Oracle Identity Analytics – Das Compliance Werkzeug für Berechtigungen

Dr. Stephan Hausmann
ORACLE Deutschland B.V. & Co. KG
Düsseldorf

Schlüsselworte:

Oracle Identity Analytics, Compliance, Zertifizierung, Attestierung, SoD, Funktionstrennung, Rollen, Access Governance, Identity Intelligence

Einleitung

Viele Unternehmen stehen heute vor der Herausforderung, dass sie hohe Aufwände bei der Umsetzung von Compliance Vorgaben haben. Zum Beispiel muss vielfach nachgewiesen werden „*Wer hat welche Berechtigungen?*“, so dass dann aus den Systemen die Berechtigungsdaten exportiert werden und aus diesen Informationen - häufig manuell - die Informationen für externe Prüfer zusammengetragen werden. Analog wird verfahren, wenn die Berechtigungen im Rahmen von „*Zertifizierungen*“ – also dem regelmäßigen Überprüfen von Berechtigungen durch Vorgesetzte – durchgeführt werden. Dazu kommt im Falle der Zertifizierung noch das Verteilen der Aufgaben für die einzelnen Vorgesetzten und natürlich das Einsammeln, Konsolidieren und Auswerten der bearbeiteten Zertifizierungen. Diese manuellen Prozesse sind zeitintensiv, unübersichtlich und fehleranfällig.

Ziel dieses Artikels ist es, eine kurze Einführung in ein Werzeug (Oracle Identity Analytics) zu geben, welches die Fachverantwortlichen bei der automatisierten Umsetzung von Compliance Vorgaben unterstützt. Hierzu werden die Bereiche

- Konsolidierung von Berechtigungen
- Durchführung einer Zertifizierung aus Fachanwendersicht

schwerpunktmäßig dargestellt.

Oracle Identity Analytics (OIA) ist ein Werkzeug, welches Unternehmen bei der Umsetzung ihrer Compliance Vorgaben im Berechtigungsumfeld unterstützt. Funktionen wie die Korrelation, Analyse und Bereinigung von Account/Berechtigungsdaten bilden die Basis. Darauf aufbauend können die Verantwortlichen für Accounts in den Systemen identifiziert werden und verwaiste Konten ("Accountleichen") aufgespürt werden. Vorgefertigte Reports ermöglichen Antworten auf die Frage „Wer hat welche Berechtigungen?“ quasi auf Knopfdruck. Umfangreiche Funktionen zum Aufspüren (Role-Mining) und Verwalten (Role Life-Cycle Management) von Rollen ermöglichen einen hybriden Ansatz für die Erstellung eines RBAC konformen Rollenkonzeptes.

Konsolidieren der Berechtigungen

Vor der Analyse und Auswertung der Berechtigungen müssen zuerst alle Informationen zusammengeführt werden. Es hat sich oft als hilfreich erwiesen, drei verschiedene Arten von Informationen zu betrachten.

Personendaten

Unter Personendaten verstehen wir interne und externe Mitarbeiter. Die Informationen für interne Mitarbeiter stehen im Allgemeinen über das Personalsystem zur Verfügung. Für externe Mitarbeiter findet sich häufig auch ein System aus welchem diese Daten bezogen werden können. Besonders interessant sind dabei die folgenden Daten:

- Name, E-Mailadresse
  Diese Informationen werden benötigt, um die Mitarbeiter per E-Mail zu informieren und korrekt ansprechen zu können.

- Vorgesetzte (bzw. Verantwortliche bei externen Mitarbeitern)
  Diese Information wird benötigt, um bei Zertifizierungen die zu zertifizierenden Personen den richtigen Vorgesetzten zuzuordnen und um bei Eskalationen die nächste Eskalationsstufe zu identifizieren

- Aufgabenbezeichnung, Jobcodes, Standort
  Für das Auffinden von Rollen (Role-Mining) ist es sehr hilfreich, neben den Berechtigungsinformationen Zugriff auf Personaldaten zu haben, die das Aufgabenfeld der Personen beschreiben.

- Zuordnung zu Organisationen, Abteilung
  Die Organisationsinformationen dienen zum einen einer möglichen Aufteilung der Zertifizierungen und zum anderen unterstützen sie das Role-Mining, da i.A. innerhalb einer Abteilung häufig identische/ähnliche Aufgabenbereiche zu finden sind. Unter dem Begriff Organisation können neben der Aufbauorganisation auch Projektstrukturen o.ä. verstanden werden. Mehrere parallele Organisationen (Matrixorganisation) sind möglich.

- Informationen, die einen Korrelation zu Accounts ermöglichen
  Dies können z.B. Personalnummer, intern verwendete Schlüssel, etc. sein. Dazu ist im Vorfeld eine Sichtung der Account Daten notwendig.

Accounts

Bei den Accounts werden die Berechtigungen und alle Informationen betrachtet, die eine Korrelation zu den Personendaten ermöglichen. Generell ist es hilfreich, alle Daten zu laden, die für einen Account zur Verfügung stehen.

Organisationsdaten

Hier wird in den meisten Fällen die Aufbauorganisation betrachtet.

Vorgehensweise beim Laden der Daten

Im ersten Schritt werden die Personendaten und Organisationsdaten geladen und die Personen den zugehörigen Organisationen zugeordnet. Im zweiten Schritt werden die Accounts jeweils System für System geladen. Dabei ist die Herausforderung, die Accounts den jeweiligen Personen (bzw. Verantwortlichen) möglichst automatisch zuzuordnen. Dies geschieht unter dem Einsatz so genannter Korrelationsregeln, die auf der Basis von Attributen (wie z.B. E-Mailadresse) eine automatische Zuordnung durchführen können. Alle Accounts, die nicht automatisch zugeordnet werden können bedürfen einer manuellen Prüfung und Zuordnung.

Nach Abschluss des Datenimports und der Korrelation können zwei wichtige Fragen beantwortet werden:

1) Wer hat welche Accounts und Berechtigungen?
Durch das Korrelieren von Accounts zu den Personendaten kann für jede Person abgefragt werden, über welche Accounts und Berechtigungen diese Person verfügt.

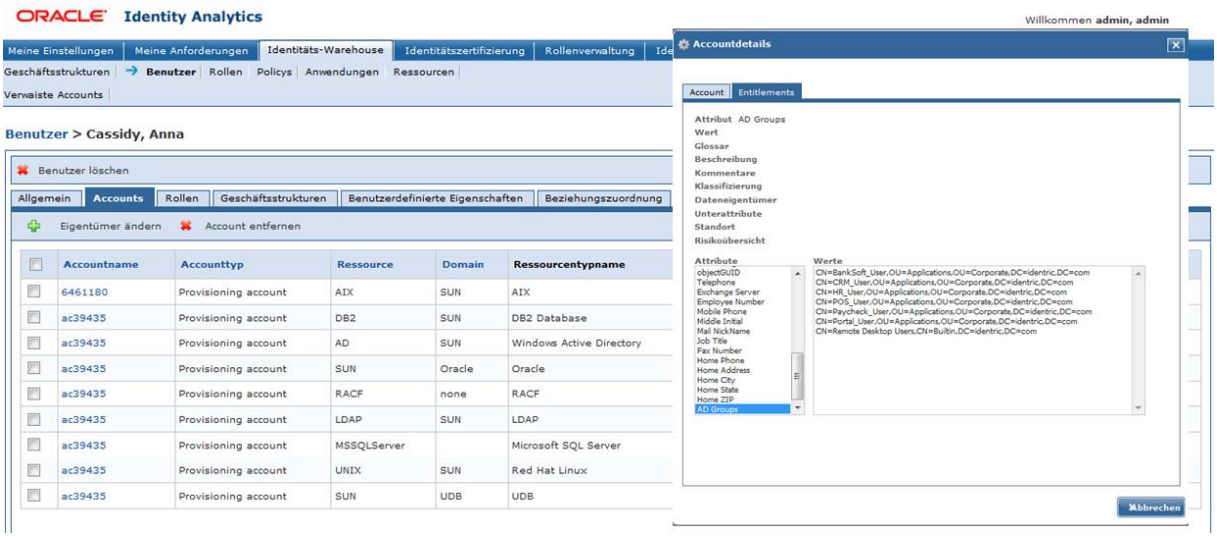

Abb. 1: Accounts einer Person und Detailsicht auf die Gruppen eines AD Accounts

2) Welche Accounts konnten keiner Person bzw. keinem Verantwortlichen zugeordnet werden?
Bei allen Accounts, die keiner Person zugeordnet werden konnten, liegt die Vermutung nahe, dass es sich um Accountleichen handelt, die ein potentielles Sicherheitsrisiko darstellen.

Aufsetzen und Durchführung einer Zertifizierung

Eine oft gestellte Anforderung ist das regelmäßige Durchführen von Zertifizierungen – also das Überprüfen der Berechtigungen eines Mitarbeiters durch den Vorgesetzten. Da wir beim Datenimport bereits auf Informationen wie E-Mailadressen, Vorgesetzte und Organisationen geachtet haben, stehen uns die Informationen zur Abbildung des Zertifizierungsprozesses zur Verfügung.

Eine Zertifizierung kann mit folgenden Eingangsparametern gestartet werden:

- Auswahl der zu überprüfenden Mitarbeiter
- Durchführung durch den Vorgesetzten
- Dauer der Zertifizierung (z.B. 4 Wochen), d.h. der Zeitraum in der der Vorgesetze die Zertifizierung abgeschlossen haben muss

OIA informiert den Vorgesetzten per E-Mail und der Vorgesetzte kann die Zertifizierung in OIA durchführen. Eskalationsprozesse in Form von Erinnerungen an den Vorgesetzten und dessen Vorgesetzten werden durch OIA unterstützt. Die Prozesse sind so generisch, dass sich die Konfiguration auf die Erstellung einer E-Mail Vorlage und der Auswahl, ob ein Prozessschritt durchgeführt werden soll, beschränkt.

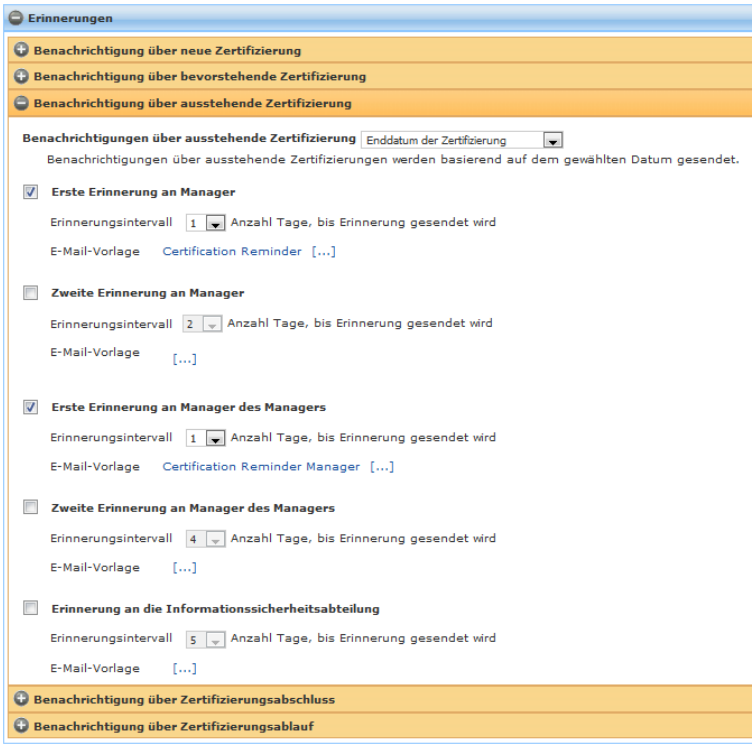

Abb. 2: Konfiguration der Erinnerungen bzw. Eskalationen für eine Zertifizierung.

Durchführung der Zertifizierung

Die Zertifizierung wird vom Vorgesetzten in OIA durchgeführt (weil das oben als Eingangsparameter definiert wurde). Der Vorgesetzte bekommt die Berechtigungen seiner Mitarbeiter in einer tabellarischen Darstellung angezeigt und kann entscheiden, welche Berechtigungen seine Mitarbeiter benötigen und vor allem kann er entscheiden, welche Berechtigungen seine Mitarbeiter nicht mehr benötigen.

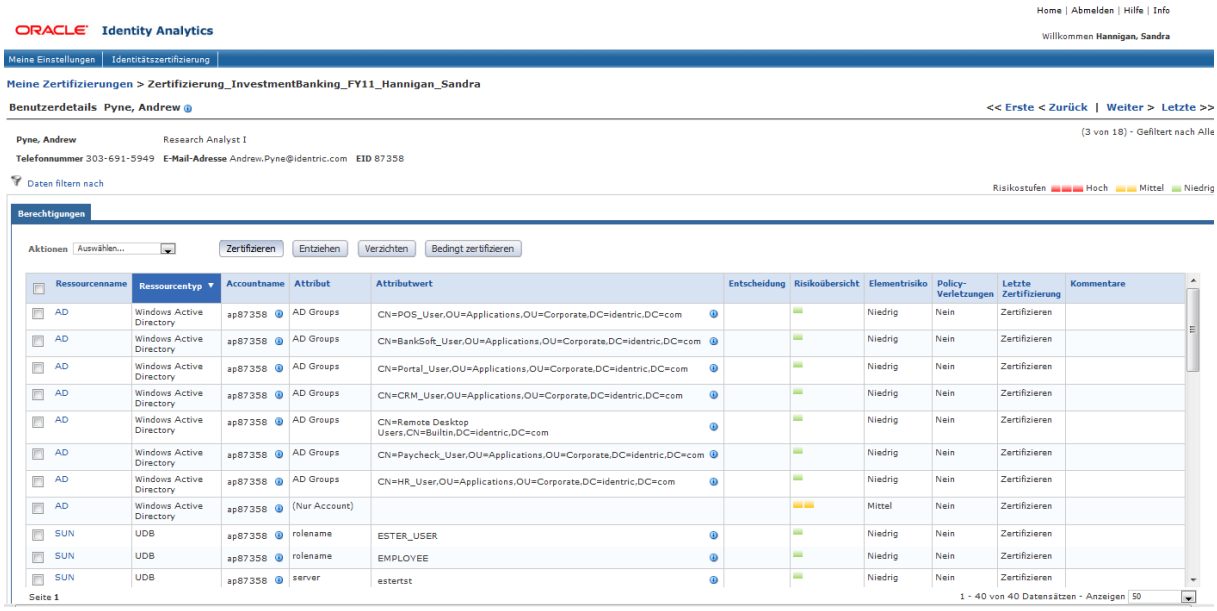

Abb. 3: Darstellung der Accounts und Berechtigungen in einer Spreadsheet Darstellung während der Zertifizierung durch den Vorgesetzten

Glossar
Die bisherige Darstellung hat sich darauf beschränkt, dass einem Vorgesetzten die „Rohdaten“ der Berechtigungen zur Zertifizierung vorgelegt werden. Diese sind i.A. für einen Vorgesetzten kaum verständlich und deshalb bietet OIA über ein Glossar die Möglichkeit, eine fachliche Beschreibung der technischen Berechtigungen zu hinterlegen. Dann wird dem Vorgesetzten für die Zertifizierung die fachliche Beschreibung an Stelle der unverständlichen technischen Beschreibung angezeigt. Es besteht natürlich weiterhin die Möglichkeit, dass der Vorgesetze sich die Werte der „Rohdaten“ anzeigen lässt.

Ergebnis der Zertifizierung
Nach der Durchführung der Zertifizierung stehen Berichte über die gesamte Zertifizierung und ausgewählten Aspekten (z.B. nicht bestätigte Berechtigungen) zur Verfügung. Diese Berichte können auf Wunsch direkt nach Abschluss der Zertifizierung versendet werden und jederzeit im OIA eingesehen werden.

Role-Mining und Role-Life-Cycle

Auf Basis der bereits importierten Berechtigungsdaten bietet OIA die Möglichkeit, automatisch Rollenvorschläge zu finden (Role-Mining). Dazu werden unterstützend Personendaten (z.B. Jobcode, Abteilungszugehörigkeit, Standort, etc.) eingesetzt. So kann OIA unterstützen, Rollen für die Personen zu finden.
Die Pflege und Weiterentwicklung von Rollen ist über die Role-Life-Cycle Funktionalität möglich. Dazu bildet OIA die Prozesse rund um die Verwaltung und Genehmigung von Rollen und deren Veränderungen ab.

Zertifizierung mit Rollen

Sind Rollen und deren Zuordnung zu Personen definiert, so kann eine Zertifizierung für den Vorgesetzten deutlich vereinfacht werden. An Stelle der Zertifizierung aller Einzelberechtigungen kann der Vorgesetzte die Zuordnung der Rollen zu einer Person zertifizieren und muss ggf. nur noch die nicht durch Rollen abgedeckten Einzelrechte zusätzlich zertifizieren.

Funktionstrennung

Nach dem Datenimport kennt OIA alle Personen und deren Berechtigungen. Es liegt nahe, dass OIA Analysen auf diesen Daten ausführen kann, um potenzielle Verstöße gegen Regelwerke zu erkennen. Regeln zur Funktionstrennung (auch Seperation of Duties / SoD genannt) können in OIA definiert und geprüft werden.

Weitere Informationen

Weitere Informationen zu Oracle Identity Analytics finden Sie unter:
http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-analytics/overview/index.html

Eine Übersicht über die Identity Management Produkte von Oracle finden Sie unter:
http://www.oracle.com/identity

Kontaktadresse:

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

Telefon: +49 (0) 211-74839775
E-Mail stephan.hausmann@oracle.com
Internet: www.oracle.com/identity