



Netzwerktechnik und Verteile Systeme

Sebastian Simon

A photograph of a server room with blue ambient lighting. Rows of server racks are visible, with some racks having glass doors that show internal components. Cables are organized on overhead trays.

Teil 4: Verzeichnisdienste

Verzeichnisdienste (1)

- Verzeichnisdienst stellt in einem Netzwerk eine zentrale Sammlung von Daten zur Verfügung
- Verzeichnis wie Telefonbuch (nicht Dateiordner)
- In der Regel verwendet um Benutzerdaten zentral zu sammeln und zur Verfügung zu stellen
- Ermöglicht Abbildung der Organisationsstruktur

Verzeichnisdienste (2)

- Bekannte Verzeichnisdienste sind
 - Active Directory (Microsoft Windows Server)
 - Open Directory (Apple macOS Server)
 - OpenLDAP (Linux, Windows, MacOS)
- Verzeichnisdienste basieren fast immer auf dem LDAP-Netzwerkprotokoll
 - Lightweight Directory Access Protocol (LDAP)

Verzeichnisdienste (3)

- Benutzer werden zentral verwaltet
 - Müssen nicht auf jedem Rechner einzeln angelegt werden
 - Administrator kann Passwort von Nutzer resetten
- Zuordnung in hierarchische Teilorganisationen
 - zB Benutzer ist Abteilung Marketing zugeordnet
- Berechtigungen der Benutzer werden geregelt
 - Berechtigung ob eigenes Passwort änderbar ist
 - Sind Zugriff auf bestimmte Netzlaufwerke erlaubt

Zugriffskontrolle

- Nicht jeder Benutzer/Prozess soll alles dürfen
 - zB Geschäftsberichte darf nur Geschäftsleitung lesen
- Bevor Nutzer Aktion ausführt muss geprüft werden, ob er dazu berechtigt ist
- Zugriffskontrolle verifiziert Zugriffsrechte
- Authorisation ist die Vergabe von Zugriffsrechten

Zugriffskontrollmatrix

Access Control Matrix

| Capability | Subject | File 1 | File 2 | File 3 | File 4 |
|------------|---------|--------------|--------------|--------------|--------------|
| | Larry | Read | Read, write | Read | Read, write |
| | Curly | Full control | No access | Full control | Read |
| | Mo | Read, write | No access | Read | Full control |
| | Bob | Full control | Full control | No access | No access |
| | | | | | |

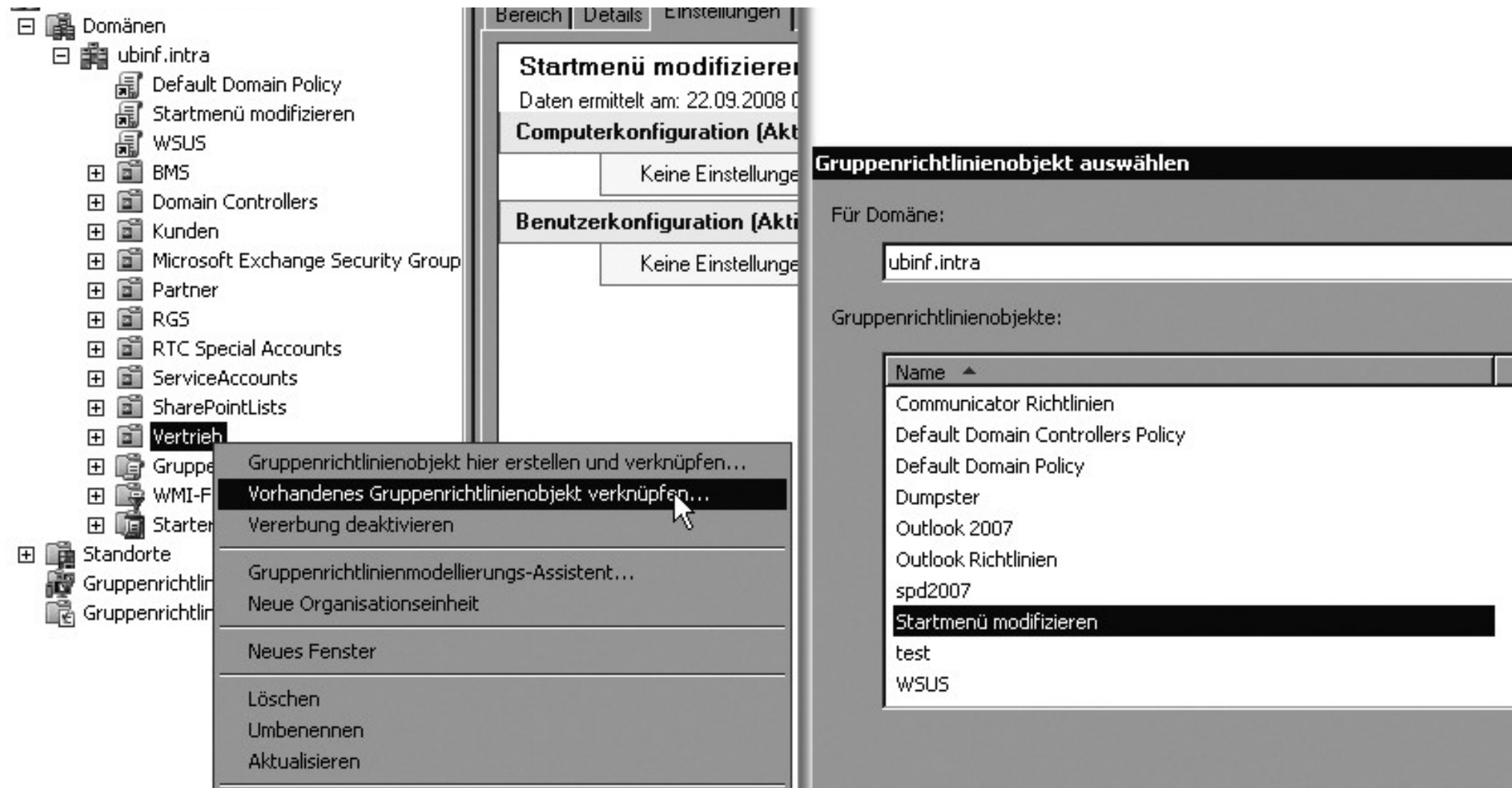
ACL

Capability = row in matrix

ACL = column in matrix

Gruppenbasierte Zugriffskontrolle

- Bei vielen Benutzern und Rechten wird die Zugriffskontrollmatrix sehr groß ($n*m$ Einträge)
- Vereinfachung durch Zusammenfassen der Nutzer zu Gruppen
- Gruppen erhalten Berechtigungen auch für alle Benutzer in der Gruppe gelten
 - zB Gruppe Geschäftsleitung definieren
 - Leseberechtigung auf Ordner Geschäftsberichte
 - Vorstandsmitglieder werden der Gruppe zugewiesen

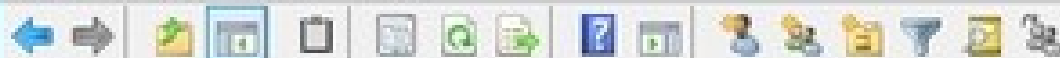


Rollenbasierte Zugriffskontrolle

- Ähnlich wie Gruppenbasierte Zugriffskontrolle
- Es werden Rollen definiert, die gewisse Berechtigungen haben
- Benutzer haben eine oder mehrere Rollen
- Durchführen von Aktionen erlaubt, wenn Benutzer die richtige Rolle hat
 - zB Ordner Geschäftsberichte ist für alle User mit Rolle Geschäftsleitung freigegeben

Active Directory Users and Computers

File Action View Help




Active Directory Users and Computers [LAB01]

- Saved Queries
- ▾ schulenburg.lab
 - Built-in
 - Computers
 - Domain Controllers
 - Exchange
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Microsoft Exchange Security Groups
 - Users

| Name | Type | Description |
|------------------------------|-------------------|------------------------------|
| Compliance Management | Security Group... | This role group will allo... |
| Delegated Setup | Security Group... | Members of this manag... |
| Discovery Management | Security Group... | Members of this manag... |
| Exchange Servers | Security Group... | This group contains all t... |
| Exchange Trusted Subsystem | Security Group... | This group contains Exc... |
| Exchange Windows Permis... | Security Group... | This group contains Exc... |
| ExchangeLegacyInterop | Security Group... | This group is for interop... |
| Help Desk | Security Group... | Members of this manag... |
| Hygiene Management | Security Group... | Members of this manag... |
| Managed Availability Servers | Security Group... | This group contains all t... |
| Organization Management | Security Group... | Members of this manag... |
| Public Folder Management | Security Group... | Members of this manag... |
| Recipient Management | Security Group... | Members of this manag... |
| Records Management | Security Group... | Members of this manag... |
| Server Management | Security Group... | Members of this manag... |
| UM Management | Security Group... | Members of this manag... |
| View-Only Organization M... | Security Group... | Members of this manag... |

< III >



```
@Secured({ "ROLE_MANAGER" })  
public void readBusinessReport(int year) {  
    ...  
}
```


A photograph of a server room with blue ambient lighting. Several server racks are visible, with one rack in the foreground having its glass door open, revealing internal components. A semi-transparent white rectangle is overlaid on the center of the image, containing the text "Active Directory".

Active Directory

Active Directory

- AD verwaltet verschiedene Objekte in einem Netzwerk
 - Benutzer, Gruppen, Computer
 - Dienste, Server, Dateifreigaben
 - andere Geräte (Drucker, Scanner, ...)
- Ermöglicht Gliederung des Netzwerks
 - Nach seiner räumlicher Verteilung
 - Nach der realen Struktur der Organisation

Active Directory (2)

- Mit AD kann man die Informationen der Objekte
 - organisieren
 - bereitstellen
 - überwachen
- Den Nutzern können Zugriffsbeschränkungen erteilt werden
 - Nicht jeder Benutzer kann auf jede Datei zugreifen
 - Es kann festgelegt werden, wer welchen Drucker verwenden darf

Bestandteile

- Active Directory ist in drei Teile aufgegliedert:
 - Schema
 - Konfiguration
 - Domain

Bestandteile(2)

- Schema ist eine Schablone für alle AD-Einträge
- Definiert Objekttypen und die dazugehörigen Klassen und Attribute
 - Objekttyp ist zB ein Benutzer
- Klassen und Attribute definieren, welche Eigenschaften ein Objekttyp hat
 - Benutzer hat Benutzername, Vorname, Nachname, Kürzel, Telefonnummer, E-mail-Adresse, etc.

Bestandteile (3)

- Die Konfiguration beschreibt die Active-Directory Gesamtstruktur und deren Bäume
 - Gliederung nach Standorten
 - Gliederung in Organisationseinheiten (OU)
- Die Domain enthält alle Information sich und und die in ihre erstellen Objekte
 - Welche Server, Computer, Nutzer, Drucker, etc. es gibt
 - Welchem Standort bzw. OU sie zugeordnet sind

Eine Domäne pro Standort, Rest OUs

