häufigsten Ausnahmesituationen in *Produktions- und Testumgebungen* sind u.a.:

- Hoher Verbrauch von System Ressourcen , System Instabilität, Überlastung oder Stuck Threads während des Server Startups, Inbetriebnahme (Deployment) oder der Laufzeit von Applikationen.
- Erhöhte Anzahl von Composite Instanzen, die auf Wiederherstellung (Recovery) warten.
- Verschlechterung der Systemleistung (Performance) während der Laufzeit.
- Probleme bei Data Sources – (z.B. Zeitüberschreitung bei Datenbanktransaktionen oder unerwarteter Abbruch von Transaktionen).

WLDF und DFW sind bestens geeignet zur Unterstützung der Ursachenanalyse in *Produktions- und Testumgebungen*, besonders wenn die Bedingungen des Auftretens von Fehlern nicht reproduzierbar sind.

Selective Tracing kann in *Produktions- und Testumgebungen* eingesetzt werden, denn es ermöglicht die Aufzeichnung von detaillierten DEBUG Informationen in den Protokolldateien für einen begrenzten Zeitraum ohne Restart. Auch in verteilten *Entwicklungsumgebungen* kann Selective Tracing eingesetzt werden, um die Sammlung von diagnostischen Informationen in den Logs auf ein

Composite oder pro Entwickler einzuschränken. Spezielle Überwachungspunkte können mit WLDF aufgesetzt werden, um evenuelle Probleme während der Inbetriebnahme (Deployment) von Composites aufzuspüren und entsprechend SOA-spezifische Dumps auszuführen.

Der gezielte Einsatz von DMS in *Test- und Integrationsumgebungen* ermöglicht die Evaluierung von wichtiger Informationen über das Laufzeitverhalten, welche zu Anpassungen von Konfigurationsparametern in der Produktionsumgebung vor dem Go-Live führen können, um eventuelle Ressource Bottlenecks proaktiv zu ermitteln und zu vermeiden.

Zusammenfassung

Die Fusion Middleware Diagnostic Frameworks unterstützen Administratoren und Entwickler bei der Ursachenanalyse und optimieren die Arbeitsabläufe zwischen unseren Kunden und Oracle Support. Mit Fusion Middleware Diagnostic Frameworks erhalten Oracle Kunden ein mächtiges Instrument zur effizienteren Diagnose und schnellen Behebung von Problemen in SOA Umgebungen.

Disclaimer

"THE FOLLOWING IS INTENDED TO OUTLINE OUR GENERAL PRODUCT DIRECTION. IT IS INTENDED FOR INFORMATION PURPOSES ONLY, AND MAY NOT BE INCORPORATED INTO ANY CONTRACT. IT IS NOT A COMMITMENT TO DELIVER ANY MATERIAL, CODE, OR FUNCTIONALITY, AND SHOULD NOT BE RELIED UPON IN MAKING PURCHASING DECISION. THE DEVELOPMENT, RELEASE, AND TIMING OF ANY FEATURES OR FUNCTIONALITY DESCRIBED FOR ORACLE'S PRODUCTS REMAINS AT THE SOLE DISCRETION OF ORACLE."

Weitere Informationen

[1] Overview of SOA Diagnostics in 11.1.1.6

[2] Introduction to the Diagnostic Framework

[3] DFW WLST Reference

[4] SOA Diagnostics

[5] ADR Command Interpreter (ADRCI) for Packaging Incidents

[6] How to Monitor Runtime SOA Performance With the Dynamic Monitoring Service (DMS) [ID 1368291.1]

[7] How to Reset a SOA 11g DMS Metric

[8] DMS Documentation

[9] ODL Documentation

[10] Diagnostic Framework Documentation

[11] DFW WLST Command Reference

[12] Documentation for SOA Diagnostic Dumps in 11.1.1.6

[13] How to Use Selective Tracing for SOA [ID 1367174.1]

[14] Selective Tracing WLST Reference

[15] How to Monitor Runtime SOA Performance With the Dynamic Monitoring Service (DMS) [ID 1368291.1]

[16] How To Script the Creation of a SOA WLDF Watch in 11g [ID 1377986.1]

[17] WLDF Documentation

[18] How to Use the Incident Packaging System (IPS) in SOA 11g [ID 1381259.1]

[19] ADRCI Documentation

[20] How to Collect Analysis Information Using RDA for Oracle SOA 11g Products [ID 1350313.1]

Kontaktadressen:

Natascha Schönfeld
Oracle Corporation – OCS Bug Diagnostics and Escalations
Riesstrasse 25
D-80992 München
Telefon: +49 (89) 1430-2787
Fax: +49 (89) 1430-1150
E-Mail: natascha.schoenfeld@oracle.com
Internet: http://www.oracle.com/support/index.html

Maria Salzberger
Oracle Corporation – OCS Proactive Team
Riesstrasse 25
D-80992 München
Telefon: +49 (89) 1430- 2672
Fax: +49 (89) 1430-1150
E-Mail: maria.salzberger@oracle.com
Internet: http://www.oracle.com/support/index.html