Patching und Provisioning von Linux-basierten Infrastrukturen

Manuel Hoßfeld
Oracle Deutschland B.V. & Co. KG
GS Frankfurt (Dreieich)

Schlüsselworte:

Patching, Provisioning, Linux, Oracle, Enterprise Manager, Ops Center, Grid Control

Einleitung

Spätestens wenn man mehrere Linux-basierte Systeme im Einsatz hat stellt sich die Frage, wie man diese ohne viel Aufwand aktuell hält und jeweils benötigte Patches und Updates einspielen kann.
Auch das initiale Aufsetzen („Provisioning“) neuer Linux-Systeme ist ein zeitraubender und potentiell fehlerträchtiger Vorgang, den man – sofern man ihn häufiger durchführen muß – gerne automatisiert hätte. Der Vortrag stellt das Thema "Patching und Provisioning" für Linux-Systeme mit den entsprechenden Oracle-Werkzeugen der Enterprise Manager Produktfamilie dar. Dabei wird nicht zwangsläufig davon ausgegangen, daß die Linux-Systeme um die es hier geht als Basis für eine Oracle-Datenbank, Application Server o.ä. dienen. Auch die Tatsache, ob die entsprechenden Systeme „nativ“ (also auf dem „bare metal“) laufen oder virtualisiert sind, spielt im folgenden keine Rolle. Vielmehr geht es darum, ganz grundsätzlich die im folgenden Abschnitt genannten Herausforderungen zu bewältigen, denen sich Linux-Admins gegenüber stehen – egal ob es sich um einen „Fulltime Linux Admin“ oder „nur“ um DBA handelt, der zusätzlich zu seinem üblichen Aufgabenbereich nun auch noch die Betriebsystem-Administration übernehmen muss.

Herausforderungen bei der Administration von Linux-Systemen

Neben den im Rahmen dieses Vortrags nicht im Fokus stehenden Aspekten wie Performance-Monitoring und Fehlerdiagnose sind es vor allem die schon in der Einleitung genannten Bereiche „Patching“ und „Provisioning“, welche ein Vielzahl von Herausforderungen beinhalten.
Im wesentlichen sind dies die folgenden Punkte:

- Wie kann ich möglichst schnell und reproduzierbar ein Linux-System aufsetzen – Idealerweise „from scratch“, d.h. ohne bereits irgendwelche „Vorarbeiten“ auf einem möglicherweise fabrikneuen System auszuführen. (Man spricht in diesem Zusammenhang auch häufig von „Bare Metal Provisioning“, oder dem Erstellen und Ausrollen von „Gold Images“ - also vorher festgelegten, für die eigenen Zwecke fertig konfigurierten Betriebsystem-Abbildern.)
- Welche Kernel-Versionen und Betriebssystem-Patches sind auf meinen Linux-Systemen installiert? Sind alle Systeme die einem gleichen Zweck dienen (z.B. „Datenbank-Server“) auch tatsächlich auf dem gleichen Stand? Wenn nicht, wie kann ich dies erreichen und anschließend sicherstellen, daß der gewünschte Patchlevel auch durchgängig eingehalten wird. (Stichwort: „Compliance“. Gemeint ist hier das Entsprechen der inzwischen in vielen Unternehmen vorhandenen Richtlinien bzgl. Release- und Patchstände.)
- Wenn bereits bekannt ist, daß ich für eine bestimmte Anwendung diesen oder jenen Patch benötige: Wie kann ich sicherstellen, daß dieser nicht mit einem anderen, evtl. bereits

vorhanden Patch kollidiert, bzw. wie kann ich inhaltliche Konflikte zwischen Versionen / Patchleveln nach Möglichkeit schon vorher ausschließen? (Zwar bieten moderne Linux-Distributionen alle ein im Paket-Management verankertes System zur Verwaltung von Paket-Abhängigkeiten an. Dies funktioniert jedoch auf einer „rein technischen“ Ebene – Fortgeschrittene / „inhaltliche“ Aspekte bleiben dabei jedoch auf der Strecke. Bsp.: Zwar mag es sein daß Patch 4711 technisch zu Paket 1234 passt, dieser aber Inkompatibilitäten und Probleme verursacht, wenn auf dem gleichen System auch Paket 1235 installiert ist und daher alternativ lieber Patch 4712 eingespielt werden sollte.)

Für einige der oben genannten Aspekte gibt es natürlich Abhilfe in Form von entsprechenden Software-Werkzeugen – sei es aus dem Portfolio der jeweiligen Linux-Distributoren, oder aber als separate Lösung von Drittanbietern. Den meisten dieser Lösungen ist jedoch gemein, daß sie entweder teuer und/oder auf ein zu kleines Einsatzgebiet beschränkt sind. Schließlich wäre es oft auch wünschenswert neben der Administration der relevanten Linux-Distributionen (Also SUSE **und** RHEL/OEL) auch andere Aspekte der Infrastruktur zu verwalten – wie z.B. die Firmware der Server oder die grundlegenden Hardware-Kennzahlen (z.B. Temperaturen oder Stromverbrauch). Last but not least ist in Unternehmen, welche viele Oracle-Produkte einsetzen (seien es Datenbanken oder auch die ursprünglich von Sun stammende Hardware) ohnehin schon ein Produkt aus der Familie des „Oracle Enterprise Managers“ im Einsatz, so daß sich zur Erreichung einer besseren Gesamtsicht auf die IT-Infrastruktur dessen Einsatz auch für betriebssystemnahe Aufgaben anbietet.

Die Oracle Enterprise Manager Produktfamilie – Einführung und Abgrenzung

Bereits seit einiger Zeit steht der Begriff „Oracle Enterprise Manager“ nicht mehr nur für ein Werkzeug zum Verwalten von Datenbanken, sondern für ein umfangreiches Gesamtframework zum Monitoring und Management einer Vielzahl von Produkten – sowohl von Oracle als auch von Drittanbietern. Dies umfasst den gesamten „Stack“ an IT-Infrastruktur – d.h. begonnen von der Applikation, über Application Server und Datenbanken, bis hinunter zu Betriebssystemen, Storage und Hardware. Durch die Übernahme von Sun ist in diesem Bereich das Produktportfolio nochmal erweitert worden, was natürlich aufgrund der ebenfalls gestiegenen Anzahl von eigenen Produkten besonders in den „unteren Ebenen des Stacks“ (also alles unterhalb des Betriebssystems) auch notwendig ist, um dem o.g. Anspruch des „Full Stack Managements“ gerecht zu werden.
Damit einhergehend gibt es nun eine – zum Glück nur auf den ersten Blick – leicht verwirrende Vielfalt unter dem Markennamen „Enterprise Manager“, welche der folgende Abschnitt kurz erläutert.
Zum einen gibt es nach wie vor die einzelnen „Product Controls“ (z.B. „Database Control“ zur Verwaltung einer einzelnen Oracle Datenbank) sowie das technisch damit enge verwandte Gesamt-Managementwerkzeug „Enterprise Manager Grid Control“. Flankiert wird letzteres nun durch das sog. „Enterprise Manager Ops Center“ (alter Name: „Sun xVM Ops Center), welches zunächst als eigenständiges Produkt weitergeführt wird.
Der unter der Marke „Oracle Enterprise Manager“ abgedeckte Gesamtzyklus an Administrationstätigkeiten sowie die grobe Aufteilung der einzelnen Ebenen des „Stacks“ zwischen Grid Control und Ops Center kann Abbildung 1 entnommen werden.
Langfristig ist natürlich ein Integration der beiden Management-Frameworks zu einem einheitlichen „Gesamt-Enterprise Manager“ geplant. Wann diese Integration genau abgeschlossen sein wird ist derzeit noch nicht bekannt – wohl aber die dreistufige Vorgehensweise in der diese vonstattengeht: Zur Zeit befinden wir uns in der mittleren Phase, die ein reines „ReBranding“ schon hinter sich gelassen hat und mittels optionaler Konnektoren zumindest die Weiterreichung und Verarbeitung von low-level (d.h. Hardware-bezogenen) Alerts von Ops Center an Grid Control ermöglicht. (Siehe dazu auch Abbildung 2)

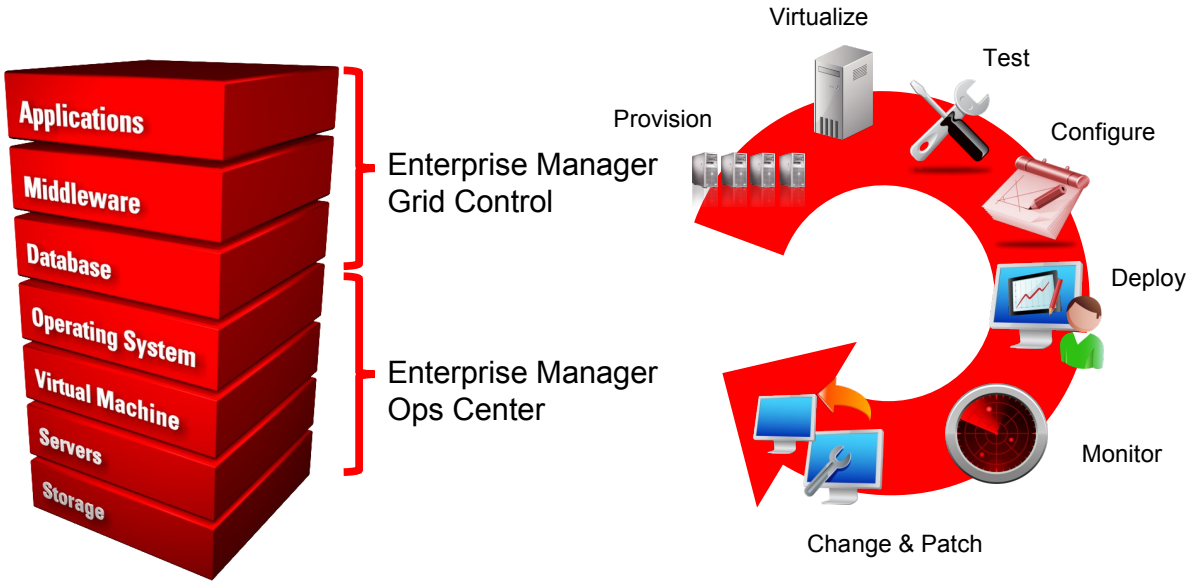

Abbildung 1: Management des gesamten Stacks "Applications to Disk" mit der Enterprise Manager Produktfamilie

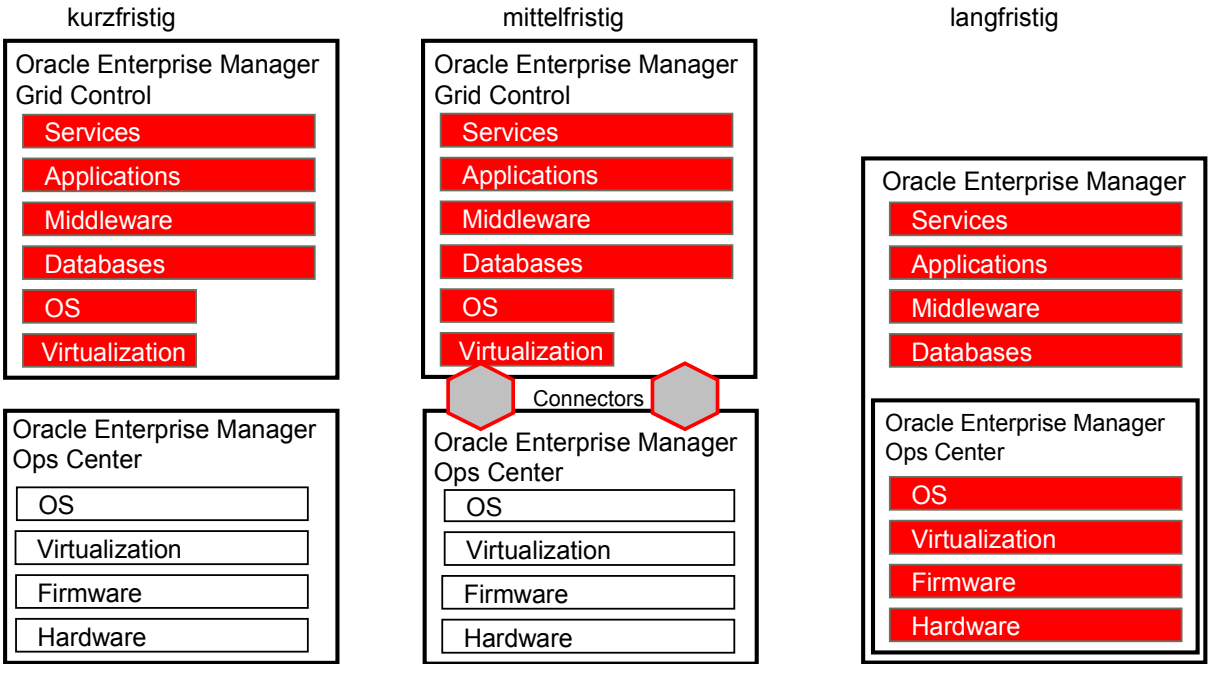

Abbildung 2: Grober Integrationsplan von Grid Control und Ops Center

Dem aufmerksamen Leser dürfte an dieser Stelle nicht entgangen sein, daß es zwischen Grid Control einerseits und OpsCenter andererseits auch ein paar Überlappungen gibt – gerade in dem Bereich „Patching und Provisioning“, um den es in diesem Vortrag geht. Als konkrete Empfehlung lassen sich daraus vereinfacht gesagt zwei Dinge ableiten: Zum einen sollten Nutzer die bereits heute die entsprechenden Features in Grid Control nutzen sich aufgrund der langfristigen Supportzeiträume bestehender Produkte (Stichwort: „Lifetime Support Policy“) keinesfalls gezwungen sehen, sofort auf Ops Center umzusteigen. Zum anderen gibt es aber aufgrund der o.g. Integrationspläne, welches für die Zukunft im Bereich Betriebsystem-Patching und -Provisioning klar die Fähigkeiten von Ops Center als „führende Features“ ausweisen, keinen Grund *neue* Vorhaben in diesem Bereich mit Grid Control anzugehen. Aus diesem Grund befasst sich dieser Vortrag im folgenden auch nicht mit Grid Control, sondern mit Ops Center.
Zum besseren Verständnis und als Abschluß dieser generellen Einführung in die Enterprise Manager Produktfamilie zeigt die folgende Tabelle einige Gemeinsamkeiten aber auch Unterschiede zwischen Grid Control und Ops Center auf:

	Enterprise Manager Grid Control	Enterprise Manager Ops Center
Oberfläche	Web GUI	Web GUI
Bezeichnung für verwaltbare Komponenten / Einheiten	Target	Asset
Bezeichnung für zentrale Instanz des Management-Frameworks	Oracle Management Server (OMS)	Enterprise Controller
Patching von Linux-Systemen	Ja	Ja
Patching von Solaris-Systemen	Nein	Ja
Patching von Windows-Systemen	Nein	Ja
Patching von Oracle-Software (z.B. Datenbanken)	Ja	Nein
Bare Metal Provisioning für Linux	Ja	Ja
Bare Metal Provisioning für Solaris	Nein	Ja
Provisioning von Oracle-Software (z.B. Datenbanken)	Ja	Nein
Administration von Oracle Datenbanken und Application Servern	Ja	Nein
Verwaltbare Virtualisierungsschichten	Oracle VM (x86)	Oracle VM (SPARC) (=ehem. LDoms); Solaris Zonen/Container

Patching von Linux mit Oracle Enterprise Manager Ops Center

"Historisch gesehen" interessant zu wissen ist, daß Ops Center im Kern die Weiterentwicklung eines (damals noch von Sun) übernommenen Spezialwerkzeugs eines israelischen Softwareunternehmens zum Patching von Linux-Systemen ist. Dies erklärt auch die starke Kompetenz in diesem Bereich, um den es ja in diesem Vortrag geht. Die Basis dieser Funktionalität ist eine umfangreiche von Oracle gepflegte Wissens-Datenbank, welche die Vielzahl der Patches und Releases für die unterstützten Zielsysteme im Detail kennt – inkl. deren Abhängigkeiten, deren Historie sowie den Sicherheitslücken oder Bugs welche diese beheben. Zusammen mit damit verbundenen fortgeschrittenen Analysen, welche über die bereits eingangs genannten Limitationen einer rein technischen Paketabhängigkeitsprüfung hinausgehen, ist es dadurch möglich, bereits VOR dem eigentlichen Einspielen von Patches zu wissen, wie die entsprechenden Systeme danach im Endergebnis aussehen werden bzw. ob eine Gesamtmenge an Patches überhaupt erfolgreich eingespielt werden kann, ohne sich womöglich als indirekte Folgen schwer zu behebende Probleme einzuhandeln. Die folgende Abbildung verdeutlicht schematisch die Funktionsweise dieser Wissensdatenbank.

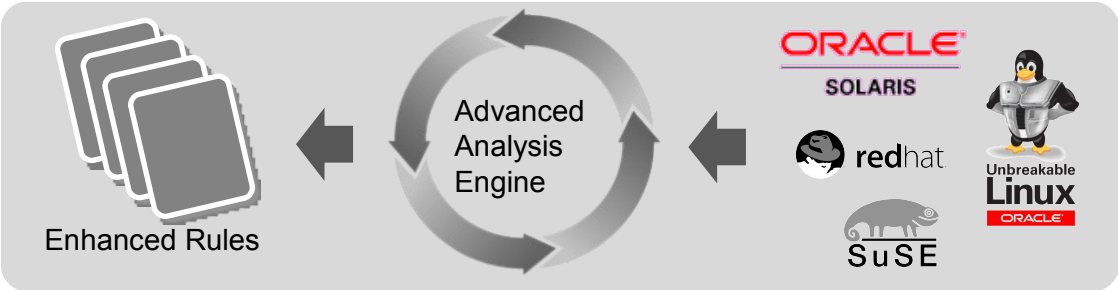

Abbildung 3: Intelligente "Knowledge Base" als Basis für Patching in Ops Center

Normalerweise erfolgt der Zugriff auf diese Wissensdatenbank online, aber für Umgebungen in denen kein direkter Internetzugriff gewünscht oder möglich ist, gibt es alternativ auch einen "disconnected mode".

Der konkrete Ablauf beim Einspielen von Patches oder Updates wird in Ops Center über "Profiles" und "Policies" geregelt:
"Profiles" geben dabei an, WAS zu installieren bzw. zu patchen ist. Bereits direkt mitgeliefert werden Profile für gängige Anwendungs-Szenarien (z.B.: "Alle Sicherheitspatches einspielen", "Alle Bugfixes einspielen", etc.) Selbstverständlich können diese Profiles auch angepasst oder für eigene Anforderungen auch neue erzeugt werden.
"Policies" schließlich sind Regeln, die bestimmen WIE etwas zu installieren oder zu patchen ist bzw. welche Besonderheiten dabei ggf. einzuhalten sind. Dies beginnt bei einfachen Anforderungen wie z.B. dem Rebooten einer Maschine nach Einspielen eines Patchs und endet bei hierarchisch einstellbaren Vorgaben, die das Rollout von Patches auch für "Sonderfälle" bestimmen. (Ein Beispiel für letzteres wäre z.B. die Vorgabe, daß auf Ebene der gesamten Maschine zwar alle neuen Patches eingespielt werden können, aber für eine bestimmte Komponente/eine bestimmte Anwendung auf diesem Server dies nicht erlaubt ist.)

Ergänzt wird die Patching-Funktionalität im Ops Center durch umfangreiche Reports, die für jedes verwaltete System ausgeführt werden können, einschließlich Berichte über sog. Common Vulnerability and Exposure Identifiers (CVE IDs) – letztere können dann natürlich auch direkt als Basis zum Einspielen der jeweiligen Security-Fixes für die einzelnen CVE IDs benutzt werden.
In der Oberfläche werden diese Reports über die generell in Ops Center verwendeten Kontext-abhängige Aufgaben („Actions“) auf der rechten Seite ausgelöst (siehe dazu auch exemplarisch den Bildschirmausschnitt in der Abbildung rechts.)

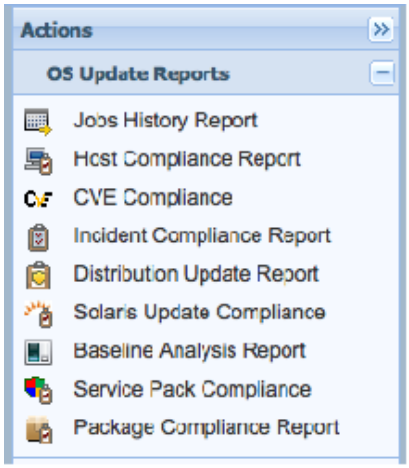

Abbildung 4: Screenshot (Ausschnitt) - Verfügbare Reports für OS Updates / Patching

Bare Metal Provisioning von Linux mit Oracle Enterprise Manager Ops Center

Das automatisierte Aufbringen von Linux-Betriebsystemen durch auf „nackte Hardware“ („Bare Metal Provisioning“) erfolgt durch die in diesem Umfeld bekannten Mechanismen des Netzwerk-basierten Bootvorgangs. Erfreulicherweise übernimmt Ops Center hier die initiale Grundkonfiguration der notwendigen Infrastruktur (d.h. PXE-Boot mittels DHCP und TFTP).
Pro Subnetz, in dem man Provisionierungsvorgänge durchführen möchte muss lediglich sichergestellt sein, daß dort ein sog. „Proxy Controller“ läuft der die entsprechende DHCP-Funktion wahrnehmen bzw. konfigurieren kann (siehe dazu auch die schematische Darstellung in Abbildung 5.) Im einfachsten Fall, d.h. der Installation in einem einzigen Subnetz, kann der Proxy Controller auf der gleichen Maschine laufen auf der auch die zentrale Instanz von Ops Center selbst läuft (der sog. „Enterprise Controller“ - vergleichbar in etwa mit dem „Oracle Management Server“ bei Grid Control.)

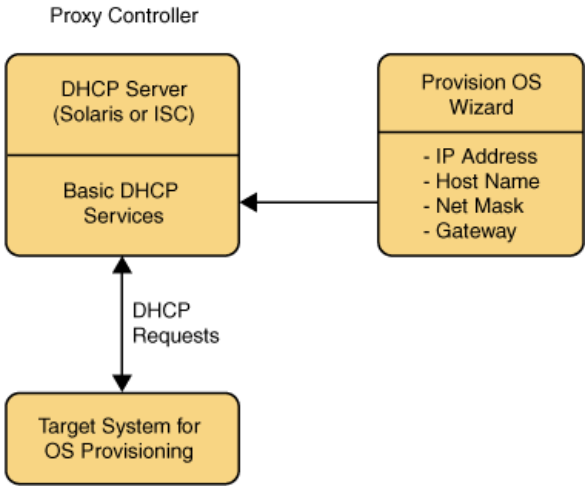

Abbildung 5: Schematische Darstellung der Rolle des "Proxy Controllers" beim Bare Metal Provisioning

Abgesehen von der gerade genannten Basis-Infrastruktur werden für das eigentliche Provisioning pro auszurollendem System zwei Bausteine benötigt: Zum einen ein sog. „OS Image“, welches entweder heruntergeladen oder z.B. von einer Linux-Installations CD oder DVD stammen

kann, zum anderen ein sog. „OS Profile“, welches bestimmt, wie ein bestimmtes Image letztlich zu einem fertig konfigurierten Linux-System wird. Bei jedem Import eines „OS Images“ wird zwar schon ein Default „OS-Profile“ erstellt, aber dieses muß in aller Regel natürlich noch angepasst werden. Zu diesem Zweck kann man in jedem „OS Profile“ eine Vielzahl von Parametern deklarativ festlegen, welche dann automatisiert (über die jeweiligen Mechanismen der Distribution, also Kickstart oder AutoYAST) während des Deployments zur Anwendung kommen. Im einzelnen sind dies z.B.:

- Spracheinstellungen
- root-Passwort
- Festplattenlayout (Partitionierungsvorgaben)
- Paketauswahl
- (optionale) Konfiguration des Systems als NIS- oder LDAP-Client
- (optionale) zusätzliche Skripte, welche nach der Installation ausgeführt werden sollen

Sobald die gewünschen „OS Images“ und „OS Profiles“ importiert bzw. erstellt wurden, kann der Provisionierungsvorgang für ein oder mehrere Systeme angestossen werden. Zuvor sollte naheliegenderweise natürlich noch sichergestellt sein, daß der oder die gewünschten Ziel-Server auch überhaupt grundsätzlich als „Asset“ in Ops Center bekannt sind. (Falls nicht, muß erst ein entsprechendes „Discovery“ durchgeführt werden.) Sollte auf der Ziel-Hardware für das zu provisionierende System bereits ein anderes („altes“) Linux laufen welches nun ersetzt werden soll, ist außerdem das System Monitoring für das entsprechende Ziel auszuschalten. (Ansonsten würde es im Ops Center während des Provisionierungsvorgangs zu Warnungen/Fehlermeldungen für das entsprechende „alte“ System kommen.)
Wie die meisten anderen Tätigkeiten in Ops Center wird der Provisionierungsvorgang durch einen entsprechenden „Wizard“ begleitet bzw. gestartet. Neben den naheliegenden Parametern welche dann zusammen mit dem ausgewählten „OS Profile“ das Betriebssystem konfigurieren (wie z.B. gewünschte Netzwerk-Konfiguration oder dem Host-Namen) kann hier auch noch bestimmt werden, daß das „frische“ System sich auch gleich selbst bei Ops Center registrieren soll, um dann von dort aus verwaltet werden zu können.

Kontaktadresse:

Manuel Hoßfeld
Oracle Deutschland B.V. & Co. KG
Robert-Bosch-Str. 5
D-63303 Dreieich

Telefon: +49 (0) 6103 397-494
Fax: +49 (0) 6103 397-111
E-Mail manuel.hossfeld@oracle.com
Internet: www.oracle.com/de