



Identity & Access Management: Das Rückgrat der Hochschul-IuK-Infrastruktur

IntegraTUM – Teilprojekt Verzeichnisdienst

24. September 2009

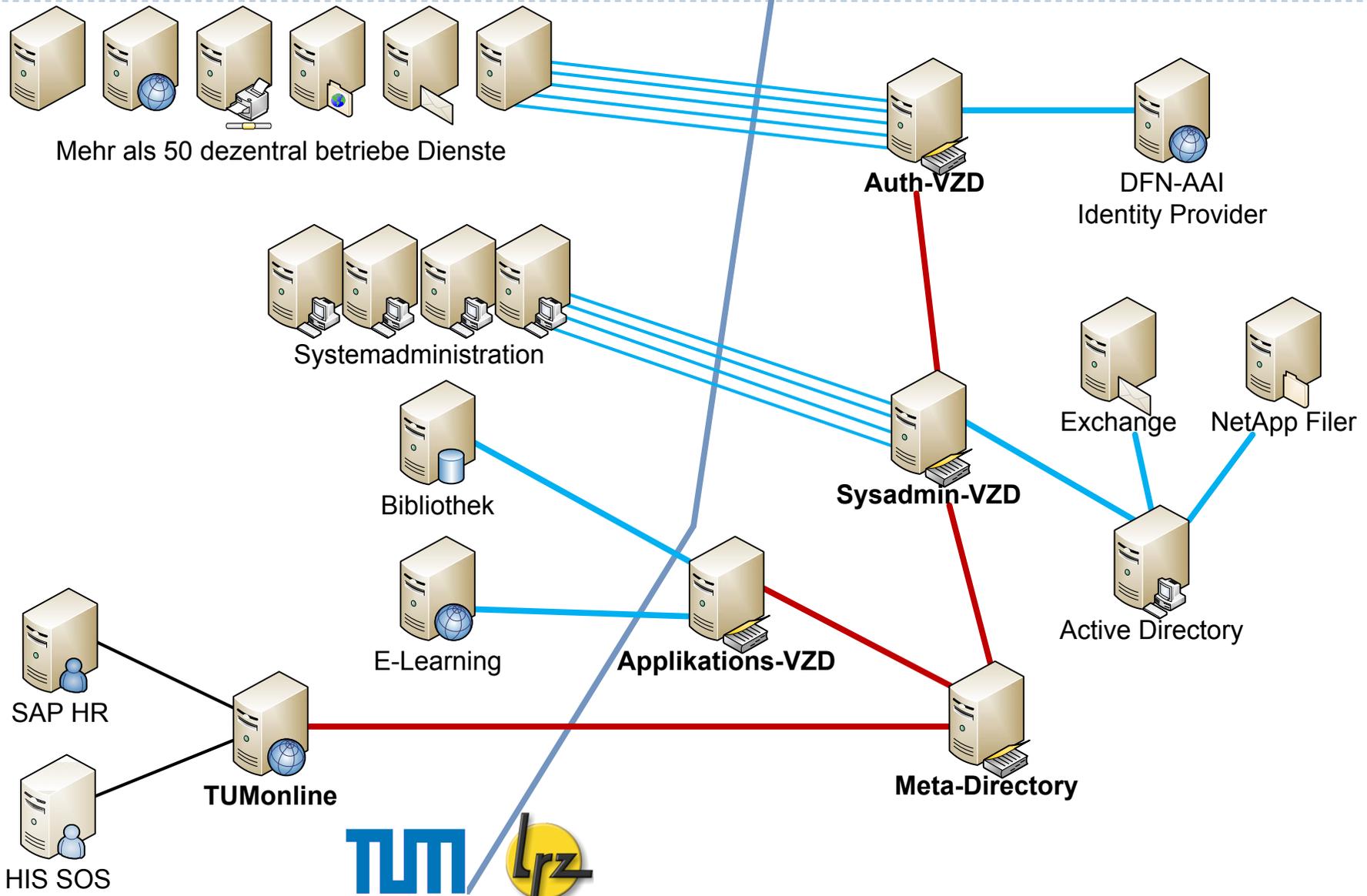
Dr. Wolfgang Hommel, Leibniz-Rechenzentrum



IntegraTUM

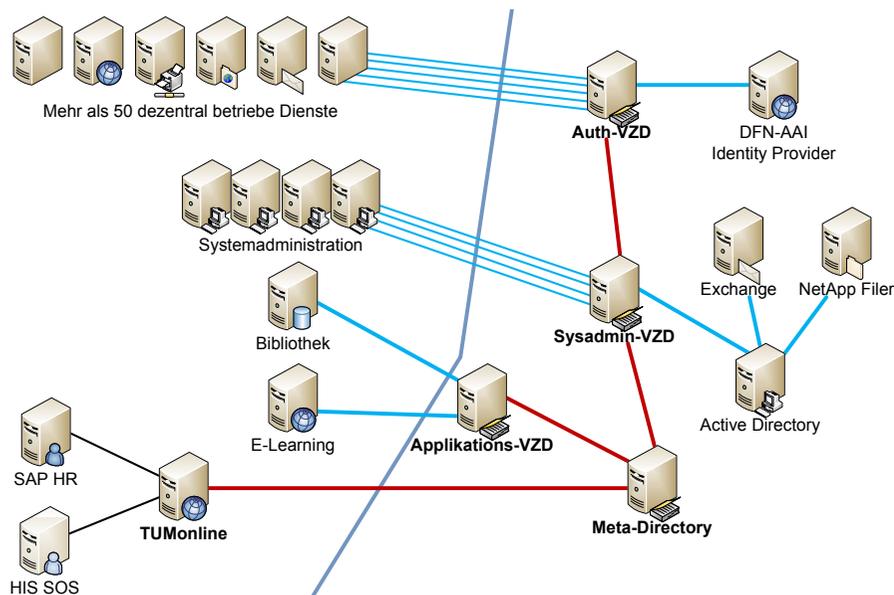


Identity & Access Management Architektur





Mehrwert durch die I&AM-Architektur



Für die Benutzer

Für die Verwaltung

Für die Dienstleister

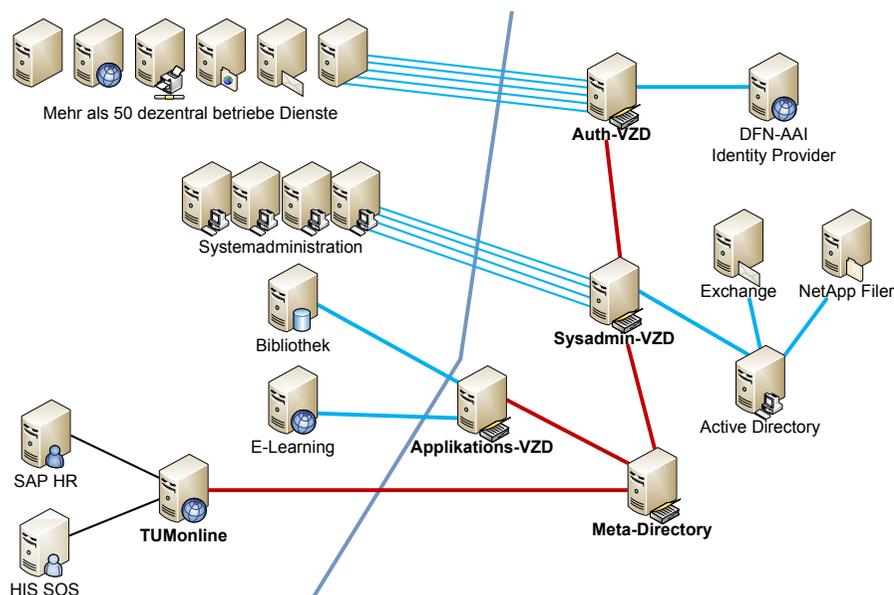
Nur eine Kennung (Loginname und Passwort) für alle IT-Dienste im Umfeld der TUM

Alle Dienste ab dem ersten offiziellen Tag an der TUM nutzbar

Stamm-/Kontaktdatenänderungen automatisch und schnell an alle IT-Dienste propagiert



Mehrwert durch die I&AM-Architektur



Nur noch ein einziges
verwaltungsexternes System mit
Benutzerdaten zu versorgen

Klare Zuständigkeiten durch
Schnittstellenvereinbarung
zwischen Verwaltung und
technischem Identity Management

Für die Benutzer

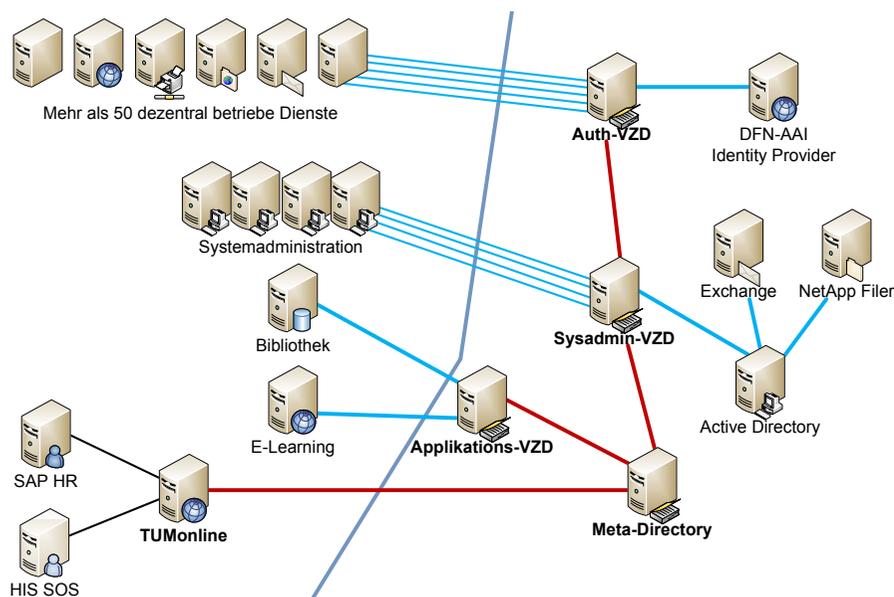
Für die Verwaltung

Für die Dienstleister

Nahtlose Integration in das
Campus Management



Mehrwert durch die I&AM-Architektur



Automatisierung von Anlegen, Freischalten, Aktualisieren und Löschen von Kennungen

Alle benötigten Benutzerdaten im richtigen Format und aus einer einzigen, autoritativen, dauerhaft verfügbaren Quelle

Für die Benutzer

Für die Verwaltung

Für die Dienstleister

Verringerter Supportaufwand
(z.B. vergessene Passwörter)



Herausforderungen im Betrieb



Unvollständige, in sich widersprüchliche oder veraltete Personendatensätze (Datenqualität)

Zurücksetzen vergessener Passwörter, Registrieren von Gästen, Überprüfen von Berechtigungen (TUM IT Service Desk)

Performance an Stichtagen zur Account-Freischaltung, Initialabgleiche mit neuen Zielsystemen, Resynchronisation nach Ausfall

Wolfgang Hommel (wolfgang.hommel@mytum.de) Di 22 Sep 17:01:34 2009

Abmelden Queue-Ansicht Telefon-Ticket E-Mail-Ticket Suche Einstellungen Sammelaktion Kalender FileManager FAQ Neue Nachricht Gesperrte Tickets

[Inhalt Ticket#: 200905121000621] LDAP Adressbuch im Mailprogramm [Alter: 133 Tage 6 Stunden]

Zurück - Sperren - Historie - Drucken - Priorität - Freie Felder - Verknüpfen - Besitzer - Kunde - Notiz - Zusammenfassen - Warten - Schließen

Erstellt: 12.05.2009 10:56:04

1 -> 1. Kunde (E-Mail an extern) (Gast) Andreas Hubel <...>: LDAP Adressbuch im M... | 12.05.2009 10:56:04
 2 -> 2. Agent (Notiz für intern) (Gast) TUM Service Desk: | LDAP Adressbuch im M... | 13.05.2009 08:47:18
 3 -> 3. Kunde (E-Mail an extern) (Gast) LRZ-Wolfgang: | Ihre Meldung hat de... | 13.05.2009 09:11:04
 4 -> 4. Kunde (E-Mail an extern) (Gast) LRZ-Wolfgang: | Antwort des LRZ - TT... | 13.05.2009 09:21:04
 5 -> 5. Kunde (E-Mail an extern) (Gast) LRZ-Wolfgang: | FYI: Das TT023292... | 13.05.2009 09:21:05
 6 -> 6. Agent (Notiz für intern) (Gast) TUM Service Desk: | Antwort des LRZ - TT... | 13.05.2009 14:21:24
 7 -> 7. Kunde (E-Mail an extern) (Gast) Andreas Hubel <...>: Antwort des LRZ - TT... | 13.05.2009 14:26:05
 8 -> 8. Agent (Notiz für intern) (Gast) Silvia Knitt <...>: Besitzer aktualisiert... | 13.05.2009 14:36:54
 9 -> 9. Agent (Notiz für intern) (Gast) Wolfgang Hommel: | Note - 13.05.2009 16:02:02
 10 -> 10. Agent (Notiz für intern) (Gast) Wolfgang Hommel: | Besitzer aktualisiert... | 13.05.2009 16:02:32
 11 -> 11. Agent (E-Mail an extern) (Gast) TUM Service Desk: | Antwort des LRZ - TT... | 14.05.2009 11:14:41
 12 -> 12. Kunde (E-Mail an extern) (Gast) Andreas Hubel <...>: Antwort des LRZ - TT... | 14.05.2009 11:21:03
 13 -> 13. Agent (Notiz für intern) (Gast) Silvia Knitt <...>: Besitzer aktualisiert... | 14.05.2009 11:37:42
 14 -> 14. Kunde (E-Mail an extern) (Gast) "Borgeest, Rolf": | Antwort des LRZ - TT... | 14.05.2009 20:16:01
 15 -> 15. Agent (Notiz für intern) (Gast) Silvia Knitt <...>: Besitzer aktualisiert... | 14.05.2009 15:50:24
 16 -> 16. Kunde (E-Mail an extern) (Gast) "Hommel, Wolfgang": | Neue Notiz: Besitzer... | 14.05.2009 17:56:03
 17 -> 17. Agent (Notiz für intern) (Gast) Silvia Knitt <...>: Schließen: 09.05.2009 15:51:09

Von: "Hommel, Wolfgang" <Wolfgang.Hommel@lrz.de>
 An: OTRS Notification Master <otrs-support@tum.de>
 Cc: "Borgeest, Rolf" <rolf.borgeest@tum.de>
 Betreff: Re: [Ticket#200905121000621] Neue Notiz (Besitzer aktualisiert...)
 Erstellt: 19.05.2009 17:56:03

Diese Nachricht wurde in einem Zeichensatz erstellt, der nicht Ihrem eigenen entspricht. Wenn sie nicht korrekt angezeigt wird, hier klicken um sie in einem neuen Fenster angezeigt zu bekommen

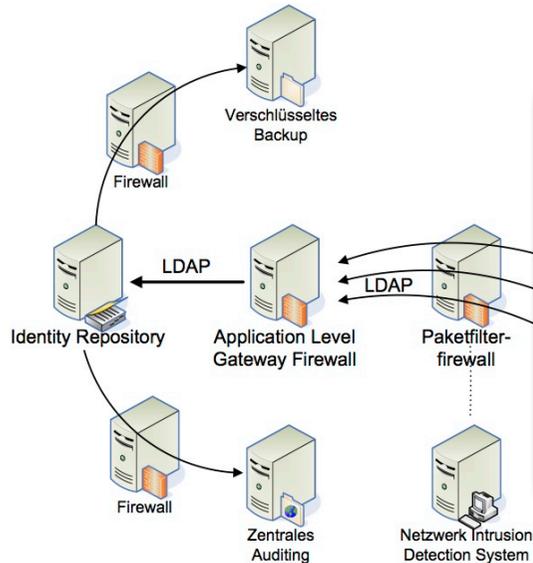
Antwort erstellen (E-Mail):
 • LRZ-Anfrage
 • LRZ-Anfrage Rückfrage

Kunden-Info:

Name	Zu...	Status	Host-CPU - MHz	Hostarbeitsspei...	Gastarbeitsspei...	Verwendung
iadm1		○○○	207	2128	54	IntegraTUM L
iauth2		○○○	148	2129	36	IntegraTUM L
imd1		○○○	439	2131	52	IntegraTUM L
imd2		○○○	148	2135	40	IntegraTUM L
iapp2		○○○	116	2130	36	IntegraTUM L
iadm2		○○○	140	2124	42	IntegraTUM L
mytumgrp		○○○	91	274	22	Web Services
imgritum		○○○	87	1082	34	Novell iManag
iauth1		○○○	176	2135	41	IntegraTUM L
transfer		○○○	80	231	4	Datenaustaus
cmdmd		○○○	195	2117	31	IntegraTUM-E
iapp1		○○○	162	2135	38	IntegraTUM L



Sicherheit und Datenschutz



Integration ins LRZ-Serverbetriebskonzept
(Zutrittskontrolle, OS-Updates, Patch-Management, ...)

LDAP Access Control Lists (ACLs)

LDAP-Zugriff bevorzugt im User-Kontext (ohne Proxy-User)

TUM		TECHNISCHE UNIVERSITÄT MÜNCHEN
		Der Beauftragte für den Datenschutz Prof. Dr. B. Radig
Verfahrensbeschreibung		
<small>Art 27 des Bayerischen Datenschutzgesetzes (BayDSG) bestimmt, dass die behördlichen Datenschutzbeauftragten ein Verzeichnis der bei der öffentlichen Stelle eingesetzten und dienstverpflichteten Mitarbeiterinnen und Mitarbeiter anzuhalten sind. Dieses Verzeichnis enthält die gemäß Art. 26 Abs. 3 Satz 1 BayDSG erforderlichen Verfahrensbeschreibungen und, falls noch nicht erfolgt, die Vorklärung einer Fragestellung als auch die Erstellung des Verzeichnisses. Zur Vorklärung des Akts der Vorklärung sind die erforderlichen Angaben in der Datei dieser Beschreibung, die Datei auf Diskette kopiert und die Diskette an den Datenschutzbeauftragten geschickt werden.</small>		
Diese Beschreibung dient		
X	der erstmaligen Beschreibung des Verfahrens	
	der Änderung der Verfahrensbeschreibung vom: 06.09.2008	Aktenzeichen:
Die Beschreibung wurde erstellt von: Dr. Rolf Borgeest am: 15.09.2008		
1. Bezeichnung des Verfahrens und allgemeine Angaben		
Bezeichnung des Verfahrens:	Connector IntegraTUM/Verzeichnis zu CLIX (eLearning-Plattform)	
Dienststellen, an denen das Verfahren eingesetzt wird:	Medienzentrum der TUM	
Nähere Auskunft erteilt:	Dr. Rolf Borgeest	
Telefon:	289-16162	E-Mail: rolf.borgeest@tum.de
2. Zweck und Rechtsgrundlagen der Erhebung, Verarbeitung oder Nutzung		
Aufgaben, zu deren Erfüllung die personenbezogenen Daten erhoben, verarbeitet oder genutzt werden?	Übernahme von Login- und Studiengangsinformationen aus dem zentralen Verzeichnis der TUM in die zentrale eLearning Plattform CLIX.	
	Art. 42(4) BayDSchG (Erhebung), Art. 55(2) BayDSchG, Art. 61 BayDSchG (Fernstudium bzw. eLearning)	
3. Art der gespeicherten Daten		
U.S.:	Bezeichnung der Daten*	
Nr.:		
1.	Nutzerklasse (Mitarbeiter oder Student)	
2.	Matrikel (Identifikator im Münchner Wissenschaftsnetz)	
3.	Kennung (LRZ Kennung)	
4.	Login Name (gleichzeitig eMail-Adresse z.B. franz.gans@tum.de , gans@mytum.de)	
5.	Gültigkeit Login	
6.	Name	
7.	Vorname	
8.	1. Studiengang Name	
9.	1. Studiengang Abschluss	
10.	Anrede	
11.	Titel	

Datensparsamkeit: Auslieferung nur wirklich benötigter Benutzerdaten ans jeweilige Zielsystem

Verfahrensbeschreibungen, Zusammenarbeit mit TUM
Datenschutzbeauftragtem und Gesamtpersonalrat

Selbstauskunft über TUMonline



Mehr als nur Technik...



Integration in die
Hochschulprozesse

Individuelle Unterstützung
bei der Dienstintegration

Erfahrungsaustausch und
Kooperationen mit anderen
europäischen Hochschulen

Integration der Thematik in
Lehrveranstaltungen,
wissenschaftliche Arbeiten



Ziele für die Weiterentwicklung



Flächendeckender Rollout

Anbindung aller Fakultäten an die
Verzeichnisdienste zur Systemadministration
Integration weiterer dezentraler IT-Dienste

Münchenweite Prozesse

Durchgängige Datensynchronisation mit dem
LRZ Identity Management
Gezielte Unterstützung hochschulübergreifender Studiengänge

Ausbau von Single Sign-On und DFN-AAI-Nutzung

Shibboleth-Anpassung weiterer zentraler und
dezentraler Dienste
Öffnung ausgewählter Dienste für externe Nutzer