Neues von der ORACLE Identity Governance Suite

Dr. Stephan Hausmann
ORACLE Deutschland B.V. & Co. KG
Hamborner Straße 51, 40472 Düsseldorf

Schlüsselworte
Identity Governance Suite, Identity Manager, OIM, Identity Analytics, OIA, Privileged Account Manager, OPAM, User-Life-Cycle, Role-Life-Cycle, 11gR2PS1

Einleitung

Die Oracle Identity Governance Suite erlebt eine stetige Weiterentwicklung zu einer immer tiefer integrierten Gesamtlösung während sich die einzelnen Komponenten immer weiter entwickeln und weiterhin einzeln verwendet werden können. Im Rahmen des DOAG Vortrages werden die aktuellen Neuerungen vorgestellt. Weitere Informationen zur Oracle Identity Governance Suite finden sich unter http://www.oracle.com/identity

Identity Governance Suite im Überblick

Die Identity Governance Suite besteht aus den drei Komponenten Oracle Identity Manager, Oracle Identity Analytics und Oracle Privileged Account Manager. Damit deckt Identity Governance die Themenbereiche User Provisioning, Access Request, Self-Service, Role-Lifecycle Management, Identity Intelligence, Re-Zertifizierungen, SoD und privilegiertes Account Management ab.

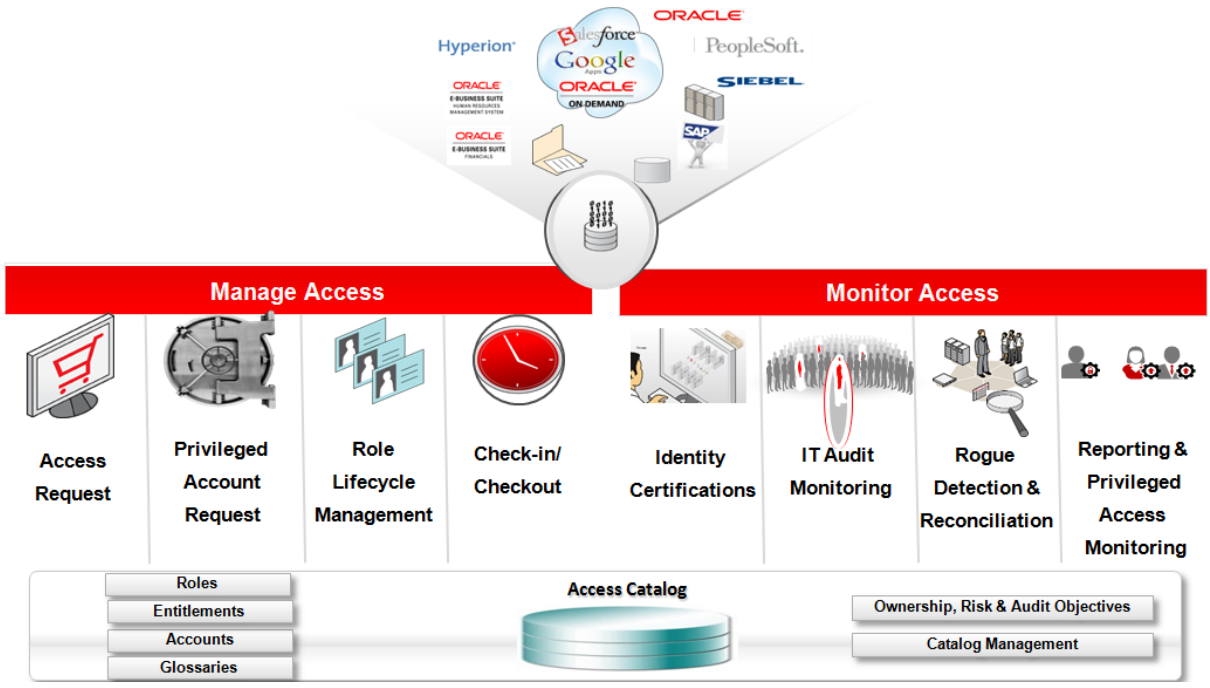

Abb. 1: Überblick über die Themen der Oracle Identity Governance Suite

Privileged Account Management

Der Privileged Account Manager (OPAM) ist die neuste Komponente und hat zur Aufgabe den nachvollziehbaren Zugriff auf privilegierte Accounts (z.B. SYS bei der Datenbank oder root bei einem UNIX System) zu ermöglichen. Berechtigte Benutzer können sich Accounts „auschecken“ (Abbildung

2), wenn sie den Zugriff auf einen privilegierten Account benötigen. Dabei wird für den privilegierten Account ein neues Passwort gesetzt, welches nur dem Benutzer zugänglich ist, um sicher zu stellen, dass nur dieser Benutzer eine neue Verbindung öffnen kann. Wenn der Benutzer den Zugang nicht mehr benötigt, so wird das Passwort auf einen allen Benutzern unbekannten Wert gesetzt. OPAM nutzt dabei die vorhandenen Konnektoren der Governance Suite, um das Passwort für die privilegierten Accounts zu setzten. Da immer nur ein Benutzer Zugang zu einem privilegierten Account erhält kann nachvollzogen werden, wer sich wann auf welchem System angemeldet hat.

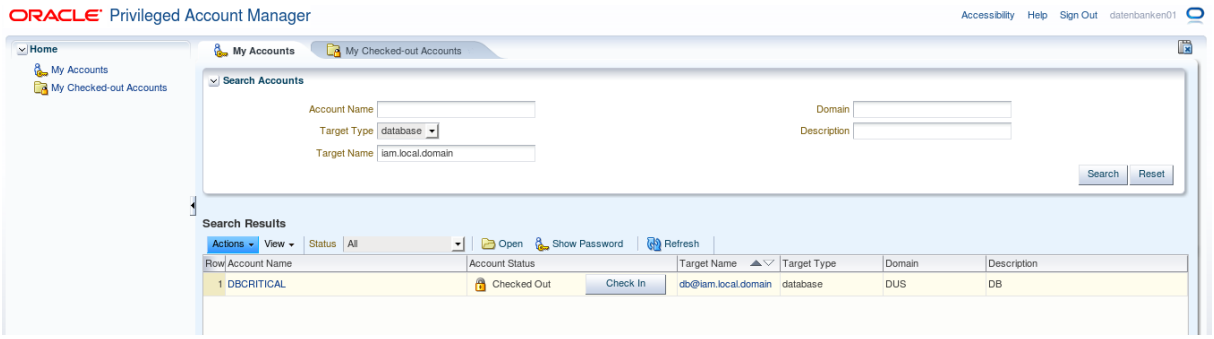

Abb.2: Interface für den Zugang zu privilegierten Accounts mit dem Oracle Privileged Account Manager

Der Zugang zu einem privilegierten Account kann über den Identity Manager beantragt werden, so dass nicht nur nachvollziehbar ist wann jemand einen privilegierten Account verwendet hat, sondern auch warum er das durfte - es liegt ein Antrag mit Genehmigung vor. In Abbildung 2 ist das Interface für einen End-Anwender gezeigt, der einen privilegierten Account „ausgecheckt“ hat.
Es besteht auch die Möglichkeit per Skript den Zugang zu einem privilegierten Account zu erhalten – dazu wird dann ein REST Interface eingesetzt. Da es in der Natur von Skripten liegt, dass mehrere Skripte den gleichen privilegierten Account verwenden und dann das Passwort des privilegierten Accounts nie geändert wird (werden kann), ist es hier mit OPAM möglich, dass zwar mehrere Skripte gleichzeitig einen privilegierten Account gleichzeitig verwenden, aber das Passwort von OPAM gewechselt wird, wenn kein Skript den privilegierten Account aktuell verwendet. Wenn mehrere Skripte gleichzeitig einen privilegierten Account verwenden dürfen ist die Nachvollziehbarkeit natürlich eingeschränkt.

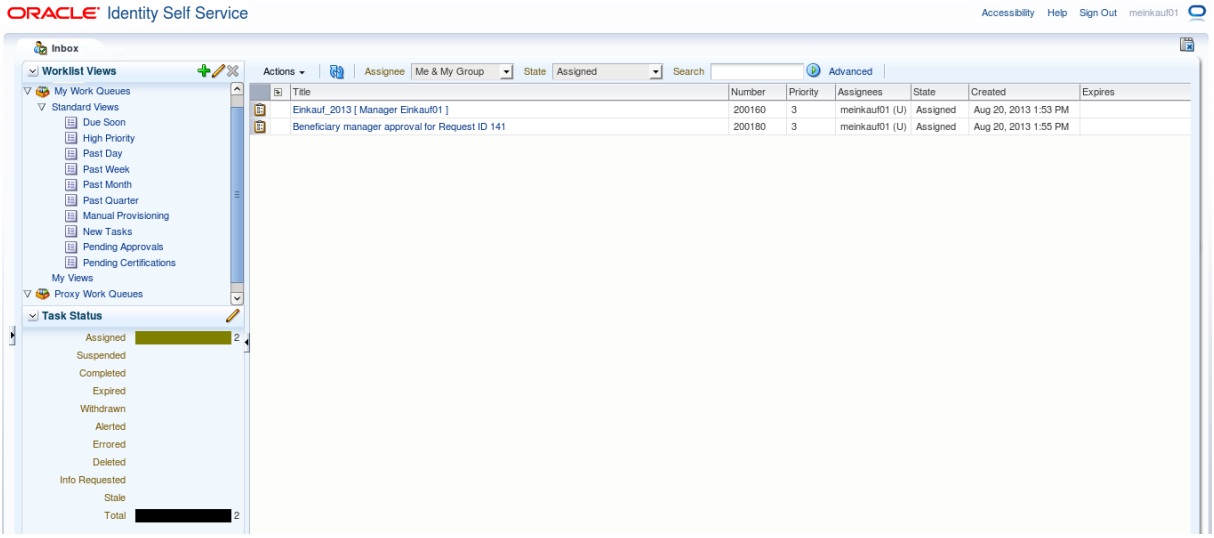

Abb.3: Genehmigungen und Re-Zertifizierungen in einer Inbox

Re-Zertifizierung
Während der DOAG 2012 wurde gezeigt, wie das neue Antragsverfahren im Oracle Identity Manager aussieht. Inzwischen ist auch die Re-Zertifizierung neu aufgelegt worden: Es bietet mehrstufige Re-Zertifizierungen, das Antragswesen ist integriert und für Manager oder fachlich Verantwortliche sind alle wesentlichen Funktionen in einem Interface vereint. Dies erstreckt sich über eine einheitliche Inbox mit Anträgen, Re-Zertifizierungen und weiteren Aufgaben bis hin zur Einsehbarkeit der ursprünglichen Anträge für die Berechtigungen im Rahmen der Re-Zertifizierung.

In Abbildung 3 ist die vereinheitlichte Inbox zu sehen, in der alle Aufgaben direkt einsehbar sind. Es besteht die Möglichkeit sich eigene Darstellungen bzw. Prioritäten der Aufgabenliste zu erzeugen und die eigene Aufgabenliste kann für andere Personen sichtbar gemacht werden.
Die Re-Zertifizierung wird wie gehabt mit grafisch aufbereiteten Risikofaktoren unterstützt und ermöglichen so der Fachseite oder dem Manager schnell Auffälligkeiten zu erkennen und darauf zu reagieren. Durch die Integration mit dem Antragswesen ist auch direkt abrufbar durch welchen Antrag ein Anwender eine bestimmte Berechtigung erhalten hat. Der Re-Zertifizierende erhält so zusätzliche Informationen über die Identitäten und deren zugeordnete Berechtigungen.

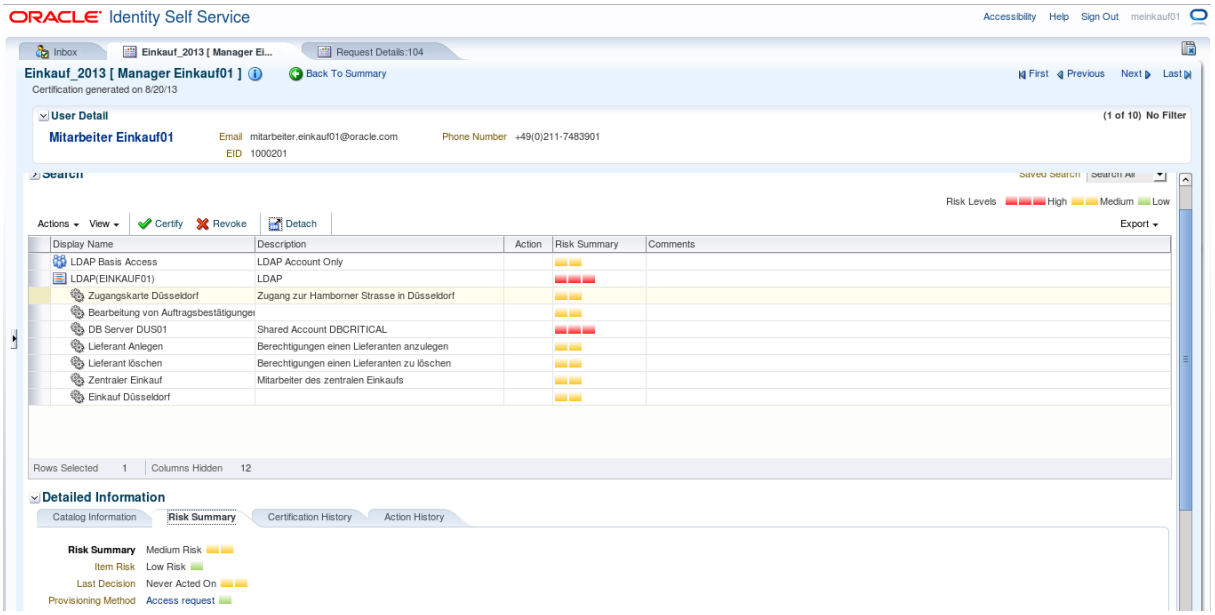

Abb.4: Re-Zertifizierung in einer Oberfläche mit dem Antragswesen – aus den Berechtigungen für eine Re-Zertifizierung kann direkt auf die Anträge für die Berechtigungen zugegriffen werden.

Eine der wichtigsten Neuerungen ist die Unterstützung von mehrstufigen Re-Zertifizierungen. Dadurch wird es möglich, dass Fachabteilung bzw. Manager und technische Spezialisten gemeinsam die Zertifizierung durchführen. Das kann z.B. so aussehen, dass die Re-Zertifizierung von der Fachabteilung durchgeführt wird und ja nach Berechtigung/System die Spezialisten die Re-Zertifizierung durchführen. In einem abschließenden Review Schritt kann die Fachseite bzw. der Manager Abweichungen in den beiden Re-Zertifizierungen erkennen und die so entstanden Konflikte auflösen. Dies ist in Abbildung 5 gezeigt. Dieses Vorgehen kann z.B. dann relevant sein, wenn aus den Berechtigungen nicht direkt erkennbar ist, dass sie für die Aufgaben des Mitarbeiters notwendig sind, aber durch die technische Implementierung auf den Systemen erforderlich sind – welche nur den technischen Spezialisten verständlich sind.
Eine weitere Neuerung ist die Möglichkeit Re-Zertifizierungen offline zu bearbeiten. Die Re-Zertifizierungen können in MS Excel heruntergeladen werden, offline bearbeitet werden und

abschließend wieder auf den Server hochgeladen werden. Dabei sind auch Mischformen möglich, dass z.B. die Re-Zertifizierung online angefangen wird, dann heruntergeladen wird und offline weiter bearbeitet wird, danach hochgeladen wird und dann online weiter bearbeitet wird.

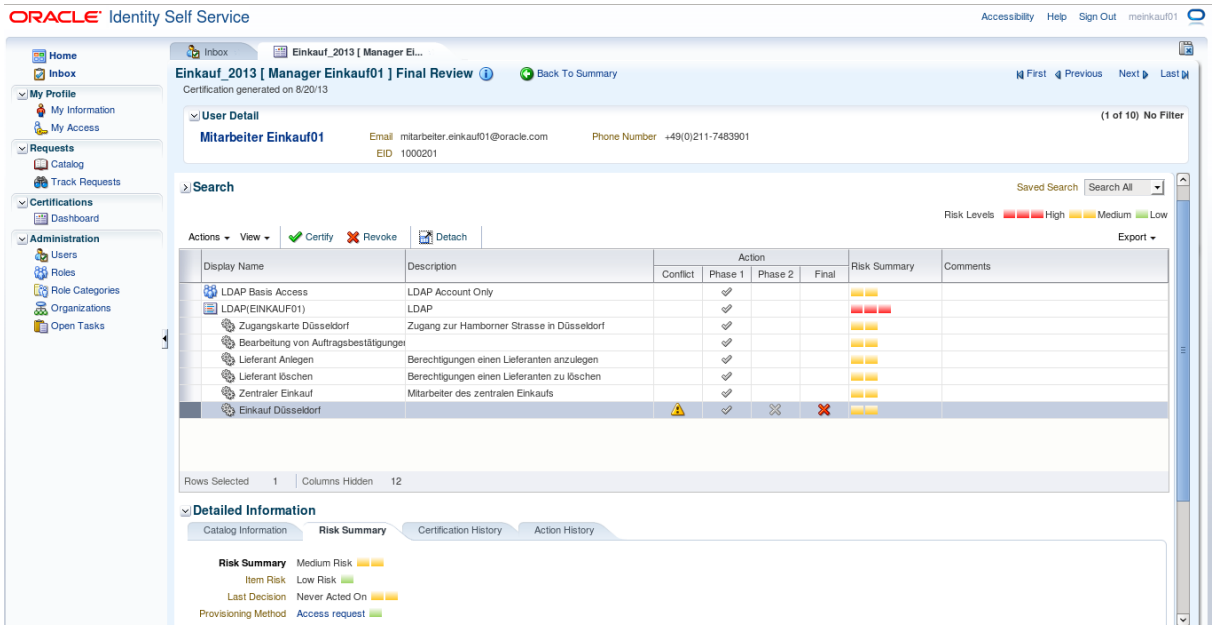

Abb. 5: Final Review und Konflikterkennung bei einer Mehrstufigen Re-Zertifizierung.

Fazit

Die Oracle Identity Governance Suite entwickelt sich stetig weiter und bieten mit jeder neuen Version Neuerungen, die es den Fachseiten erleichtern ihre Aufgaben effizienter zu erledigen. Mit Version 11gR2 PS1 ist vor allem die Re-Zertifizierung modernisiert worden und tiefer mit dem Antragswesen für Berechtigungen integriert. Im Rahmen des DOAG Vortrages wird auch auf weitere Neuigkeiten eingegangen.

Kontaktadresse:

Dr. Stephan Hausmann
ORACLE Deutschland B.V. & Co. KG
Hamborner Straße, 51
D-40472 Düsseldorf

Telefon: +49 (0) 211-74839-775
Fax: +49 (0) 211-74839-222
E-Mail stephan.hausmann@oracle.com
Internet: www.oracle.com/identity