MySQL HA & Security

SLAC 2013

5. - 7. Juni 2013, Berlin

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)
- Mitglied bei SOUG, DOAG /ch/open

www.fromdual.com

Wir suchen noch:

- MySQL Enthusiast/in für Support / remote-DBA / Beratung

  und
- C++ Entwickler (mit Affinität zu DB, MySQL und Replikation)

Inhalt

MySQL HA

- Scale-Out vs. Scale-Up
- Master/Slave Replikation
- Master/Master Replikation
- Aktiv/passiv failover Cluster mit SAN
- Aktiv/passiv failover Cluster mit DRBD
- Galera Cluster für MySQL
- MySQL (NDB) Cluster

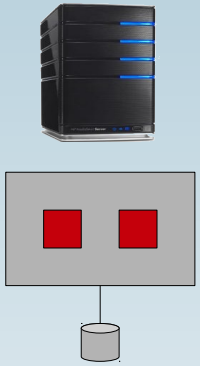
MySQL Security

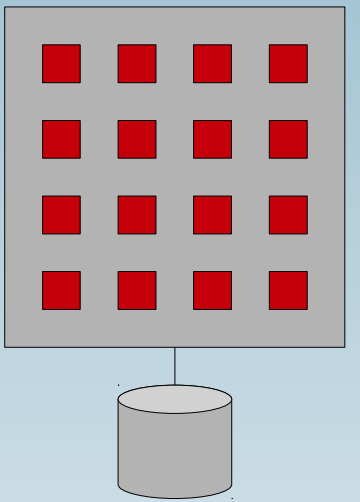
...

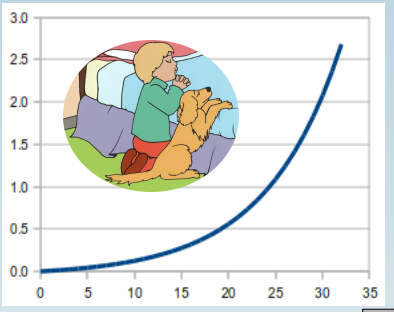
MySQL Scale-Out vs Scale-Up

Scale-Up

- Kosten
- MySQL Design
- Physische Flaschenhälse

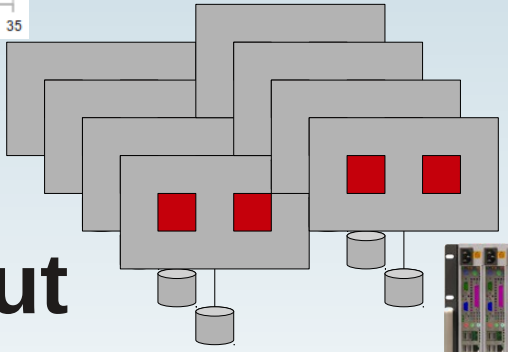






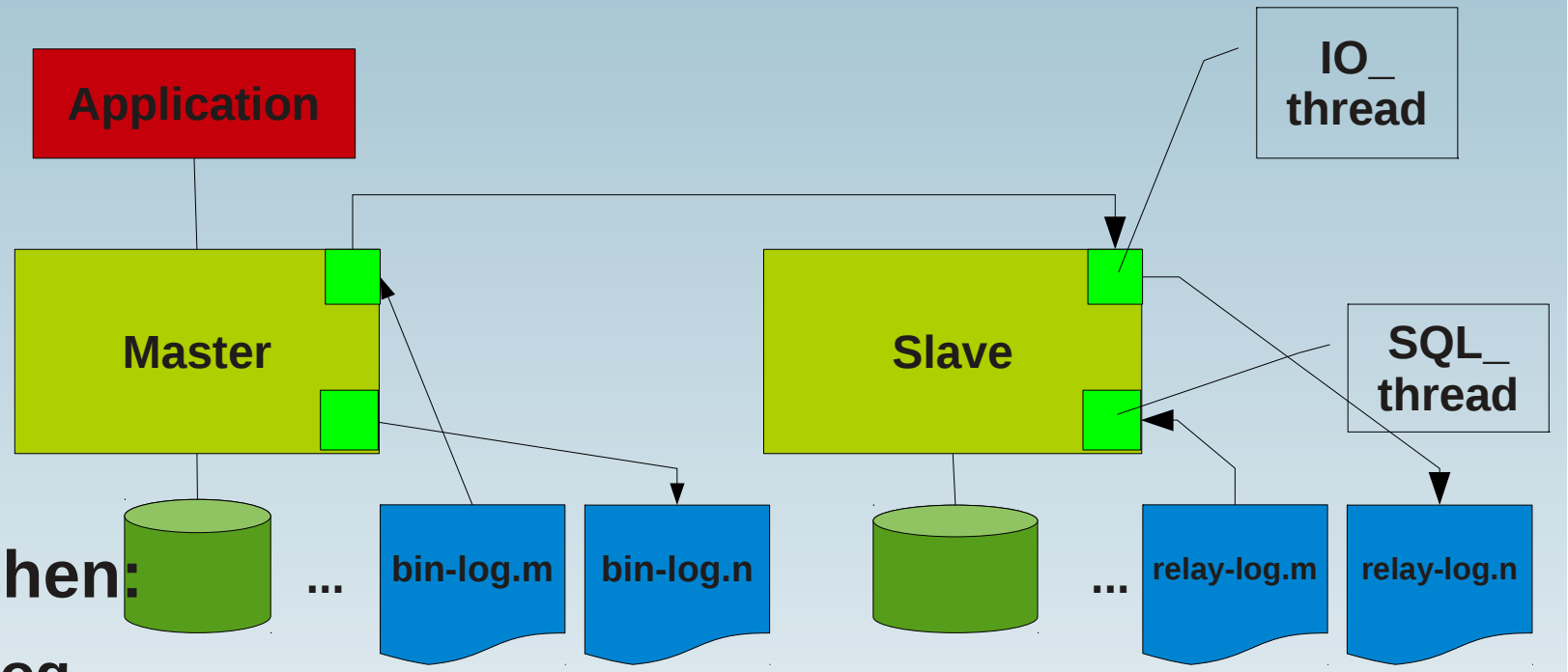
- „Relaxation of Constraints“

Scale-Out



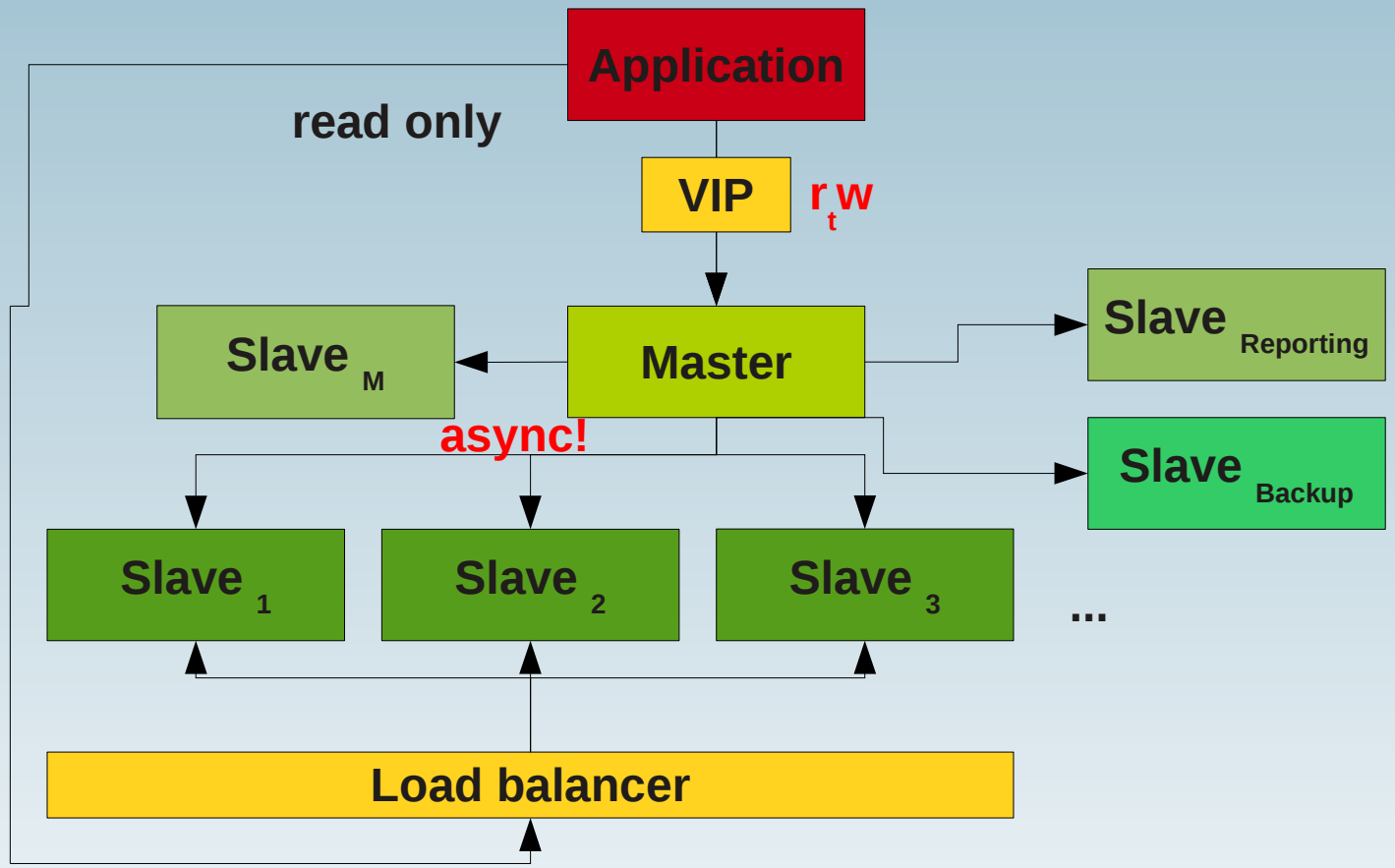
Master – Slave Replikation


```
log_bin = on
server_id = 42
```



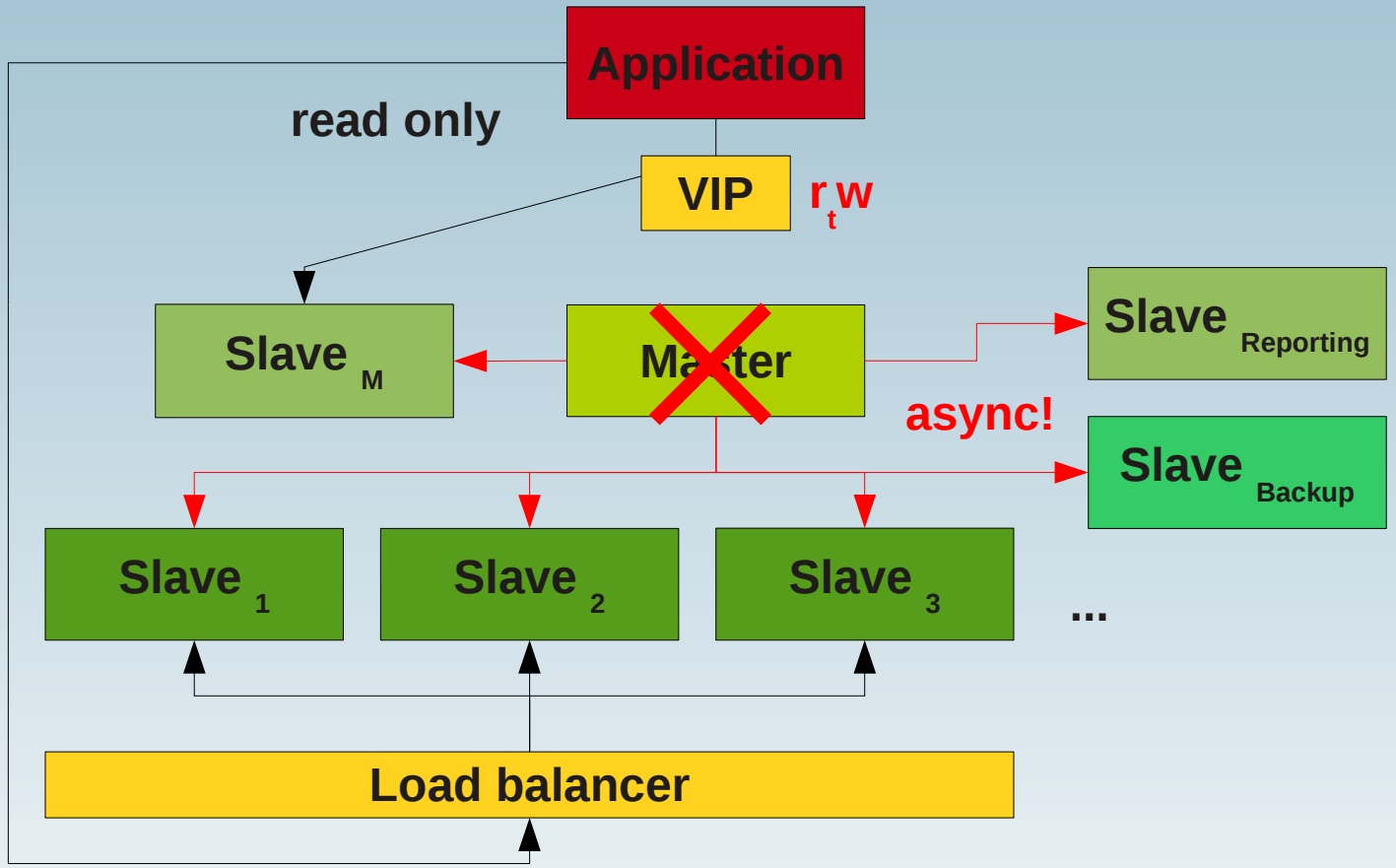
- **Wir brauchen:**
  - **Binary Log**
  - **Server Id**
  - **User für die Replikation (auf dem Master)**
  - **Konsistentes Backup MIT Binary Log Position**

High-Availability mit Replikation



- Fail-over?

Replikation Fail-over



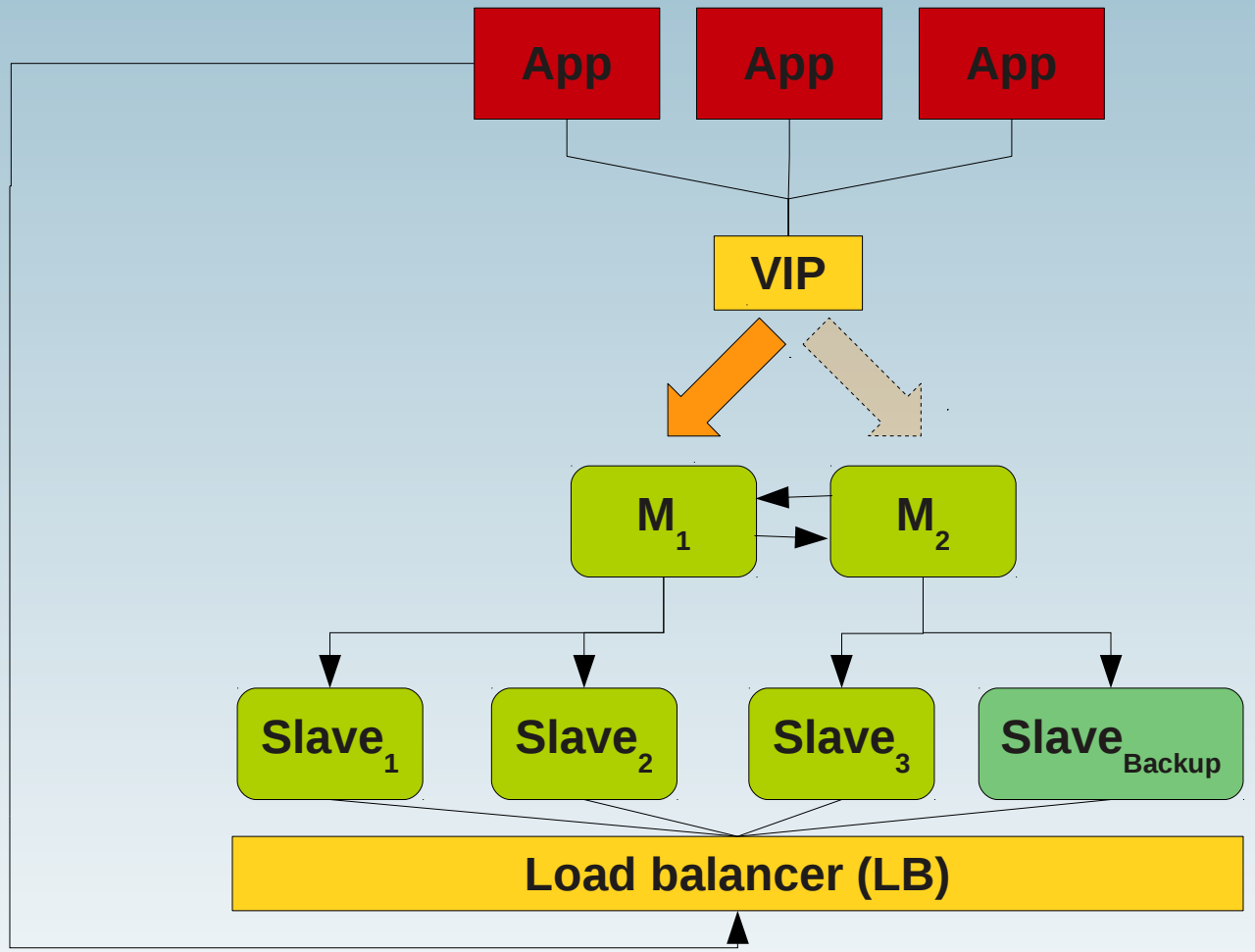
Vorteile / Nachteile

- Einfaches „standard“ Set-up
- Sehr gut wenn r >> w
- Fail-over Seite ist bereits warm/heiss!
- Zeitversatz Master/Slave (asynchron!)
- Slave kann hinterherhinken (Slave ist oft Flaschenhals)
- Daten In-konsistenz (`pt-table-checksum`/`pt-table-sync`)
- Read/write Split ist mühsam, da nicht transparent
- Wenn Master stirbt → welcher Slave wird neuere Master?

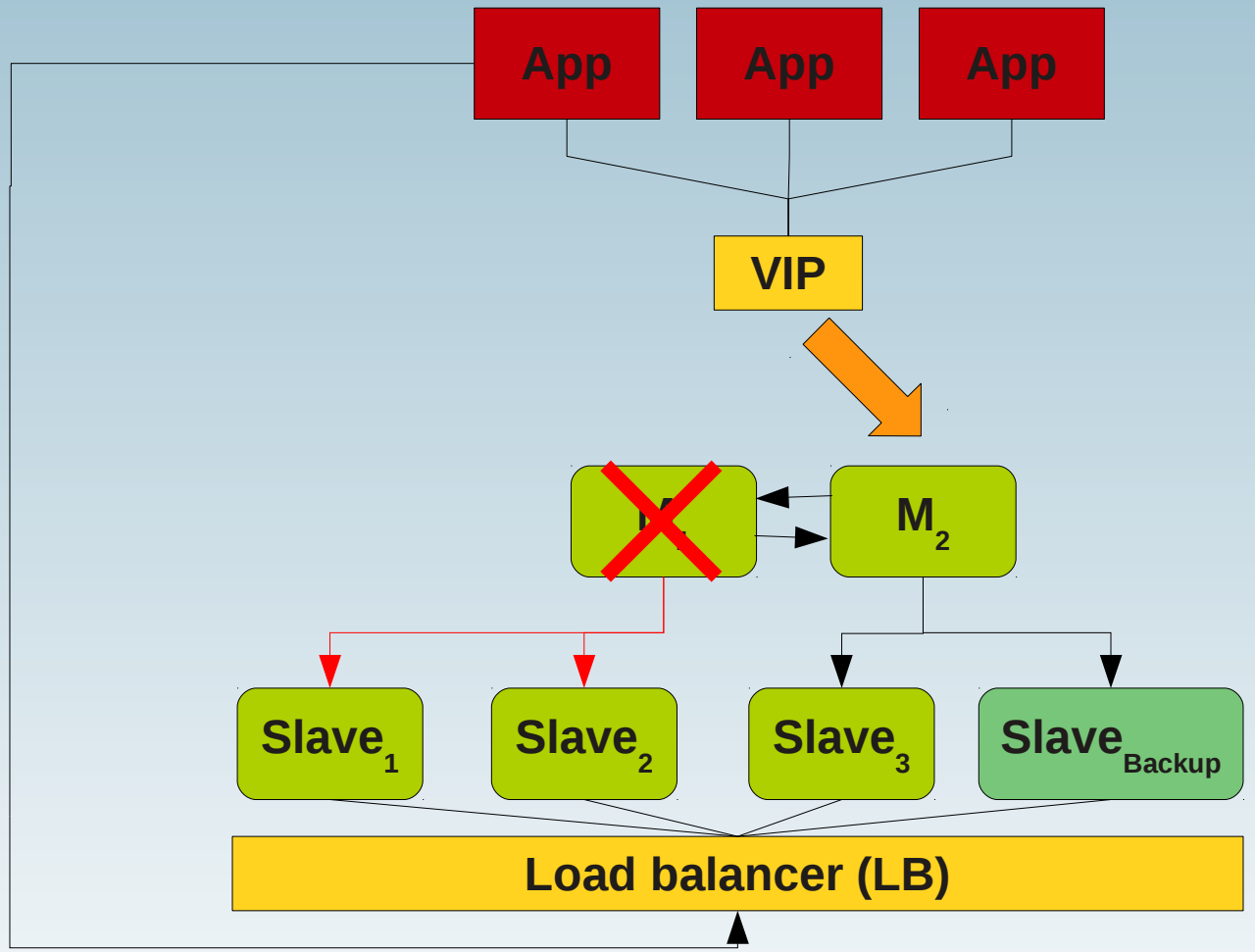
  Switch → viel Arbeit, etwas heikel!

  Es gibt Tools die helfen (MMM ~~v1~~/v2, MHA, Tungsten, ...)

Master-Master Replikation



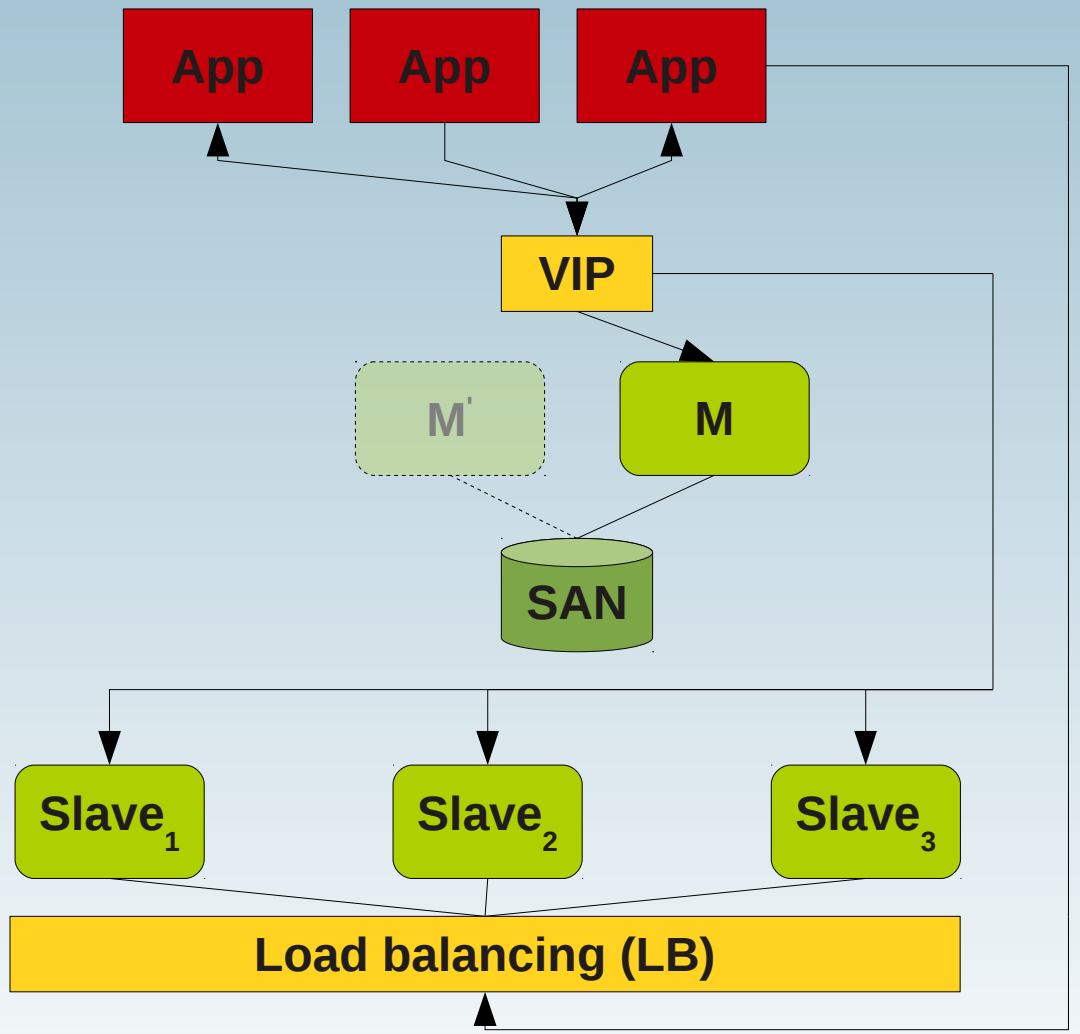
Master-Master Replikation



Vorteile / Nachteile

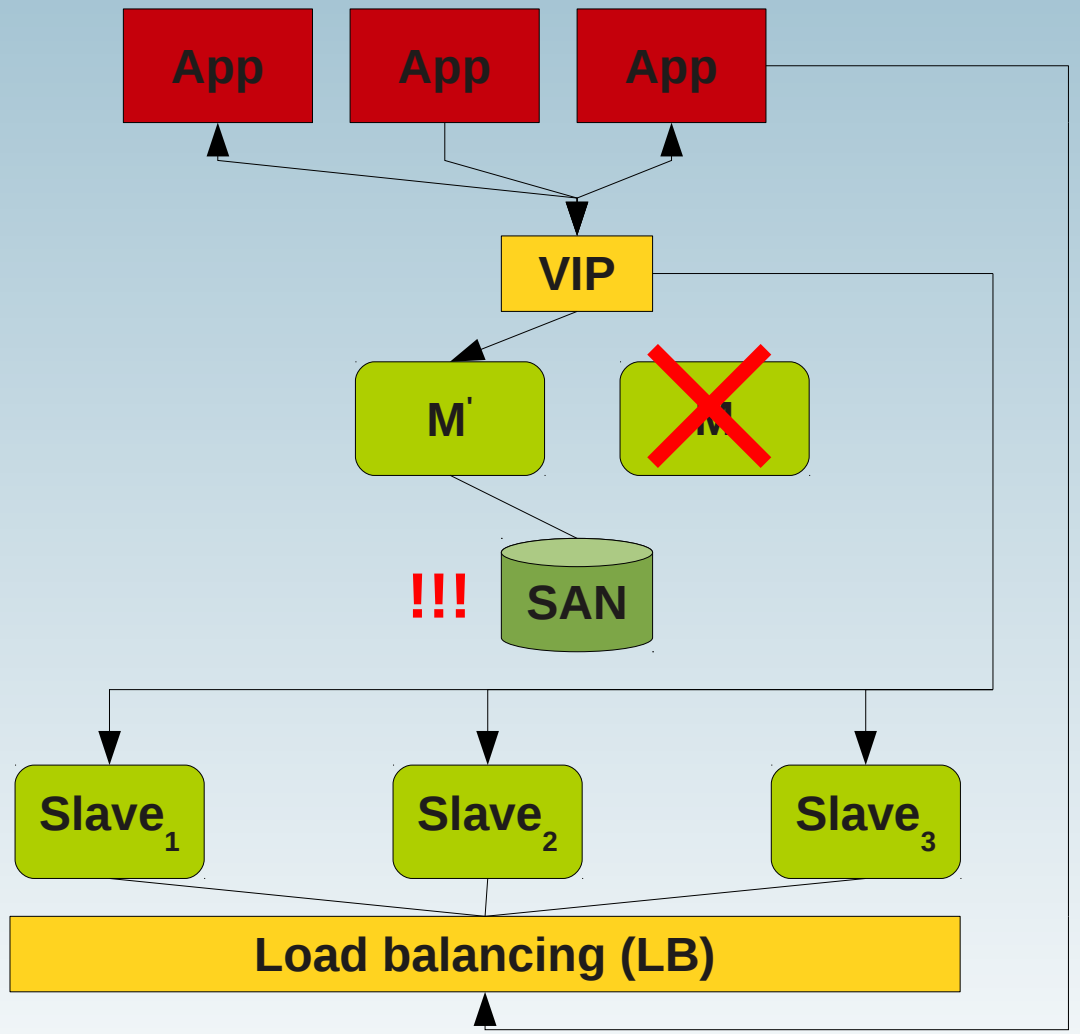
- Nur wenig komplexer als Master/Slave
- Sehr gut wenn r >> w
- Fail-over Seite ist bereits warm/heiss!
- Zeitversatz Master/Slave (asynchron!)
- Slave kann hinterherhinken (Slave ist oft Flaschenhals)
- Daten In-konsistenz (`pt-table-checksum/pt-table-sync`)
- Wenn Master stirbt, ist die Hälfte der Slaves „out of sync“!
- Vorsicht beim Schreiben auf beide Master!
- Read/write Split ist mühsam, da nicht transparent
- Man erhält dadurch NICHT mehr I/O Durchsatz!
- Ein wenig komplizierter (wieder-)aufzusetzen

Aktiv/passiv fail-over mit SAN



Aktiv/passiv fail-over mit SAN

- SPOF 2!

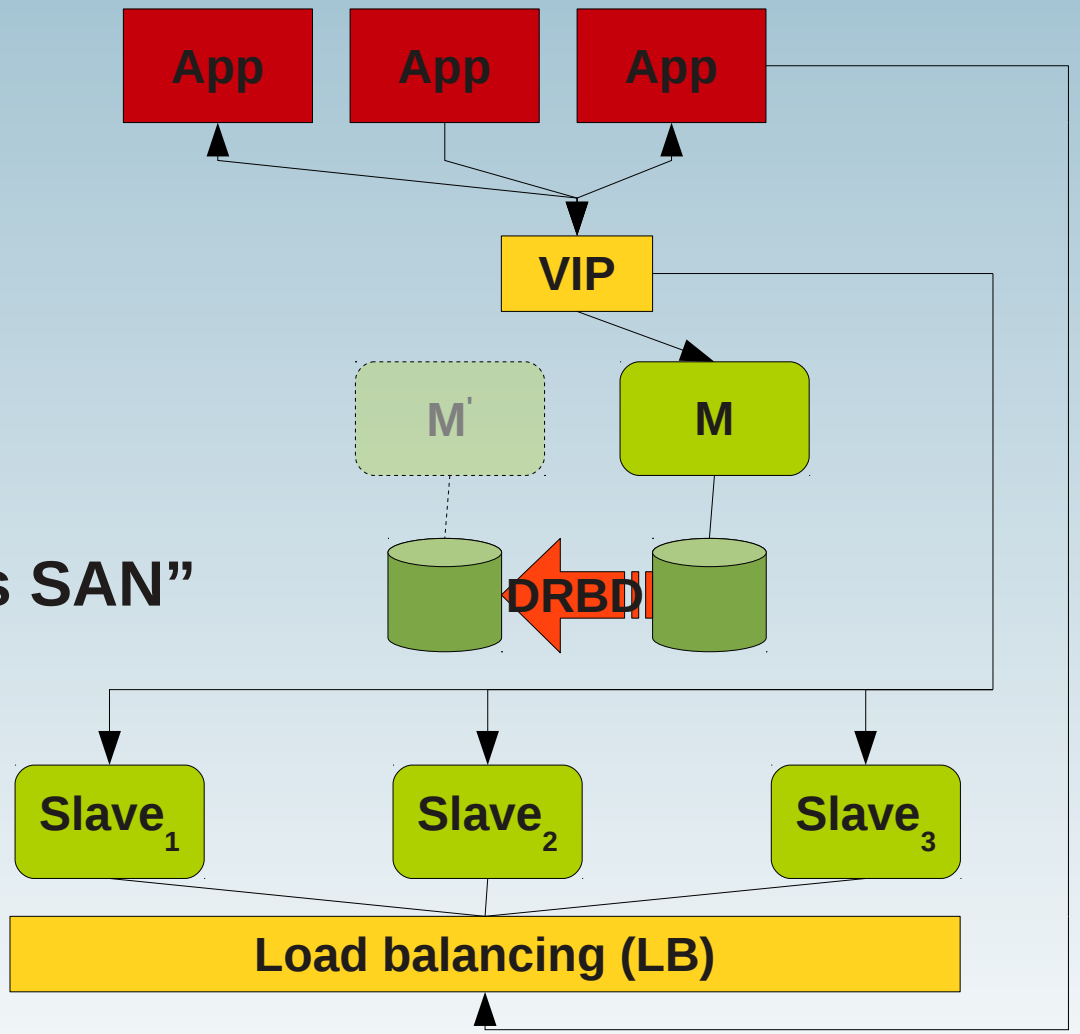


Vorteile / Nachteile

- Synchrone Replikation
- I/O Durchsatz hängt vom SAN (I/O System) ab
- Keine Daten IN-Konsistenzen möglich
- Nur eine mögliche Datenquelle
- Slaves werden automatisch und sauber geschwenkt
- SAN und Filesystem sind SpoFs!
- Teuer wenn SAN noch nicht vorhanden ist.
- SAN's sind nicht einfach richtig zu betreiben!
- Andere Seite ist kalt nach Fail-over!
- Hälfte der Hardware idelt
- Wesentlich komplexer aufzusetzen

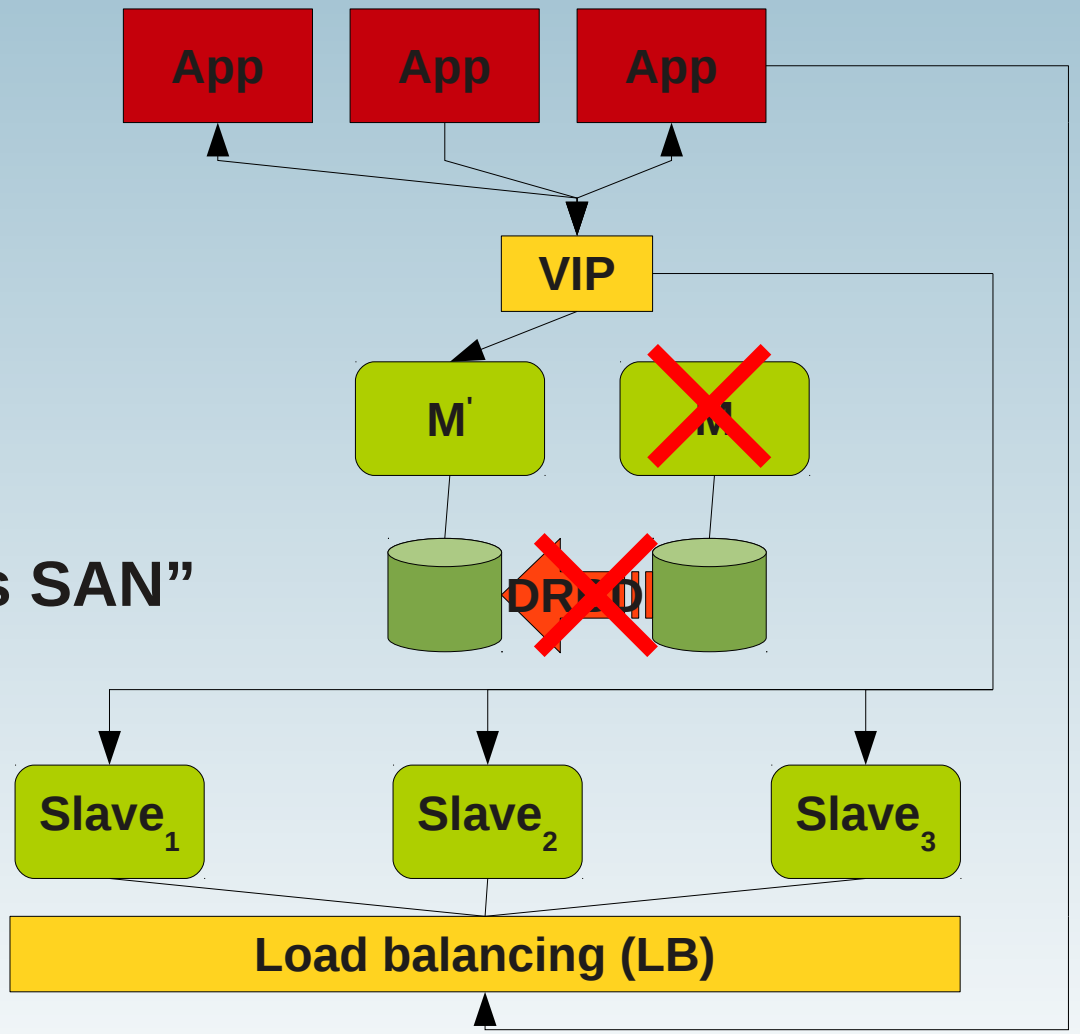
Aktiv/passiv fail-over mit DRBD

“Poor man's SAN”



Activ/passiv fail-over mit DRBD

- SPOF 1!

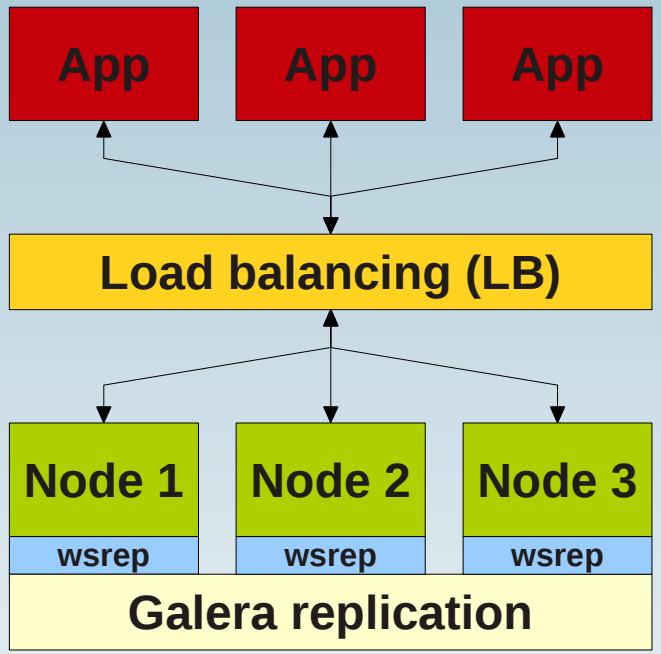


"Poor man's SAN"

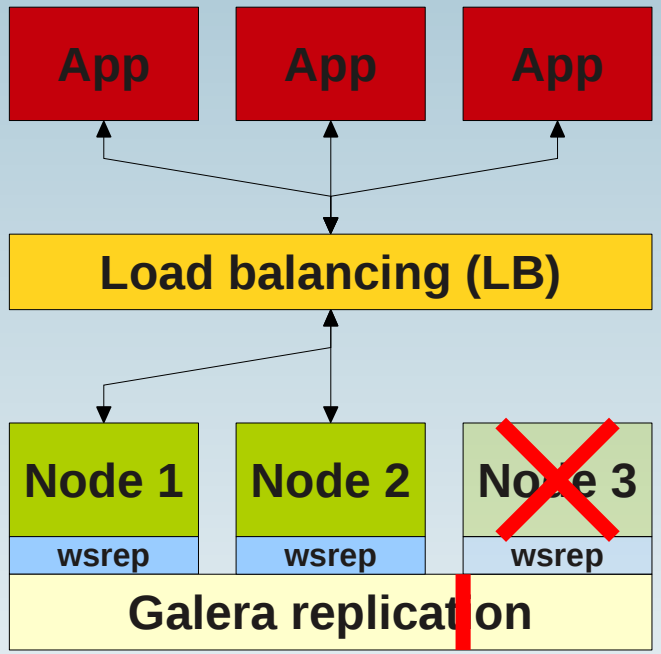
Vorteile / Nachteile

- Synchrone Replikation
- Keine Daten IN-Konsistenzen möglich
- Nur eine mögliche Datenquelle
- Slaves werden automatisch und sauber geschwenkt
- Filesystem ist SpoF!
- I/O Durchsatz tendenziell geringer als mit SAN
- Andere Seite ist kalt nach Failover!
- Hälfte der Hardware idelt
- Wesentlich komplexer aufzusetzen

Galera Cluster für MySQL



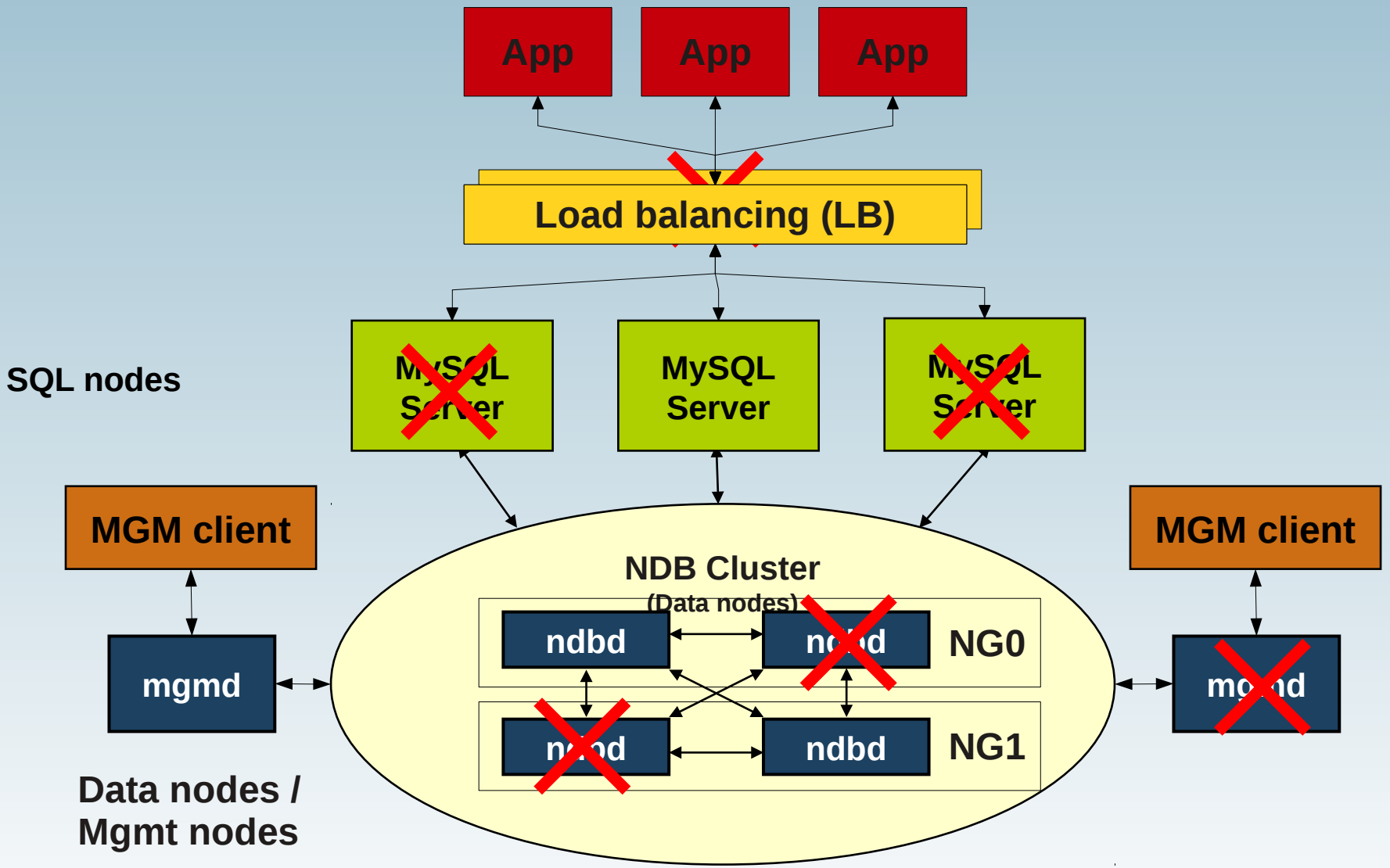
Galera Cluster für MySQL



Vorteile / Nachteile

- Synchrone Replikation
- Aktiv-aktiv multi-Master Topologie
- Lesen und Schreiben auf alle Cluster-Knoten (KEIN r/w Split notwendig)
- Automatische Knotenverwaltung
- Echtes paralleles Replizieren auf Zeilenebene
- Kein Hinterherhinken des Slaves
- Keine verlorene Transaktionen
- Lese-Skalierbarkeit (read Scale-Out!) und mehr Schreiben (+ SSD)
- Wartung im „laufenden Betrieb“ möglich (Rolling Restart)
- Basiert auf InnoDB Storage Engine (nur auf InnoDB!)
- Galera Binaries (nicht Oracle/MySQL)
- Achtung vor Hots-Spots auf einzelnen Zeilen (z. B. Sequenzen-Tabelle)
- Dadurch höhere Wahrscheinlichkeit von Deadlocks
- Voll-Synchronisation (SST) blockiert Lesen und Schreiben → 3 Koten

MySQL (NDB) Cluster



Vorteile / Nachteile

- Synchrone Replikation
- Nur eine mögliche Datenquelle
- Keine Daten IN-Konsistenzen möglich
- Extrem hoher Durchsatz (wenn richtig gemacht)
- Skaliert sehr gut für Lesen UND Schreiben (wenn richtig gemacht)
- Wartung im „laufenden Betrieb“ möglich
- Kein drop-in Ersatz für InnoDB/MyISAM!
- Hoher Bedarf an RAM (in-memory DB) und Netzwerk
- Mindestens 3 Server (besser 4) sind erforderlich.
- Neue Datenbank zu lernen (MySQL Cluster != MySQL!)
- Komplexer aufzusetzen und zu betreiben als normales MySQL
- Schlecht für Joins (Network Database, Push Down Joins in v7.2)

MySQL Security

Inhalt

MySQL HA

- ...

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

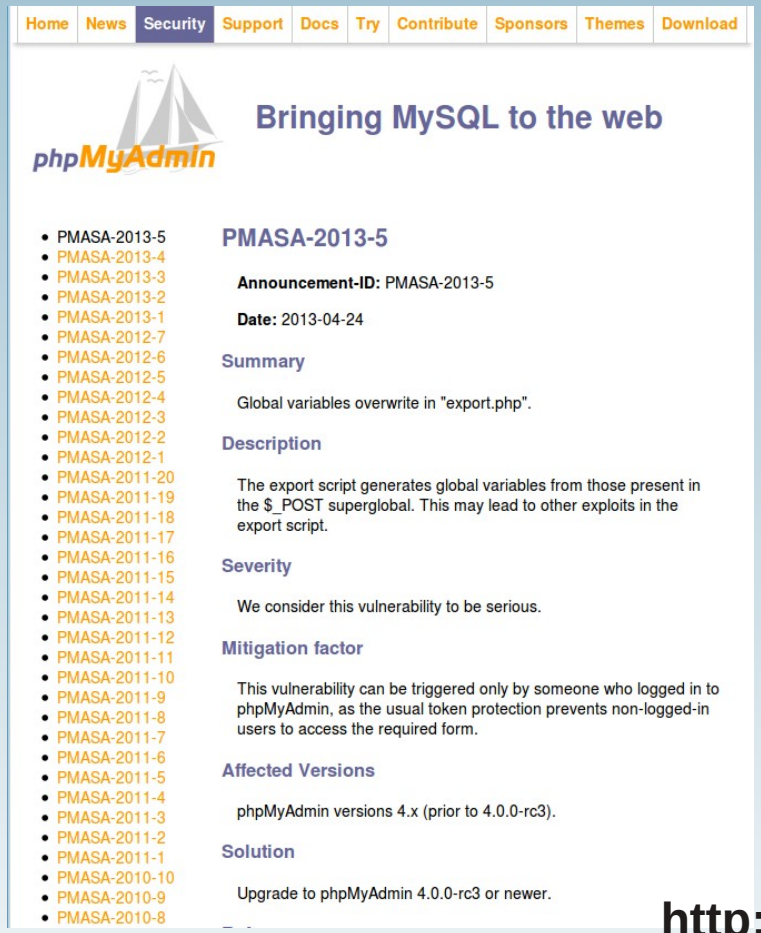
Zugriffsbeschränkung

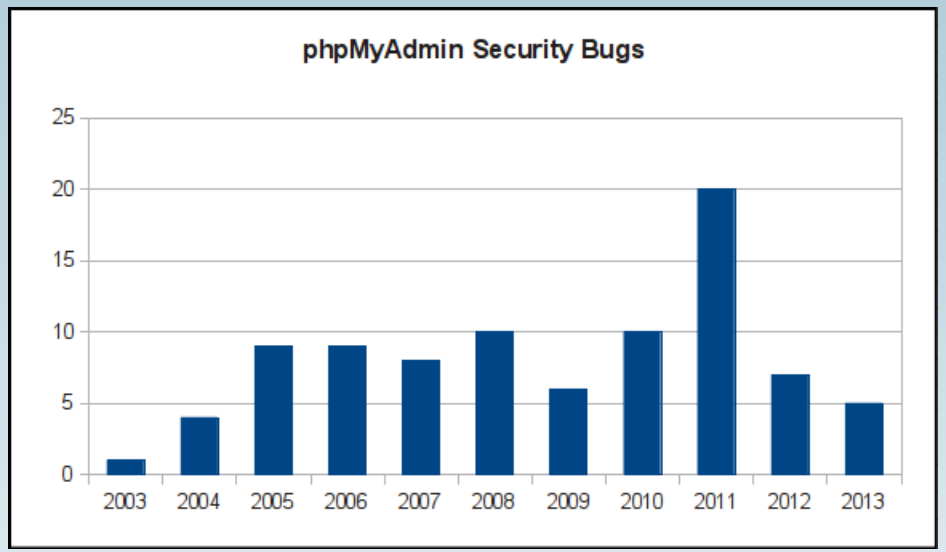
- Betriebssystem (`root` user)
- Zugriff aufs DB Filesystem!
- DB Zugriff
  - `root` von remote?
  - Passwörter: leer, default, gleich, ändern
  - Privilegien: `ALL ON *.*`

Abwehrmassnahmen

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

phpMyAdmin





http://www.phpmyadmin.net/home_page/security/

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?**

Warum Upgrade Demo

Integrität

Datenintegrität

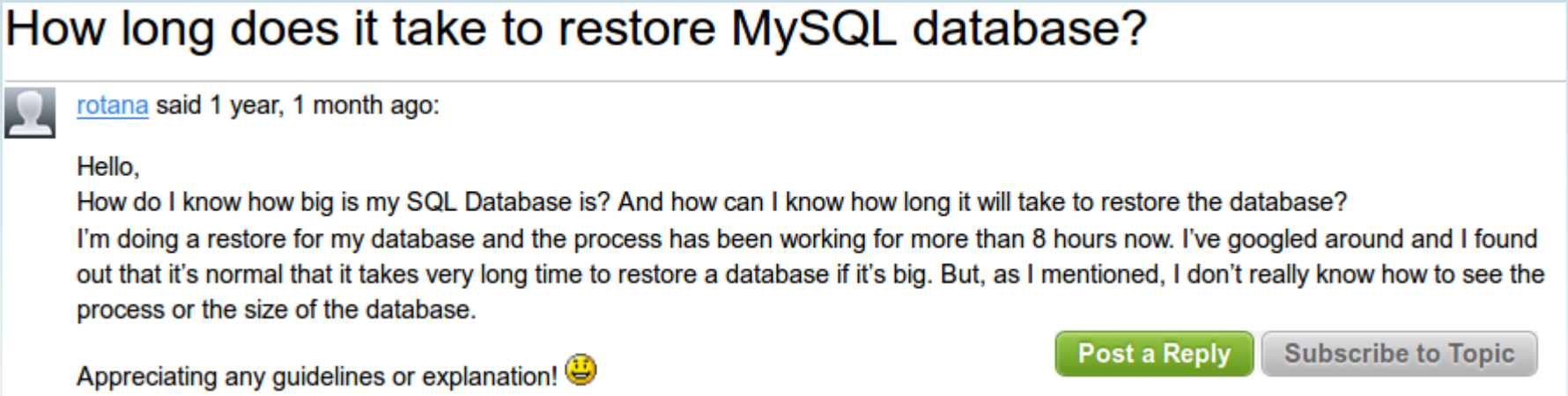
- Binary Log
- General Query Log
- Logon Trigger (`init_connect`)

- Audit Log Plugin (Enterprise Feature)
- McAfee MySQL Audit Plugin

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?

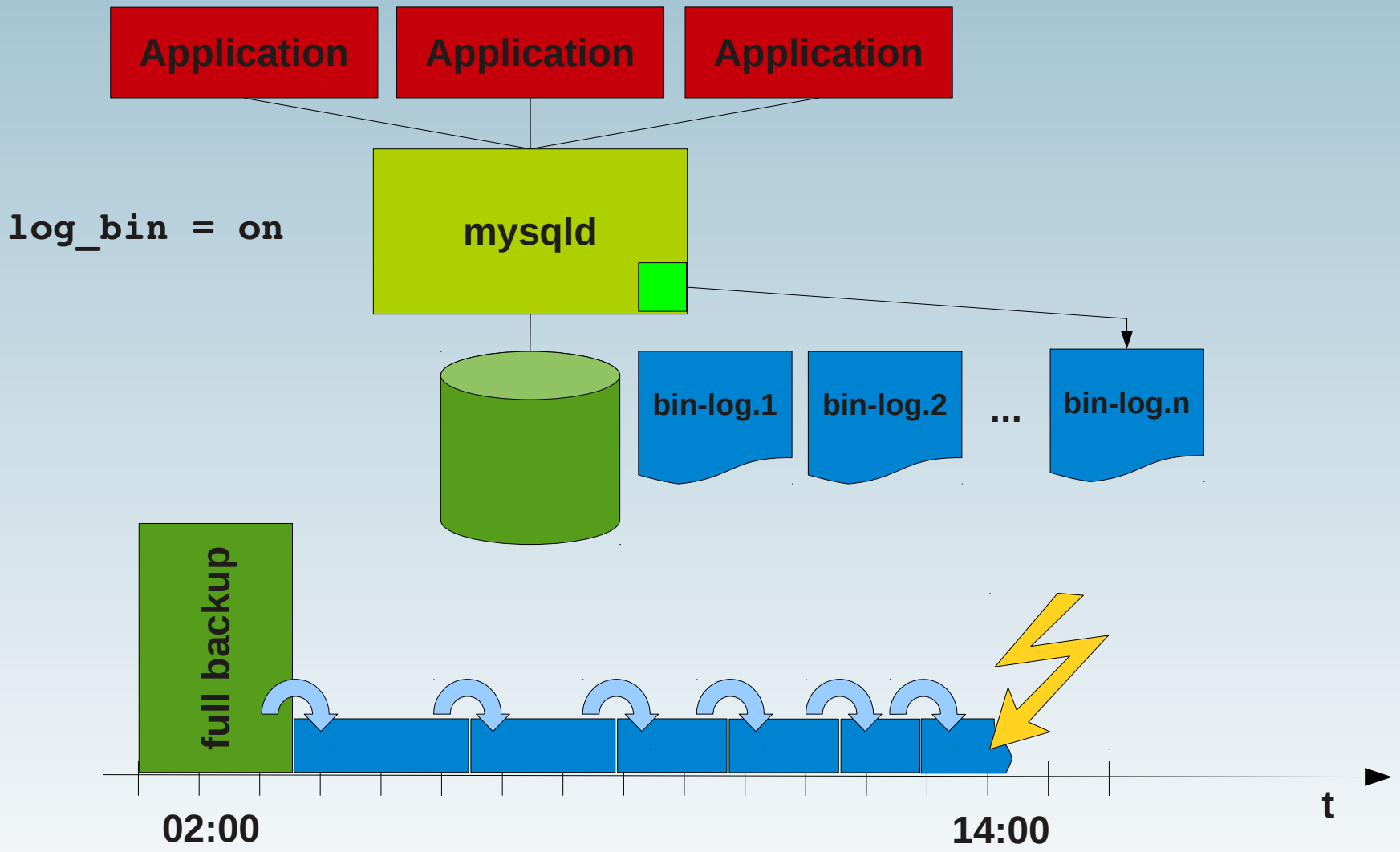
rotana said 1 year, 1 month ago:

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)



Warum Restore Test Demo

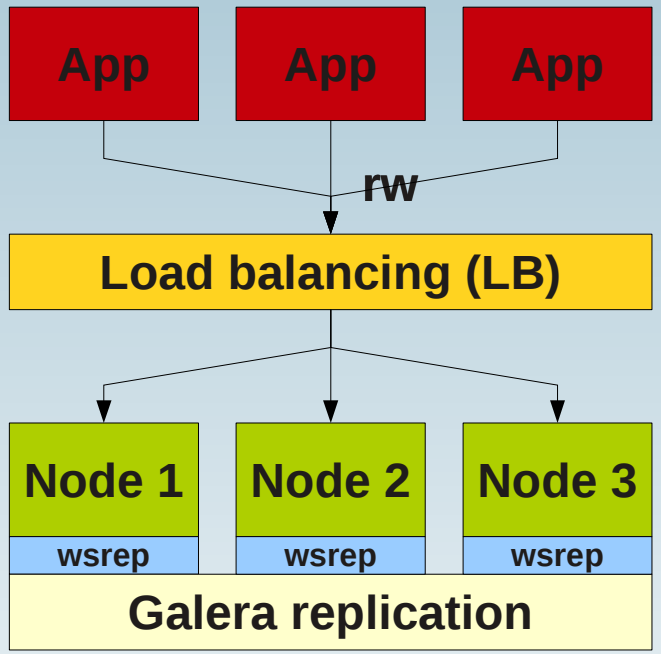
HA Lösungen

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

- → Hatten wir ja schon zu Beginn.

- Achtung: NICHT für logische Fehler → Backup!

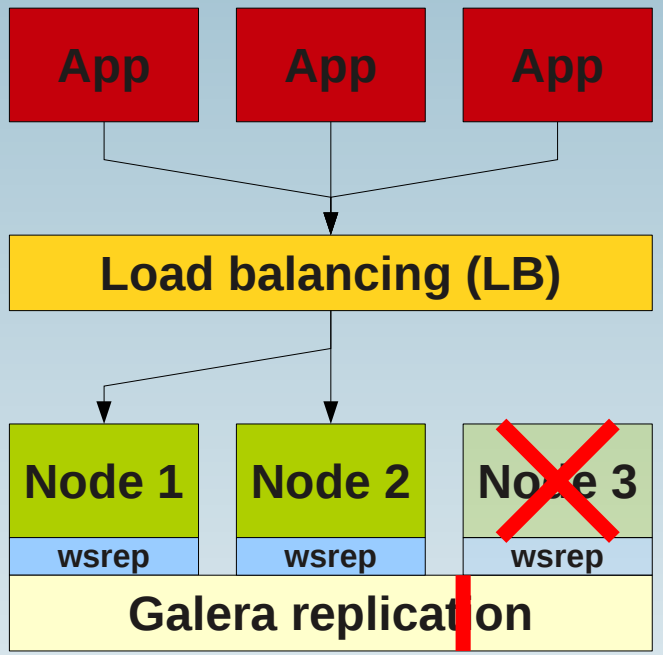
Galera Cluster für MySQL



synchrone Replikation

Galera Cluster für MySQL

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



Demo Galera Cluster

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
- GreenSQL: MySQL SQL Firewall

  http://www.greensql.com
- McAfee: MySQL Audit Plugin

  https://github.com/mcafee/mysql-audit/downloads

Wir suchen noch:

www.fromdual.com

- MySQL Enthusiast/in für Support / remote-DBA / Beratung

  und
- C++ Entwickler (mit Affinität zu DB, MySQL und Replikation)

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