MySQL Kullanıcı Hakları

Bünyamin Demir, Şubat 2010, WGT E-Dergi 4. Sayı

Veritabanı sistemlerine erişim yetkisi olan kullanıcıların hakları üzerine, biraz yardımcı döküman, biraz da yorum içeren bir makale hazırlamaya çalıştım. Öncelikle yetki/haklar üzerine bir sınıflama yapalım.

- Yönetici hakları, MySQL veritabanının yönetimi için verilir. Fakat bu yetkiler geneldir, özellikle bir veritabanı için verilmez.
- Veritabanı yetkileri ise veritabanı bazında verilebilir, fakat veritabanı içindeki tüm objeler için geçerlidir. Aynı zamanda sadece bir veritabanı için verilebileceği gibi, tüm veritabanları için verilmesi de sağlanabilir.
- Bir de tablo, indeks, view, store prosedür`ler için verilen haklar vardır. Bu haklar ise belirli bir veritabanının herhangi bir objesi için de verilebilir, tüm veritabanlarının tüm objeleri için de verilebilir.

Veritabanı kullanıcılarının yetkileri "mysql" veritabanında tutulmaktadır. Bu veritabanında user, db, host, tables_priv, colmus_priv ve procs_priv tablolarında görülebilir. MySQL server başladığında, bu yetkiler tablolardan okunur ve memory de tutulmaya baslar. Daha sonraki işlemlerde yetki kontrolleri her zaman bellekten yapılır. Tabi memory den okuma islemi derken, MySQL de HEAP tablolara da bir göz atmanızı tavsiye ederim.

Şimdi ise MySQL in kullanıcı haklarını bir liste halinde yazalım. Listemiz de haklar, bunların bulunduğu yer ve bu hakların etki altında bulunduğu kısımları göreceğiz.

Kısaltmalar için;

V = Veritabanları
T = Tablolar
SP = Store prosedürler
I = Indeksler
VW = Görüntüler (view)
Y = Yöneticiler

Yetki	Bulunduğu Yer	Etkilenenler
CREATE	Create_priv	V, T, I
DROP	Drop_priv	V ya da T
GRANT OPTION	Grant_priv	V, T, SP
REFERENCES	Reference_priv	V ya da T
EVENT	Event_priv	V
ALTER	Alter_priv	T
DELETE	Delete_priv	T
INDEX	Index_priv	T
INSERT	Insert_priv	T
SELECT	Select_priv	T

UPDATE	Update_priv	T
CREATE TEMPORARY TABLES	Create_tmp_table_priv	T
LOCK TABLES	Lock_tables	T
TRIGGER	Trigger_priv	T
CREATE VIEW	Screate_view_pric	VW
SHOW VIEW	Show_view_priv	VW
ALTER ROUTINE	Alter_routine_priv	SP
CREATE ROUTINE	Create_routine_priv	SP
EXECUTE	Execute_priv	SP
FILE	File_priv	Dosya erişimi (V)
CREATE USER	Create_user_priv	Y
PROCESS	Process_priv	Y
RELOAD	Reload_priv	Y
REPLICATION CLIENT	Repl_client_priv	Y
REPLICATION SLAVE	Repl_slave_priv	Y
SHOW DATABASES	Show_db_priv	Y
SHUTDOWN	Shutdown_priv	Y
SUPER	Super_priv	Y
ALL [PRIVILEGES]		Y
USAGE		Y

MySQL veritabanında bu listede verilen başlıklar şeklinde yetkiler bir birinden ayrılmıştır. Fakat sizler kullanıcı açtığınızda herhangi bir işlem için birden fazla yetki vermek zorunda kalabilirsiniz. Bu da rol yerine, işlev`e göre verilen yetkilerden kaynaklanmaktadır. Nasıl olduğunu biraz açarsak ve listede verilenlerinde üzerinden geçersek;

- CREATE; Yeni bir veritabanı ya da tablo oluşturmak için kullanılır.
- DROP; Bir veritabanı, tablo ya da görüntü silmek için kullanılır.
    - Bazen tabloyu silmek yerine yapıyı koruyup, için de bulunan veriyi silmek isteyebilirsiniz. Aslında Silip/Oluşturmak işlemini yapmaya benzer. Bunun için TRUNCATE TABLE kullanmak gerekecektir. Fakat bu DELETE yetkisi için de bulunmaktadır.
- GRANT OPTION; Kullanıcının kendi sahip olduğu yetkileri başkasına verme/alma yetkisidir.
- REFERENCES; Şu an stable olarak kullanılmamaktadır fakat foreign key verme yetkisidir.
- EVENT; Örneğin; daha önce hazırlamış olduğunu ve belirli aralıklar ile çalıştıracağınız bir SQL cümleciği var. EVENT yardımı ile bunu schedule edip, belirttiğiniz zamanlarda çalışmasını otomatik olarak sağlayabilirsiniz. Dolayısıyla EVENT yetkisi de bu tür olayları schedule etmek için kullanılır.
- ALTER; Bu yetki ALTER TABLE olarak kullanılır ve tablo üzerinde değişiklikler yapmaya yarar. Aynı zamanda INSERT ve CREATE yetkilerini de içerir.
- DELETE; Tablo da bulunan satırları silmeye yarar.
- INDEX; Tablo üzerinde index oluşturup, silmenize yarar.
- INSERT; Tablo içine veri girmek için kullanılır. INSERT yetkisi ile birlikte;
- ANALYZA TABLE

    - OPTIMIZE TABLE
    - REPAIR TABLE

      yetkileri de gelmektedir.

- SELECT; Veritabanı üzerinde satırlara erişim sağlamanız için verilecek yetkidir. Okuma yetkisi de diyebiliriz. Fakat bu yetki verilmese bile yine de bazı SELECT cümlecikleri kullanılabilir.
    - SELECT VERSION();
    - SELECT 1+1;
- UPDATE; Tablo da bulunan satırları güncellemeye yarar.
- CREATE TEMPORARY TABLES; Temp tablolar oluşturmak içindir.
- LOCK TABLES;Tavloyu SELECT lere kapatmaya yarar.
- TRIGGER; Trigger oluşturup/silme yetkisidir. (Bazı versiyonlar da trigger işlemleri SUPER yetkisindedir)
- CREATE VIEW; Görüntü (view) oluşturma yetkisidir.
- SHOW VIEW; SHOW CREATE VIEW komutunu calistirma yetkisidir.
- ALTER ROUTINE; Store prosedürler ve fonksiyonlar üzerinde değişiklik ve silmeye yetkisidir.
- CREATE ROUTINE; Store prosedür ve fonksiyon oluşturma yetkisidir.
- EXECUTE; Store prosedür çalıştırma yetkisidir.
- FILE; Veritabanı sunucusu üzerinde LOAD FILE , LOAD DATA INFILE gibi fonksiyonları kullanma yetkisidir.
    - Dikkat edilmesi gereken; bu yetkiye sahip bir kullanıcı mysql kullanıcısının, veritabanı sunucusu üzerinde yazma/okuma yetkisi olan yerlere erişim sağlamasına sebep olur.
- CREATE USER; Kullanıcı oluşturma, silme veya rename etme gibi yetkileri barındırır.
    - CREATE USER
    - DROP USER
    - RENAME USER
    - REVOKE ALL PRIVILEGES

      gibi komutları çalıştırabilir.

- PROCESS; Veritabanı sunucusu uzerinde o an oluşturulmuş sessionlar üzerinde çalıştırılan processleri görüntüleme hakkı verilmiş olur. Bu yetki sayesinde
    - SHOW PROCESSLIST
    - Mysqladmin processlist
- Kullanımı hakkı verilmiş olur. Tabi bu sayede an itibariyle çalıştırılan, askıda olan sorgular listelenebilir.
- EXECUTE; Store prosedür çalıştırma yetkisidir.
- RELOAD; FLUSH ile başlayan komutları kullanma hakkı sağlar.
    - Flush hosts
    - Flush logs
    - Flush privileges
    - Flush status
    - Flush tables

    - Flush threads
    - Refresh
    - Reload
- REPLICATON CLIENT; Master ve Slave olarak belirlenmiş veritabanları için
    - SHOW MASTER STATUS
    - SHOW SLAVE STATUS

      görüntüleme hakkını verir.
- REPLICATION SLAVE; Bu yetki, slave olarak belirlenen veritabanına verilmektedir. Bu yetki sayesinde slave veritabanı, kendisine master olarak belirlenen veritabanına güncelleme isteği bulunabilir. Eğer bu yetki yoksai slave veritabanı master den bilgi alamayacaktır.
- SHOW DATABASES; Veritabanı sunucusu üzerinde oluşturulmuş veritabanlarını görüntüleme yetkisidir.
- SHUTDOWN; SQL ümleciği değildir. Mysqladmin shutdown komutunu calistirma izni verir.
- SUPER; Aslında bir çok kritik yetkiyi içinde barındırır. Özellikle veritabanı uzerinde çalışan process`leri kill etme yetkisi kritiktir. Bunun dışında bazı limitler belirlemek, global değişkenler tanımlamak, binary log`larını temizlemek gibi işlemler de yapılabilir.
- ALL [PRIVILEGES]; ALL PRIVILEGES olarak da kullanılır, ALL olarak ta. Tüm yetkiler anlamına gelmektedir.

Görüldüğü gibi, bazen bir amaç için oluşturmuş olduğunuz kullanıcıya birden fazla yetki vermeniz gerekecektir. Buda aslında MySQL de bir rol oluşturup, bu role verilecek yetkiler sonucu, rol bazlı bir yönetim olmayışındandır. Aslında rol oluşturmayıp, işlevlere verilen yetkilerle her kullanıcı için bir rol biçmenizi sağlıyor. Bazen esnek gibi gözükse de yorucu olabilir.

Minimum Yetki Prensibi

Asıl değinmek istediğim kısım. Tabi tüm bunlar güvenli bir veritabanı sunmayacaktır ama zaten amaç bu konuyu komple ele almak değil, güvenlik bacağının kullanıcı yetkileri kısmında fikir sahibi olmak.

1. Öncelikle “test” gibi kendi içinde ön tanımlı gelen ve bazen şifresiz de erişim sağlanabilen veritabanını silmeliyiz.
2. “root” hesabı “no-password” olarak gelebiliyor. Bu yüzden tahmini zor bir şifre atamalıyız.
3. “root” kullanıcısı için sadece “localhost” erişimi vermeliyiz.
4. “anonymous” gibi ön tanımlı gelen kullanıcıları silmeliyiz.
5. kullanıcı oluştururken ‘kullanıcı’@’host_name’ kısmında muhakkak, kullanıcının bağlanacağı IP adresini belirtmeliyiz. “%” gibi genel ifadeler kullanmak, hür türlü yerden bağlantı isteği yapılacağı anlamına gelecektir.
6. Özellikle uygulama güvenliği tarafında, uygulamaya verilen kullanıcının hakları, yapacağı işlevler le sınırlandırılmalıdır. Örneğin; sadece SELECT yapacaksa, bunun dışında yetki verilmemesi gerekmektedir. Bu yüzden uygulamalar da kullandığımız kullanıcıların SELECT, UPDATE, INSERT v.s gibi temel yetkileri dışında, fazladan yetki vermemeliyiz.