

# Sicherheitsrelevante Änderungen (und einige andere) in MySQL 5.7

**SLAC, 15. Juni 2016, Berlin**

**Cédric Bruderer / Jörg Brüche**

MySQL Support Engineer, FromDual GmbH

**[cedric.bruderer@fromdual.com](mailto:cedric.bruderer@fromdual.com) / [joerg.bruehe@fromdual.com](mailto:joerg.bruehe@fromdual.com)**

# Über FromDual GmbH



www.fromdual.com



**Support**



**Beratung**



**remote-DBA**



**Schulung**



# Über mich: Cedric

- **Cédric Bruderer**
- **Ausbildung**
  - 2010 – 2014: Lehre zum Informatiker**
  - Teilnahme an den Schweizer  
Berufsmesterschaften**
- **Junior Engineer**
  - In einem international tätigen Unternehmen.**
- **MySQL Support Engineer bei FromDual**
  - seit Oktober 2015**

# Über mich: Jörg

- **Entwicklung verteiltes SQL-DBMS:**  
Unix-Portierung,  
Anschluss Archivierungs-Tools (ADSM, NetWorker)
- **MySQL Build Team:**  
Release-Builds inkl. Tests, Paketierung, Skripte, ...
- **DBA:**  
MySQL für eine Web-Plattform  
(Master-Master-Replikation)
- **Support-Ingenieur (FromDual):**  
Support + Remote-DBA für MySQL / MariaDB / Percona  
mit oder ohne Galera Cluster

# Inhalt

- **Release-Familien, Status**
- **Anders / Neu in 5.7:**
  - **Neue Sicherheits-Features**
  - **Änderungen bei Passwörtern**
  - **Datensicherheit**
- **Migration nach 5.7**
- **Neu-Installation**
- **Lese-Tipps**
- **Ausblick**

# MySQL Release-Familien

- **5.7: GA seit 5.7.9 (2015-Okt-21)  
aktuell: 5.7.13**
- **5.6: GA seit 5.6.10 (2013-Feb-5)  
aktuell: 5.6.31**
- **5.5: GA seit 5.5.8 (2010-Dez-3)  
aktuell: 5.5.50  
EOL Dez. 2015 (extended: Dez. 2018)**
- **5.1: GA Dez. 2008, EOL Dez. 2013**
- **5.0: GA Okt. 2005, EOL Dez. 2011**

**Stand: Juni 2016**

# Anders in 5.7 (Auswahl)

- **Authentifizierung**
- **SQL mode:** u.a. **STRICT\_TRANS\_TABLES** Default, **ONLY\_FULL\_GROUP\_BY** verbessert + Default
- **InnoDB:**
  - Kein "disable" möglich
  - Mehr **ONLINE (INPLACE)** bei **ALTER TABLE**
  - **Monitoring-Kontrolle** geändert
- **Integration mit systemd und syslog**
- **Installation: Skript -> Server-Option**

# Neu in 5.7 – Auswahl (1)

- **InnoDB:**
  - Mehr ONLINE (INPLACE) bei ALTER TABLE
  - Geo-Datentypen und -Indexe
  - "General Tablespace"
  - "Tablespace Encryption" (braucht Keyring Plugin)
- **Multi-Source Replikation**
- "Group Replication" (ähnlich Galera Cluster)
- ...



# Neu in 5.7 – Auswahl (2)

- ...
- **Generierte Spalten**  
"virtual" oder "stored", Index möglich
- **Datentyp JSON + JSON-Funktionen**
- **Index über JSON nicht direkt möglich, aber über aus JSON-Funktion generierte Spalte**
- **"X Plugin" und "X DevAPI" für Document Store (NoSQL), "MySQL Shell" als Client**

# Sicherheit

- **Authentifizierung immer über Plugin (auch Passwort)**
- **Tabelle `mysql.user`:**
  - 1) **neue Spalte `plugin`**
  - 2) **`password` -> `authentication_string`**
- **Keine alten Passwörter (pre-4.1) mehr**
- **”User Account Locking“**
- **Bessere SSL-Unterstützung, Erzeugung von Schlüsseln und Zertifikaten**

# Passwörter

- **Password Lifetime (global + pro Benutzer):**  
Default 0, war 360 von 5.7.4 bis 5.7.10 (!!!)
- **"Password Validation Policy"**  
Default: Länge 8, "mixed", Ziffer, "special"
- **Installation: nur noch 'root'@'localhost',**  
setzt Zufalls-Passwort (schreibt ins Error-Log),  
setzt "expired" (wie schon RPMs in 5.6)
- **Nächster Befehl muss sein:**  
**ALTER USER USER() IDENTIFIED BY '...';**
- **SET PASSWORD usw. sind deprecated**

# Datensicherheit

- **Ziel: Schutz gegen Lesen durch OS-root**
- **Methode: "encryption at rest"**  
**(Verschlüsselung der Tablespaces auf Platte)**
- **Zweistufig (vgl. LUKS), nur "file\_per\_table"**
- **Master-Schlüssel liegt in "keyring"**
- **Community: "keyring\_file" (Demo-artig?),  
Enterprise: "keyring\_okv" (Oracle Key Vault)**
- **Config-Änderung in 5.7.12!**

# Migration: Vorab-Kontrolle

- Nur über MySQL 5.6!
- Kein `mysqld_safe` mehr (`systemd`)
- `mysql_old_password` nicht mehr unterstützt
- `sql_mode`: `ONLY_FULL_GROUP_BY` standardmässig aktiviert
- Support für `YEAR(2)` entfernt (deprecated seit 5.6.6)
- Neues Format der „InnoDB undo logs“
- `ROW_FORMAT` standardmässig `DYNAMIC` (bisher `COMPACT`): längere Schlüssel möglich, Vorsicht bei Replikation!

# Migration: Durchführung

- **Nur aus 5.6 !**
- **`innodb_fast_shutdown=0`**
- **Altes MySQL (5.6) stoppen**
- **Neue Binaries installieren**
- **Neues MySQL (5.7) starten**
- **`mysql_upgrade`**
- **MySQL neu starten**

# Aufsetzen von MySQL 5.7

- Im Prinzip gleich wie früher.
- Server-Option `--bootstrap` ersetzt durch `--initialize` / `--initialize-insecure`
- `mysql_install_db` und `mysql_secure_installation` entfallen
- Kein Eingriff in die Initialisierung möglich!

# Lese-Tipps (1): Manual

## MySQL Manual:

<http://dev.mysql.com/doc/refman/5.7/en/...>

- What is new in MySQL 5.7 [.../mysql-nutshell.html](#)
- Password Expiration Policy [.../password-expiration-policy.html](#)
- Authentication Plugins [.../authentication-plugins.html](#)
- Password Validation Plugin [.../validate-password-plugin.html](#)
- The MySQL Keyring [.../keyring.html](#)

## MySQL 5.7 Release Notes:

<http://dev.mysql.com/doc/relnotes/mysql/5.7/en/>



# Lese-Tipps (2): Entwickler

**”MySQL Server Team Blog“ <http://mysqlserverteam.com/...>**

- **ONLY\_FULL\_GROUP\_BY: Guilhem Bichot**  
[.../mysql-5-7-only\\_full\\_group\\_by-improved-recognizing-functional-dependencies-enabled-by-default/](.../mysql-5-7-only_full_group_by-improved-recognizing-functional-dependencies-enabled-by-default/)  
[.../when-only\\_full\\_group\\_by-wont-see-the-query-is-deterministic/](.../when-only_full_group_by-wont-see-the-query-is-deterministic/)
- **JSON: Morgan Tocker**  
<.../taking-the-new-mysql-5-7-json-features-for-a-test-drive/>  
<.../indexing-json-documents-via-virtual-columns/>
- **SSL: Todd Farmer**  
<.../simplified-ssl-tls-setup-for-mysql-community/>
- **Document Store, X Protokoll: Diverse Autoren**  
**Sechs (6) Beiträge ”MySQL 5.7.12 ...“, April 2016**
- **Installation, root Passwort: Georgi Kodinov**  
<.../initialize-your-mysql-5-7-instances-with-ease/>

# Lese-Tipps (3): Benutzer

- **Blog Simon Mudd (Booking.com), Replikation:**  
**[http://de.slideshare.net/sjmudd/  
mysql-57-the-first-few-months](http://de.slideshare.net/sjmudd/mysql-57-the-first-few-months)**
- **Blog Giuseppe Maxia, Replikations-Strukturen:**  
**[http://datacharmer.blogspot.de/2015/08/  
mysql-replication-in-action-part-4-star.html](http://datacharmer.blogspot.de/2015/08/mysql-replication-in-action-part-4-star.html)**
- **Planet MySQL: <http://planet.mysql.com/>**

# Ausblick

- **Galera Cluster auf 5.7: in Arbeit**
- **Bedeutung von InnoDB wächst weiter (5.6: Volltext-Suche, 5.7: Geo-Daten)**
- **Absehbar: System-Tabellen in InnoDB**
- **IMO kein Grund mehr für MyISAM: weder Performance- noch Funktions-Vorteil über InnoDB, aber funktionale Schwächen**

# Q & A



**Fragen ?**

**Diskussion?**

**Wir haben Zeit für ein persönliches Gespräch...**

- **FromDual bietet neutral und unabhängig:**
  - **Beratung**
  - **Remote-DBA**
  - **Support für MySQL, Galera, Percona Server und MariaDB**
  - **Schulung**

**[www.fromdual.com/presentations](http://www.fromdual.com/presentations)**