Von der Datenbank zum LDAP-Server schnell und einfach mit Oracle Virtual Directory

Hans-Ulrich Beres
Ruhr-Universität Bochum
Bochum
Suvad Sahovic
Oracle Deutschland GmbH
Potsdam

Schlüsselworte:

Oracle Virtual Directory, OVD, Oracle Fusion Middleware, LDAP, Identity Management, Authentifizierung, Autorisierung

Einleitung

Die Ruhr-Universität Bochum (RUB) betreibt seit über 15 Jahren ein selbstentwickeltes Identitäts- und Zugriffsmanagementsystem RUBiKS (RUB integrierter Kunden-Service), das heute ca. 70.000 Identitäten verwaltet. Über das System wird konfiguriert, auf welche IT-Dienstleistungen und Produkte ein Benutzer Zugriff erhält und welche Bereiche zu schützen sind. Es hält die Passwörter synchron und ermöglicht Single Sign-On.
In diesem Vortrag wird erläutert, wie die in einer Oracle-Datenbank gespeicherten Daten mit Hilfe von Oracle Virtual Directory als LDAP-Server verfügbar gemacht wurden.

Identity and Access Managementsystem RUBiKS

RUBiKS verwaltet die elektronischen Identitäten in einer Oracle Datenbank 11gR2.
Studierende erhalten bereits bei der Immatrikulation eine Zugangskennung (LoginID), sonstige Angehörige der Universität auf Antrag, Mitarbeiter demnächst sofort bei ihrer Einstellung.
Für Kongresse lassen sich termingebundene Accounts generieren, darüber hinaus gibt es temporäre Accounts mit einer konfigurierbaren Lebenszeit von einer Stunde bis zu mehreren Monaten.

Derzeit werden rund 150 Online-Dienstleistungen auf Basis eines Rollenkonzepts angeboten.
Dazu gehören

- email
- Internet-Zugang (Studentenwohnheime, HIRN, WLAN, VPN, ISDN, DFN@home, Shibboleth)
- eLearning-System Blackboard
- Prüfungsverwaltungssystem VSPL
- Bibliothekskatalog OPAC
- Haushaltsinformationssystem
- Wikis
- Blogs
- Unix-Server
- Windows-Server
- Software-Lizenzen

Die Verwaltung geschieht über Web-Interface, Web-Services und Stored Procedures.

Die Systemlandschaft besteht aus folgender

Hardware:	7-Knoten RAC mit Fiberchannel-SAN Dell Compellent
	(3 für RUBiKS, 2 für eLearning, 1 für Batch-Läufe, 1 als Reserve)
	3 Oracle Application-Server
	3 LDAP-Server
	2 Loadbalancer
	1 Enterprise-Manager-Server
Betriebssystem:	RedHat Enterprise Linux 5/6(64 Bit)
Datenbanksoftware:	Oracle Database 11gR2 Enterprise Edition (64 Bit)

Einige Dienste nutzen das zentrale Active Directory, das regelmäßig mit Hilfe eines perl-Scripts aktualisiert wird.
Eine zunehmende Anzahl von Diensten nutzt den LDAP-Server. Dieser wurde bis Mitte des Jahres 2010 mit OID, danach mit OVD realisiert.

LDAP-Server real

Oracle Internet Directory (OID) ist ein LDAPv3-konformer Verzeichnisdienst, der die Daten in einer eigenen Oracle Datenbank ablegt. Diese Daten wurden bisher mit Prozeduren des DBMS_LDAP-Paketes gepflegt. Dieser Zugriff ist relativ langsam, außerdem kam es immer wieder zu Inkonsistenzen zwischen RUBiKS- und LDAP-Daten.

LDAP-Server virtuell

Oracle Virtual Directory (OVD) ist ein virtueller Verzeichnisdienst, der Identitätsinformationen unterschiedlichster Quellen LDAPv3-konform bereitstellt, ohne dass die Daten in einem gesonderten Repository zwischengespeichert werden, Inkonsistenzen sind dadurch ausgeschlossen.
Die Software gibt es seit 2005 in Oracle-Portfolio und aktuell ist die Version 11.1.1.6.
Die verschiedenartigen Quellen werden über sogenannte Adapter angebunden.

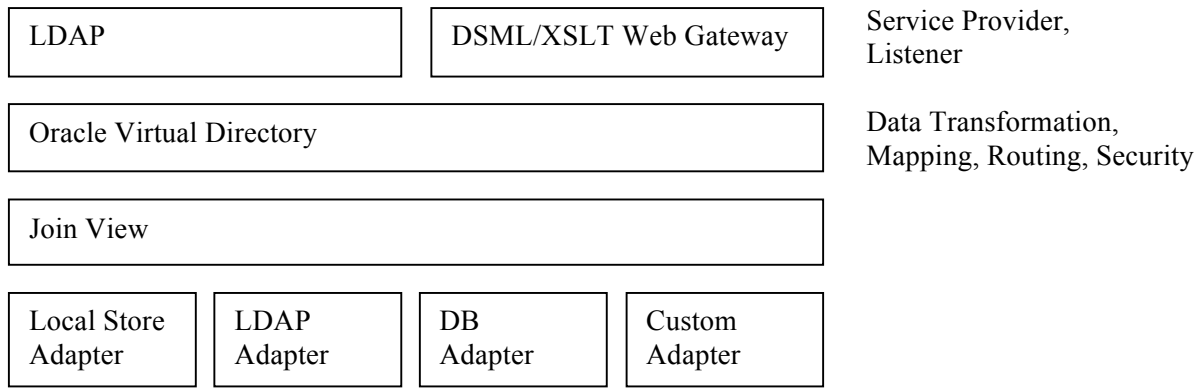

Abb. 1: Architektur von Oracle Virtual Directory

Die Adapter lassen sich durch java-plugins erweitern. Wir haben ein bind-plugin entwickelt, um z.B. für die temporären Accounts den Zeitpunkt der Erstnutzung in die RUBiKS-Datenbank zurückzuschreiben oder auch Passwort-Fehleingaben zu verwalten.

OVD installiert

Als Betriebssystem installierten wir RedHat Enterprise Linux 6 (64 Bit).
Eine komplette OVD-Installation besteht aus 2 Teilen:
- der WebLogic Server Domain (Managed und Admin Server) und
- der eigentlichen OVD-Instanz

Für eine Minimal-Installation kann man alles auf dem gleichen Server installieren.
Der WebLogic-Server erfordert als Voraussetzung ein passendes Java, wir installierten JRockit Mission Control 3.1.2 for Java Version 6 (Linux x86-64).
Den aktuellen WebLogic-Server 11g Rel 1 gibt es in der Version 10.3.6.
Das Identity Management muss man in zwei Schritten installieren:
- zuerst die Version 11.1.1.2.0
- dann das Upgrade auf Version 11.1.1.6.0.

Bei der Auswahl der zu installierenden Komponenten wählten wir **nur** das Virtual Directory.

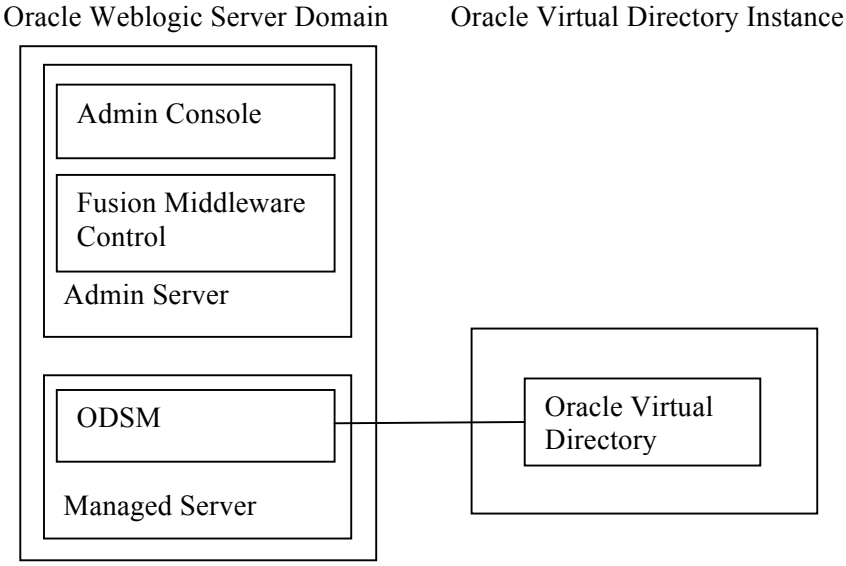

Abb. 2: Komponenten einer Oracle Virtual Directory - Installation

Die Start- und Stop-Skripte bestehen wie die Struktur der Software-Installation aus 3 Teilen:
- der Admin-Server mit
  - der Administrationskonsole für den WebLogic-Server
  - dem Enterprise-Manager
- der Managed-Server mit
  - dem Directory Service-Manager zur Konfiguration des Virtual Directory
- die Instanz des Oracle Virtual Directory

OVD konfiguriert

Das standardmäßig vorhandene LDAP-Schema wurde durch eigene Objektklassen und Attribute erweitert.

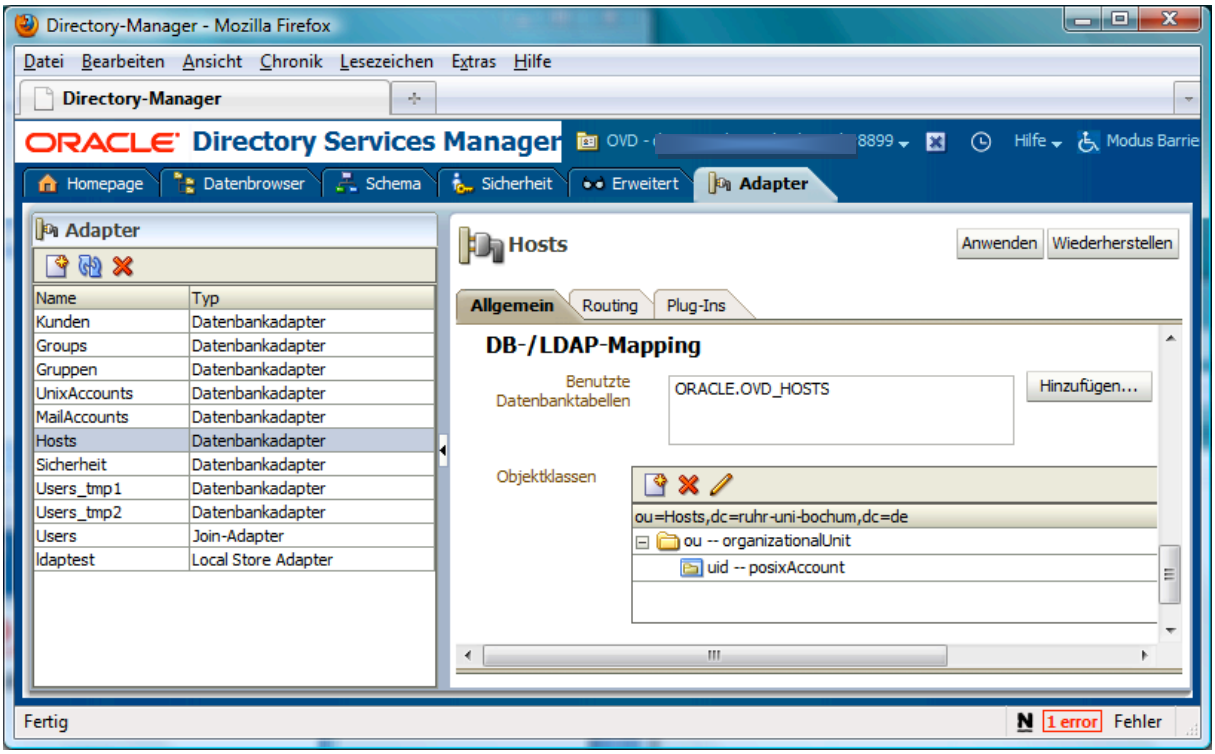

Abb. 3: Adapter-Konfiguration mit dem Directory Services Manager

Für jeden LDAP-Zweig gibt es einen eigenen Datenbank-Adapter, der seine Daten aus passenden Views der RUBiKS-Datenbank bezieht. Für jedes LDAP-Attribut wird dort das Mapping zur entsprechenden Tabellen-Spalte festgelegt. Durch entsprechende Konfiguration ist auch die automatische dynamische Bildung von Unterstrukturen möglich, z.B.

- Hosts
  - organizationalUnit1
    - uid1
    - uid2
  - organizationalUnit2
    - uid3

Durch fein abgestimmte Access-Control-Listen wird der Zugriff auf die einzelnen LDAP-Zweige bzw. LDAP-Attribute geregelt. Niemand hat schreibenden Zugriff, Änderungen der Daten erfolgen grundsätzlich nur in der RUBiKS-Datenbank. Einzige Ausnahme ist die erstmalige Anmeldung mit einem temporären Account, dann wird vom bind-plugin das Freischaltdatum und das entsprechende Löschdatum in die RUBiKS-Datenbank zurückgeschrieben.
Selbstverständlich ist mit OVD auch der schreibende LDAP-Zugriff möglich, dadurch würden dann die entsprechend gemappten Quelldaten geändert werden.
Ein mehrstufig konfigurierbares Logging erleichterte die Suche nach Konfigurationsproblemen und Optimierungsmöglichkeiten.

OVD optimiert

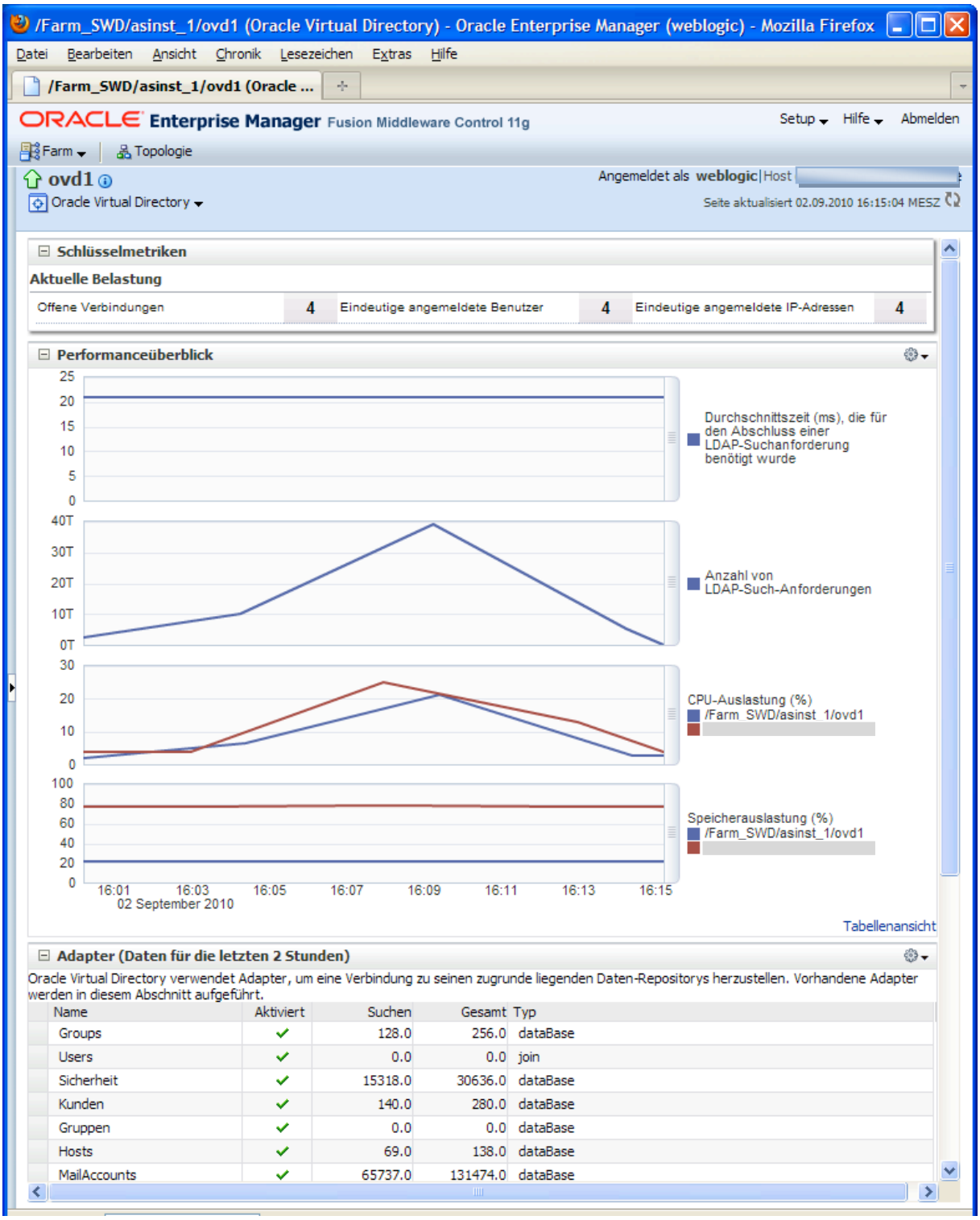

Abb. 4: Leistungsübersicht auf der OVD-Homepage des Enterprise-Managers

Standardmäßig sind die Listener nur für 10 Threads konfiguriert, für optimale Performance empfiehlt Oracle einen Wert von 50.
Die Datenbank-Adapter belasteten die RUBiKS-Datenbank merklich durch viele select-Statements. Deshalb ersetzten wir die Views durch Materialized Views, die im 10-Minuten-Takt aktualisiert werden. Da wir alle Datenbankadapter für „Suche ohne Berücksichtigung der Groß-/Kleinschreibung“ konfiguriert haben, ist es unbedingt erforderlich, für alle Spalten, die in einer solchen Suche vorkommen können, einen entsprechenden function-based Index upper(<Spaltenname>) zu erzeugen, um die sonst notwendigen Full-Table-Scans zu vermeiden.
In einem weiteren Schritt verlagerten wir diese Materialized Views in eine eigene lokale Datenbank auf jeden LDAP-Server. Dadurch stehen die LDAP-Server sogar bei einem Ausfall der gesamten RUBiKS-Datenbank zur Verfügung.
Die LDAP-Vorgänge (bind, search) sind stateless und voneinander unabhängig, eine Skalierung der Leistungsfähigkeit und Ausfallsicherheit erreicht man daher ganz einfach durch Parallelschalten mehrerer gleich konfigurierter LDAP-Server hinter zwei Loadbalancern. Mit Hilfe eines mitgelieferten Skripts kann man die Konfiguration eines Servers auf die anderen Server kopieren.
Die beiden vorgeschalteten Loadbalancer regeln mittels Heartbeat, welcher von beiden aktiv ist, Clients merken nichts davon, für sie gibt es nur den LDAP-Server.

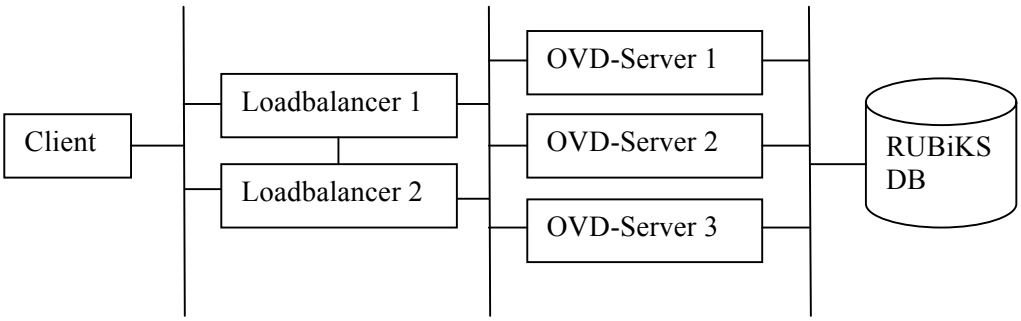

Abb. 5: Lastoptimierte und fehlertolerante OVD-Installation

OVD resultiert

Oracle Virtual Directory ist eine komfortable Möglichkeit, Daten aus verschiedensten Datenquellen als LDAP-Server bereitzustellen. Wenn das Mapping der LDAP-Attribute zu den Eingabedaten einmal korrekt definiert ist, geschieht alles Weitere völlig automatisch. Änderungen der Quelldaten sind sofort im LDAP sichtbar, weil der OVD-Server keine Daten zwischenspeichert. Änderungen im LDAP werden sofort in die Quelldaten zurückgeschrieben.
Nach unseren Erfahrungen hängt die Performance des OVD-Servers allein von der Performance der Daten-Lieferanten ab.

Kontaktadresse:

Hans-Ulrich Beres
Dipl.-Math.
Ruhr-Universität Bochum
Universitätsstraße 150
44801 Bochum

Telefon: +49 (0) 234-32-24012
Fax: +49 (0) 234-32-04012
E-Mail: Hans-Ulrich.Beres@ruhr-uni-bochum.de
Internet: http://www.ruhr-uni-bochum.de

Suvad Sahovic
Senior Systemberater
Oracle Deutschland B.V. & Co. KG
Schiffbauergasse 14
14467 Potsdam

Telefon: +49 (0) 331-2007-181
Fax: +49 (0) 331-2007-561
E-Mail: suvad.sahovic@oracle.com
Internet: http://www.oracle.com