MySQL Security

DOAG 2013 Datenbank

14. Mai 2013, Düsseldorf

Oli Sennhauser

Senior MySQL Berater, FromDual GmbH

oli.sennhauser@fromdual.com

Über FromDual GmbH

- FromDual bietet neutral und unabhängig:
  - Beratung für MySQL
  - Support für MySQL und Galera Cluster
  - Remote-DBA Dienstleistungen für MySQL
  - MySQL Schulungen
- Oracle Silver Partner (OPN)

ORACLE Silver Partner

www.fromdual.com

Inhalt

MySQL Security

- Was ist Security?
- Probleme, Anforderungen, Konsequenzen, Massnahmen
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Informationsquellen

Was ist Security/Sicherheit?

- Vertraulichkeit
  - Zugriff nur durch autorisierte Nutzer
- Integrität
  - Veränderung der Daten
  - Nachvollziehbarkeit
- Verfügbarkeit
  - Verhinderung von Systemausfällen

Sicherheitsprobleme (1)

- Technische Sicherheitsprobleme
  - Sind einfach in den Griff zu bekommen
- Hardware geht kaputt
  - Gut wenn schnell kaputt
  - Schlecht wenn langsam kaputt
  - CPU, RAM, I/O-Controller, NW, Motherboard
- Stromausfall
- Disk läuft voll, DB crashed, Replikation bleibt stehen...
- Monitoring → Error Log anschauen!
- Bugs

Sicherheitsprobleme (2)

- Menschliche Sicherheitsprobleme
  - Sind etwas schwieriger in den Griff zu bekommen!
- Unfall: Ups!!!

```
UPDATE emp SET salary = salary + 10000; WHERE
position = 'manager';
```

  `DROP` auf Produktion anstatt auf Entwicklungssystem :-(
- Interner Datenklau (Schweizer Daten-CD's in D)
- Externer Angriff (Zerstörung, DoS, Datenklau)
- Gemäss Statistiken kommt interne Angriffe häufiger vor als externe...?

Sicherheitsanforderungen

- Was sind die Anforderungen?
- vs. was sind die Kosten?
- Wie lange darf ein Restore/Recovery dauern?
  - MTTR
- Welcher Datenverlust kann akzeptiert werden?
  - Alte Daten, neue Daten?
- Ist es akzeptable, alte Daten erst später zurückzukriegen?
- Wer hat Zugriff auf welche Daten?

Konsequenzen

- Wenn man nicht vorbereitet ist:
  - Firma muss geschlossen werden
  - Rechtliche Konsequenzen
  - Finanzieller Schaden €€€
  - (fristlose) Entlassung
  - Reputationsschaden

Massnahmen

- Was können wir für die Sicherheit tun?
- Technische Massnahmen:
  - Backup + Restore + Restore-Tests
  - HA-Lösungen
  - Logging
- Organisatorische Massnahmen
  - Regelmässige Upgrades (DB, O/S)
  - Zugriffskontrolle/-beschränkungen

Vertraulichkeit

Warum so pingelig?

- Fuss in der Türe → Hocharbeiten
- Denial of Service DoS
  - Script Kiddies, Mitbewerber, Erpressung, Schaden
- Reputationsschaden
- Datendiebstahl
  - Kunden- oder Produktionsdaten, Steuersünder, etc.
- Hoster!
  - 100e von Nutzern

Zugriffsbeschränkung

- Betriebssystem (`root` user)
- Zugriff aufs DB Filesystem!
- DB Zugriff
  - `root` von remote?
  - Passwörter: leer, default, gleich, ändern
  - Privilegien: `ALL ON *.*`

Abwehrmassnahmen

- MySQL Konfiguration
- `.history` oder `.mysql_history`
- Datenbank NIE Internet aussetzen → DMZ
- Firewall
- SQL-Firewall gegen Angriff aus der Applikation
- Bekannte Angriffsziele meiden: phpMyAdmin

Upgrades

COMPUTERWORLD

White Papers Webcasts Newsletters Rese

Topics News In Depth Reviews Blogs Opinion Shar

Networking Broadband LAN/WAN Network Hardware Network Security Wireles

Home > Networking > Network Security

News

MySQL vulnerability allows attackers to bypass password verification

Exploit code is available for a MySQL authentication bypass vulnerability

By Lucian Constantin

June 11, 2012 03:47 PM ET Add a comment

Share +1 Like 20 More

IDG News Service - Security researchers have released details about a vulnerability in the MySQL server that could allow potential attackers to access MySQL databases without inputting proper authentication credentials.

The vulnerability is identified as CVE-2012-2122 and was addressed in MySQL 5.1.63 and 5.5.25 in May. However, many server administrators might not be aware of its impact, because the changelog for those versions contained very little information about the security bug.

- **Upgrade Strategie?**

Integrität

Datenintegrität

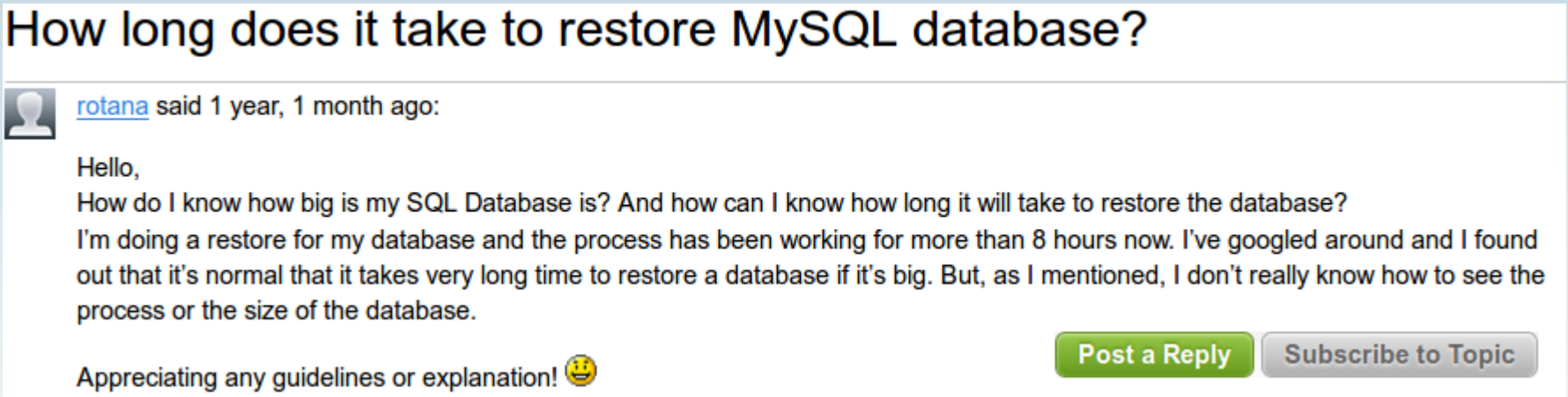
- Binary Log
- General Query Log
- Logon Trigger (`init_connect`)

- Audit Log Plugin (Enterprise Feature)

Verfügbarkeit

Backup + Restore

- Backup + Binary-Logging
- Point-in-Time-Recovery (PiTR)
- Restore-Tests um Überraschungen zu vermeiden



How long does it take to restore MySQL database?

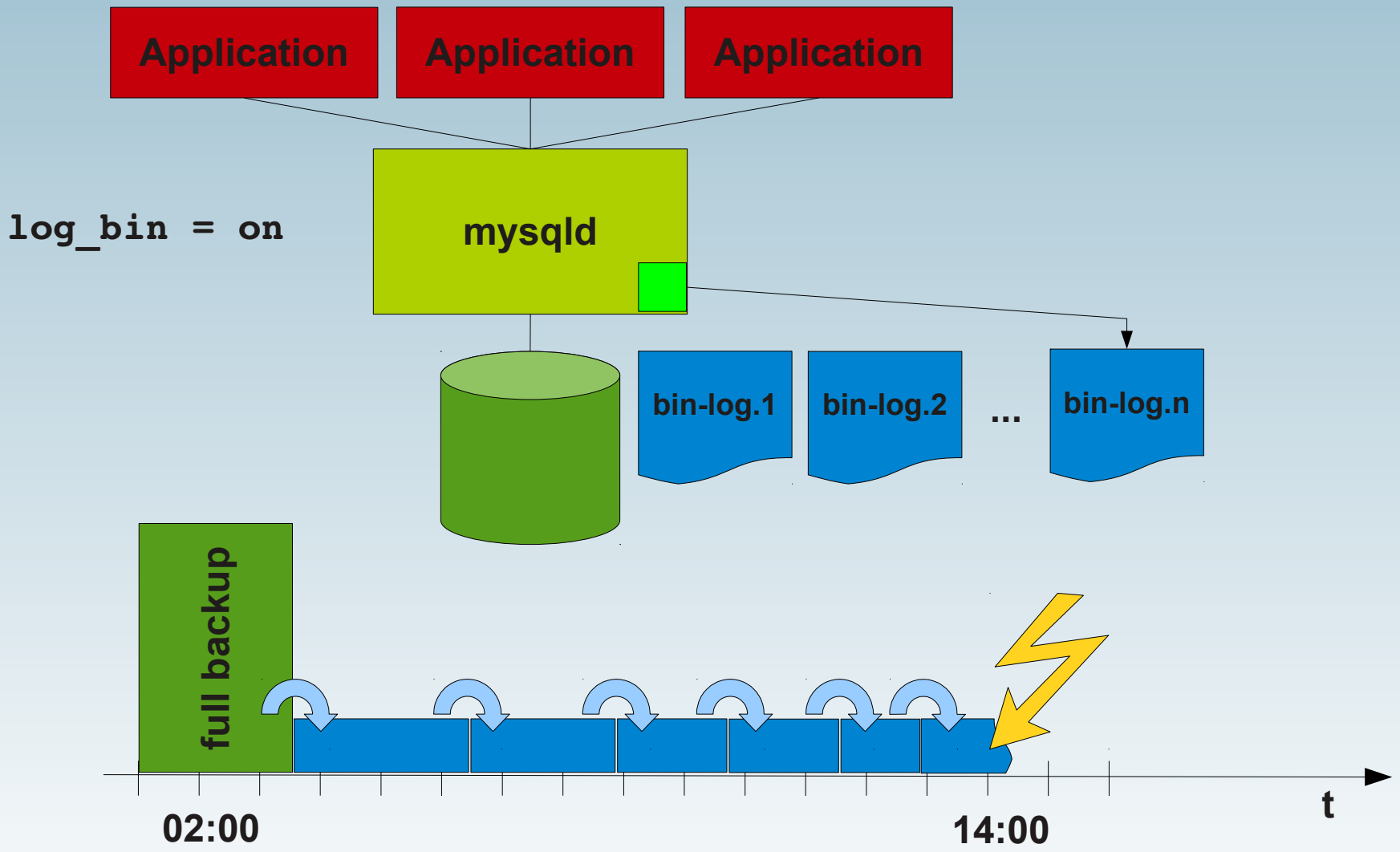
rotana said 1 year, 1 month ago:

Hello,
How do I know how big is my SQL Database is? And how can I know how long it will take to restore the database?
I'm doing a restore for my database and the process has been working for more than 8 hours now. I've googled around and I found out that it's normal that it takes very long time to restore a database if it's big. But, as I mentioned, I don't really know how to see the process or the size of the database.

Appreciating any guidelines or explanation!

Post a Reply | Subscribe to Topic

Point-in-Time-Recovery (PITR)

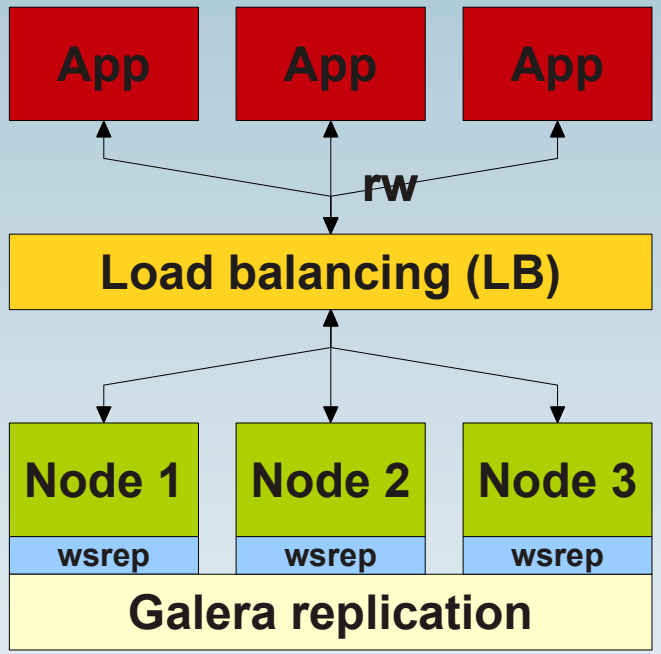


HA Lösungen

- RAID für Platten
- Cluster-Lösungen
  - Master-Slave Replikation
  - Galera Cluster für MySQL
  - Aktiv/passiv Failover-Cluster SAN/DRBD
  - MySQL Cluster

- Achtung: NICHT für logische Fehler → Backup!

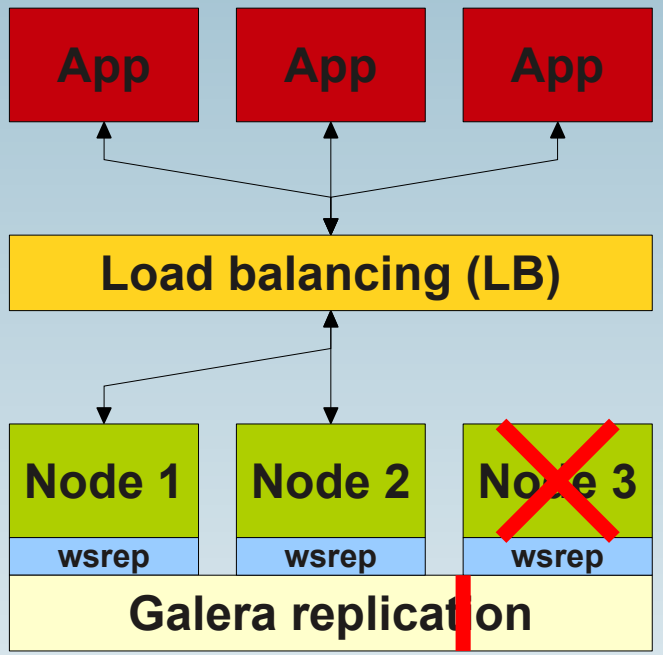
Galera Cluster für MySQL



synchrone Replikation

Galera Cluster für MySQL

- Hardware-Ausfall
- Wartungsarbeiten
  - HW/OS/DB Upgrade



Informationen

- http://www.fromdual.com/security
- MySQL/MariaDB/Percona: Release-Notes
- Oracle CPU
- MySQL Dokumentation: Security
- CVE
- RedHat Security Advisors
- full-disclosure@lists.grok.org.uk
- MySQL Security Forum

Q & A

Fragen ?

Diskussion?

Wir haben Zeit für ein Security Audit...

- **FromDual bietet neutral und unabhängig:**
  - **Beratung**
  - **Remote-DBA**
  - **Support für MySQL und Galera Cluster**
  - **Schulung**

www.fromdual.com/presentations