Mit Ops Center fest im Blick: Hardware- und OS-Monitoring für Oracle Server und Solaris

Elke Freymann, ORACLE Deutschland B.V. & Co. KG

Das beste Überwachungstool für Hard- oder Software sollte der Hersteller selber liefern, denn schließlich sitzt er ja an der Quelle der notwendigen Informationen. Natürlich hängt damit auch die Messlatte für die zu erfüllenden Ansprüche recht hoch; wenn es aber um die Überwachung von Oracle-Sun-Server-Hardware und das Betriebssystem Solaris geht, muss Oracle Enterprise Manager Ops Center 12c sich mit seinen Fähigkeiten keinesfalls verstecken.

Für die Hardware ist es fast schon zwingend notwendig: Wenn Oracle die inneren Werte des Servers nicht überwachen kann, wer dann? Aber auch im Bereich „Solaris-Monitoring" bietet Ops Center Funktionen, die andere Tools so nicht zur Verfügung stellen. Ganz unschlagbar: ein Oracle-Server, auf dem Solaris läuft. Da kann Ops Center noch weiteres Zusatzwissen in die Monitoring-Aufgabe mit einbringen.

Wer hier wen überwacht

Enterprise Manager Cloud Control und Enterprise Manager Ops Center sind zwei eigenständige Produkte mit Management-Aufgaben im weitesten Sinne. Ops Center konzentriert sich dabei auf das Infrastruktur-Management (Hardware- und Betriebssystem-Schichten) sowie Virtualization Management mit Fokus auf Solaris-Zonen und Oracle VM Server for SPARC – historisch bedingt als Logical Domains bekannt. Jedes dieser beiden Produkte der Enterprise Manager Suite hat auch seine eigene Architektur. Abbildung 1 zeigt diese für Ops Center.

Bei der Installation von Ops Center wird zunächst der sogenannte „Enterprise Controller" samt seinem Data Repository eingerichtet. Dieses Data Repository, eine Oracle-Datenbank, wird entweder lokal auf dem Management-Server mit installiert oder „remote" auf einem anderen Server eingerichtet. Als nächste, serverseitig notwendige Software-Komponente wird mindestens ein sogenannter „Proxy Controller" installiert. Und genau dieser ist derjenige, der die eigentliche Arbeit übernimmt, also auch zum Beispiel die Monitoring-Daten von den überwachten Objekten einsammelt und an den Enterprise Controller weiterleitet.

Der Enterprise Controller füllt damit das Data Repository, bringt die Daten in der grafischen Benutzeroberfläche zur Anzeige, löst Alarmierungen aus und sorgt bei entsprechenden Konfigurations-Einstellungen und Internet-Zugang dafür, dass bei gemeldeten Problemen auch Service Requests in My Oracle Support eröffnet werden.

Der Proxy Controller hat, je nachdem, was für einen Objekt-Typ er überwacht, unterschiedliche Kommunikations-Mechanismen zur Verfügung. Mit einem Hardware-Objekt

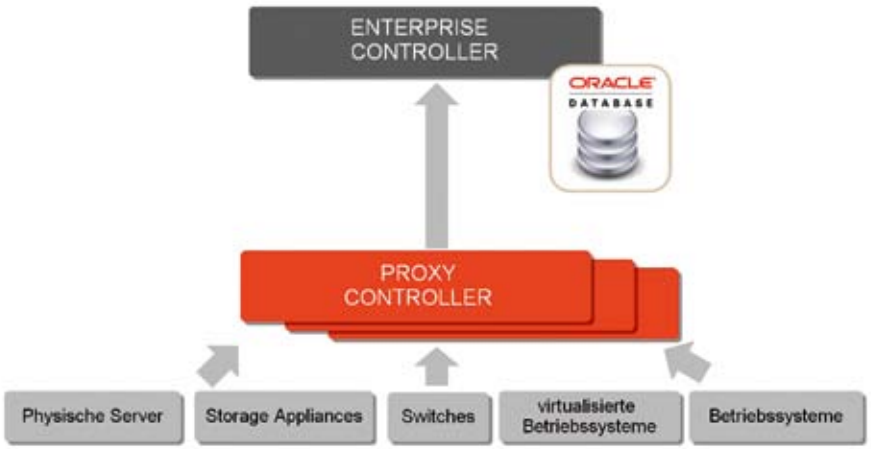

Abbildung 1: Architektur-Überblick Enterprise Manager Ops Center

– genauer dem Service-Prozessor eines Servers, einer ZFS Storage Appliance oder eines Ethernet- beziehungsweise InfiniBand-Switch – werden genau diejenigen Protokolle, die die Hardware nach außen hin anbietet, angesprochen. Typischerweise sind das IPMI und „ssh". Hardware, die dabei verstanden wird, muss vom Hersteller Oracle oder ehemals Sun Microsystems stammen.

Soll ein Software-Objekt überwacht werden, im Falle von Ops Center eine Betriebssystem-Instanz, egal ob „bare metal" oder virtualisiert installiert, so hat Ops Center die Wahl: Sind nur reine Überwachsaufgaben wahrzunehmen, so kann ein „agentless monitoring" erfolgen. Der Proxy Controller sammelt dann per „ssh login" die relevanten Daten in zyklischen Abständen ein.

Sollen aber auch aktive Management-Aufgaben wie Virtualization-Management oder Patching-Aufgaben inklusive der Erstellung von Reports über Paketstände auf dem überwachten Betriebssystem erledigt werden, so wird ein installierter Ops-Center-Agent benötigt. Dieser hält dann die Verbindung mit dem Proxy und empfängt zum Beispiel auch auszuführende Jobs über diesen Kanal.

Überwachung der Oracle-Hardware

Für die reine Hardware-Überwachung wendet sich der Proxy Controller direkt an den Service-Prozessor der Maschine und bietet ein komplettes Monitoring mit dem gleichen Abdeckungsgrad, den auch der Service-Prozessor nativ selbst liefert. Das Ganze erfolgt jedoch zentralisiert: Von der graphischen Benutzeroberfläche aus hat man alle überwachten Server im Blick – und nicht nur einen individuellen (siehe Abbildung 2).

Da es sich um Hardware aus dem eigenen Haus handelt, ist Ops Center auch in der Lage, Hardware-nahe Aufgaben zu erledigen:

- Firmware-Updates für den Service-Prozessor
- Firmware-Updates für verbaute Server-Komponenten
- Klassisches Lights-Out-Management, also Power off/Power on für den eigentlichen Server und Zugriff auf die serielle Konsole des Betriebssystems

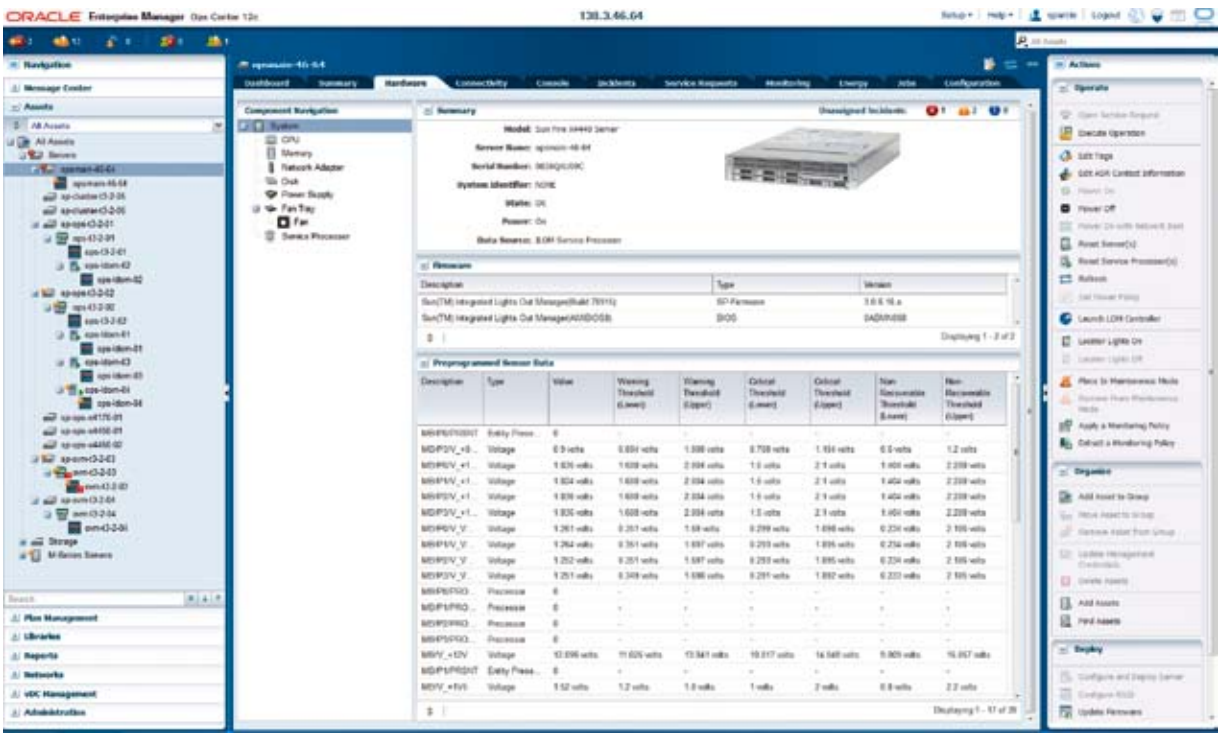

Abbildung 2: Hardware-Monitoring

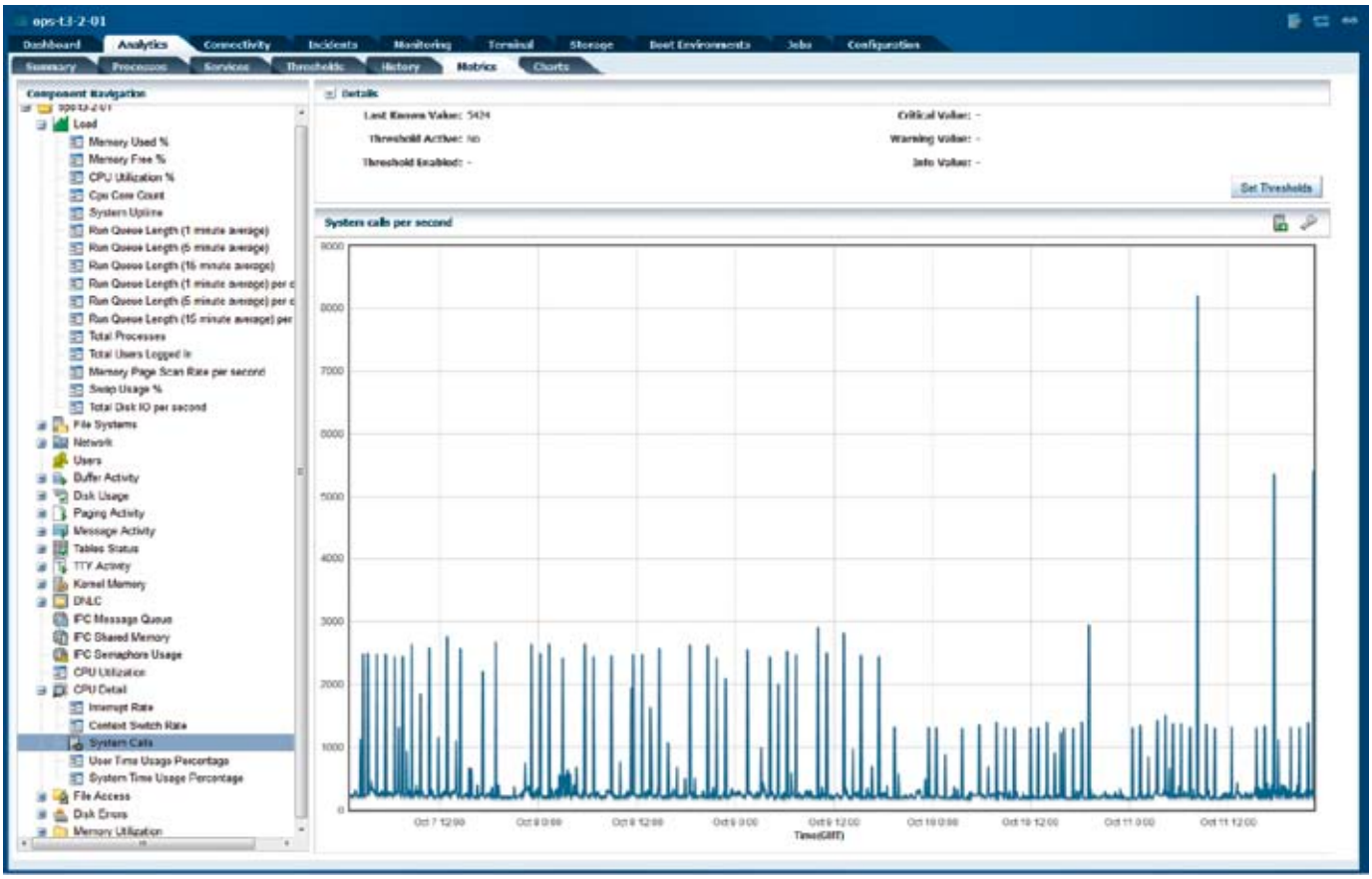

Abbildung 3: Anzahl System Calls als Beispiel für einen Metrikwert

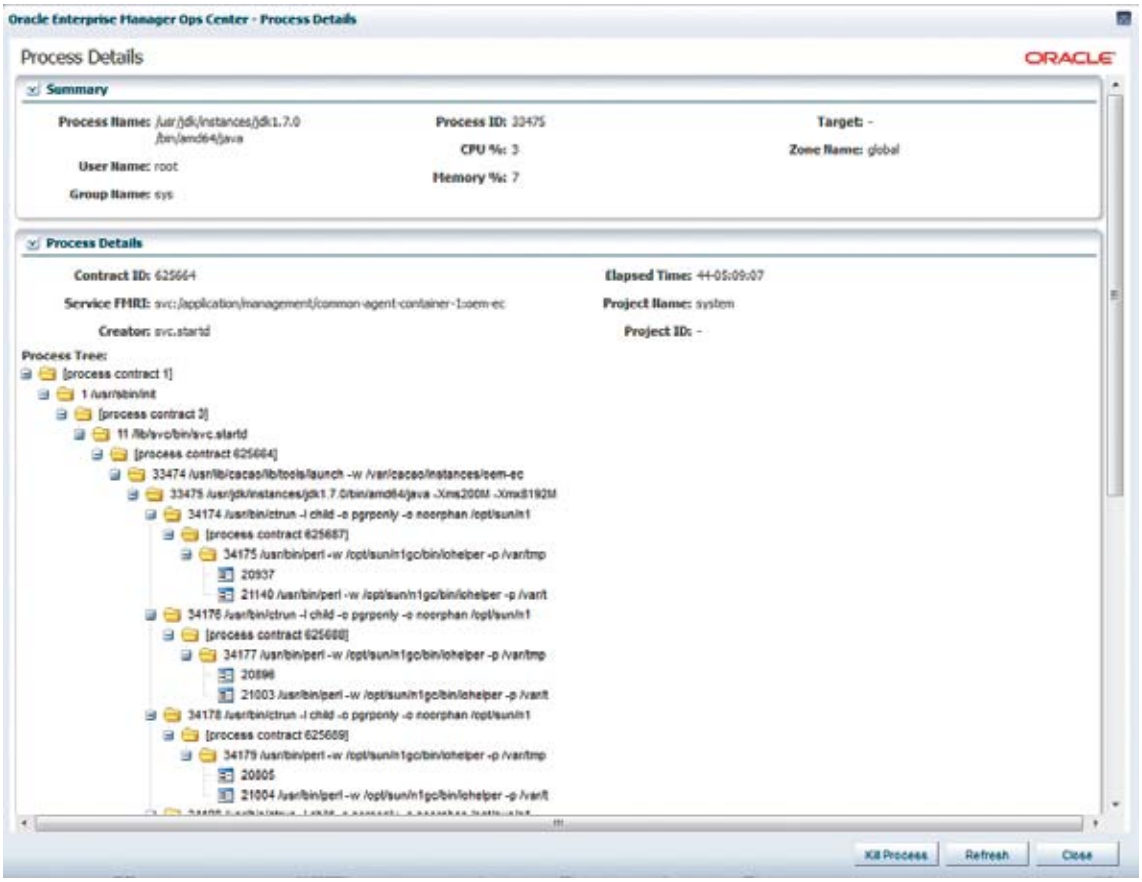

Abbildung 4: Detail-Ansicht für einen Ops-Center-Prozess

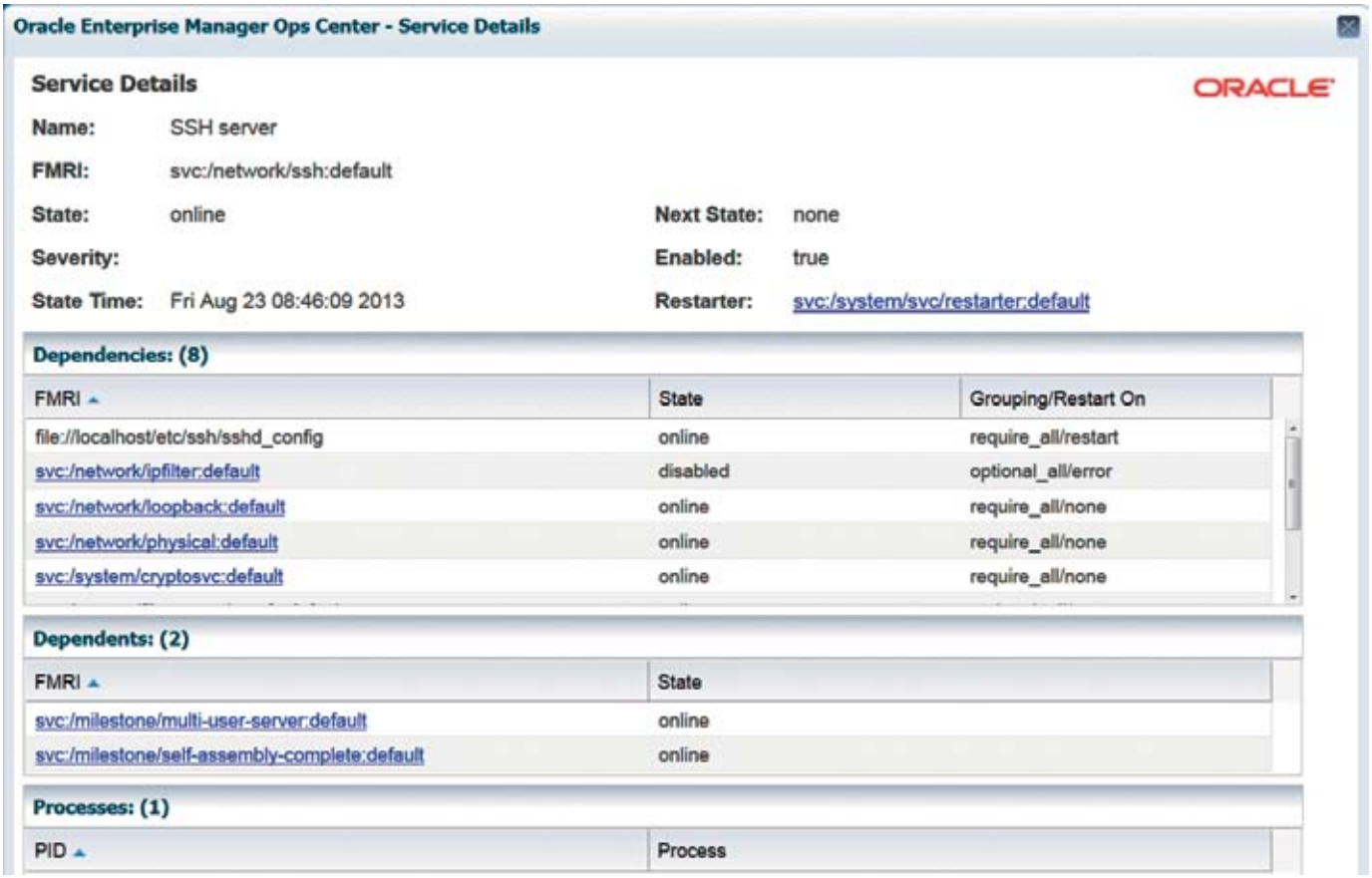

Abbildung 5: SSH-Server-Service in Detail-Ansicht

Überwachung von Solaris

Zunächst bietet Ops Center natürlich die ganz klassische Überwachungsmöglichkeit für Kennzahlen, sogenannte Metriken, des Betriebssystems. Diese Metriken decken die folgenden Funktionsbereiche ab:

- Load
- File Systems
- Networks
- Users
- Buffer Activity
- Disk Usage
- Paging Activity
- Message Activity
- Tables Status
- TTY Activity
- Kernel Memory
- DNLC
- IPC Message Queue
- IPC Shared Memory
- IPC Semaphore Usage
- CPU Detail
- File Access
- Disk Errors
- Memory Utilization

Neben den reinen Metrikwerten ist auch immer eine Ansicht aller laufenden Prozesse interessant. Ops Center stellt diese mit den Parametern „Bezeichnung“, „Benutzer“, „Status“, „CPU- und Memory-Verbrauch“ in einer Liste dar, die sortiert und durchsucht werden kann (siehe Abbildung 3).

Ist ein spezieller Prozess von Interesse, so können seine Details inspiziert werden: der „Process Tree“, „Thread-Informationen“, „Handles“, „Aufruf-Parameter“ und Details zur Memory-Belegung sind abrufbar (siehe Abbildung 4).

Für einen schnellen Überblick werden Top-Consumer nach dem Bereichen CPU-, Memory-, Netzwerk- und I/O-Auslastung auch noch in einer separaten Übersicht zusammengestellt. Um darüber hinaus dem Anspruch gerecht zu werden, Spezifika von Solaris zu kennen, ist in Ops Center zum Beispiel die Überwachung der Solaris-Services implementiert.

Alle Services werden in einer ähnlichen Liste wie die Prozesse dargestellt. Parameter, die ausgewertet werden, sind „Service Name“, „Identifier“, „Startzeitpunkt“ und ganz wichtig der aktuelle Status des Service.

In Ops Center bereits von Haus aus eingebaute Monitoring-Regeln überwachen diesen Status und lösen eine Alarmierung aus, wenn ein Service nicht mehr laufen sollte.

Wer sich für die Details eines Service interessiert und sich zum Beispiel per Klick auf einen Link das Logfile des Service anzeigen lassen will, wird in der Detail-Ansicht fündig (siehe Abbildung 5).

Außerdem arbeitet Ops Center mit der „Fault Management Architecture“ von Solaris zusammen: So werden zusammengehörige Fehlermeldungen auf Hardware- und Betriebssystem-Ebene zu geeigneten Alarmierungen zusammengefasst und liefern die bestmögliche Überwachung für die Einheit aus Server und Betriebssystem.

Kommen Server-Virtualisierungs-Technologien wie Logical Domains oder Solaris-Zonen zum Einsatz, ver-

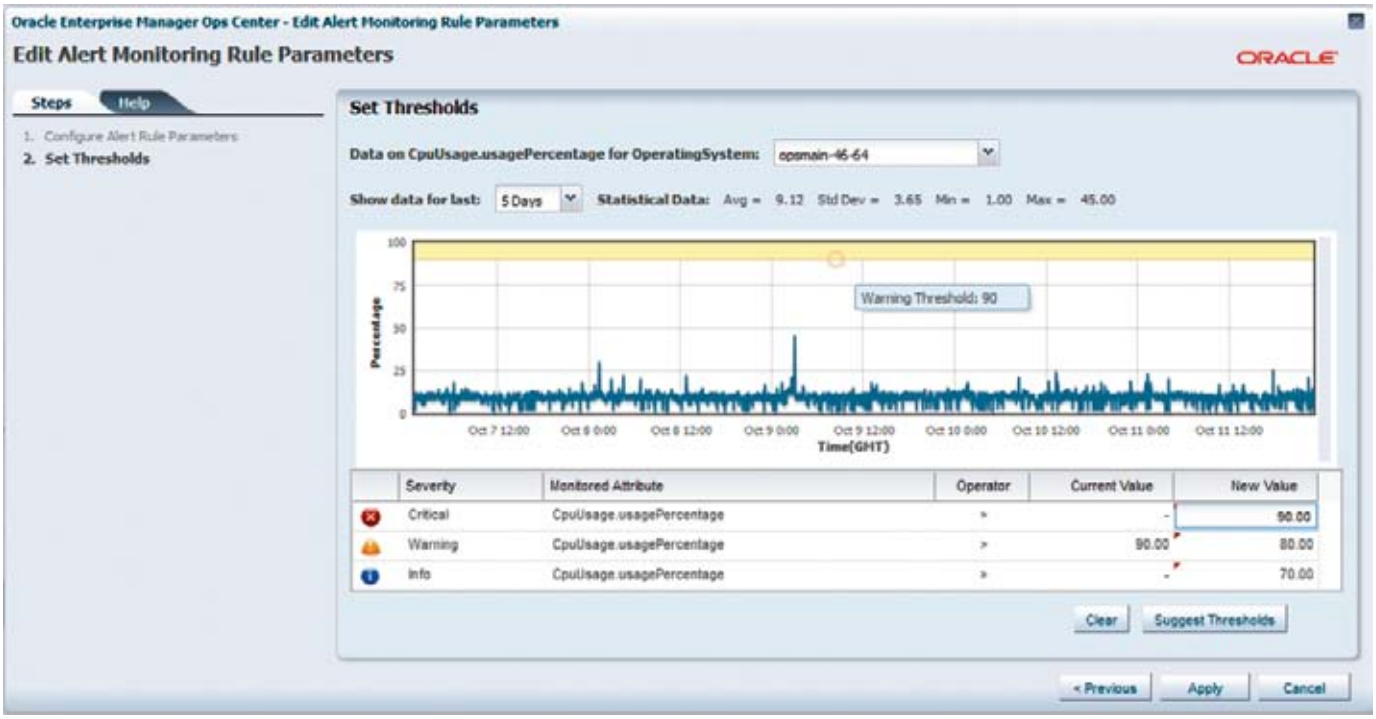

Abbildung 6: Smart Thresholding zur Überwachungsregel „CPU-Auslastung“

schafft Ops Center einen klaren Überblick über die Zuordnung der virtualisierten Instanzen zu den physischen Servern und stellt Funktionen zum „Virtualization Management“ bereit. Ansichten, die den Ressourcen-Verbrauch der virtualisierten Instanzen im Vergleich ausweisen, bieten weitere Übersichtsmöglichkeiten.

Historische Daten zu überwachten Betriebssystem-Parametern und Gesamtkurven für die CPU-, Memory-, Dateisystem- und Netzwerk-Auslastung sowie die komplette System Load werden gesammelt, angezeigt und können exportiert werden.

Noch etwas kann Ops Center gut im Blick behalten: Auf welchem der Server fehlen zum Beispiel noch empfohlene Patches für Solaris 10? Auf welchem Server sollte noch ein Firmware-Upgrade für den Service-Prozessor durchgeführt werden, denn dieser Server weicht von der Standardvorgabe ab, die für diesen Typ getroffen wurde?

Solche Überwachungsaufgaben erledigt Ops Center, wenn man entsprechende Abfrage-Reports definiert und nach einem festgelegten Zeitplan zyklisch ablaufen lässt.

Monitoring-Rules und Policies

Out-of-the-box bringt Ops Center eine ganze Reihe vordefinierter Überwachungsregeln mit, die sogenannten „Alert Monitoring Rules“. Bestandteile einer solchen Monitoring-Policy sind zusammengehörige Überwachungsregeln. Zusammengehörig heißt in diesem Fall: Dieser Regelsatz passt zum Beispiel für die Hardware-Überwachung eines M-Klasse-Servers oder für die Überwachung einer Instanz von Solaris. Mit einer Monitoring-Policy ist immer auch die Information verknüpft, auf welchen Typ der überwachten Objekte dieser Regelsatz passt.

Die vordefinierten Regeln kann man, wenn es um den Bereich der Software-Überwachung geht, modifizieren und so auf die individuellen Bedürfnisse anpassen. Regeln, die Hardware im Auge behalten, lassen sich nicht ändern. Aber in beiden Bereichen – Hard- und Software – lassen sich die Monitoring-Policies um weitere, selbst definierte Regeln erweitern, oder Regeln können auch aus einer Policy entfernt werden.

Die angepassten Policies werden dann unter eigenem Namen abgelegt und können als anzuwendender Default für Objekte passenden Typs deklariert werden, die man neu ins Ops Center einhängt. Man kann natürlich die modifizierten Policies auch auf die Server oder Server-Gruppen ausrollen, die bereits im Ops Center bekannt sind.

Definiert man eine eigene Regel, so gibt man ganz klassisch den zu überwachenden Parameter und die Schwellwerte verschiedener Abstufung an („critical“, „warning“, „info“), bei deren Überschreitung eine entsprechende Alarmierung erfolgen soll. Für die Festlegung der Schwellwerte ist das sogenannte „smart thresholding“ von Ops Center hilfreich: Sofern historische Werte für den betreffenden Überwachungsparameter vorhanden sind, werden diese dargestellt und man bekommt einen Anhaltspunkt dafür, wie man den Schwellwert definieren will (siehe Abbildung 6).

Außerdem gibt man bei der Definition einer Alert-Monitoring-Rule an, wie lange der entsprechende Schwellwert überschritten sein muss, damit ein Alarm ausgelöst wird und welche „immediate action“ – also welches Skript – ausgeführt werden soll, wenn der Alarm auftritt.

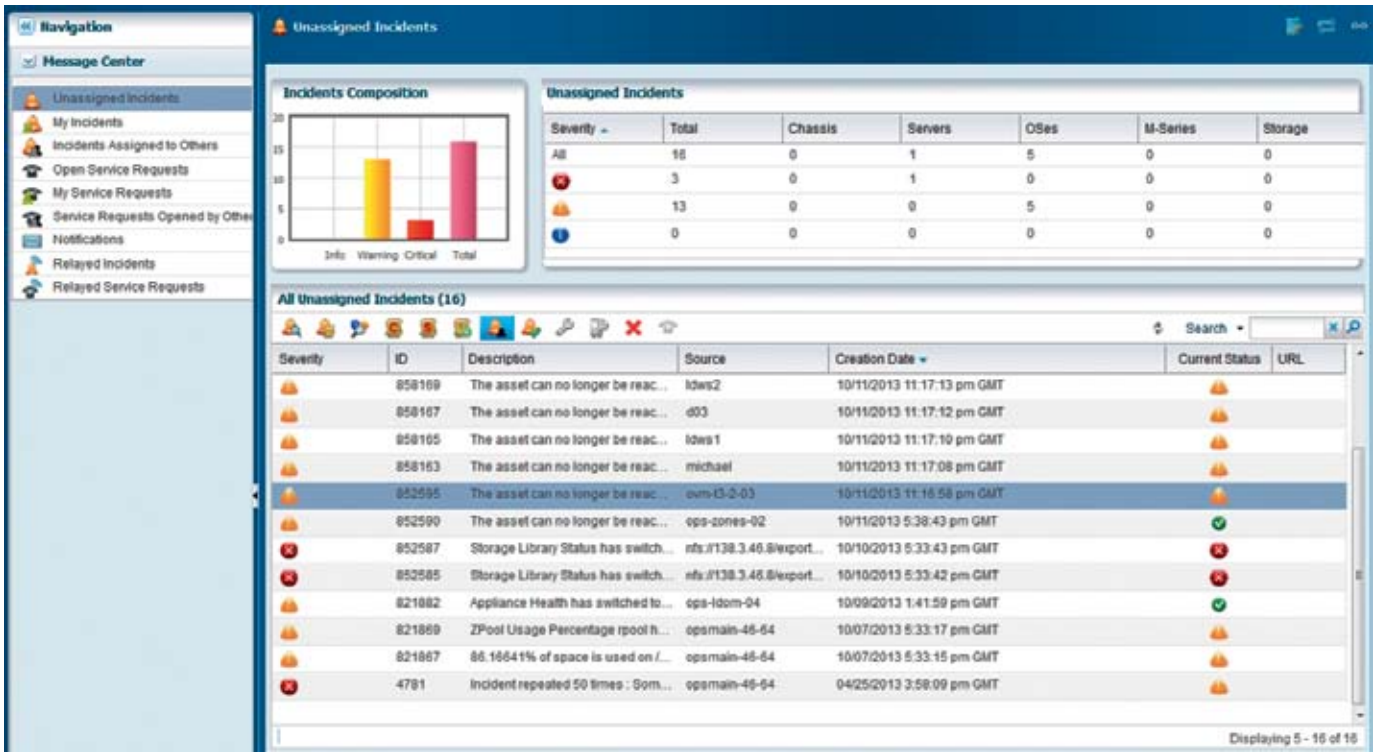

Abbildung 7: Incidents im Message-Center

Incidents und das Message Center

Kommt es zu einer Alarmierung, wird die „immediate action" ausgeführt. Benutzer, die ein entsprechendes Notification Profile zugewiesen bekommen haben, erhalten eine Benachrichtigung per E-Mail. Außerdem wird das entdeckte Problem auch als Incident mit einem Status und Angaben zum zugeordneten Bearbeiter verwaltet.

Offene Incidents kommen sowohl auf Ebene der betroffenen Einheit (zum Beispiel Hardware-Eintrag für einen Server oder Betriebssystem-Schicht) als auch in einem zentralen Message-Center, das systemweit alle entsprechenden Informationen sammelt, zur Anzeige und Bearbeitung (siehe Abbildung 7).

Fazit

Ops Center ist das vom Hersteller empfohlene Tool, um Oracle-Server und das Betriebssystem Solaris optimal zu überwachen. Anfallende Lizenzkosten stellen auch keine Hürde für den Einsatz dar: Die Nutzung und die Wartung (Service-Anspruch) von Ops Center sind kostenfrei im Oracle Premier Support enthalten.

Weiterführende Informationen

- Zentrale Quelle für Ops Center 12c Informationen im OTN: http://www.oracle.com/technetwork/oem/ops-center/index.html
- Dokumentation mit How-to-Guides: http://docs.oracle.com/cd/E27363_01/index.htm
- Ops-Center-Everywhere-Programm: http://www.oracle.com/us/corporate/features/opscenter-everywhere-program-1567667.html
- Download über OTN: http://www.oracle.com/technetwork/oem/ops-center/oem-ops-center-188778.html

Elke Freymann
elke.freymann@oracle.com