Projektbericht

Aufbau & Implementierung eines neuen Identity & Access-Management Systems basierend auf den Forefront Identity Manager 2010 – Technischer Teil

Daniel Löffler
E-Mail: daniel.loeffler@fernuni-hagen.de
Tel.: +49 2331 987-2868

Rüdiger Berndt
E-Mail: b-rubern@microsoft.com
Tel.: +49 151 19550101

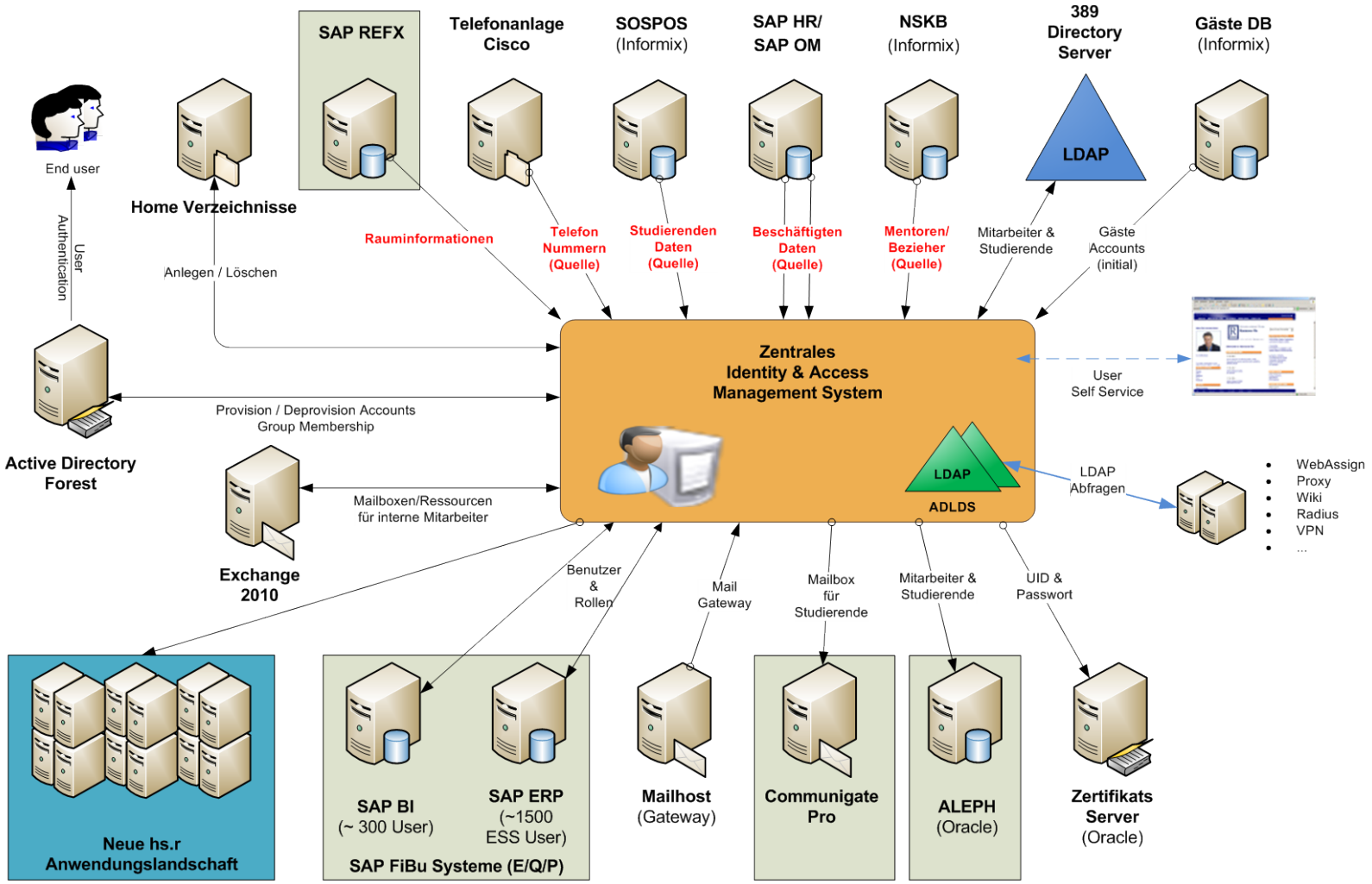
Inhalt

- Die FernUniversität in Hagen
- IAM-Systemlandschaft
- Funktionsweise des Microsoft Forefront Identity Manager (FIM)
- FIM Management Agents
- BAPIs für SAP HR und SAP OM
- Microsoft PCNS
- Name Generation Service
- Live-Demo

Die FernUniversität in Hagen

- 1974 gegründet als Universität und Gesamthochschule des Landes Nordrhein-Westfalen
- Erste und einzige öffentlich-rechtliche Fernuniversität in Deutschland
- Mit über 84.000 Studierenden die größte Universität Deutschlands
- Vier Fakultäten
  - Fakultät für Kultur- und Sozialwissenschaften
  - Fakultät für Mathematik und Informatik
  - Fakultät für Wirtschaftswissenschaften
  - Rechtswissenschaftliche Fakultät
- 1800 Mitarbeiter

IAM-Systemlandschaft

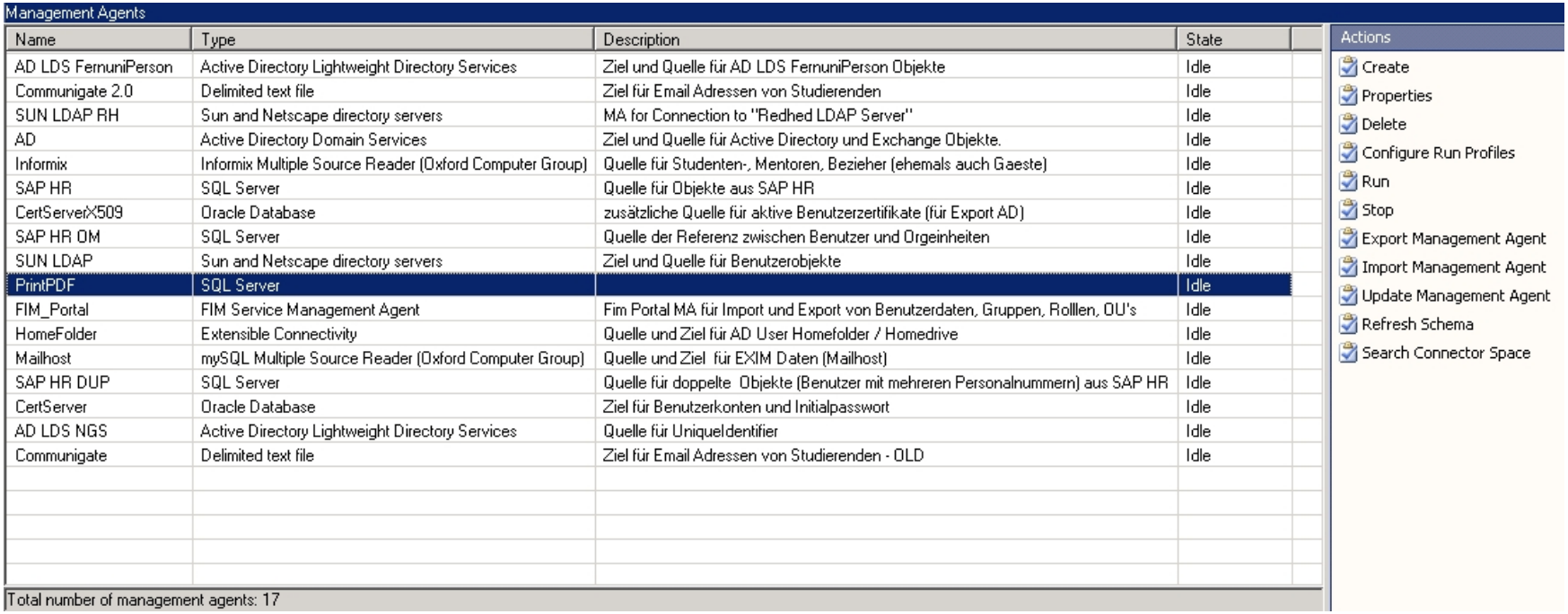


Funktionsweise/Funktionen des Microsoft FIM

- Stage basierendes Identity Management System
  - Täglich alle 20 Minuten laufen delta Synchronisationen zu allen Quell- und Zielsystemen
    - Neuanlagen
    - Änderungen
    - Löschungen
- 1mal pro Woche läuft eine voll Synchronisation, um evtl. entstandene Fehler zu korrigieren
- Es müssen KEINE Agenten auf den Quell- und Zielsystemen installiert werden
- Die Schnittstellen zwischen dem FIM und den Quell- und Zielsystemen bilden die Management Agents

FIM Management Agents

- Der FIM bringt eine Reihe von Standard Management Agents mit
- Management Agents der FernUni:



Management Agents

Name	Type	Description	State
AD LDS FernuniPerson	Active Directory Lightweight Directory Services	Ziel und Quelle für AD LDS FernuniPerson Objekte	Idle
Communigate 2.0	Delimited text file	Ziel für Email Adressen von Studierenden	Idle
SUN LDAP RH	Sun and Netscape directory servers	MA for Connection to "Redhed LDAP Server"	Idle
AD	Active Directory Domain Services	Ziel und Quelle für Active Directory und Exchange Objekte.	Idle
Informix	Informix Multiple Source Reader (Oxford Computer Group)	Quelle für Studenten-, Mentoren, Bezieher (ehemals auch Gaeste)	Idle
SAP HR	SQL Server	Quelle für Objekte aus SAP HR	Idle
CertServerX509	Oracle Database	zusätzliche Quelle für aktive Benutzerzertifikate (für Export AD)	Idle
SAP HR OM	SQL Server	Quelle der Referenz zwischen Benutzer und Orgeinheiten	Idle
SUN LDAP	Sun and Netscape directory servers	Ziel und Quelle für Benutzerobjekte	Idle
PrintPDF	SQL Server		Idle
FIM_Portal	FIM Service Management Agent	Fim Portal MA für Import und Export von Benutzerdaten, Gruppen, Rolllen, OU's	Idle
HomeFolder	Extensible Connectivity	Quelle und Ziel für AD User Homefolder / Homedrive	Idle
Mailhost	mySQL Multiple Source Reader (Oxford Computer Group)	Quelle und Ziel für EXIM Daten (Mailhost)	Idle
SAP HR DUP	SQL Server	Quelle für doppelte Objekte (Benutzer mit mehreren Personalnummern) aus SAP HR	Idle
CertServer	Oracle Database	Ziel für Benutzerkonten und Initialpasswort	Idle
AD LDS NGS	Active Directory Lightweight Directory Services	Quelle für Uniqueldentifier	Idle
Communigate	Delimited text file	Ziel für Email Adressen von Studierenden - OLD	Idle

Total number of management agents: 17

Actions
- Create
- Properties
- Delete
- Configure Run Profiles
- Run
- Stop
- Export Management Agent
- Import Management Agent
- Update Management Agent
- Refresh Schema
- Search Connector Space

FIM 2010 Management Agents

- Active Directory®supporting Windows 2003-2012, Exchange 2003-2013
- Active Directory LDS
- Global Address List (GAL) Synch—supporting Exchange 2003-2013
- iPlanet/Sun ONE Directory
- IBM DB2 Universal Database (on Windows or Linux)
- IBM Directory Server (> 4.x)
- SQL Server™— (2003-2012)
- Oracle Databases—supporting version 8i, 9i, 10g, 11x
- Directory Services Markup Language (DSML
- LDAP Interchange Format (LDIF) / De-Limited Text, Attribute-Value Pair Text
- Open-LDAP
- Lotus Notes – supporting 4.6, 5.0, 6.0, 7.x, 8.x
- Novell eDirectory—supporting versions > 8.6.x
- CLM
- Microsoft SAP HR + SAP R3 > V4.7

Über 150 weitere Systemanbindungen über Partner

- Highly Scalable SAP MA (incl. SAP Concentrator) for
  - HR, CUA
  - UM, OM, PDORG / Workflow integration
- File Share MA for User Home Shares, Project Shares, …
- Host RACF via LDAP
- Host DB2 via native IBM API
- Unix systems (VMS, HPUX, SUN, Linux, SCO, other)
- additional HR systems (e.g. Peoplesoft, Paisy,…)
- Various telephone systems (Alcatel, HIPATH, AVAYA, …)
- Sharepoint 2010/12 (Lizenz!)
- IBM RACF (IdentityForge Lizenz!)
- Live ID, Office Live
- Centrify/Omada OIM/Quest-VAS/Völker AE
- RSA SecurID
- LDAP Servers e.g. Siemens DirX, CP, Syntegra, …
- Oracle native users & Roles

BAPIs für SAP HR und SAP OM

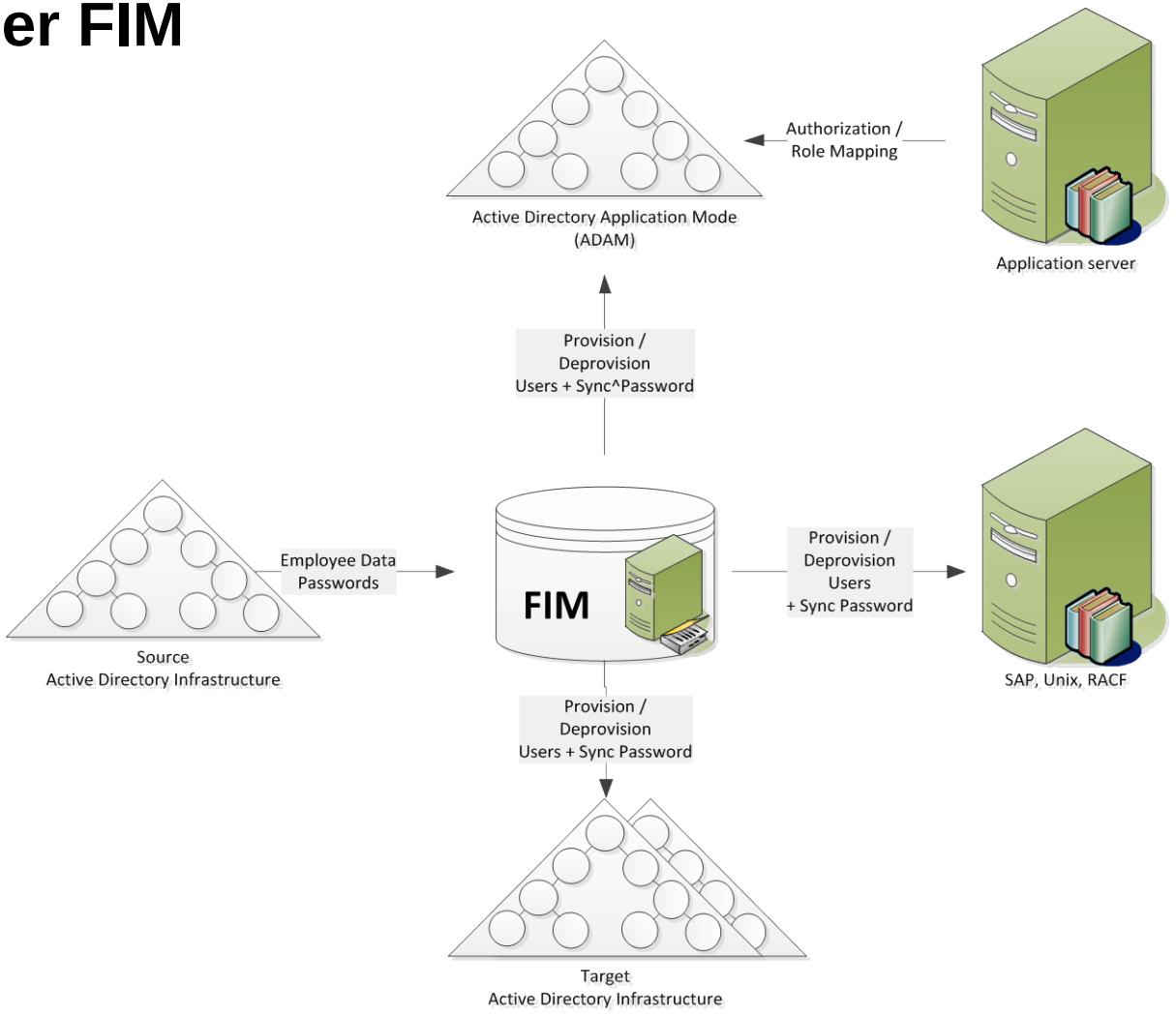
Name	SAP Version (min)	Funktionen
BAPI_EMPLOYEE_GETLIST	4.7	Liste mit allen aktiven Personalnummern
BAPI_EMPLOYEE_GETDATA	4.7	Wird verwendet, um Basis Beschäftigtendaten zu lesen. IT0001 – IT0002, Abteilung, Kostenstelle ***(Keine global Personalnummer; keine Daten von inaktiven Beschäftigten)***
BAPI_ORGUNITEXT_DATA_GET	ERP 2004	Organisationsstruktur, Positionen und Zuordnung Personen auf Positionen
Custom BAPI		Um globale Personalnummern, inaktive Mitarbeiter und zusätzliche/ benutzerdefinierte Daten zu lesen

Microsoft PCNS

- Password Change Notification Service
  - Synchronisiert die Passwortänderungen in Echtzeit aus dem Active Directory in den FIM
- Der FIM transportiert die Passwortänderungen direkt weiter an die angeschlossenen Zielsysteme (AD LDS, 389 Directory Server, Oracle, SAP)

Passwort Sync über FIM

1. Benutzer ändert Passwort im AD (Ctrl+Alt+Del)
2. Passwort wird auf zusätzliche Policies geprüft (SAP/Unix/Hosts)
3. Passwort ist encrypted und wird zum FIM Server gesendet
4. Der FIM Server setzt das Passwort dieses Benutzers in jedem Zielsystem



Name Generation Service

- Tool zur Generierung, Speicherung, Modifizierung und Suche von eindeutigen Namen
- Erstellen von UniqueIdentifier zur eindeutigen Identifizierung von Objekten
- Regelbasiertes Generieren von Anmeldenamen / E-Mail Adressen / UserID‘s
- Einfach zu konfigurierende Vorlagen
- Bei Änderung von Anmeldenamen werden die vorherige Werte in einer History gespeichert

Live Demo