

Praxisbericht

[kein produktives System]

Konzeption, Umsetzung, Einführung

Beispiele für Datenbestände mit Personendaten:

- Studentenverwaltung (HIS-SOS)
- Zentrales Vorlesungsverzeichnis (ZVVZ, HIS-LSF)
- Prüfungsverwaltungssystem (HIS-POS)
- Mitarbeiterverwaltung (HIS-SVA)
- Elektronische Zutrittsberechtigung zu Gebäuden
- Nutzerverwaltung im Telefonbereich
- Nutzerverwaltung für Rechner, Anwendungen, Kommunikation (e-mail, UID/Password für Rechner, WLAN-, Modemzugang, ...)
- Lokales Bibliothekssystem (LBS)
- Mitgliederverwaltung für Wahlen
- Lehr-, Lernmanagementsystem (StudIP)
- Digitale Bibliothek (CM/MyCore) und Dokumentenmanagement

Vorhaben:

- Universitätsweiter Service zur Bereitstellung von Personendaten
- Verbesserung der Qualität und Aktualität der Daten
- Reduzierung auf wenige Anmeldeformulare
- Keine Neuerfassung - nur Ergänzungen!
- Vereinheitlichte Namensgebung (Accounts, MailAdr., Zugangsberechtigungen, etc.)
- Konsequenterer Umsetzung der Nutzerordnung
- Reduzierung des Administrationsaufwandes

Projektstart:

- Beschäftigung mit dem Thema seit 2001



Pragmatisches Vorgehen:

- Workshop im Februar 2001 (1 Tag) mit Teilnehmer aus:
 - Dezernat Studium und Lehre
 - Dezernat Personalangelegenheiten
 - Dezernat Technik
 - Dezernat Recht, Akademische Selbstverwaltung
 - Universitätsbibliothek
 - Referat EDV der Verwaltung
 - Universitätsrechenzentrum
 - Datenschutzbeauftragter der Universität
 - Personalrat
 - Kein Bereich Medizin!

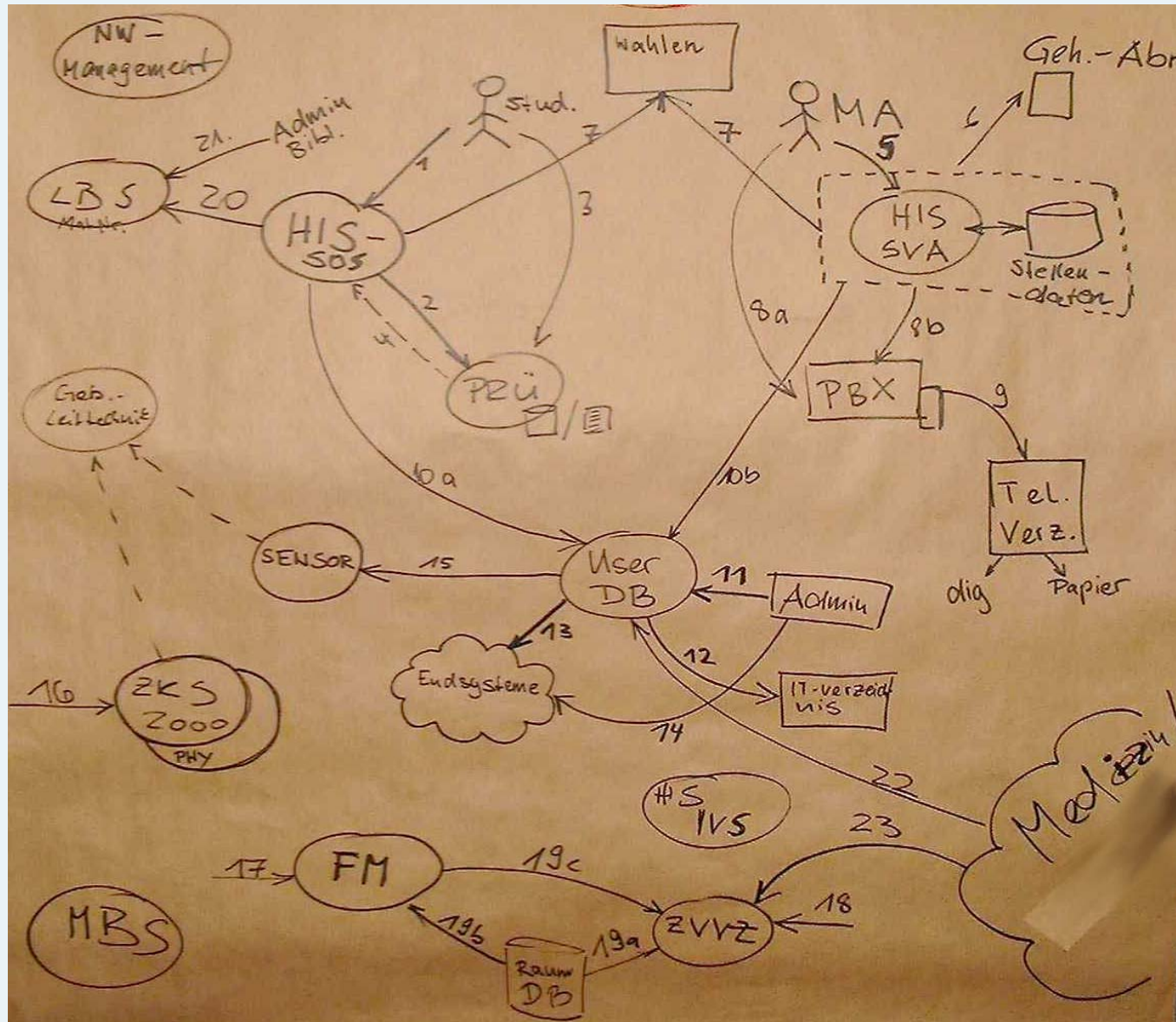
Workshop-Ziele:

- Schaffung eines gemeinsamen Verständnisses über Einsatzmöglichkeiten, prinzipielle Architektur und Nutzung eines Verzeichnisdienstes
- Darstellung der spezifischen Problematik an der Universität Rostock
- Ableitung eines möglichen Einsatzszenarios

Ergebnis:

- Aufzeigen der Σ aller „kleinen Datenverwaltungen“ 
- alle Teilnehmer stimmten für Einf. eines Metadirectory
- vereinfachter Lösungsansatz 

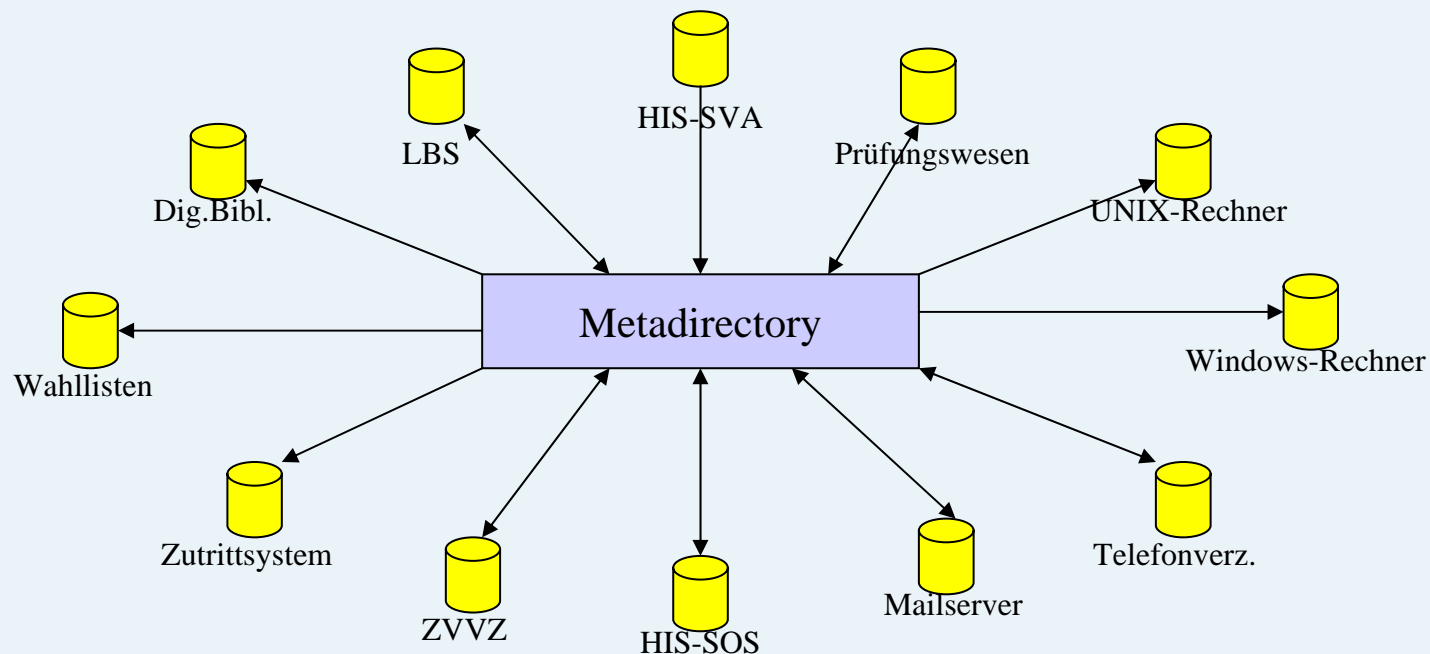
Workshop unter Leitung von Siemens



Verteilung
der
wichtigsten
Daten im
Jahre 2001

Vereinfachter Lösungsansatz:

- automatische Synchronisation heterogener Datenbestände
- nur unbedingt notwendige Daten im zentralen Verzeichnis



Weiteres Vorgehen

- Erstellung eines Grobkonzeptes
- Bewusstsein schaffen für
„gemeinsames Projekt an der Universität“
(Rektor, Kanzler, Dezernenten, Mitarbeiter u.a.)
- Personal (Stellenverstetigung bei lfd. Personalabbau)
- Definition der erforderlichen Dienstleistungen
- Kalkulation der erforderlichen Investitionen
- Produktauswahl

Produktauswahl (Januar – Juli 2002)



- Präsentation von Lösungen durch Firmen vor Ort (Microsoft Metadirectory Services, Novell DirXML, Siemens DirX, Sun ONE Meta Directory)
- Angebote der Firmen

Auswahlkriterien

- ausgereiftes, zuverlässiges Produkt (Referenzinstallationen)
- möglichst wenig Entwicklungsaufwand wegen fehlender Personalkapazität in der Universität
- SW (Entwicklungsstand, Konnektoren, Scriptsprache)
- HW-Anforderungen (Leistung, Kosten, Betriebssystem)
- Dienstleistungen / Zusammenarbeit mit der Firma
- Kosten für Investition, Consulting, Service

Entscheidung zwischen ...

DirXML Novell und **DirX** Siemens

- Verhandlg. mit Siemens über ein spezielles F&L-Paket
 - Preisreduzierung von Juni'02 im Juni'03 auf gut die Hälfte
 - Vertrag mit Siemens im August 2003
 - Erstellung eines Stufenplanes durch RZ 
 - Auftrag an Siemens für Feinkonzept 

Personaleinsatz im MetaDirectory Project

- RZ: 1 Stelle für Konzipierung, Realisierung und Betrieb
- punktuelle Zuarbeit durch andere Mitarbeiter aus RZ, Verwaltungs-DV, Dezernaten
- Siemens: fixer Stundenumfang mit 1100€/Tag

Stufenplan *[erster Versuch]:*

1. Synchronisation von
 - Studentenverwaltung HIS-SOS,
 - lokale Nutzerverwaltung-RZ (Gäste, funkt. Accounts),
 - Windows ADS (incl. LDAP) für Auth. diverser Dienste,
 - LDAP des Mailservers
 - übliche Systeme eines RZ
 - keine Beteiligung Personalrat notwendig
2. Mitarbeiterverwaltung HIS-SVA
 - Personalratsbeteiligung (Abnahme lfd. System)
3. Anbindung weiterer Systeme
 - lokales Bibliotheksystem, etc.
 - Rückschreiben von Inform. in's HIS (RZ-,Bibl.-Daten)
 - Ersatz für Laufzettel bei Exmatrikulation



Erstellung Feinkonzept durch Siemens

- August bis November 2003
- Zuarbeit durch Mitarbeiter der Universität
- Dienstleistungen von Siemens: 28 Personentage

Workshop zur Feinkonzepterstellung




Grundlage:

- Fragenkatalog von Siemens zu den Systemen

Teilnehmer:

- Studentenverwaltung, EDV-Referat der Verwaltung, Rechenzentrum, Datenschutzbeauftragter

Inhalt:

1. Spezifikation der Datenpflegeprozesse 
2. Definition des Datenaustausches mit den Systemen 
3. Datenverwaltung im Metadirectory 



Workshop zur Feinkonzepterstellung

Datenpflegeprozesse:

- Welche aktuellen Datenpflegeprozesse existieren bereits?
 - Neuanlage, Ändern, Löschen
- Welche Datenpflegeprozesse sollen vom Metadirectory abgelöst werden und in welcher Form?
- Welche Prozesse sind zur Status-Pflege notwendig?
 - Active, Inactive, tobeActive, tobeInactive, etc.
- Welches eindeutige Kriterium existiert zur Identifizierung der Objekte in den Anwendungen?



Workshop zur Feinkonzepterstellung

je System ...

- Datenquelle, Datenziele
- welche Schnittstellen existieren
- Auflisten aller relevanten Datenfelder/-attribute
 - Name, Inhalt, Syntax, Wertebereiche
 - eindeutiger Schlüssel
 - Pflichtfeld
 - Datenbesitzer (Priorität)
 - Wer darf anlegen, ändern bzw. löschen?
 - Bemerkungen zu Sonderzeichen
 - Exceptions (z.B. setzen von default-value)
 - Rahmenbedingungen, Abhängigkeiten
 - zeitlicher Ablauf der Datenpflegeprozesse



Workshop zur Feinkonzepterstellung

Metadirectory

- Namensraum festlegen
- Welche Daten sollen wo & wie abgelegt werden?
- Welche Daten müssen generiert werden?
 - Global-Identifizier (MdID, Uid, UidNumber, GidNumber), Email (woraus?), Gültigkeitsbereiche (von/bis), etc.
 - Wie lautet die Bildungsregel?
- Welche zukünftigen Anwendungen könnten Einfluss haben? (Schema)
- Definition administrativer Nutzer & Gruppen
- Festlegung der jeweiligen Rechte



Erfasste Daten und ... {1/2}

Allgemein:

- Name, Vorname, Geschlecht, Geburtsdatum, Titel

Studenten:

- **MatrikelNr**, Rückm.-Status, Semester, WahlFb, Anschrift

Mitarbeiter:

- **PersNr**, Vertragslaufzeit, Kostenstelle, Dienstbez.

Gäste:

- **MD-ID**, Einrichtung, GültigBis

FunktionsAccounts:

- **MD-ID**, RefUser, Beschreibung, ...

MailingLists:

- **MD-ID**, RefUser, Beschreibung, ...

Erfasste Daten und ... auftretende Probleme {2/2}

- Vorerfassung von Mitarbeitern
 - u. U. zu wenig Parameter
- HIS-Anbindung:
 - kein Informix-Agent unter Linux verfügbar
 - keine native LDAP- bzw. ODBC-Schnittstelle
 - Windows-ProxyRechner mit Informix-ODBC-Driver
- ohne Stagingtables nur „Beinahe-Full“-Update möglich
- Problem im HIS-SVA:
 - Strikte Trennung zw. Studenten- und Personaldaten
 - Einträge nach Verträgen nicht nach Personen

Zusätzliche Arbeiten/Änderungen im Projektverlauf

- Emulation HIS-SVA für Phase 1
- Emulation Datenbank Mitarbeiter Bereich Medizin
- Entwurf von diversen SQL-Scripten („schlechte“ Daten der Verwaltung)
- Umstellung der Kostenstellenverarb. (Email-Gruppen ...)
- Einsatzgebiet des WebInterfaces verändert von Info-System zu Admin-System (Sicherheit, autages Netz)
- frühzeitige Einsatz echter HW/SW – kein Entwicklungssystem: gut für Leistungsabschätzung!!!

Zeitliche Umsetzung des Stufenplans



- Anbindung der Quell-Systeme Nov 2003 – Mai 2004
 - Studentenverwaltung HIS-SOS Feb. online
 - Mitarbeiterverwaltung HIS-SVA HS-Bereich Apr. online
 - Mitarbeiterdaten Bereich Medizin (komplett) Apr. offline
 - lokale Daten des RZ Mai online
- Anbindung der Ziel-Systeme Juni 2004 bis Dez 2004
 - ADS, LDAP, Mail, diverse Systeme via SQL-Server
- Installation eines administrativen Web-Frontend Jan 2005
- OnlineTest : ab Jan. 2005??? Wie???
- Produktiv ab Feb. 2005 (ca. 4 Wo. „Parallel“-Betrieb)

Eingesetzte Hard- und Software

Angebot Januar 2003:

- Master und Shadow für „Metastore“:
- 2 x Sun Fire 280R 1x900MHz, 1GB, 2x36GB, Solaris
- Sun StorEdge D2 (105 GB Raid5) kein Cluster!!!
- „Metahub“: Primergy C200 (1,3GHz, 1GB, 2x18GB), W2K

Umsetzung Juli 2003:

- HW:
 - Dell - Cluster 
- SW:
 - 2x W2k3 Server - Enterprise Edition
 - DirX v6.0,
 - DirXmetahub v6.5 
 - DirXweb v6.0

CLUSTER - Lösung



Metastor + Metahub:

- 2x PowerEdge 2650
*Xeon 2x 2,8GHz, 4GB,
2x 36GB*
- Dell „PowerVault 220s“
135GB Raid5 Clusterdrv.

ProxyServer für Verwaltung:

- PowerEdge 650
P4 3GHz, 1GB, 2x72GB

DirXmeta Manager

File Edit View Help

DirXmetahub

Monitor View

Global View
Expert View
Monitor View

Status Data

- Default
- UniR
 - ADS
 - InitialLoad
 - LDAP
 - ODBC
 - PostProc
 - PreProc
 - SendMail
 - Web
 - Zeitgesteuerte Workflows
 - Result=Aborted
 - Result=Error
 - Result=Not OK
 - Result=OK**
 - Primaerdaten Workflows 20041111072614Z
 - UniR_AccessFile_Init_FunktionsAccounts 20041118164746Z
 - UniR_AccessFile_Init_Gaeste 20041118170222Z
 - UniR_AccessFile_Init_MitarbeiterMedizin 20041118165917Z
 - UniR_AccessFile_Init_MitarbeiterVerwaltung 2004111817002Z
 - UniR_AccessFile_Init_Studenten 20041118164828Z
 - UniR_HIS-SOS_costc_ODBC2Meta 20041118041624Z
 - UniR_HIS-SOS_costc_ODBC2Meta 20041123141557Z
 - UniR_HIS-SOS_kfb_ODBC2Meta 20041118041629Z
 - UniR_HIS-SOS_kfb_ODBC2Meta 20041123141617Z
 - UniR_MailServer2MetaStore_ML_Init 20041123102740Z
 - UniR_Meta2ADS_Nachverarbeitung 20041118031523Z
 - UniR_Meta2ADS_Standard_Gruppen 20041118031801Z
 - UniR_MetaStore2MailServer_Sync 20041118032608Z
 - UniR_MSSQL_Pers_ODBC2Meta 20041118041116Z
 - UniR_MSSQL_Pers_ODBC2Meta 20041123144035Z
 - UniR_PostProc2MetaStore (Entries) 20041118041620Z
 - UniR_PreProc2MetaStore 20041118030541Z
 - UniR_PreProc2MetaStore 20041123113732Z
 - UniR_PreProc2MetaStore 20041123140056Z
 - UniR_RZ-MED_ODBC2Meta 20041123092612Z
 - UniR_RZ-MED_ODBC2Meta 20041123115423Z
 - UniR_RZ-MED_ODBC2Meta 20041123115818Z
 - UniR_RZ-MED_ODBC2Meta 20041123120058Z
 - UniR_RZ-MED_ODBC2Meta 20041123134551Z
 - UniR_RZ-SVA_ODBC2Meta 20041123092811Z
 - UniR_RZ-SVA_ODBC2Meta 20041123120233Z
 - Result=Warning
 - Time Constraint
 - Process table

Data View

Name	In Folder	Start	End	Expiration	Result
Primaerdaten W...	Status Data/UniR/Z...	20041111072614.0...	20041111073640.0...	20041211072615.0...	closed.completed.ok
UniR_AccessFil...	Status Data/UniR/O...	20041118164746.0...	20041118164828.0...	20041218164746.0...	closed.completed.ok
UniR_AccessFil...	Status Data/UniR/O...	20041118170222.0...	20041118170344.0...	20041218170223.0...	closed.completed.ok
UniR_AccessFil...	Status Data/UniR/O...	20041118165917.0...	20041118170025.0...	20041218165918.0...	closed.completed.ok
UniR_AccessFil...	Status Data/UniR/O...	20041118170025.0...	20041118170222.0...	20041218170026.0...	closed.completed.ok
UniR_AccessFil...	Status Data/UniR/O...	20041118164828.0...	20041118165917.0...	20041218164828.0...	closed.completed.ok
UniR_HIS-SOS...	Status Data/UniR/O...	20041118041624.0...	20041118041629.0...	20041218041624.0...	closed.completed.ok
UniR_HIS-SOS...	Status Data/UniR/O...	20041123141557.0...	20041123141615.0...	20041223141557.0...	closed.completed.ok
UniR_HIS-SOS...	Status Data/UniR/O...	20041118041629.0...	20041118041631.0...	20041218041629.0...	closed.completed.ok
UniR_HIS-SOS...	Status Data/UniR/O...	20041123141617.0...	20041123141620.0...	20041223141617.0...	closed.completed.ok
UniR_MailServe...	Status Data/UniR/L...	20041123102740.0...	20041123102750.0...	20041223102740.0...	closed.completed.ok
UniR_Meta2AD...	Status Data/UniR/A...	20041118031523.0...	20041118031801.0...	20041218031523.0...	closed.completed.ok
UniR_Meta2AD...	Status Data/UniR/A...	20041118031801.0...	20041118032226.0...	20041218031801.0...	closed.completed.ok
UniR_MetaStore...	Status Data/UniR/L...	20041118032608.0...	20041118032614.0...	20041218032608.0...	closed.completed.ok
UniR_MSSQL...	Status Data/UniR/O...	20041118041116.0...	20041118041619.0...	20041218041117.0...	closed.completed.ok
UniR_MSSQL...	Status Data/UniR/O...	20041123144035.0...	20041123144651.0...	20041223144035.0...	closed.completed.ok
UniR_PostProc...	Status Data/UniR/P...	20041118041620.0...	20041118041624.0...	20041218041620.0...	closed.completed.ok
UniR_PreProc2...	Status Data/UniR/P...	20041118030541.0...	20041118031314.0...	20041218030542.0...	closed.completed.ok
UniR_PreProc2...	Status Data/UniR/Pr...	20041123113732.0...	20041123114606.0...	20041223113732.0...	closed.completed.ok
UniR_PreProc2...	Status Data/UniR/O...	20041123140056.0...	20041123140904.0...	20041223140056.0...	closed.completed.ok
UniR_RZ-MFD	Status Data/UniR/O...	20041123092612.0...	20041123092647.0...	20041223092612.0...	closed.completed.ok

UniR_MSSQL_Pers_ODBC2Meta 20041123144035Z

Workflow Status Data | Structure

Name: UniR_MSSQL_Pers_ODBC2Meta 20041123144035Z

Workflow: UniR_MSSQL_Pers_ODBC2Meta

DirXmetahub Server: main

Parent Activity:

Initiator:

Timing Information

Start Time: 11/23/2004 3:40:35 PM

End Time: 11/23/2004 3:46:51 PM

Expiration Time: 12/23/2004 3:40:35 PM

Result Information

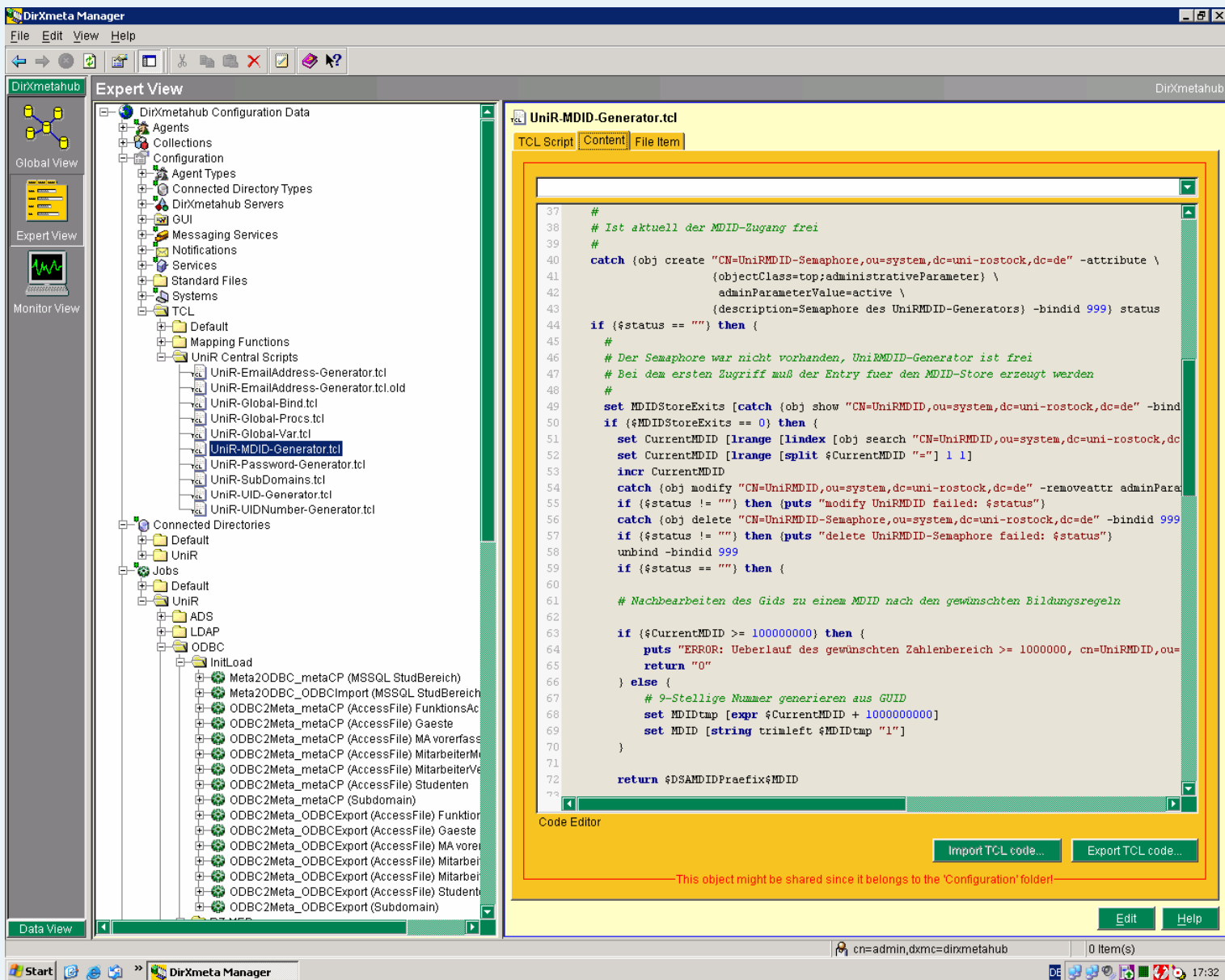
Status: closed.completed.ok

Remark: 0 values

Help

Start DirXmeta Manager

cn=admin,dxmc=dirxmetahub 27 Item(s), 1 selected 17:27



The screenshot displays the DirXmeta Manager application window. The left sidebar contains navigation icons for Global View, Expert View, and Monitor View. The main window is divided into two panes. The left pane, titled 'Expert View', shows a hierarchical tree structure of configuration data, including Agents, Collections, Configuration, Agent Types, Connected Directory Types, DirXmetahub Servers, GUI, Messaging Services, Notifications, Services, Standard Files, Systems, and TCL. The right pane, titled 'UniR-MDID-Generator.tcl', displays the content of a TCL script. The script is a TCL script that manages the MDID (MetaDirectory ID) for a specific object. It includes comments in German and TCL code for creating, updating, and deleting the MDID entry. The script is titled 'UniR-MDID-Generator.tcl' and is located in the 'TCL Script' folder. The script content is as follows:

```

37 #
38 # Ist aktuell der MDID-Zugang frei
39 #
40 catch {obj create "CN=UniRMDID-Semaphore,ou=system,dc=uni-rostock,dc=de" -attribute \
41         {objectClass=top;administrativeParameter} \
42         {adminParameterValue=active \
43         {description=Semaphore des UniRMDID-Generators} -bindid 999} status
44 if {$status == ""} then {
45     #
46     # Der Semaphore war nicht vorhanden, UniRMDID-Generator ist frei
47     # Bei dem ersten Zugriff muß der Entry fuer den MDID-Store erzeugt werden
48     #
49     set MDIDStoreExits [catch {obj show "CN=UniRMDID,ou=system,dc=uni-rostock,dc=de" -bind
50     if {$MDIDStoreExits == 0} then {
51         set CurrentMDID [lrange [lindex [obj search "CN=UniRMDID,ou=system,dc=uni-rostock,dc
52         set CurrentMDID [lrange [split $CurrentMDID "="] 1 1]
53         incr CurrentMDID
54         catch {obj modify "CN=UniRMDID,ou=system,dc=uni-rostock,dc=de" -removeattr adminPara
55         if {$status != ""} then {puts "modify UniRMDID failed: $status"}
56         catch {obj delete "CN=UniRMDID-Semaphore,ou=system,dc=uni-rostock,dc=de" -bindid 999
57         if {$status != ""} then {puts "delete UniRMDID-Semaphore failed: $status"}
58         unbind -bindid 999
59         if {$status == ""} then {
60             #
61             # Nachbearbeiten des Gids zu einem MDID nach den gewünschten Bildungsregeln
62             #
63             if {$CurrentMDID >= 1000000000} then {
64                 puts "ERROR: Ueberlauf des gewünschten Zahlenbereich >= 10000000, cn=UniRMDID,ou=
65                 return "0"
66             } else {
67                 # 9-Stellige Nummer generieren aus GUID
68                 set MDIDtmp [expr {$CurrentMDID + 1000000000}]
69                 set MDID [string trimleft $MDIDtmp "1"]
70             }
71             return $DSAMDIDPraefix$MDID
72         }
73     }

```

The script is displayed in a 'Code Editor' window. Below the code editor, there are buttons for 'Import TCL code...' and 'Export TCL code...'. A status bar at the bottom of the window indicates the current user is 'cn=admin,dn=cn=dirxmetahub' and the current item is '0 item(s)'. The system tray at the bottom right shows the time as 17:32.

Testumgebung / Sicherungen / Fehlerbereinigung

Softwareupdate:

- (autom.) Erstellen eines Images mit „Acronis TrueImage“
- Simuliertes MetaDir-Cluster auf VMware GSX-Server

Disaster Recovery:

- tägl. Export aus DirX, Metahub, Registry ins Filesystem
- tägl. Sicherung des Filesystems
- Image-Generierung nach entscheidenden Änderungen

Fehlererfassung und -bereinigung:

- zentraler Mailaccount
- Hierarchie von Administratoren

Beteiligung Personalrat / Datenschutzbeauftragter

- Teilnahme am START-Workshop
 - grundsätzliche Zustimmung durch beide
- Stufe 1 (ohne Mitarbeiterverwaltung)
 - Datenschutzbeauftragter dabei
- Stufe 2 (mit HIS-SVA)
 - Personalrat ist beteiligt
 - Datenschutzbeauftragter dabei

Fazit für „uns“:

- neben technischem Aufwand ex. bes. hoher org. Aufwand
- Abhängig von aktiver Mitarbeit aller beteiligten Einrichtungen
- Bewusstsein für gemeinsames Projekt schaffen
- Quelldaten (HIS-SOS/SVA) müssen vorher überarbeitet werden
- lokale Sytem-Änderungen wirken nun global (Absprache!!!)
- während der Realisierung lfd. Fortschreibung d. Feinkonzeptes
- Inanspruchnahme von Consultants der Hersteller ist effektiv und empfehlenswert
- Identity-Management nicht “von der Stange” zu haben, sondern sehr individuelles System entspr. der Prozesse in der Univers.