

## Identity Management mit Microsoft Forefront Identity Manager an der FH Düsseldorf

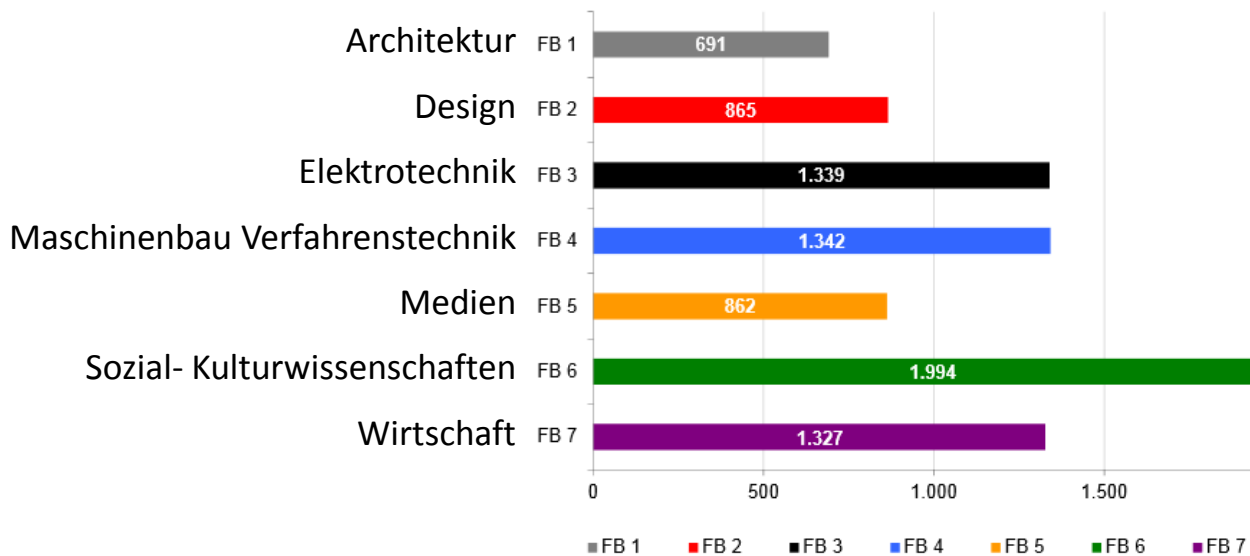
Roland Conradshaus, Campus IT



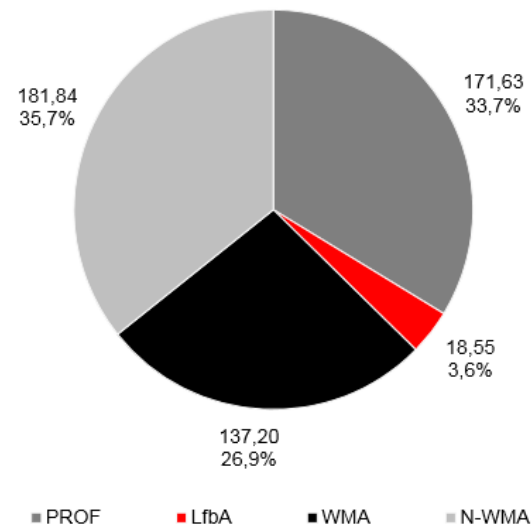


## Die Hochschule in Zahlen

Studierende nach Fachbereichen im WS 2012/13 (absolut)



Personal Gesamt nach Personaltypen



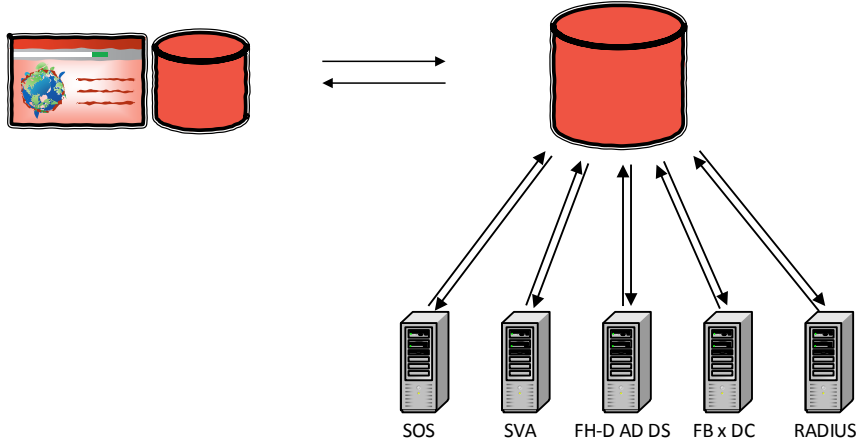
## **1 Ein Identitätenmanagementsystem**

**Eigentlich ist es egal, welches man hat - Hauptsache man hat eines.**

**Meines macht zusätzlich noch Spaß.**

**Den Spaß muss man sich auch leisten können.**

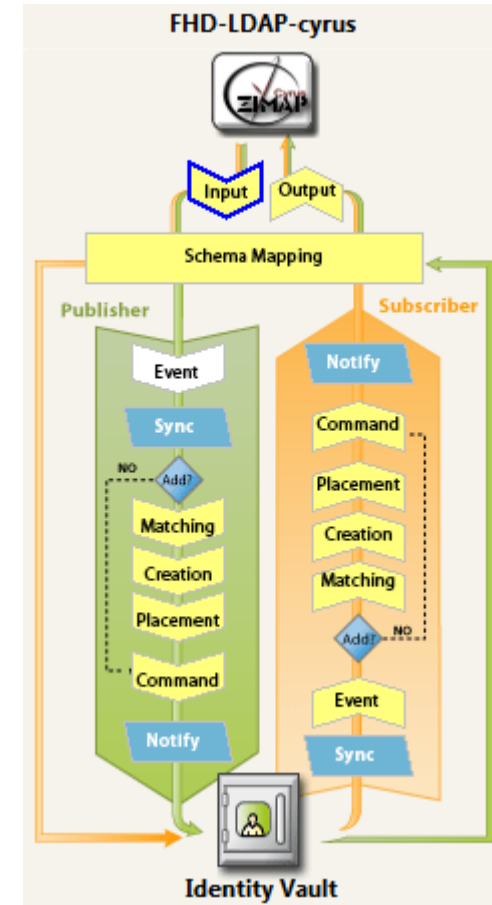
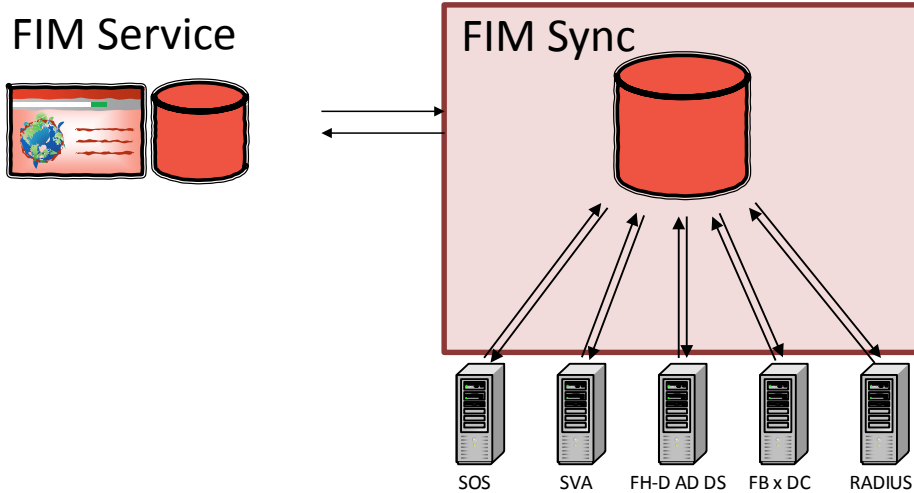
## Ein Identitätenmanagementsystem



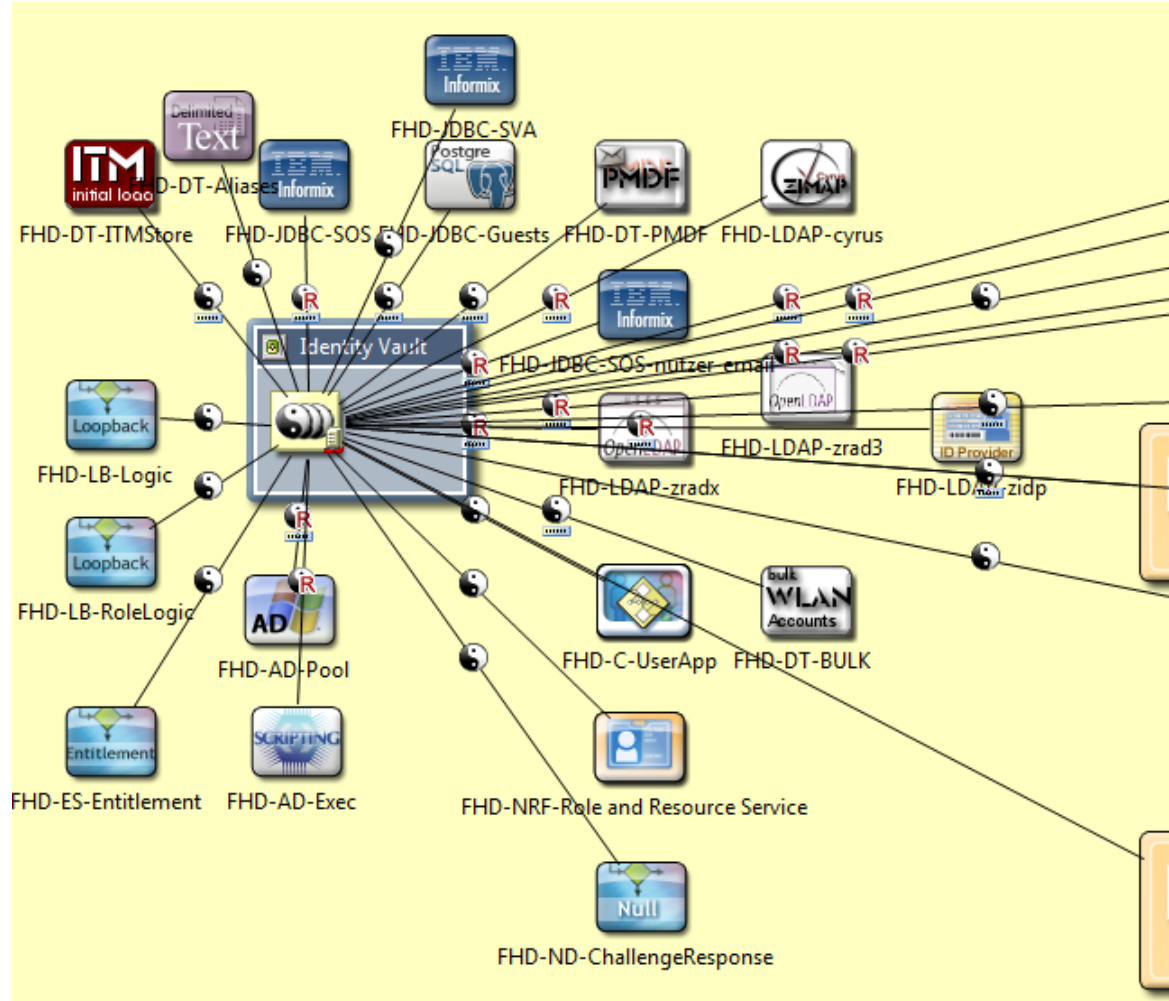
- Aggregation
- Erstellen von UID/PUK und Email
- Provisionierung erst nach Aktivierung
- Synchronisieren
- Helpdeskunterstützung
- personenunabhängiger Betrieb

## Ein Identitätenmanagementsystem

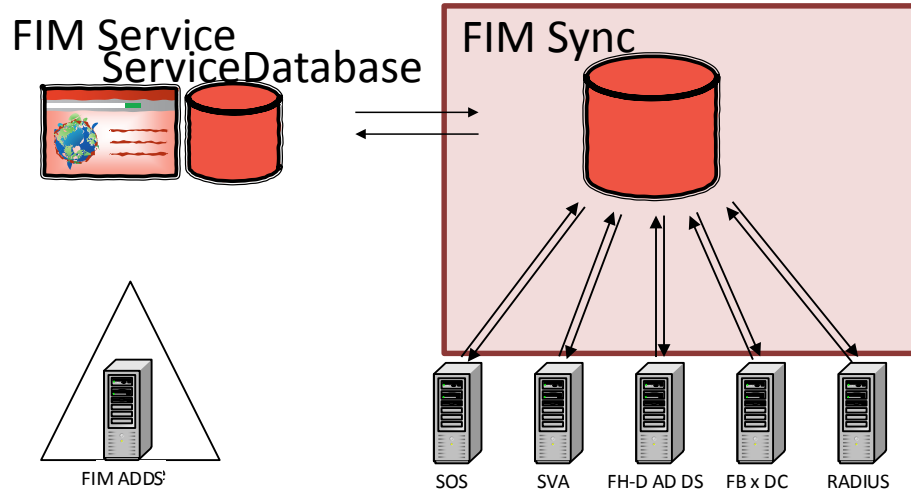
### FIM Service



## konkrete Umsetzung mit Novell



## Topologie



Virtual Machines			
Name	State	CPU Usage	Assigned Memory
FADDS	Running	0 %	6000 MB
FS	Running	0 %	16160 MB
FSDB	Running	0 %	16160 MB
FSync	Running	0 %	16160 MB

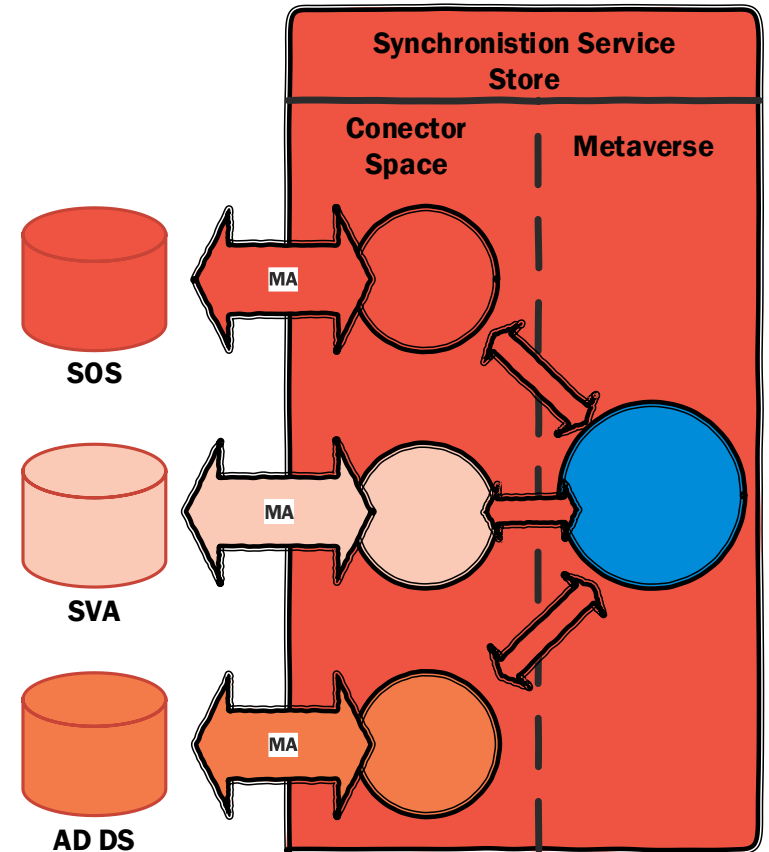
## 2 FIM als Entscheidung

- FIM kann man mieten
- FIM benutzt als Schnittstelle zu den Usern die Sharepoint Services
- Umgekehrt benutzt Sharepoint die Syncengine von FIM
- DirSync, das Tool zur Synchronisierung in O365, benutzt die Syncengine



## FIM in deep

- Es ist Status basierend
- Die MA laufen gesteuert
- FIM speichert Daten redundant
- Business Rules werden durchgesetzt



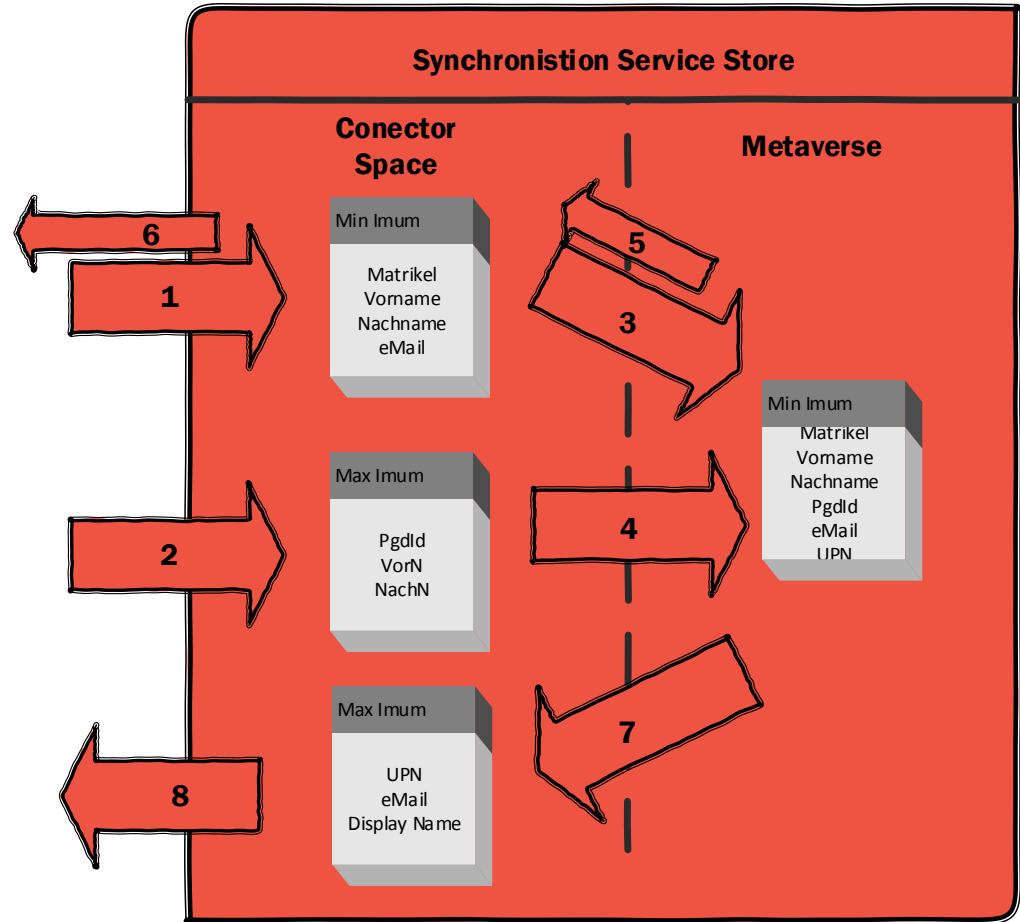
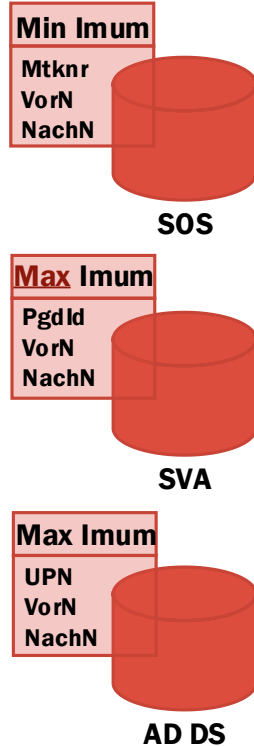
## FIM SyncSrv DB

- [-] FIMSynchronizationService
  - [+] Database Diagrams
  - [-] Tables
    - [+] System Tables
    - [+] dbo.mms\_connectorspace
    - [+] dbo.mms\_cs\_link
    - [+] dbo.mms\_csmv\_link
    - [+] dbo.mms\_extensions
    - [+] dbo.mms\_joiner\_log
    - [+] dbo.mms\_lineage\_cross\_reference
    - [+] dbo.mms\_management\_agent
    - [+] **dbo.mms\_metaverse**
    - [+] dbo.mms\_metaverse\_lineagedate
    - [+] dbo.mms\_metaverse\_lineageguid
    - [+] dbo.mms\_metaverse\_multivalue
    - [+] dbo.mms\_mv\_link
    - [+] dbo.mms\_partition
    - [+] dbo.mms\_recompute\_indicators
    - [+] dbo.mms\_run\_history
    - [+] dbo.mms\_run\_profile
    - [+] dbo.mms\_server\_configuration
    - [+] dbo.mms\_step\_history
    - [+] dbo.mms\_step\_object\_details
    - [+] dbo.mms\_tracking\_entries
    - [+] dbo.mms\_tracking\_entries\_history

```
[ad_UserCannotChangePassword]
[address]
[type]
[c]
[city]
[cn]
[co]
```

Results			Messages
	object_id	object_type	
78	52A8FC72-D6DC-4279-AC7C-A5A0F0A40566	Identity	
79	EAB75184-EAAD-49D0-8158-C18494730D6B	Identity	
80	208D5346-A7E8-4503-8AC0-34DF66CB68FB	Identity	
81	0E357BA6-19E9-4741-AA39-0FDD704AE622	Identity	
82	4A31F0C7-3A20-479B-9128-451B2166117C	Identity	
83	60054EA7-22DB-4D49-A474-F5F3D6C17FA8	Identity	
84	812CBA11-7862-46B4-BA64-725119355561	Identity	
85	00E61D30-090B-4F26-BB8A-AEEA7EFBEA99	Identity	
86	9B020D90-C5A2-448E-9FAF-497DC2259C0B	Identity	
87	15960583-DED7-4C8C-A503-F3BA848309B2	Identity	
88	252277E0-3615-4CDE-BC22-750BF81A1E0F	Identity	

## FIM Datenflüsse



- management agents Tool
- operations Tool
- metavers designer Tool
- metavers search Tool
- joiner Tool



## FIM Management Agent

The screenshot shows the 'Properties' dialog box for the 'Management Agent Designer'. The 'Configure Attributes' tab is selected. The 'Attributes:' section contains a list of attributes with their names and permissions. The 'Configure special' section is partially visible at the bottom.

Name	Permissions
Kurz_akad_c	
Permissions	
Pk_pgd_join	
Text_anredet	
Userid	
affiliations	
pgd_geburts	
pgd_geschle	
pgd_name	
pgd_namens	
pgd_vomame	

Configure special

Set Anchor...

Advanced...

The screenshot shows the 'Properties' dialog box for the 'Management Agent Designer'. The 'Configure Extensions' tab is selected. The 'Configure rules extension for the management agent' section is visible, showing the 'Rules extension name' as 'SVA-RulesExtension.dll'. The 'Password management' section is also visible, with the 'Enable password management' checkbox checked. The 'Supported password operations' section shows three radio buttons: 'Set only', 'Change only', and 'Set and change'. The 'Password synchronization target settings' section is partially visible at the bottom.

Management Agent Designer

Configure Extensions

Configure rules extension for the management agent

Rules extension name: SVA-RulesExtension.dll

☐ Run this rules extension in a separate process

Password management

☒ Enable password management

Extension name:

Connection information for password extension:


Supported password operations:

☐ Set only ☐ Change only ☒ Set and change

Password synchronization target settings:















Configure partition display name(s):

## FIM Extensions

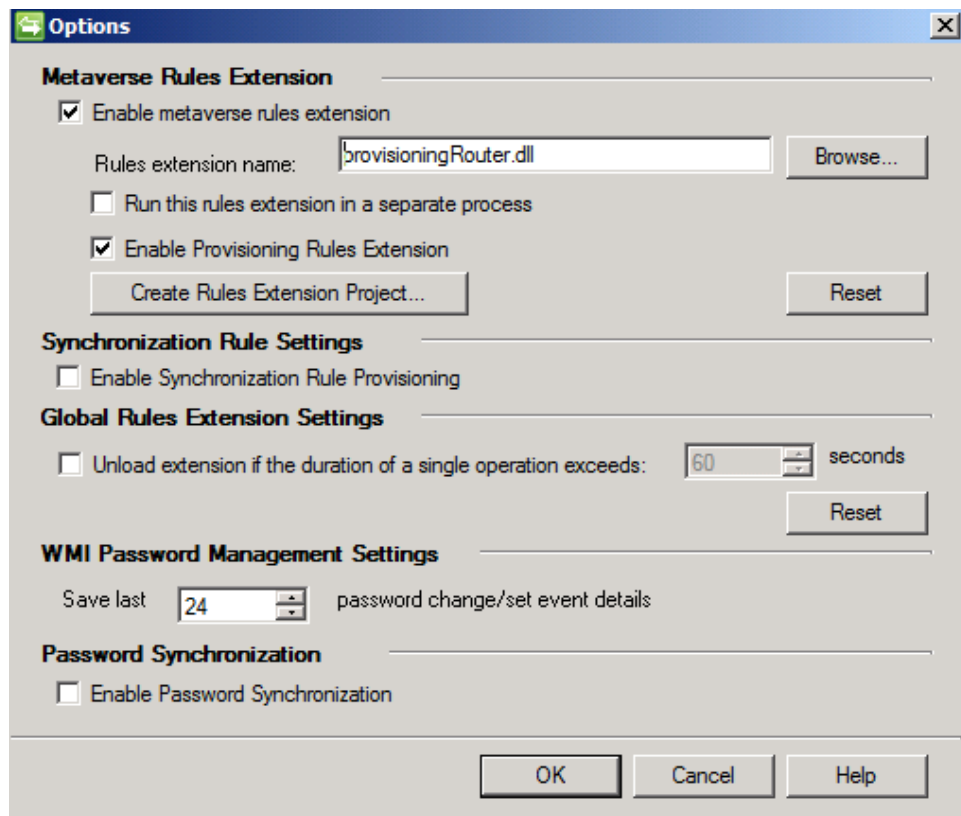
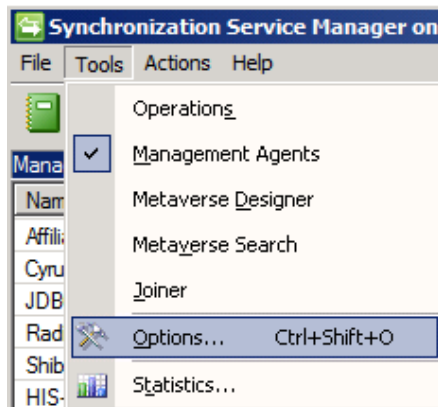
Forefront Identity Manager ▾ 2010 ▾ Synchronization Service ▾ Extensions ▾  Search Extensions

Organize ▾ Include in library ▾ Share with ▾ New folder

- Microsoft Analysis Services
- Microsoft Forefront Identity Manager
  - 2010
    - Synchronization Service
      - Ablaufsteuerung
        - LogFiles
      - Bin
      - Data
      - Extensions**
      - ExtensionsCache
      - MaData
        - Affiliations
        - Cyrus
        - fh-d.lan
        - fh-d.tst
        - FIM Portal
        - fh.fh-d.local

Name	Date modified ▾	Type	Size
 SOS-Export-RulesExtension.dll	11/13/2012 3:36 PM	Application extension	20 KB
 SOS-Export-RulesExtension.pdb	11/13/2012 3:36 PM	PDB File	14 KB
 SOS-RulesExtension.dll	11/13/2012 11:00 AM	Application extension	32 KB
 SOS-RulesExtension.pdb	11/13/2012 11:00 AM	PDB File	26 KB
 SVA-RulesExtension.dll	11/13/2012 10:04 AM	Application extension	32 KB
 SVA-RulesExtension.pdb	11/13/2012 10:04 AM	PDB File	24 KB
 common.dll	11/13/2012 9:42 AM	Application extension	13 KB
 common.pdb	11/13/2012 9:42 AM	PDB File	22 KB
 Cyrus-RulesExtension.dll	7/18/2012 10:39 PM	Application extension	10 KB
 Cyrus-RulesExtension.pdb	7/18/2012 10:39 PM	PDB File	16 KB
 xemail.dll	7/18/2012 12:36 PM	Application extension	30 KB
 xemail.pdb	7/18/2012 12:36 PM	PDB File	92 KB
 FH-D.MetaverseExtension.AD.dll	7/17/2012 11:07 AM	Application extension	20 KB
 FH-D.MetaverseExtension.AD.pdb	7/17/2012 11:07 AM	PDB File	14 KB

## FIM Provisioning Rules



## Gruppenmanagement

**Properties**

Management Agent Designer

- Properties
- Connect to Database
- Configure Columns
- Configure Connector Filter
- Configure Join and Projection Rules
- ➔ Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

**Configure Attribute Flow**

Data Source Attribute	Metaverse Attribute	Type
<b>Object Type: affil...</b>	<b>Object Type: group</b>	
	domain	Constant - F...
	membershipLocked	Constant - tr...
	membershipAddWorkfl...	Constant - ...
<dn>,string_value_in...	memberFilter	Rules Exten...
	type	Constant - S...
	scope	Constant - ...
<dn>,string_value_in...	accountName	Rules Exten...
<dn>,string_value_in...	description	Rules Exten...

Build Attribute Flow...

- Configure Directory Partitions
- Configure Provisioning Hierarchy
- Select Object Types
- Select Attributes
- Configure Connector Filter
- Configure Join and Projection Rules
- ➔ Configure Attribute Flow

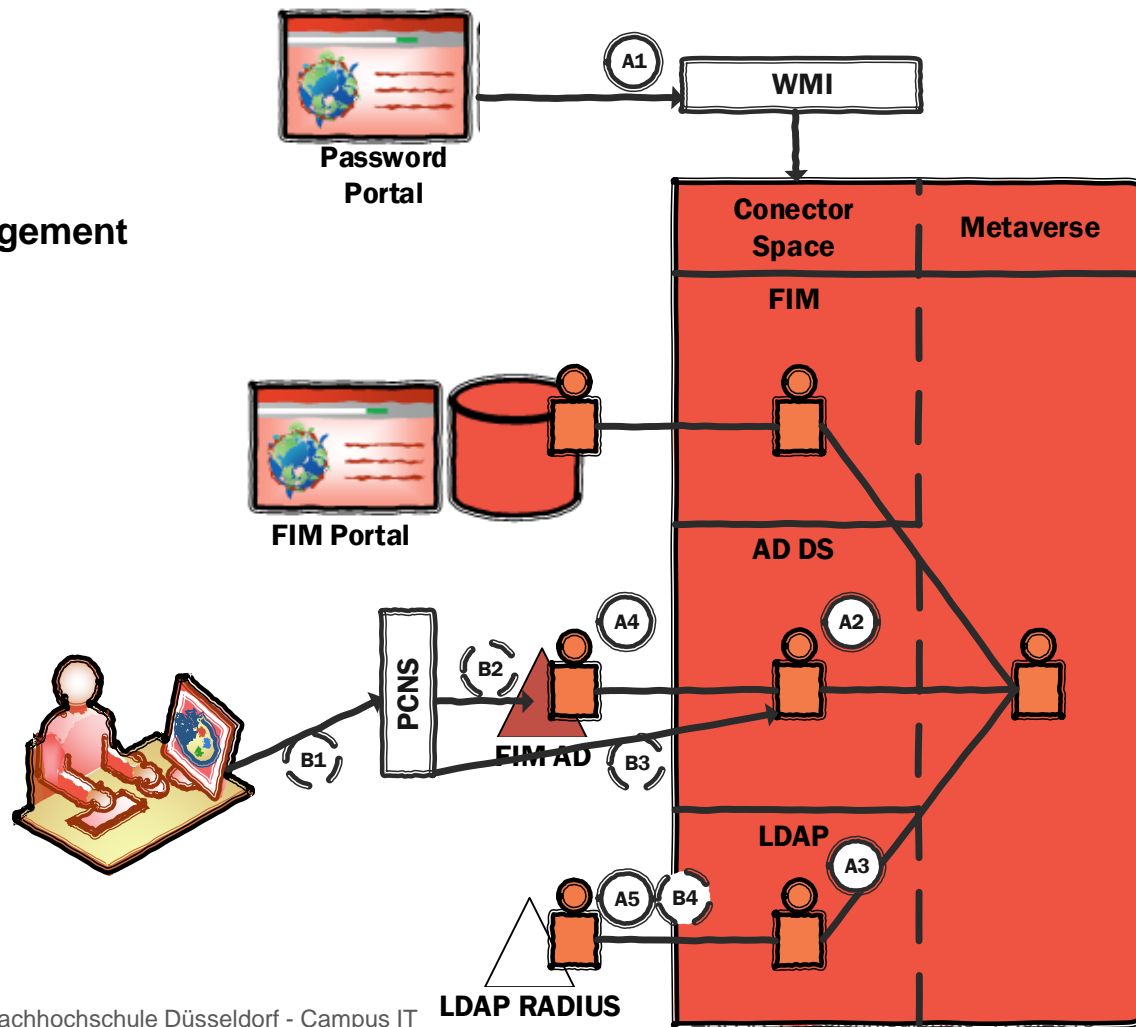
**Configure Attribute Flow**

Data Source Attribute	Metaverse Attribute	Type
<b>Object Type: user</b>	<b>Object Type: Identity</b>	
<b>Object Type: group</b>	<b>Object Type: group</b>	
sAMAccountName	accountName	Direct
member	member	Direct
description	description	Direct
groupType	<object-id>,scope,type	Rules Exten...

Build Attribute Flow...



## Passwortmanagement



**Synchronization Manager on FSYNC**

File Tools Actions Help

Operations Management Agents Metaverse Designer Metaverse Search Joiner

**Management Agents**

Name	Type	Description	State
Affiliations	SQL Ser		
Cyrus	Extensib		
JDBC-GUEST	Extensib		
Radius	Extensib		
Shibboleth	Extensib		

**Properties**

Management Agent Designer

Configure Directory Partitions

Select directory partitions: Refresh ☐ Show All

☒ DC=fim,DC=fh-d,DC=produktion

**Target Management Agents**

Target management agents:

Management Agent Name	Password Management
<input type="checkbox"/> Affiliations	Disabled
<input checked="" type="checkbox"/> Cyrus	Enabled
<input type="checkbox"/> JDBC-GUEST	Disabled
<input checked="" type="checkbox"/> Radius	Enabled
<input type="checkbox"/> Shibboleth	Disabled
<input type="checkbox"/> HIS-SOS	Disabled
<input type="checkbox"/> HIS-SOS-Export	Disabled
<input type="checkbox"/> HIS-SVA	Disabled
<input type="checkbox"/> SVA-Vertrag2Rolle	Disabled

☐ Specify maximum number of password changes for a 24 hour period 5

OK Cancel Help

Connection settings:

Selected domain controllers Configure...

Authentication Security: Options...

Address: fim.fh-d.produktion

Test credentials

Test credentials for this directory partition Set Credentials...

For this partition: Containers...

Authentication: ...

Authentication as a password synchronization source.

Selected synchronization targets: Targets...

## FIM Service und Portal

### FIM Service



Request  
Processor & Permissions



Delegation



AuthN  
Workflow



AuthZ  
Workflow

## Management Policy Rules



New



Details



Delete



Explore

Search for:

Search within:

Advanced Search ▾

## Sets



New



Details



Delete

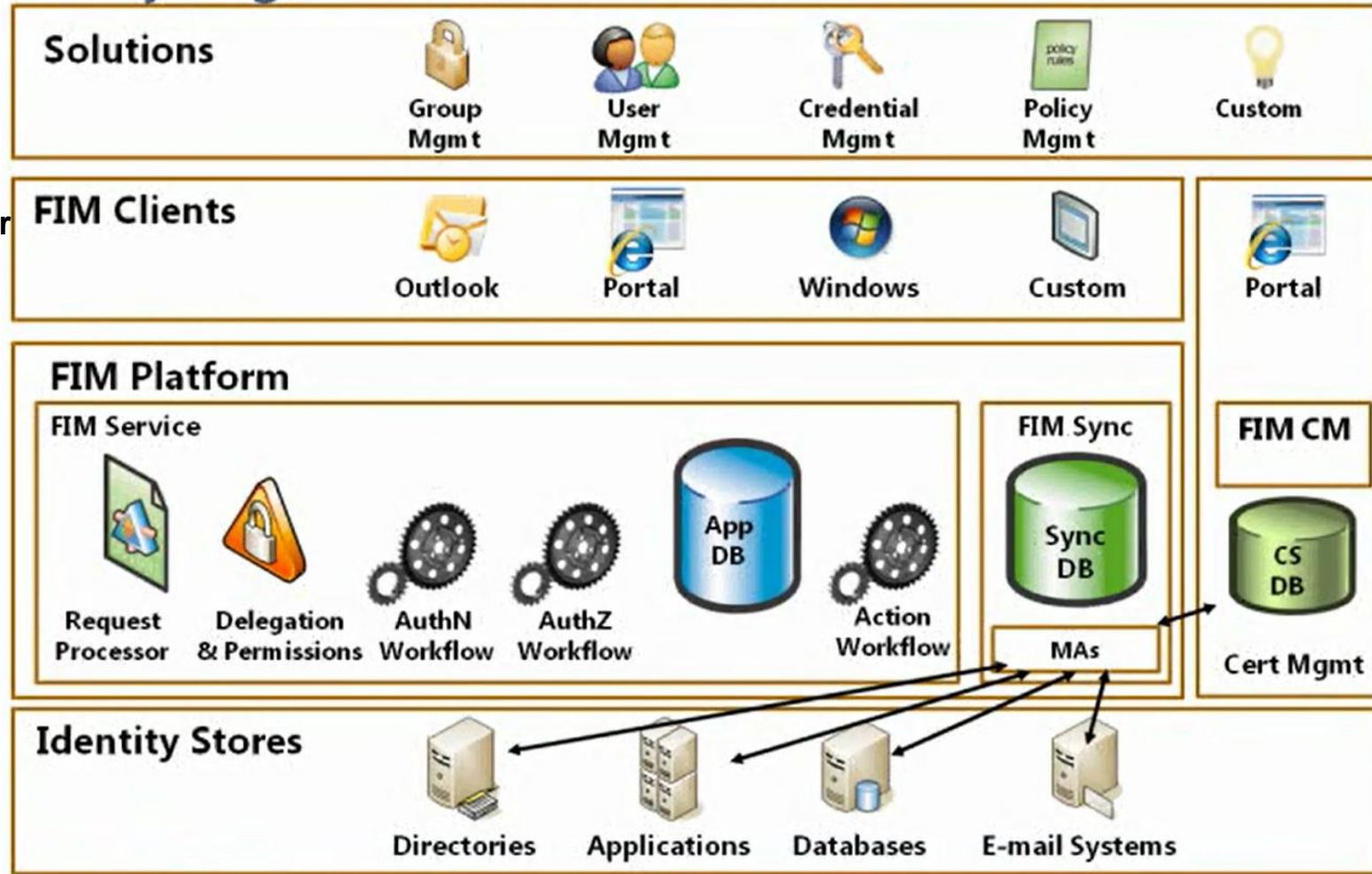
Search for:

Search within:

Advanced Search ▾

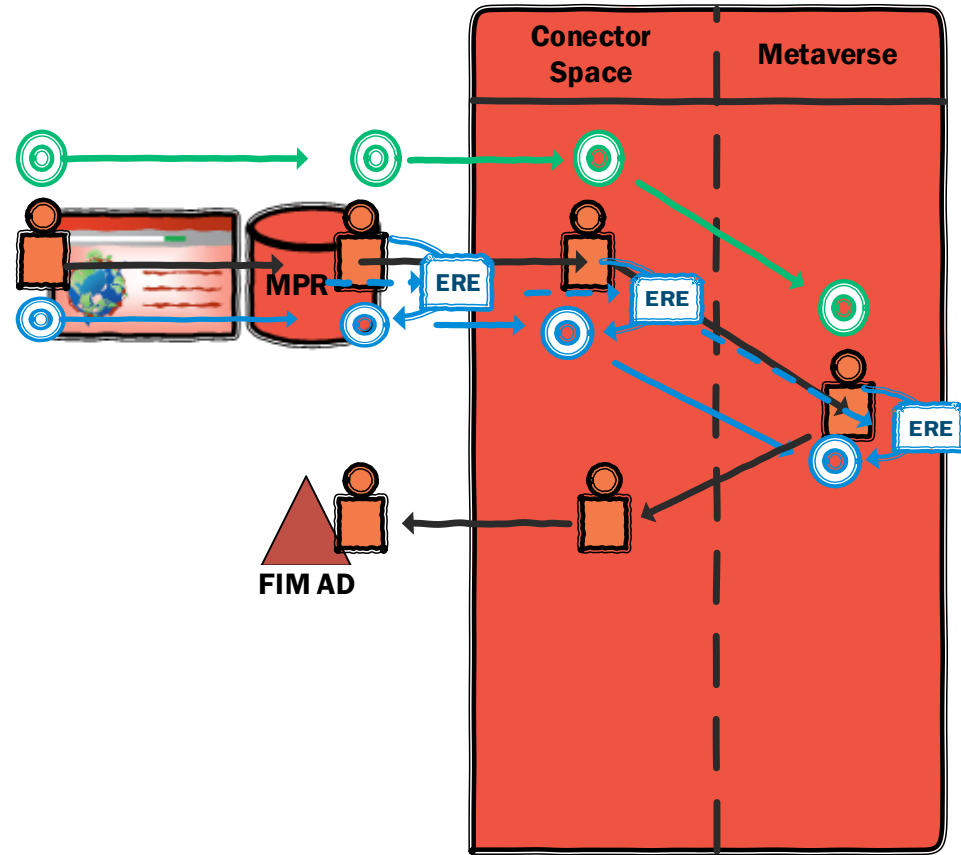
<input type="checkbox"/> Display Name ^	Description								
<input type="checkbox"/> Administrators									No
<input type="checkbox"/> All Active People									No
<input type="checkbox"/> controls detected rule entry resources	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No	No	No	No
<input type="checkbox"/> Synchronization: Synchronization account controls group resources it synchronizes	Create, Delete, Add, Modify, Remove	No	Yes	No	No	No	No	No	No
<input type="checkbox"/> Synchronization: Synchronization account controls synchronization configuration resources	Create, Delete, Add, Modify, Remove, Read	No	Yes	No	No	No	No	No	No
<input type="checkbox"/> Synchronization: Synchronization account controls users it synchronizes	Transition In	No	No	No	No	No	No	Yes	No
<input type="checkbox"/> Temporal policy workflow: Impending group resource expiry notification	Read	No	Yes	No	No	No	No	No	No
<input type="checkbox"/> User management: Users can read attributes of their own	Read	Yes	Yes	No	No	No	No	No	No
<input type="checkbox"/> User management: Users can read selected attributes of other users	Create, Modify	No	Yes	No	No	No	No	No	No
<input type="checkbox"/> Users can create registration objects for themselves									

## FIM Architektur



## FIM Synchronisation Rules

- Klassische Regeln
- beschreibende Regeln
  - Outbound
  - Inbound



### 3 FIM Synchronisierung

- Klassische Synchronisierungsregeln sind
  - mächtig
- Deklarative Synchronisierungsregeln sind
  - flexibel
  - transparent

## **FIM nächste Schritte**

- Anbindung einer Sharepoint Liste mittels WS MA
- Einverständniserklärung zu O365
- Gruppenmanagement für Emaillisten
- Update auf die aktuelle Version
- Umbau auf Sync Rules



FACHHOCHSCHULE DÜSSELDORF  
UNIVERSITY OF APPLIED SCIENCES DÜSSELDORF

**Vielen Dank für Ihre Aufmerksamkeit**