Door Toine van Beckhoven

Themabijeenkomst over Oracle Identity Management & Database Security

'Gecentraliseerde controle, auditing en afdwingen van gebruiksrechten'

Afgelopen najaarwas de Morse zaal bij Oracle in De Meern flink gevuld met in security geïnteresseerde OGh-leden. De themabijeenkomst bestond uit een presentatie van de aimabele Belg Antonio Mata Gomez, die een verhandeling hield over met name Identity Management en nog een half uurtje besteedde aan een reeks van andere Oracle10g security features.

Identity Management

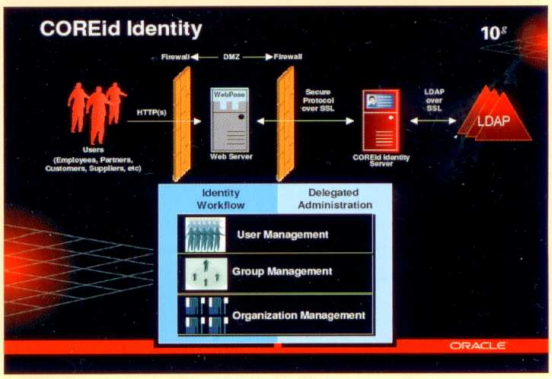
Naarmate organisaties geconfronteerd worden met een toenemende openheid van hun systemen en integratie met applicaties van partners, wordt de controle over de toegang tot hun systemen steeds belangrijker, maar ook complexer. Van oudsher wordt gebruikerstoegang veelal geregeld in elke applicatie afzonderlijk en voor elke database opnieuw. Denk aan maatwerksystemen, ERP en CRM systemen. Voeg daar e-mail en faxsystemen, portals, netwerktoegang en externe toegang aan toe en de beheerders worden geconfronteerd met versnipperd beheer van rechten. Niet alleen maakt dit de aanmaak van nieuwe accounts met al hun rechten en het volledig verwijderen van alle gebruikersrechten lastig, het is ook nog eens niet inzichtelijk. Als organisaties dan ook nog moeten voldoen aan regelgeving op het gebied van Sarbanes-Oxley, HIPAA, Graham-Leach-Bliley en dus moeten bewijzen dat de juiste gebruikers op de juiste tijd de juiste rechten hadden dan vormt dit allemaal een enorme uitdaging.

Identity Management komt tegemoet aan deze complexiteit. Oracle Identity Management bestaat momenteel uit een reeks producten, onder meer samengesteld uit producten van overgenomen bedrijven zoals Oblix, die een volledige oplossing bieden voor alles wat met Identity management (IdM) te maken heeft. Dit artikel behandelt de verschillende onderdelen van Oracle IdM. Achtereenvolgens bekijken we de LDAP directory, Delegated Administration, Single Sign-On, Reporting/Regulatory Compliance, Provisioning, Certificate Authority, Federation en Web Services Security.

Directory

Het hart van Oracle IdM is Oracle Internet Directory (OID). Een product dat al enige jaren meegaat. Dit is een volledige LDAP V3 Directory waarin de identity informatie daadwerkelijk wordt opgeslagen. De gegevens in OID staan vervolgens in een Oracle database. OID is ruim schaalbaar tot miljoenen gebruikers en kan gebruik maken van Oracle's High Availability mogelijkheden, zoals clustering. Interfaces om de Directory informatie te onderhouden biedt Oracle vooral via het (door de overname van Oblix verkregen) product COREid. De verderop te behandelen componenten Provisioning, Federation en Webservices management van IdM zijn ook afkomstig van Oblix.

COREid Access and Identity, zoals de samengevoegde twee afzonderlijke produkten van Oblix nu genoemd worden binnen IdM, zijn servers die aangesproken worden als gebruikers een applicatie gebruiken waarbij ze via de Identity management laag moeten gaan. Speciale plug-ins voor de Webserver (WebPass en Webgate) verzorgen de communicatie met de COREid Identity server en COREid Access server. Deze communicatie verloopt overigens via SSL en is daarmee goed beveiligd: identity informatie die over het netwerk



loopt is daarmee versleuteld. COREid Identity (zie bijgaand schema) bevat uitgebreide administratie mogelijkheden om identity informatie te bewerken in de Directory. Overigens kan COREid niet alleen overweg met Oracle Internet Directory, maar ook met een reeks andere populaire LDAP servers, zoals die van Microsoft, Novell en Sun. Opname van de Oblix product range in Oracle IdM heeft de toegang tot andere (niet Oracle-)producten flink verruimd, zodat meer dan voorheen nu vrijwel elk systeem binnen de organisatie (en zelfs buiten de organisatie d.m.v. Federation) binnen de Identity Management oplossing van Oracle beheerd kan worden. In vrijwel alle gevallen zullen organisaties ervoor kiezen om hun gebruikers in te delen in groepen om die groepen vervolgens bepaalde rechten te geven.

COREid biedt verschillende groeperingmogelijkheden, zoals statische groepen (onderhoudsgevoelig), dynamische groepen (lidmaatschap van de groep is afhankelijk van bepaalde gebruikers attributen zoals bijvoorbeeld de functie of afdeling van de gebruiker), geneste groepen (groepen bestaande uit groepen), hybride groepen (een mix van eerder genoemde) en 'subscription based' groepen (bijvoorbeeld ter ondersteuning van special interest groepen).

Delegated Administration

COREid Identity bezit een reeks van Workflow mogelijkheden om de administratie van identity informatie te versimpelen en in goede banen te leiden. Zo biedt het mogelijkheden voor zelfregistratie van gebruikers (via aanwezige standaard schermen) alsmede password wijzigingsopties voor gebruikers. Maar ook gedelegeerde administratie en aanvragen tot attribuut wijzigingen zijn voorzien. In al deze gevallen kunnen regels opgesteld worden die de workflow van de identity wijziging voorschrijven voordat de informatie wordt opgeslagen in de LDAP server. Delegated Administration geeft beheerders de mogelijkheid om andere beheerders aan te wijzen die verantwoordelijk zijn voor hun deel van de identity informatie. Via optionele approval regels wordt het uitbestede beheer alsnog in de gaten gehouden. COREid bezit nog enige presentatiemogelijkheden om de identity informatie te ontsluiten naar het web via zogeheten 'Portal Inserts' en 'PresentationXML'.

Single Sign-On

De COREid Access server (een aparte server naast de Identity server) bevat een cache van identity informatie ten behoeve van performance. Wijzigingen die gemaakt worden via de Identity server worden naast doorvoeren in de LDAP server ook direct doorgevoerd in de Access cache. Dit voorkomt security valkuilen.
Single Sign-On (SSO) is zeer gebruikersvriendelijk: een gebruiker hoeft slechts eenmaal aan te loggen (hetzij via username/ password, hetzij via tokens of via biometrics) en alle applicaties waar normaal gezien een inlogscherm zou verschijnen zijn toegankelijk zonder dit scherm: de identity informatie wordt doorgespeeld naar deze applicaties. Oracle had uiteraard al zijn eigen SSO oplossing, maar door de opname van Oblix producten is de weg geopend naar applicaties van andere leveranciers. Oracle heeft hiertoe ook partnerships afgesloten met andere softwareleveranciers. Voor elke fase van het authenticatie en autorisatieproces zijn er API's beschikbaar waarmee je externe componenten in IdM kunt hangen (bijvoorbeeld een RSA authenticatie server). De COREid Identity en Access servers zijn overigens ook High Available te maken ten behoeve van schaalbaarheid, stabiliteit en beschikbaarheid.

Reporting/Regulatory Compliance

Om te voorzien in regelgeving zoals Sarbanes-Oxley en HIPAA is COREid uitgerust met een uitgebreide rapportage- en auditingmogelijkheid. Omdat elke toegang tot applicaties via de Access en Identity servers gaat, is op dat punt een auditing engine ingebouwd die een audittrail bijhoudt van geautoriseerde en ongeautoriseerde toegang. Deze audittrail komt terecht in een database via ODBC. Deze informatie kan daarna opgevraagd worden om inzicht te krijgen in gebruikers, systeembronnen en gebruik ervan.

Provisioning

Zodra gebruikers worden aangemaakt, verwijderd of gewijzigd in een bepaald systeem, is het voor de transparantie en vereenvoudiging van beheer noodzakelijk deze actie op de achtergrond te synchroniseren met andere systemen. Zo maakt IdM het mogelijk dat gebruikers die in Microsoft Active Directory worden aangemaakt automatisch ook in Oracle Internet Directory terechtkomen en vice versa. Deze eigenschap van IdM wordt Provisioning genoemd en de faciliterende engine heet 'Directory Integration and Provisioning' (DIP). DIP bevat een event notificatie mechanisme, een mapping engine, policy enforcement mechanisme en kan via connectors praten met externe applicaties en systemen om de identity informatie uit te wisselen. Zo gebruikt Oracle voor Oracle Portal bijvoorbeeld Provisioning (Oracle Portal bevat zelf account informatie in zijn repository): een gebruiker aangemaakt in OID wordt doorgesynchroniseerd naar Portal en aangevuld met de voor Portal noodzakelijke default instellingen. Zonder dit mechanisme zou een in OID aangemaakte gebruiker niet van Portal gebruik kunnen maken zonder extra manuele beheerderinspanningen.

Certificate Authority

Authenticatie van gebruikers kennen we vooral door middel van username/password combinaties, maar deze zijn minder veilig dan token based oplossingen al dan niet in combinatie met digitale certificaten: tokens voegen aan iets dat je moet weten (het password) nog iets toe dat je moet hebben (het token). Digitale certificaten kunnen verkregen worden van een gelimiteerd aantal 'Certificate Authorities' (CA), zoals VeriSign en Thawte, maar deze kosten veel geld en zijn daarom niet bruikbaar als een organisatie intern voor zijn (potentieel duizenden of tienduizenden) gebruikers certificaten wil uitgeven ten behoeve van authenticatie. Oracle voorziet daarom in een eigen CA, een out-of-the-box Public Key Infrastructure (PKI) oplossing voor het uitgeven van X.509V3 certificaten. Voorzien van een web based certificate management en administratie tool en met een (volgens Oracle) naadloze integratie met de Oracle Applicatieserver Single Sign-On en Internet Directory.

Federation

Federation in IdM heeft alles te doen met integratie van business partners en de zogeheten 'Partner Circle of Trust'. Antonio noemde het voorbeeld van Boeing, een producent van vliegtuigen. Deze vliegtuigen worden bijvoorbeeld gebruikt door vliegtuigmaatschappijen als British Airways. Nu zou Boeing bijvoorbeeld kunnen voorzien in een applicatie (bijvoorbeeld een Portal) om de documentatie van de verschillende vliegtuigen in te zien. Deze applicatie wil ze ter beschikking stellen van de vliegtuigmaatschappijen, maar wel op een gecontroleerde wijze. Het mag niet zo zijn dat een bij British Airways ontslagen werknemer na zijn ontslag nog bij de documentatie kan. Wat Boeing hier wil is dat werknemers van British Airways die ge-authenticeerd zijn binnen de systemen van British Airways, via een Single Sign-On mechanisme doorgesluisd worden naar de applicatie van Boeing (een 'Federated SSO') en zo alleen toegang hebben tot de applicatie van Boeing via de applicaties van British Airways. Het mechanisme hierachter bevat zaken als 'trusted tickets' met identity informatie en een Federation protocol zoals SAML(Security Assertion Markup Language) om deze tickets uit te wisselen. Voorwaarde is dat de beide bedrijven een trusted partnerschap zijn aangegaan. Ook deze component van Oracle IdM is afkomstig van Oblix (COREid Federation). Aan beide zijden van de Trusted link dient een COREid Federation Server te staan om de trusted tickets uit te wisselen en te verifiëren. Federation is derhalve tevens een oplossing voor het wel ter beschikking stellen van een applicatie aan gebruikers in een andere organisatie, maar het niet willen beheren van de gebruikersaccounts van die externe gebruikers.

Web Services Security

Web services zijn een exponent van de SOA: Service-Oriented Architecture. Ze bieden de mogelijkheid om systemen met elkaar te laten praten. Maar een Identity Management oplossing zou niet volledig zijn als naast het reguleren van de gebruikersaccounts de interfaces tussen systemen onderling ongecontroleerd zouden opereren. Dezelfde beveiliging als voor gebruikers is dus van toepassing op web services. Om hierin te voorzien bezit Oracle IdM een Web Services Management component. Hiermee kunnen bestaande en nieuwe webservices van een beveiligingslaag voorzien worden (authenticatie en autorisatie) en tevens geaudit worden ten behoeve van Regulatory Compliance. Door middel van bijgeleverde monitoring en performance analyse tools kunnen webservices in de gaten gehouden worden.

Conclusie

Antonio Mata toonde aan dat Oracle Indentity management zeer serieus neemt en één van de beste oplossingen hiervoor in de markt heeft gezet. De overname van Oblix speelt hierin een heel grote rol. Het heeft de scope van Oracle IdM danig verruimd. Nu de aandacht voor beveiliging van informatiesystemen groter en groter wordt is het goed te zien dat Oracle hierin stevig bijdraagt.

Toine van Beckhoven is werkzaam bij IT-dienstverlener Motiv

Link:
Oracle Technet Network Identity Management:
www.oracle.com/technology/products/id_mgmt/index.html