Praktikum

Workgroup Computing 1

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

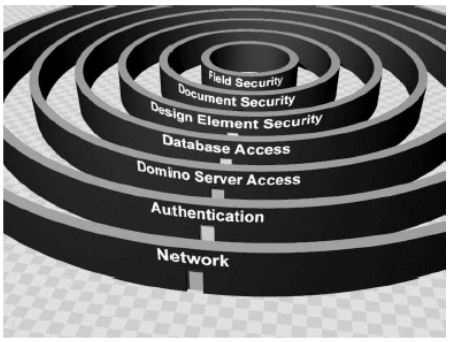
Sicherheit der Datenbank

- **Schützen der Datenbank vor unautorisiertem Zugriff**
- **Zugriffsrechte innerhalb der Datenbank verwalten**

Access Control Level:

- **Regeln des Zugriffs auf Netzwerk- und Serverebene ist Aufgabe des Netzwerk- und Systemadministrators**
- **Zugriff auf die Datenbank →Access Control List (ACL)**
  - Manager weisen Benutzern eine Zugriffsebenen zu, die sie zur Arbeit innerhalb der Anwendung berechtigt
  - Will ein User eine bestimmte Aktion durchführen, greift Domino auf die Zugriffskontrollliste zu, um die Privilegien innerhalb der Datenbank zu ermitteln
  - Um die ACL zu ändern ist Manager Access notwendig!

Domino Sicherheitsmodell in Schichten



Access Control Level 1

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

Access Control Level 2

Access Control Level	Rechte
Autor / Author	Können Dokumente erstellen und lesen. Bearbeiten nur, wenn das im Dokument selber festgelegt ist.
Editor	Alle Dokumente erstellen, lesen, bearbeiten bis auf spezielle Ausnahmen
Entwickler / Designer	s. Editor, können Gestaltung der Datenbank verändern, aber nicht löschen
Manager	Können alle Funktionen ausüben inkl. Ändern der ACL

Benutzer in der ACL identifizieren

Option/ Beschreibung	Definiert den Zugriff für…
-Default-	Alle Benutzer, die in der ACL nicht speziell aufgeführt sind
Gruppen	Liste von Personen, die auf gleiche Funktionen zugreifen können Falls ein Benutzer Mitglied in zwei Gruppen ist, wir ihm die Rechte der höheren Ebene zugewiesen
Einzelne Namen	Ein spezieller Benutzer Falls der Benutzer zu einer Gruppe gehört, werden die Einstellungen der Gruppe überschrieben
Anonymous	Jeder nicht authentifizierte Benutzer Gibt es keinen Anonymous Eintrag, gelten für nicht authentifizierte Benutzer die Rechte von Default

Setzen der ACL: Beispiele

Um…	Setze…
Den Zugriff unbekannter Benutzer zu verhindern	Default auf No Access
Jedem das Lesen von Dokumenten zu ermöglichen	Anonymous auf Reader
Allen Usern in der Gruppe „Studenten“ das Modifizieren der Applikation zu ermöglichen	Studenten auf Designer
Deine Forms zur Vorschau im Webbrowser anzuzeigen, während Du an der Datenbank arbeitest	Anonymous auf Author

Präzisieren der Access Control Level

Access Level	festgelegte Optionen	Optionale Optionen
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 Access Control Level

Access Level	festgelegte Optionen	Optionale Optionen
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 document	Delete documents Create private agents Create personal folders/views Create shared folders/views Create LotusScript/Java agents Replicate or copy documents

Präzisieren der Access Control Level

Access Level	festgelegte Optionen	Optionale Optionen
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

Zusätzliche Sicherheit durch Festlegen des User Type

- **Der „User Type“ legt fest, ob ein Eintrag in der ACL ein Person, ein Server oder eine Gruppe ist**
- **Sie können vor dem folgenden Szenario schützen:**
  - Chris Jones öffnet die Datenbank Policies und stellt fest, das Terry Smith Editor Rechte hat
  - Chris Jones bekommt Zugriffsrechte für den Server, erstellt dort eine Gruppe Terry Smith und fügt sich selbst der Gruppe hinzu
  - Als Mitgliede der Gruppe hat Chris jetzt Zugriffsrechte auf die Datenbank
  - Um das zu verhindern, sollte der Eintrag Terry Smith als Person gekennzeichnet werden
- **Verschiedene User Types**
  - Person, Server
  - Server Group, Person Group, Mixed Group
  - Unspecified