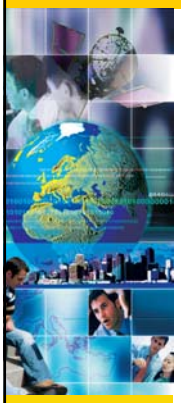
Groupware Competence Center GCC



Workgroup Computing Praktikum

Defining Access to a Database

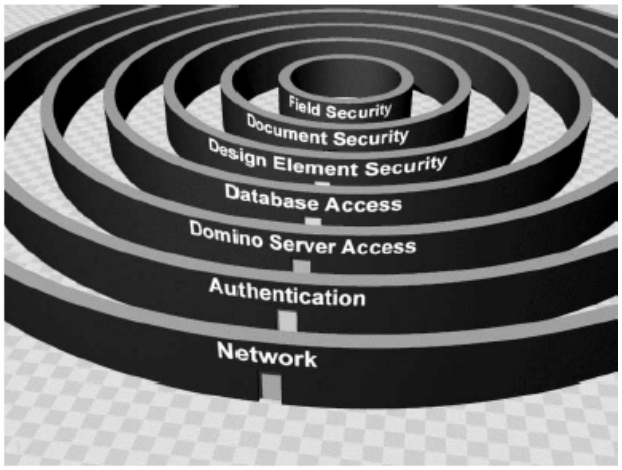
University of Paderborn
Business Computing 2 – Information Management & Office Systems
Faculty of Business Administration, Business Computing & Economics
Prof. Dr. Ludwig Nastansky
Warburger Str. 100, D-33098 Paderborn
Tel.: +49--5251--60-3368
http://gcc.upb.de

Sicherheit der Datenbank

- **Eine Lotus Notes Datenbank und deren Inhalte können mittels der Access Control List (ACL) vor unautorisiertem Zugriff geschützt werden**
  - Einzelnen Nutzern, Servern sowie Gruppen von Nutzern und Servern können unterschiedliche Zugriffsprivilegien (Access Control Level) auf die Datenbank gewährt werden
- **Das Regeln des Datenbankzugriffes auf Netzwerk- und Serverebene ist Aufgabe des Netzwerk- und Systemadministrators**
- **Bei jedem Zugriff eines Nutzers oder eines Servers auf die Datenbank werden mittels der Access Control List (ACL) die aktuellen Zugriffsrechte ermittelt**
  - Manager weisen Benutzern eine Zugriffsebene zu, die sie zur Arbeit innerhalb der Anwendung berechtigt
  - Will ein User eine bestimmte Aktion durchführen, greift Domino auf die ACL zu, um die Privilegien innerhalb der Datenbank zu ermitteln
  - Um eine Modifikation der ACL vornehmen zu können muss der jeweilige Server oder Nutzer Manager-Rechte in dieser Datenbank besitzen

Domino Sicherheitsmodell

- **Das Sicherheitsmodell von Lotus Domino ist in verschiedene Schichten unterteilt, welche dem Entwickler ein größtmögliches Maß an Konfigurierbarkeit der Zugriffe auf eine Datenbank gestatten.**



ACL - Privilegien I

Access Control Level	Rechte
No Access	Kein Zugriff auf Datenbank
Depositor	Dokumente erstellen, jedoch nicht lesen, bearbeiten oder löschen
Reader	Dokumente lesen, jedoch nicht erstellen, bearbeiten oder löschen

ACL - Privilegien II

Access Control Level	Rechte
Author	Dokumente erstellen und lesen. Ein Bearbeiten ist nur dann möglich, wenn dieses im Dokument selber explizit festgelegt worden ist.
Editor	Dokumente erstellen, lesen und bearbeiten bis auf spezielle Ausnahmen
Designer	Wie Editor, können zudem das Design der Datenbank verändern, die Datenbank aber nicht löschen
Manager	Uneingeschränkter Zugriff auf die Datenbank, das Design und die ACL

Besondere ACL-Einträge

- **Mit dem ACL-Eintrag „Default“ werden die Zugriffsprivilegien für alle Benutzer festgelegt, die in der ACL nicht explizit oder implizit aufgeführt sind.**
- **Mit dem ACL-Eintrag „Anonymous“ werden die Zugriffsrechte für nicht-authentifizierte Nutzer festgelegt**
  - Wenn in der ACL kein „Anonymous“-Eintrag vorhanden ist, dann gelten für alle nicht-authentifizierten Benutzer die Default-Rechte
  - Jeder Web-Nutzer bekommt Anonymous-Zugriffsrechte, wenn der Eintrag in der ACL vorhanden ist. Ist kein Anonymous-Eintrag vorhanden, so erhält er Default-Rechte!
- **Aus Sicherheitsgründen sollte in einer Datenbank immer ein Benutzer mit dem Namen „Anonymous“ angelegt und konfiguriert werden!**

Benutzerarten I

- **Der Eintrag „User Type“ legt fest, ob ein Eintrag in der ACL eine Person, ein Server oder eine Gruppe ist**
  - Domino kennt verschiedene „User Types“:
    - Person, Server
    - Server Group, Person Group, Mixed Group
    - Unspecified

- **Das Festlegen der Art des Benutzers kann vor folgendem Szenario schützen:**
  1. Tobias öffnet die Datenbank Policies und stellt fest, dass Angela Editorrechte besitzt
  2. Tobias bekommt Zugriffsrechte für den Server, erstellt dort eine Gruppe mit der Bezeichnung „Angela“ und fügt sich selbst dieser Gruppe hinzu
  3. Als Mitglied der Gruppe „Angela“ hat Tobias jetzt Zugriffsrechte auf die Datenbank
  4. Um das zu verhindern, sollte der Eintrag Angela als Person gekennzeichnet werden

Benutzerarten II

User Type	Beschreibung
Person	Wird vergeben, wenn der ACL-Eintrag für einen einzelnen Benutzer steht **Spezifische Zugriffsrechte („einzelne Benutzer“) haben immer Vorrang vor unspezifischen Zugriffsrechten („Gruppe“)**
Server	Wird vergeben, wenn der ACL-Eintrag für einen Server steht
Mixed group / Person group / Server group	Wird vergeben, wenn der ACL-Eintrag für eine Liste von Personen und / oder Servern steht, die auf gleiche Funktionen zugreifen sollen und die gleichen Rechte hierfür benötigen **Falls ein Nutzer Mitglied in zwei Gruppen ist, werden ihm die Rechte der Gruppe mit dem höheren Zugriffslevel zugewiesen**

Setzen der ACL: Beispiele

Um…	… so setze…
... den Zugriff unbekannter Benutzer zu verhindern, ...	... Default auf No Access.
... jedem das Lesen von Dokumenten zu ermöglichen, ...	... Default und Anonymous auf Reader.
... allen Usern in der Gruppe „Studenten“ das Modifizieren des Datenbankdesigns zu ermöglichen, ...	... Studenten auf Designer.
... Forms zur Vorschau im Webbrowser anzuzeigen, während an der Datenbank gearbeitet wird, ...	... Anonymous auf Author.

Präzisieren der ACL I

Access Level	Berechtigungen	Optionale Berechtigungen
No Access	Keine	Read public documents Write public documents
Depositor	Create documents	Read public documents Write public documents
Reader	Read public documents	Create private agents Create personal folders/views Create LotusScript/Java agents Write public documents Replicate or copy documents

Präzisieren der ACL II

Access Level	Berechtigungen	Optionale Berechtigungen
Author	Read public documents	Create documents Delete documents Create private agents Create personal folders/views Create LotusScript/Java agents Write public documents Replicate or copy documents
Editor	Create documents Read public documents Write public documents	Delete documents Create private agents Create personal folders/views Create shared folders/views Create LotusScript/Java agents Replicate or copy documents

Präzisieren der ACL III

Access Level	Berechtigungen	Optionale Berechtigungen
Designer	Create documents Create private agents Create personal folders/views Create shared folders/views Read public documents Write public documents	Delete documents Create LotusScript/Java agents Replicate or copy documents
Manager	Wie Designer, zusätzlich: Create LotusScript/Java agents	Delete documents Replicate or copy documents

Konsistente ACL

- **Die Option „Enforce a consistent Access Control List across all replicas“ stellt sicher, dass sämtliche Repliken der Datenbank (lokal oder auf Servern) die gleiche ACL besitzen**
  - Vereinfachung der Administration komplexer Applikationen
  - Kein Sicherheitsfeature!