Mit dem seit August 2012 verfügbaren neuen Release der „Identity & Access Management"-Lösungen greift Oracle aktuelle Trends auf, die viele Security-Manager ganz oben auf ihrer Agenda haben. So sind neben zahlreichen neuen Funktionen vor allem zwei neue Lösungen entstanden: „Oracle Privileged Account Manager" unterstützt Kunden bei der Verwaltung von privilegierten Accounts beispielsweise in Datenbanken und Betriebssystemen und „Oracle Mobile & Social" ermöglicht Single Sign-on für Applikationen auf mobilen Endgeräten und die Einbindung von Identitätsinformationen aus sozialen Netzwerken in den Authentifizierungsprozess.

Oracle Identity Management 11*g* Release 2

Michael Fischer und Rüdiger Weyrauch, ORACLE Deutschland B.V. & Co. KG

Oracle Identity Management 11*g* Release 2 ist ein weiterer großer Schritt von Oracle hin zu einer vollständigen, offenen und integrierten Suite von Komponenten, die Kunden bei der Lösung folgender aktueller Anforderungen unterstützt:

- Wie können Konsumenten/Endkunden mit einem einfachen Registrierungsprozess und durch Einbindung von Daten aus sozialen Netzwerken sowie der Unterstützung mobiler Endgeräte an den eigenen Internetauftritt gebunden werden?
- Wie können stetig wachsende regulative Anforderungen („Compliance") bedient werden, ohne dass hohe Integrationskosten die ohnehin knappen Budgets verschlingen?
- Wie kann mit einfachen Mitteln die Passwortvergabe von privilegierten Zugängen wie „SYSTEM" oder „root" kontrolliert werden?

Mit dem neuen Release vereinfacht Oracle die Identity-Management-Lösungen und bündelt sie in drei Kategorien: Identity Governance, Access Management und Directory Services.

Oracle Identity Governance

Oracle Identity Governance umfasst eine für die Fachseite konzipierte, einfache und flexible Suchmöglichkeit für Accounts, Rollen und Berechtigungen im Rahmen von Antrags- und Genehmigungsprozessen sowie eine leistungsfähige Funktion zur Überprüfung von Berechtigungen bei regelmäßigen Soll/Ist-Abgleichen. Diese Berechtigungsüberprüfungen führen immer mehr Kunden durch, um die Qualität der Identitätsdaten zu erhöhen oder auch – wie bei Banken – regulatorischen Anforderungen nachzukommen, denn die „Mindestanforderungen an das Risikomanagement" schreiben Banken eine regelmäßige Prüfung der Berechtigungsvergabe vor. Durch integrierte Bausteine stehen die beschriebenen Funktionen in einem einheitlichen „Look & Feel" und ohne Medienbruch zur Verfügung.

Mit dem Oracle Privileged Account Manager reagiert Oracle auf Anforderungen von Kunden, gemeinsam genutzte Konten („shared accounts") und privilegierte Nutzer wie „SYSTEM" oder „root" besser überwachen zu können. Ist Oracle Privileged Account Manager im Einsatz, muss sich ein Administrator mit seiner normalen Identität gegenüber Oracle Privileged Account Manager authentisieren und bekommt die Liste der ihm zugewiesenen privilegierten Nutzer und zugehöriger Systeme angezeigt. Ist das zu administrierende System ausgesucht, wird ein Passwort generiert, im Zielsystem aktualisiert und dem Administrator zur Nutzung angezeigt. Abbildung 1 zeigt die Sicht auf die Endbenutzeroberfläche.

Der Administrator erbringt seine administrativen Tätigkeiten und gibt das Passwort danach wieder zurück (Check-in), wodurch das Zielsystem einen Passwort-Wechsel initiiert und damit einen erneuten Zugriff mit dem bekannten Passwort verhindert. Über das „Logfile/Reporting" des Oracle Privileged Account Manager kann nun nachvollzogen werden, welcher Mitarbeiter zu welchem Zeitpunkt administrativen Zugang hatte. Neben dieser interaktiven Vorgehensweise ist die Nutzung der gleichen Funktionen über ein dokumentiertes Kommandozeilen- und REST-API auch für Skripte und Applikationen möglich.

Oracle Identity Manager wurde durch ein neues, auf den fachlichen Endanwender ausgerichtetes Benutzer-

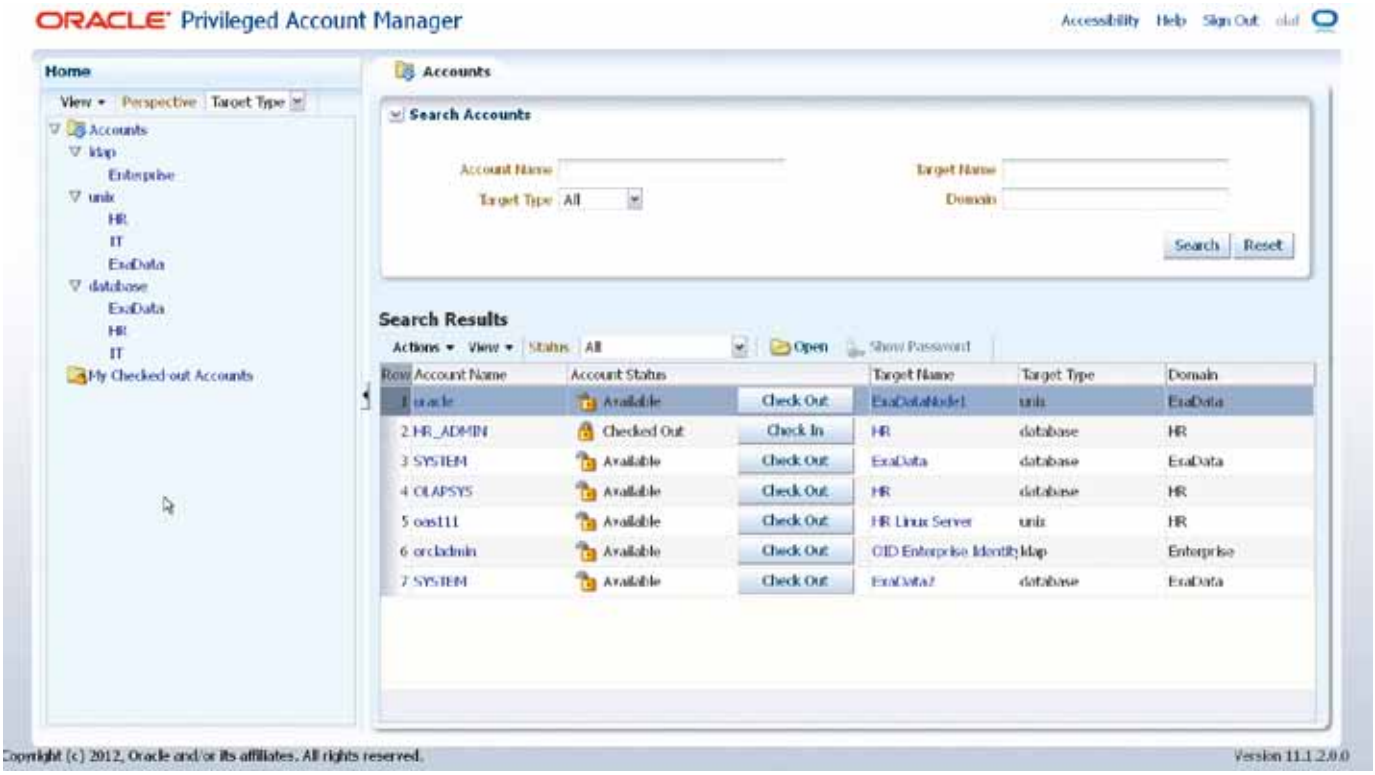

Abbildung 1: Check-Out eines privilegierten Accounts

Interface aufgewertet, das ein intuitives Finden von Accounts, Rollen und Berechtigungen über den sogenannten „Access Catalog" ermöglicht. Vergleichbar mit der Suche eines Buchs auf einer Online-Plattform gibt man Wörter in die Suchleiste ein und bekommt Vorschläge angezeigt, die weiter eingrenzbar sind (zum Beispiel „Zeige nur Rollen"). Natürlich kommen nur die Berechtigungen zur Anzeige, die der Nutzer überhaupt beantragen kann. Einmal ausgewählt, werden die Anträge in einem neu eingeführten Warenkorb abgelegt. Sind alle Anträge durchgeführt, werden über einen Check-out die notwendigen Genehmigungsprozesse angestoßen, deren Status der Antragsteller jederzeit einsehen kann.

Ein weiteres neues Feature ist die browserbasierte Anpassung der ADF-Benutzeroberfläche, die es dem Endbenutzer ermöglicht, auf einfache Weise seine Einstiegsseite nach dem Tätigkeitsprofil (beispielsweise Genehmiger) anzupassen. Auch größere Änderungen wie weitere Eingabefelder oder zusätzliche Informationen im Access Catalog können in der Regel direkt im Browser editiert werden. Durch die eingeführte sogenannte „Sandbox-Technologie" lassen sich die Änderungen zunächst lokal testen und anschließend in die Test- und Produktionsumgebung übertragen, wo sie auch bei Patches und Upgrades des Kernsystems weiter Bestand haben.

Oracle Access Management

Oracle Access Management umfasst eine „End-to-End"-Lösung für die Anmeldung an Systemen oder Anwendungen (Authentifizierung) sowie die Sicherstellung über die ausreichende Berechtigung beim Zugriff auf Systeme, Anwendungen und Daten (Autorisierung). Single-Sign-on-Komponenten von Oracle ermöglichen dem Benutzer, sich nahtlos in der desktopbasierten Applikationswelt, in webbasierten Anwendungen sowie in Anwendungen von Cloud- oder Service-Providern (wie Google über OpenID, Behörden über SAML etc.) zu bewegen. Auch wenn ein angemeldeter Benutzer über verschiedene Ebenen zugreift, etwa direkt auf eine Datenbank, über Web-Services oder eine Anwendung, ist dieser Schutz sichergestellt. Bei Nutzung unterschiedlicher Endgeräte wie Laptops, Tablet-PCs, Smartphones oder Zugriff von unterschiedlichen Orten wie Internetcafé, Büro oder Home-Office kann die Oracle-Access-Management-Lösung diesem Rechnung tragen und kontextabhängig reagieren.

Eine Bewertung des Risikos durch die verschiedenartigen Zugriffsmöglichkeiten ist mit der weiterentwickelten „Risk & Fraud Detection" möglich. Wird ein typisches Benutzerverhalten (Zugriff immer zu Bürozeiten von einer bekannten IP-Adresse) verlassen, erhöht sich ein Risikowert, auf den der Oracle Access Manager oder die geschützte Applikation reagieren kann, etwa durch eine weitere Authentifizierungsfrage. So lässt sich beispielsweise der Download auf ein unbekanntes Tablet unterbinden, aber auf einem Firmen-Laptop erlauben.

Im neuen Release wurden mit „Oracle Mobile and Social" weitere Funktionalitäten eingeführt, um soziale Netzwerke wie Facebook, Google, Yahoo, Twitter und LinkedIn hinsichtlich der Benutzer-Informationen transparent in Lösungen zu integrieren. Hierbei werden deren Authentifizierung akzeptiert und Attribute wie

Abbildung 2: Voll integriertes Access-Management

Name oder E-Mail-Adresse aus den Netzwerken weiterverwendet beziehungsweise zur automatischen Vorbelegung von Registrierungsformularen genutzt. Zusätzlich ermöglicht „Oracle Mobile and Social" über die Nutzung eines mobilen Entwicklerwerkzeugs ein Single Sign-on für native Applikationen wie Apple iOS.

Der integrierte Produktansatz ermöglicht eine einfache und schnelle Nutzung der verschiedenen Services wie Authentifizierung, SSO, Autorisierung, Federation, Mobile Identity, Social Logon, Webservice Security, Fraud Prevention und eigener Entwicklungs-Frameworks. Aus Sicht der Administration wurden mit einer neuen, durchgängigen Bedienoberfläche alle Komponenten der Access-Management-Lösung unter einer Oberfläche vereint (siehe Abbildung 2).

Oracle unterstützt in den Access-Management-Lösungen offene Standards wie Federation, SAML, RBAC, ABAC, XACML, OpenID und OAuth, um eine Interoperabilität mit Produkten anderer Hersteller, Provider und Individual-Lösungen zu unterstützen.

Oracle Directory Services

Oracle bietet eine umfassende und im Markt etablierte Directory-Service-Plattform an, die Identitätsspeicher, Proxy-Services, Synchronisierung und Virtualisierung in einer Suite vereint. Neu in 11*g* R2 sind erweiterte Funktionen für die mobile und durch soziale Netzwerke veränderte Welt. Die Speicherung von ortsbezogenen Daten oder Nahbereichssuchen von Kontakten aus sozialen Netzwerken sind Aufgaben, die hohe Anforderungen an Skalierbarkeit und Schreib-Performance stellen. Oracle stellt hierzu mit der „Optimized Solution für Oracle Unified Directory" eine auf Wunsch vorintegrierte Hard- und Software-Lösung bereit, die höchste Zuverlässigkeit und Skalierbarkeit vor allem für Telekommunikations- und Service-Provider bietet.

Fazit

Oracle hat mit seiner neuen Version der Identity-Management-Lösungen zahlreiche neue Funktionen eingeführt, die Unternehmen bei den vielfältigen Aufgaben zur Absicherung der Applikationswelt und der Regelung und Transparenz von Zugriffen unterstützen. Insbesondere der rasanten Entwicklung im Bereich mobiler Applikationen wurde mit der Einführung von „Oracle Mobile and Social" Rechnung getragen. Auf der DOAG 2012 Konferenz vom 20. bis 22. November 2012 in Nürnberg werden diese Neuerungen in Vorträgen und Kino-Sessions vorgestellt. Weitere Informationen stehen unter http://www.oracle.com/identity im Internet.

Michael Fischer
michael.fischer@oracle.com

Rüdiger Weyrauch
ruediger.weyrauch@oracle.com