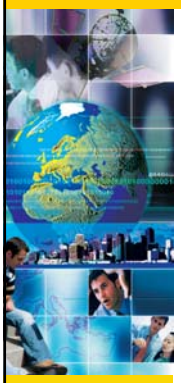


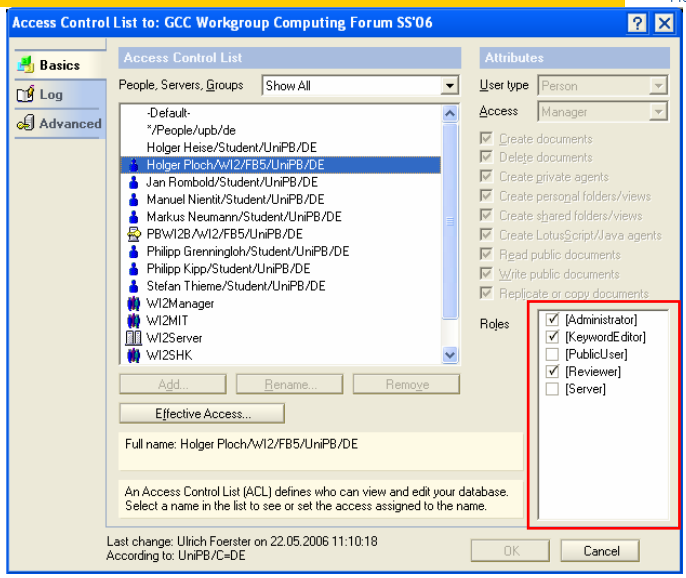
Workgroup Computing Praktikum

Accessing Elements Within a Database

University of Paderborn
Business Computing 2 – Information Management & Office Systems
Faculty of Business Administration, Business Computing & Economics
Prof. Dr. Ludwig Nastansky
Warburger Str. 100, D-33098 Paderborn
Tel.: +49--5251--60-3368
http://gcc.upb.de

- **Rollen werden insbesondere verwendet, um die Administration vieler Benutzer einer Datenbank zu vereinfachen**
  - Rollen werden in der ACL einer Datenbank definiert und Benutzern und Gruppen zugewiesen
- **Rollen werden in Designelementen verwendet, um den Zugriff von Nutzern zu beschränken**
  - Einsatz z. B. in Views, Forms, Dokumenten, Sections

Rollen in der ACL



Vorteile von Rollen

- Für einen Teil der Benutzer können flexibel Zugriffsrechte festgelegt werden
- Rollen können in Formeln verwendet werden
- Rollen bieten eine einfache Möglichkeit, eine Untergruppe von Benutzern zu definieren
- Rollen müssen nicht im Domino Directory eingetragen werden, sondern werden in der jeweiligen DB definiert
- Anwendungen müssen nicht geändert werden, wenn Mitarbeiter hinzukommen oder das Unternehmen verlassen

Rollen in Formeln I

- **Rollen können zur Festlegung von Zugriffsrechten auf einzelne Designelemente herangezogen werden**
  - Zugriffe auf Views und Folders
  - Dokumente erstellen, lesen oder bearbeiten
  - Zugriffe auf Sections (Abschnitte) innerhalb von Dokumenten
- **Nutzung von @Functions zur Ermittlung der Rollen des aktiven Benutzers**
  - @UserRoles: Liefert eine Textliste mit den Rollen des aktuellen Benutzers
  - @UserNamesList: liefert eine Textliste mit:
    - den Namen des aktuellen Benutzers
    - allen Gruppen des aktuellen Benutzers
    - allen Rollen des aktuellen Benutzers
- **Achtung: Rollen setzen nicht die Access Control Levels der jeweiligen Nutzer in der ACL außer Kraft!**

Rollen in Formeln II

- **Das Vergleichen von den aktuell zugewiesenen Rollen des Benutzers mit den für den Zugriff auf die jeweilige Funktionalität vorausgesetzten Rollen erfolgt wieder mit @Functions**
  - @IsMember (textValue; textListValue)
  - @IsNotMember (textValue; textListValue)
- **Beispiel:**

  @IsMember ("[Redaktion]";@UserRoles)

  liefert 1, wenn dem Benutzer die Rolle „Redaktion" zugewiesen wurde

Übung: Rollen in Formeln

- UserRoles:= “[Commander]":“[Designer]":“[Student]":“[Prof“];
- Albert:=“[Designer]":“[Student]";
- Berta:=“[Schüler]":“[Student]";
- Cecilia:=“[Kandidat]":“[Manager]";

- !@IsMember(Albert;UserRoles) = 0
- @IsNotMember(Albert;UserRoles) = 0

- !@IsMember(Berta;UserRoles) = 1
- @IsNotMember(Berta;UserRoles) = 0

- !@IsMember(Cecilia;UserRoles) = 1
- @IsNotMember(Cecilia;UserRoles) = 1

Übung: Rollen erstellen

- **Erstellt folgende Rollen in der „Garage“-Datenbank**

Rolle	Beschreibung
DEmployee	**Vertriebsmitarbeiter**
GEmployee	**Werkstattmitarbeiter**
Designer	**Designer**
Manager	**Manager**

- Die Rollen werden später verwendet

Zugriffskontrolle für Dokumente

Zugriff	Kontrolliert von ...
Lesezugriff auf Dokumente	... Lesezugriffslisten ... Leserfeldern (Reader Fields)
Bearbeitungszugriff auf Dokumente	... Autorenfeldern (Author Fields) ... Abschnitten mit Zugriffskontrolle
Erstellzugriff	... Form-Properties: include in menu: „Create menu“ ... Erstellzugriffslisten

Leserfelder verwenden

- **Ein Leserfeld (Reader Field) beschränkt das Leserecht für ein Dokument auf die Benutzer, Benutzergruppen und Rollen, die in diesem Feld aufgelistet sind**
- **Leserfelder schränken die in der ACL gewährten Zugriffsrechte ein**
  - Jene Benutzer, welche in der ACL keine Rechte haben, können die Dokumente auch dann nicht lesen, wenn sie im Leserfeld eingetragen sind
  - Benutzer, die in der ACL mit Editorzugriff oder höher bedacht sind, können Dokumente nicht lesen, wenn ein Leserfeld in ihnen vorhanden ist und sie in diesem nicht eingetragen sind

Leserfelder und Replikation

- **Bei Dokumenten mit Leserfeldern werden nur die Dokumente repliziert, bei denen der aktuelle Benutzer bzw. Server im Leserfeld eingetragen ist**
- **Damit die Anwendung vollständig repliziert wird, muss der Name von Replizierservern in die Leserfelder aufgenommen werden**
- **Ist ein Leserfeld leer, so kann jeder mit mindestens Reader-Zugriff in der ACL das Dokument lesen**
- **Beim Nutzen von Leserfeldern sollte man immer aufpassen, dass man nicht sich selbst oder andere Nutzer vom zu nutzenden Datenbestand ausschließt**
  - Fehlerhafte Eingaben in einem Leserfeld können praktisch einem Datenverlust gleichgesetzt werden, wenn kein Anwender mehr Zugriff auf das Dokument hat

Autorenfelder verwenden

- **Benutzer mit Autorzugriff auf einer Datenbank dürfen Dokumente erstellen und lesen, standardmäßig aber keine Dokumente - auch nicht die selbst erstellten - bearbeiten**
- **Damit Autoren die von ihnen selbst erstellten Dokumente bearbeiten können, müssen sie im Autorenfeld aufgeführt sein**
- **Autorenfelder überschreiben nicht die Einstellungen in der ACL**
  - Benutzer mit Editorzugriff oder höher können jedes für sie sichtbare Dokument bearbeiten, auch wenn ihr Name nicht im Autorenfeld aufgeführt ist
  - Benutzer mit dem ACL-Level Reader oder niedriger können ein Dokument nicht bearbeiten, auch wenn ihr Name im Autorenfeld aufgeführt ist

Zusammenspiel der Felder

ACL Level	Authors Field Exists and User Is in It	Readers Field Exists and User Is in It	Can Read Document	Can Edit Document
Author	Yes	No	Yes	Yes
Author	No	Yes	Yes	No
Author	No	No	No	No
Manager	Yes	No	Yes	Yes
Manager	No	Yes	Yes	Yes
Manager	No	No	No	No
Editor	Yes	No	Yes	**Yes**
Editor	No	Yes	Yes	Yes
Editor	No	No	No	No
Reader	Yes	No	**Yes**	**No**
Reader	No	Yes	Yes	No
Reader	No	No	No	No

Zugriff für anonyme Web-Benutzer

- **Benutzer mit Webzugriff auf eine Datenbank können von Notes nicht auf die gleiche Weise identifiziert werden wie die Nutzer des Notes Clients**
  - Erinnerung: Anonymous-Eintrag in der ACL
- **Domino bietet die Möglichkeit, die maximale Zugriffsebene bei Zugriff mit Internet-Namen und Kennwort festlegen**
  - Einstellung im ACL-Dialog: „Advanced“ → „Maximum Internet name & password“
  - Die höchste Zugriffsebene, welche man im Web zulassen sollte, ist Editor

Beispiel-ACL I

- **Eine ACL für eine Diskussionsdatenbank mit niedrigen Sicherheitsanforderungen**
  - Es sollten aus Sicherheitsgründen maximal Editorrechte für den Zugriff auf die Datenbank aus dem Web heraus vergeben werden (siehe Advanced-Tab in ACL-Dialog)

ACL-Eintrag	Zugriffsebene
-Default-	Author
Anonymous	Author
Vorgesetzte	Editor

Beispiel-ACL II

- **Eine ACL für eine vertrauliche Datenbank mit hohen Sicherheitsanforderungen**
  - Es sollten aus Sicherheitsgründen maximal Leserrechte für den Zugriff auf die Datenbank aus dem Web heraus vergeben werden (siehe Advanced-Tab in ACL-Dialog)

ACL-Eintrag	Zugriffsebene
-Default-	no access
Anonymous	no access
Berechtigte Leser	Reader
Mitarbeiter	Author
Vorgesetzte	Editor

Ziel: Zugriffskontrolle für die „Garage“ Datenbank

Modifiziere die Sicherheitseinstellungen in der „Garage“ Datenbank

- Alle Mitarbeiter sollten alle Dokumente lesen können
- Nur die Personen mit der Rolle „DEmployee“ sollen Aufträge und Fragen erstellen können
- Nur Werkstattmitarbeiter sollen Annotions-Dokumente erstellen können
- Nur die Personen, die ein Frage-Dokument erstellt haben, sollten dieses Dokument bearbeiten können