THEMENWOCHE 1 · LERNFELD 8

Benutzer und Rechte verwalten

Zugriffe nach dem Prinzip der minimalen Rechte

Aufgabenpaket 5

Name	Klasse	Lerngruppe

Arbeitsorganisation

Dieses Aufgabenpaket baut auf Aufgabenpaket 4 auf: Du verwaltest die Zugriffe auf deine dort angelegte Datenbank dbverkauf mit ihren Tabellen und Testdaten. Verwende lokale Übungskonten und Beispielpasswörter. Ein Konto besteht aus Benutzername und Host. Beginne jede Aufgabe mit der angegebenen Stelle im Nachschlagewerk.

Materialien

- LF8_TW1_1_Nachschlagewerk_Datenbanken_SQL.docx
- BBK_TW_1_LF8.xlsx
- lauffähige Datenbank dbverkauf mit Tabellen und Testdaten aus Aufgabenpaket 4
- Anwendungsbeispiele zur Nutzer- und Rechteverwaltung im Nachschlagewerk

Nachschlagwissen für Aufgabenpaket 5

- CREATE USER legt das Konto an, GRANT vergibt Rechte, REVOKE entzieht Rechte und DROP USER löscht das Konto.
- SHOW GRANTS; zeigt die Rechte des angemeldeten Kontos. Ein Administrationskonto kann mit SHOW GRANTS FOR auch die Rechte anderer Konten anzeigen.
- Bei MySQL und MariaDB ist Schema gleichbedeutend mit Datenbank. Die Datenbank mysql enthält Systeminformationen zu Konten und Rechten. MariaDB nutzt mysql.global_priv für globale Kontodaten; mysql.user ist dort eine Kompatibilitätsansicht.
- Grant-Tabellen werden nicht direkt verändert.

Abgabe und ePortfolio

Gib die SQL-Anweisungen direkt in der Konsole ein und protokolliere sie samt Ergebnissen mit tee. Erstelle dafür keine zusätzlichen SQL-Skripte. Übernimm aussagekräftige Anweisungen und zugehörige Ergebnisse als kopierbaren Text in dein persönliches ePortfolio; erläutere Aufgabe, Lösungsweg und Herausforderungen. Dieser Nachweis ist auch bei Gruppenarbeit verbindlich. Die vollständige tee-Protokolldatei muss nicht abgegeben werden. Die Vorschläge bei den Aufgaben lassen Raum für eigene Ideen. Dokumentationsstandard: Nachschlagewerk Abschnitt 7; Bedienung von tee: Abschnitt 6.8.

A5.1 · Rollen und Rechte planen

Status	Sozialform
Pflichtaufgabe	Teamarbeit

Ziel: Du leitest Rechte aus Aufgaben ab.

Nachschlagewerk: 6.2 „Konten anlegen und Rechte vergeben“, Tabelle „Verwendung – Typischer Rechtebedarf – Nicht erforderlich“ und Hinweis zur Beschränkung auf benötigte Rechte (S. 8).

Arbeitsauftrag

1. Definiert drei Aufgabenbereiche (hier „Rollen“ genannt): Lesen, Datenpflege und Datenbankstruktur bearbeiten. Der letzte Bereich wird auch Schemaentwicklung genannt.
2. Erstellt eine Rechteübersicht als Tabelle: eine Zeile je Aufgabenbereich, Spalten für die benötigten Rechte auf dbverkauf und eure Begründung. Überlegt anhand der Befehle aus Aufgabenpaket 4, welche Zugriffe jeweils nötig sind.
3. Tragt auch ein, welche Rechte bewusst nicht vergeben werden, und begründet dies. Ein Konto zum Lesen benötigt beispielsweise SELECT, aber kein UPDATE oder DELETE.

Arbeitsergebnis

- Rechteübersicht mit Aufgabenbereichen, erlaubten und nicht vergebenen Rechten sowie Begründungen

Gestufte Lösungshilfen

Hilfe 1 · Eine Rechteübersicht (auch Rechtematrix genannt) ist eine Tabelle, die zeigt, wer was tun darf. Beispiel: Aufgabenbereich „Lesen“ – erlaubt: SELECT – nicht vergeben: INSERT, UPDATE und DELETE. Ergänzt die beiden anderen Aufgabenbereiche selbst.

Hilfe 2 · Schema bedeutet in MySQL und MariaDB Datenbank. dbverkauf.* steht für alle Tabellen dieser Datenbank. Globale Rechte auf *.* sind für die drei Übungskonten nicht nötig. Ihr plant Aufgabenbereiche; SQL-Rollen mit CREATE ROLE sind hier nicht erforderlich.

Selbstkontrolle

- Jede Rolle hat einen klaren Zweck.
- Keine Rolle erhält unnötige Administratorrechte.

Was sollte in das ePortfolio übernommen werden

- Du könntest deine Rechteübersicht aufnehmen und an einem Aufgabenbereich die Auswahl der Rechte erläutern.

A5.2 · Lokale Benutzerkonten anlegen

Status	Sozialform
Pflichtaufgabe	Partnerarbeit

Ziel: Du erzeugst eindeutig adressierte Testkonten.

Nachschlagewerk: 6.2 „Konten anlegen und Rechte vergeben“, Benutzername, Host und CREATE USER (S. 8). Zur Kontrolle: „Vorhandene Konten finden“ in 6.4 „Speicherorte von Konten und Rechten“ (S. 9).

Arbeitsauftrag

1. Melde dich in der Administrationskonsole als root an. Starte tee wie in Abschnitt 6.8 beschrieben. Lege mit CREATE USER je Aufgabenbereich ein Konto mit @localhost an, z. B. lf8_lesen, lf8_pflege und lf8_struktur.
2. Verwende für die Übung Beispielpasswörter, z. B. LF8_Beispiel_2026!; berücksichtige dabei die Passwortregeln deines Servers.
3. Zeige die Konten als root mit SELECT User, Host FROM mysql.user; an und prüfe Benutzername und Hostteil deiner drei neuen Konten.

Arbeitsergebnis

- Mit tee aufgezeichnete CREATE USER-Anweisungen und Serverrückmeldungen
- Kontenabfrage mit Ergebnis als Nachweis der angelegten Konten

Gestufte Lösungshilfen

Hilfe 1 · Setze Benutzer- und Hostteil jeweils in einfache Anführungszeichen. Übertrage das CREATE USER-Beispiel aus Abschnitt 6.2 auf deine drei Konten und deine Datenbank dbverkauf.

Hilfe 2 · Für diese lokale Übung lautet der Hostteil localhost. Öffne die Administrationskonsole aus deiner Entwicklungsumgebung; der Anmeldebefehl lautet mysql -h localhost -u root -p. Das Passwort wird danach abgefragt.

Selbstkontrolle

- Alle Konten erscheinen mit localhost.
- Für die Übungskonten wurden Beispielpasswörter verwendet.

Was sollte in das ePortfolio übernommen werden

- Du könntest deine CREATE USER-Anweisungen mit den zugehörigen Rückmeldungen aus dem tee-Protokoll übernehmen.
- Ergänze eine passende Kontenabfrage samt Ergebnis, die die erfolgreiche Anlage belegt.

A5.3 · Rechte vergeben und anzeigen

Status	Sozialform
Pflichtaufgabe	Partnerarbeit

Ziel: Du vergibst die in deiner Rechteübersicht geplanten Zugriffe mit GRANT und kontrollierst das Ergebnis.

Nachschlagewerk: 6.2 „Konten anlegen und Rechte vergeben“, GRANT-Beispiele und Erklärung von dbtest.*, sowie 6.3 „Vergebene Rechte anzeigen“ zur Kontrolle mit SHOW GRANTS (S. 8).

Arbeitsauftrag

1. Vergib als root die geplanten Rechte auf dbverkauf.*. Gib die GRANT-Anweisungen direkt in der Administrationskonsole ein und protokolliere sie mit tee.
2. Kontrolliere als root jedes Übungskonto mit SHOW GRANTS FOR, z. B. SHOW GRANTS FOR 'lf8_lesen'@'localhost';. Mit SELECT User, Host FROM mysql.user; findest du die vorhandenen Konten; SHOW GRANTS FOR zeigt anschließend die Rechte des angegebenen Kontos.
3. Vergleiche die angezeigten Rechte mit deiner Rechteübersicht. Für diese Kontrolle als root ist kein Kontowechsel nötig. Die Anmeldung mit den einzelnen Konten und die praktischen Zugriffstests folgen in A5.4.

Arbeitsergebnis

- Mit tee aufgezeichnete GRANT-Anweisungen und Serverrückmeldungen
- SHOW GRANTS FOR-Ausgaben für die drei Übungskonten mit Vergleich zur Rechteübersicht

Gestufte Lösungshilfen

Hilfe 1 · CREATE USER und GRANT sind getrennte Schritte.

Hilfe 2 · FLUSH PRIVILEGES ist nach GRANT normalerweise nicht erforderlich.

Selbstkontrolle

- Jedes Konto besitzt genau die geplanten Rechte.

Was sollte in das ePortfolio übernommen werden

- Du könntest ausgewählte GRANT-Anweisungen und ihre Rückmeldungen aus dem tee-Protokoll aufnehmen.
- Zeige mit den zugehörigen SHOW GRANTS FOR-Ausgaben, dass die Rechte deiner Planung entsprechen.

A5.4 · Berechtigungen praktisch testen

Status	Sozialform
Pflichtaufgabe	Einzelarbeit

Ziel: Du weist erlaubte und verbotene Operationen nach.

Nachschlagewerk: 6.5 „Anmeldung und Zugriffe praktisch prüfen“ (S. 10). Übertrage den Vergleich von erlaubtem SELECT und abgewiesenem UPDATE auf deine Konten und deine Rechteübersicht. Zur Mitschrift in jeder Sitzung: Abschnitt 6.8 (S. 11).

Arbeitsauftrag

1. Lass die Administrationskonsole geöffnet. Öffne eine zweite Konsole und melde dich dort nacheinander mit jedem deiner drei Übungskonten an. Verwende jeweils dessen Benutzernamen und Beispielpasswort. Beende die bisherige Testsitzung vor jedem Wechsel mit notee und quit; melde dich anschließend neu an (siehe Hilfen).
2. Starte nach jeder Anmeldung tee mit einem zum Konto passenden Dateinamen. Prüfe mit SELECT CURRENT_USER(); das tatsächlich verwendete Konto und mit SHOW GRANTS; dessen Rechte. Führe dann mindestens zwei erlaubte und zwei verbotene Befehle je Aufgabenbereich aus.
3. Halte zu jedem Test Konto, Befehl, erwartetes und tatsächliches Ergebnis sowie gegebenenfalls die Fehlermeldung fest. Übernimm die passenden Anweisungen und Ergebnisse aus dem tee-Protokoll mit deinen Erläuterungen ins ePortfolio.

Arbeitsergebnis

- Dokumentierte Zugriffstests für alle drei Konten mit SQL-Anweisungen und Ergebnissen aus den jeweiligen tee-Protokollen

Gestufte Lösungshilfen

Hilfe 1 · Starte den Client in der zweiten Konsole, z. B. aus deiner Entwicklungsumgebung oder aus dem Clientverzeichnis. Ersetze lf8_lesen durch den Namen des gerade zu prüfenden Kontos:

```
mysql -h localhost -u lf8_lesen -p
```

-p ohne angehängtes Passwort führt zur verdeckten Passwortabfrage. Gib dort das Beispielpasswort dieses Kontos ein. Bei MariaDB kann der Client auch mariadb heißen. Den Anmeldebefehl gibst du außerhalb der SQL-Sitzung ein.

Hilfe 2 · In der angemeldeten Sitzung startest du tee erneut. Der Ordner muss vorhanden sein; passe Pfad und Dateiname an das jeweilige Konto an:

```
tee C:/LF8/A5_4_lf8_lesen.txt
SELECT CURRENT_USER();
SHOW GRANTS;
USE dbverkauf;
```

Hilfe 3 · Nutze eigens angelegte Testdaten. Eine erwartete Ablehnung ist ein erfolgreicher Nachweis der Rechtebegrenzung. Beende nach den Tests die Mitschrift mit notee und die Verbindung mit quit. Beide Clientbefehle stehen jeweils in einer eigenen Zeile.

Selbstkontrolle

- Die tatsächlich erlaubten und abgewiesenen Zugriffe entsprechen deiner Rechteübersicht.
- Fehlermeldungen sind vollständig dokumentiert.

Was sollte in das ePortfolio übernommen werden

- Du könntest für jedes Konto passende Auszüge mit Kontoidentifikation, SHOW GRANTS und Zugriffstests samt Erwartungen und Ergebnissen aufnehmen.

A5.5 · Speicherorte der Rechte untersuchen

Status	Sozialform
Pflichtaufgabe	Partnerarbeit

Ziel: Du unterscheidest Kontrollbefehle und interne Speicherung.

Nachschlagewerk: 6.3 „Vergebene Rechte anzeigen“ (S. 8) und 6.4 „Speicherorte von Konten und Rechten“ (S. 9). Unterscheide Kontrollbefehle von den Systemobjekten mysql.user, mysql.db und mysql.global_priv.

Arbeitsauftrag

1. Untersuche als root die Ausgaben von SHOW GRANTS FOR und SHOW CREATE USER für deine Übungskonten. Protokolliere die Anweisungen und Ergebnisse mit tee.
2. Untersuche die Kontodaten in MySQL über mysql.user, in MariaDB ab 10.4 über mysql.global_priv und die Kompatibilitätsansicht mysql.user. Prüfe anschließend bei beiden Produkten in mysql.db die auf dbverkauf.* vergebenen Datenbankrechte deiner Übungskonten. Vergleiche sie mit SHOW GRANTS FOR.
3. Erkläre, warum direkte Änderungen an diesen Systemobjekten ungeeignet sind.

Arbeitsergebnis

- Vergleichstabelle zu Anzeige und Speicherung

Gestufte Lösungshilfen

Hilfe 1 · Systemtabellen dienen hier nur der lesenden Untersuchung durch root. Die Übungskonten benötigen dafür keine zusätzlichen Rechte.

Hilfe 2 · Nutze die Abfrage „Datenbankbezogene Rechte nachvollziehen“ in Abschnitt 6.4 und passe Datenbank- und Kontonamen an. mysql.global_priv speichert globale Kontodaten; die Rechte auf dbverkauf.* stehen auch bei MariaDB in mysql.db. Produkt und Version bestimmen die genaue Struktur.

Selbstkontrolle

- Produkt und Version sind angegeben.
- Kontodefinition, globale Rechte und Datenbankrechte sind unterschieden. Die Einträge in mysql.db sind mit den vergebenen Rechten auf dbverkauf abgeglichen.

Was sollte in das ePortfolio übernommen werden

- Du könntest deine Vergleichstabelle durch passende SQL-Anweisungen und Ergebnisse aus dem tee-Protokoll belegen.

A5.6 · Rechte entziehen und Umgebung aufräumen

Status	Sozialform
Pflichtaufgabe	Einzelarbeit

Ziel: Du kannst Berechtigungen kontrolliert zurücknehmen.

Nachschlagewerk: 6.6 „Rechte entziehen und erneut prüfen“ sowie 6.7 „Übungskonten entfernen“ (S. 11). Achte auf den erneuten Zugriffstest nach REVOKE und die Kontenprüfung nach DROP USER.

Arbeitsauftrag

1. Entziehe in der Administrationskonsole als root einem Übungskonto ein ausgewähltes Recht mit REVOKE. Gib die Anweisung direkt ein und protokolliere sie mit tee.
2. Kontrolliere als root die Änderung mit SHOW GRANTS FOR. Melde dich für den praktischen Test in der zweiten Konsole erneut mit dem betroffenen Übungskonto an. Starte tee, prüfe das Konto mit SELECT CURRENT_USER(); und teste den entzogenen Zugriff.
3. Beende nach der Dokumentation die Testsitzungen. Entferne als root ausschließlich die drei in A5.2 angelegten Übungskonten mit DROP USER. Prüfe anschließend die Kontenliste. Die Projektdatenbank und das Administrationskonto bleiben erhalten.

Arbeitsergebnis

- Mit tee aufgezeichnete REVOKE- und DROP USER-Anweisungen mit Rückmeldungen
- Praktischer Nachweis des Rechteentzugs und Kontenabfrage nach dem Entfernen der Übungskonten

Gestufte Lösungshilfen

Hilfe 1 · Kontrolliere vor DROP USER den genauen Hostteil.

Hilfe 2 · Lösche nicht das administrative Hauptkonto.

Selbstkontrolle

- Entzogenes Recht ist praktisch nicht mehr nutzbar.
- Alle Übungskonten sind entfernt.

Was sollte in das ePortfolio übernommen werden

- Du könntest den Rechteentzug mit Anweisung, erneutem Zugriffstest und Ergebnis aus dem tee-Protokoll belegen.
- Passende DROP USER-Anweisungen und die abschließende Kontenabfrage zeigen, dass die Übungskonten entfernt wurden.