Identity-Management für Datenbanken

Karsten Müller-Corbach, ORACLE Deutschland GmbH

Compliance-Vorschriften wie SOX oder Basel II zwingen ein Unternehmen zur Beantwortung von Fragen wie „Wer hat(te) welches Recht, wann und in welcher Datenbank-Instanz?".

Die Verwaltung von Identitäten in Datenbanken stellt eine große Herausforderung an DBAs. Identity-Management für Datenbanken ist ein Ansatz, um diese Arbeit zu vereinfachen und Unternehmen zu ermöglichen, Compliance-Vorschriften einzuhalten.

Benutzer von Datenbanken und Applikationen können sowohl in Form von direkten Datenbank-Accounts und Proxy-Usern angelegt sein, die eigenständig auditierbare Sessions in der Datenbank öffnen, oder als Applikationsbenutzer, für die Fälle, in denen eine Applikation über einen Service-User mit der Datenbank kommuniziert und ihre eigene Benutzerverwaltung in einer Datenbank-Tabelle pflegt und für die Authentifizierung verwendet.

Administratoren müssen Benutzer-Informationen auf dem neuesten Stand halten und sicher für das gesamte Unternehmen zur Verfügungen stellen. Diese Aufgabe wird dadurch erschwert, dass die Zahl der Anwendungen und Benutzer ständig ansteigt. Jeder Benutzer hat mehrere Konten auf unterschiedlichen Datenbanken, was dazu führt, dass sich jeder Benutzer mehrere Passwörter merken muss. Durch den Zugriff von Tausenden von Benutzern auf Datenbank-Konten müssen Administratoren erhebliche Ressourcen zur Benutzerverwaltung ver(sch)wenden.

Die Verwaltung von Identitäten besteht aus Tätigkeiten wie Erstellen, Ändern oder Löschen von Benutzern, Vergabe von Rollen und dem Zurücksetzen von Passwörtern. Diese Tätigkeiten stellen DBAs vor aufwändigen Einsatz von manuellen Handlungen. Zudem produzieren diese Bedingungen Sicherheitsprobleme wie zum Beispiel:

- Bei einem Wechsel eines Mitarbeiters sind die entsprechenden Accounts zu entfernen oder zu deaktivieren
- Wenn sich ein Anwender zu viele Passwörter merken muss, fängt er an, diese auf Papier zu schreiben und unter seiner Tastatur aufzubewahren
- Temporäre Zugriffsrechte durch Vertreter-Regelungen oder externe Mitarbeiter werden meistens nie wieder entzogen beziehungsweise in zeitlichen Intervallen hinterfragt und neu beglaubigt

Alle diese Punkte können von einem Identity-Management adressiert werden. Dieses Identity-Management für Datenbanken kann in Form von Enterprise User Security oder Identity-Provisionierung erfolgen.

Identity-Management mit Enterprise User Security

Das Konzept der Enterprise User Security (EUS) integriert das native Konzept aus der Datenbankwelt. Der Einsatz von EUS hebt die strenge Kopplung zwischen Datenbank-Benutzer und Datenbank-Schema auf. Die Benutzer werden zusammen mit ihren individuellen Privilegien und Rollen zentral in einem LDAP-Verzeichnis verwaltet und beliebigen Datenbank-Schemata (shared schema) auf unterschiedlichen Datenbanken zugeordnet. Neben dem Oracle Internet Directory (OID) kann auch das Oracle Virtual Directory (OVD) zum Einsatz kommen. Die Kombination von OVD in Verbindung mit einem beliebigen LDAP-Verzeichnis und EUS ist mit Oracle 10*g* (oder höher) möglich.

Ein Vorteil der Enterprise User Security besteht darin, dass die Benutzer-Rechte zentral an einer Stelle (im LDAP-Verzeichnis) gepflegt werden. Dieses zentrale Verzeichnis wird von mehreren Datenbanken genutzt. Eine aufwändige Mehrfachpflege von Benutzer-Informationen entfällt. EUS hat jedoch folgende Einschränkungen (siehe Metalink Note 272196.1, Step By Step Guide To Configuring 10*g* Password Authenticated Enterprise User Security):

- Es ist limitiert auf Datenbank-Benutzer
- Die endgültigen Rechte eines Benutzers setzten sich zusammen aus seinen individuellen Rechten sowie den allgemeinen Rechten des Schemas, gegen das er jeweils gemappt wird. Dies erschwert die Verwaltung
- Das für EUS notwendige LDAP-Verzeichnis muss hochverfügbar aufgebaut sein, um Ausfälle bei Datenbank-Anmeldungen auszuschließen
- Audits und Reports über Datenbank-Benutzer sind nicht „out-of-the-box" in EUS enthalten
- Temporäre Zugriffsrechte, Genehmigungsworkflows etc. sind nicht Teil von EUS

Eine Alternative zu EUS ist die direkte Identity-Provisionierung über den Oracle Identity Manager oder die Provisionierung von EUS-Benutzern in das LDAP-Verzeichnis.

Identity-Management mit Oracle Identity Manager

Oracle Identity Manager (OIM) ist ein mächtiges und flexibles Identity-Management-System für Unternehmen. Es erlaubt die automatisierte Verwaltung von Benutzern auf IT-Systeme eines Unternehmens. Seine flexible Architektur – basierend auf den etablierten Standards von J2EE – gestattet die Handhabung restriktiver Sicherheitsanforderungen, die aus IT- oder Geschäftsprozessen hervorgehen. OIM gliedert sich in die bestehende Systemlandschaft ein und übernimmt schrittweise den Anwendungsverwaltungsprozess.

OIM wurde für die Anlage von Anwenderkonten sowie für die Verwaltung der Zugriffsrechte konzipiert, um den Anwenderlebenszyklus über alle IT-Systeme einer Organisation hinweg zu steuern. OIM speichert alle Identitäten, Prozesse und Konfigurationsdefinitionen in einem separaten Daten-Repository in Form einer relationalen Datenbank. Als Datenbank-System für den Identitätsspeicher kommt eine Oracle-Datenbank zum Einsatz.

Der Unterschied zu EUS besteht in der direkten Provisionierung von Benutzern und Berechtigungen. OIM greift nicht in die Architektur der Datenbank-Authentisierung ein. Ein Datenbank-Benutzer wird vom OIM direkt in der definierten Datenbank-Instanz erstellt und verwaltet. Alle benötigten Datenbank-Rollen werden abhängig von unternehmensweiten Businessrollen-Schemata in der Datenbank für den Benutzer hinzugefügt. OIM bietet folgende Vorteile:

- OIM provisioniert sowohl Datenbank- als auch Applikations-Benutzer
- Benutzer erhalten nur die Datenbank-Rollen, die ihnen über ein unternehmensweites Businessrollen-Schema zugewiesen wurden
- OIM muss nicht hochverfügbar sein, da es nicht für Datenbank-Anmeldungen genutzt wird
- OIM verfügt über integrierte Audits und Reports über Datenbankbenutzer. Ein „Wer hat(te) was, wann, in welcher Datenbankinstanz?"-Report kann „out-of-the-box" angezeigt werden
- OIM bietet die Möglichkeit, Compliance-Vorschriften über Beglaubigungsvorgänge von Datenbank-Benutzern einzuhalten
- OIM unterstützt Reconciliation (Abgleich) von Datenbank-Feldern pro Benutzer wie Login, Tablespace, Profil oder Rolle
- OIM bietet Self-Service und Passwort-Management für Datenbank und andere Applikationen

In einer typischen Architektur wird OIM mit Identitäten aus einem führenden Quell-System befüllt. In der Abbildung enthält ein HR-System die

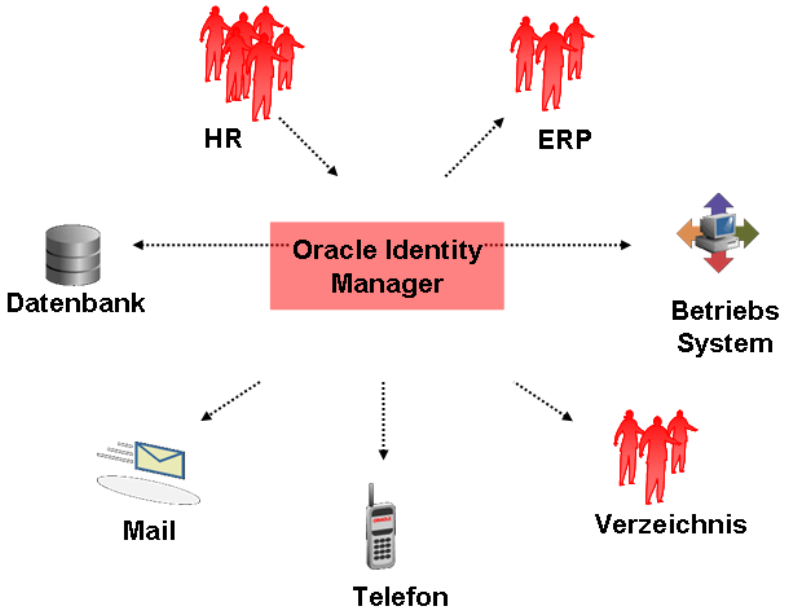

Abbildung 1: OIM-Architektur

Benutzeridentitäten in Form von Personalstammdaten. Diese werden von OIM eingelesen und dort als Unternehmensidentität abgelegt. Rollen und Regeln in OIM entscheiden über die automatische Provisionierung von Benutzerkonten in Applikationen und Datenbanken.

Reporting und Beglaubigung für Datenbank-Benutzer

Zusätzlich zum Provisionieren unterstützt OIM auch das Abgleichen von Datenbanken. Bestehende Datenbanken können nach Benutzern abgesucht werden, der Vorgang läuft pro Datenbank-Instanz. Die gefundenen Datenbank-Benutzer werden durch Mapping-Regeln ihren Unternehmensidentitäten im OIM zugeordnet. Der Reconciliationprozess sammelt pro Datenbank-Instanz für jeden Benutzer die Datenbank-Felder und speichert diese ab. Das Reporting des OIM zeigt diese Informationen an. OIM enthält 35 Reports, die operative oder historische Daten ausgeben können. Das Reporting in OIM lässt sich über Stored Procedures erweitern, wodurch eigene, angepasste Compliance Reports erstellt werden können. Ebenso ist es möglich, das Datenmodell über ein externes Reportingtool, wie BI Publisher, anzusteuern und das Reporting automatisiert zu betreiben. OIM unterstützt das Einhalten von Compliance-Vorschriften durch die Beglaubigung (Attestation) von angebundnen IT-Systemen und Datenbanken.

Compliance Vorschriften sehen vor, dass Beglaubigungsvorgänge in regelmäßigen Abständen durchgeführt werden. Nur so kann nach manuellen Änderungen beispielsweise durch einen

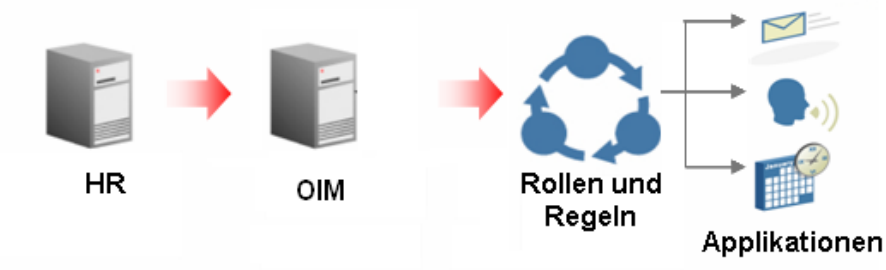

Abbildung 2: OIM-Architektur mit Rollen und Regeln

Abbildung 3: Reporting durch OIM

genehmigten Antrag nachvollzogen werden, ob Ressourcen oder Berechtigungen noch aktuell sind und ob die definierten Provisionierungsprozesse einwandfrei funktionieren. OIM beinhaltet zudem Beglaubigungsvorgänge für einen Manager, welche Benutzerkonten und Berechtigungen einem Anwender zustehen.

Self-Service und Passwort-Management für Datenbanken

Der Self-Service von OIM ermöglicht nicht nur die Änderung von Profil-Informationen eines Anwenders, sondern auch das Passwort-Management. Ein Anwender kann über den OIM sein Passwort ändern. Diese Passwort-Änderung kann sich auf alle angeschlossen IT-Systeme und Datenbanken synchronisieren. Zusätzlich kann der Self-Service gezielt Passworte durch den Anwender in Datenbanken zurücksetzen.

Ebenso enthält OIM die nötigen Funktionen, ein Passwort-Reset, das mit Challenge Response gesteuert wird, umzusetzen, sollte ein Anwender sein Passwort vergessen haben.

Fazit

Datenbank-Security ist ein ganzheitliches Thema. Die Datenbank bietet dabei selbst viele Security-Dienste. Eine zentrale, datenbankübergreifende Benutzerverwaltung ist für DBAs vor dem Hintergrund von Compliance und Benutzer-Lebenszyklen heute eine Herausforderung. Der Mehrwert eines Tools wie dem Oracle Identity Manager ist eine reibungslose und vor allem sichere Anbindung an andere Unternehmensprozesse, Corporate-Identity-Management-Systeme beziehungsweise Directories und dadurch auch die Anbindung heterogener Infrastrukturen. Die weiteren Reporting- und Beglaubigungsfunktionen runden dieses Angebot ab.

Kontakt:
Karsten Müller-Corbach
karsten.mueller-corbach@oracle.com