

# ةيناثل ةلوجل MariaDB: يناربيسل نمأل

Sylvain ARBAUDIE · 8 ويناوي 2025

MARIADB SECURITY HARDENING SYSTEMD SELINUX

## CYBERSEC MARIADB — ROUND 2: ADVANCED HARDENING

5 layers of defense — init\_file + LUKS + systemd + chattr + SELinux



### LAYERED DEFENSE — each layer increases attack cost

Layer 1: Runtime restore

Layer 2: At-rest encryption

Layer 3: Process isolation

Layer 4: Immutability

Layer 5: Mandatory access control at kernel level

Security is a spectrum — make the attack costly enough to discourage it

## تاساسأل ءارو ام

نم ىندأل دلحو، ةيوق رورم تاملك: تاساسأل MariaDB / MySQL نامأل نم ىلوال ةلوجل يطغت نحن. كلذ نم دعبأل ةل ةيناثل ةلوجل. ةيامحل رادج نيوكتو، TLS نيكمتو، نيمدختسمل تانايبل دءاوق يلوؤسم نم ليلق دءاوق بطل تانقت يهو - مدقتمل ددشتل ةقطنم لخدن ممصم مجاهم دص آقرف ثدحت اهنكلو.

## تماصلل صنلل init\_file:

متيس يذلاو SQL فلم ديدحت MariaDB / MySQL ب صاخل init\_file ريرتلم كل حيتي بصلل ةيوق ةادأ اهنإ. مدخال ليغشت ءدب دنع آيئائل هذيفن:

```
[mysqld]
init_file = /etc/mysql/conf.d/init_security.sql
```

ىل ع init\_security.sql فلملليوتحي دق:

```
-- Désactiver les comptes par défaut
ALTER USER 'root'@'localhost' ACCOUNT LOCK;

-- Révoquer les privilèges excessifs
```

```
REVOKE ALL PRIVILEGES ON *.* FROM 'app_user'@'%';
GRANT SELECT, INSERT, UPDATE, DELETE ON app_db.* TO 'app_user'@'%';

-- Supprimer les bases de test
DROP DATABASE IF EXISTS test;

-- Activer l'audit
INSTALL SONAME 'server_audit';
SET GLOBAL server_audit_logging = ON;
```

إدعاء لإيقاف، لفظت الة لمة مع انثأ تاناي الة دعاق لة دعبت ني مجاهم الة دحأ ماق اذ ي تحت: ة زيمل ا نم آل ني وك الة دعاع س ا لة أي ئا ق لة يدؤت م داخ الة لي غشت

## تافل م الة ماطن ري فشت: LUKS

نكل، ة لصل الة لودج الة حاسم ري فشت InnoDB معدي. ة رفشم ريغ MariaDB تاناي ب نوكت نأ ب جي تافل م الة ماطن ري فشت ب موق ي وهف: الومش رثكأ ة يامح رفوي (LUKS (Linux Unified Key Setup) ن. ني وك الة تافل م و ة تقؤم الة تافل م الة و الة ح س الة ك ل ذ ي ف ماب، ه ل م ك أب

```
# Créer un volume chiffré LUKS pour le datadir
cryptsetup luksFormat /dev/sdb1
cryptsetup luksOpen /dev/sdb1 mariadb_data
mkfs.ext4 /dev/mapper/mariadb_data
mount /dev/mapper/mariadb_data /var/lib/mysql
```

و، TPM مدختسا. تاناي الة هب دجوت يذال صرق الة سفن يلع LUKS حات فم ني زخت أدبأ يغب ني الة (Vault, AWS KMS) ة جي راخل الة ح ي تافل م الة ة راد ا ة مدخ و، USB زم

## PrivateMounts و ة ي ضارت فال ا ت اداع الة فلم: systemd

ق رط ة دع ب systemd MariaDBunit فلم ة ي وقت نكم ي

### ح ي رص ي ضارت فال م --

```
[Service]
ExecStart=/usr/sbin/mariadb --defaults-file=/etc/mysql/mariadb.cnf
```

فلم لثم) يخال ني وك الة تافل م ة ارق نم MariaDB عنم ي لة --defaults-file دي دحت ي دؤي (مجاهم الة هطق س أ ي ذال ا رض الة ~/my.cnf



```
chattr -i /etc/mysql/mariadb.cnf
# ... modifier le fichier ...
chattr +i /etc/mysql/mariadb.cnf
systemctl restart mariadb
```

## ةصصخ م ل ا ت ا س ا ي س ل ا SELinux:

SELinux ة س ا ي س ب ا د و ز م MariaDB ي ت ا ي . ة ل م ه م ن ا م ا ة ق ب ط ي و ق ا ض ر ف ل ا ع ض و ي ف SELinux د ع ي ر ي ث ك ب ك ل ذ ن م د ع ب ا ب ه ذ ت ن ا ة ص ص خ م ل ا ت ا س ا ي س ل ل ن ك م ي ن ك ل و ، ة ي ض ا ر ت ف ا

### ص ص خ م SELinux ع و ن ء ا ش ن ا ب م ق

```
# Définir un type pour les fichiers de configuration sensibles
semanage fcontext -a -t sec_custom_path_t "/etc/mysql/conf.d(/.*)?"
restorecon -Rv /etc/mysql/conf.d/
```

## ةصصخ م ل ا ة د ح و ل ا ة س ا ي س

MariaDB: ل ل ا ل و ص و ل ا د ي ق ي ي ذ ل ا (ع و ن ل ا ض ر ف) .te ف ل م ء ا ش ن ا ب م ق

```
# mariadb_custom.te
module mariadb_custom 1.0;

require {
    type mysqld_t;
    type sec_custom_path_t;
    class file { read open getattr };
}

# MariaDB peut lire les configs mais pas les modifier
allow mysqld_t sec_custom_path_t:file { read open getattr };
# Pas d'écriture autorisée sur les configs
```

ت ي ب ث ت و ع ي م ح ت:

```
checkmodule -M -m -o mariadb_custom.mod mariadb_custom.te
semodule_package -o mariadb_custom.pp -m mariadb_custom.mod
semodule -i mariadb_custom.pp
```

نم نكم تي نلف ، MariaDB اليمع قارتخاب نيمجاهم لادح اذ اذى تح ، ةسايسلا هذه مادختساب ةاونلا يوتسم يلعل لوصولا رطحب SELinux موقى شيح - نيوكتلاتافل م ليذعت

## تاقبطلاددعت م عافد

أمهم أعرد نولكشي ، أع م . هذو يفكي ءيش ال . عافدلا نم ةقبط يه انه ةضورعم ةينقت لك

ةقبط	ةيامحلا	دص
init_file	ةيئاقلت ةداعتسا	ليغشلتل تقو نيوكت تاريغت
سكول	ةحارلا ةلاح يف ريفشلتلا	يلعفلل صرقلل ةقرس
systemd ءامسألاتاحاسم	ةيلمعلل لزع	زايتمالا دي عصت
+i ةشدردلا	تان نيوكتلاتا بت	قرتخملا رذجلل قي رط نع ليدعتلا
سكنيل يس	لوصولا يف يمازلإل مكحتلا	MariaDB اليمع لالغتسا

## ةصالخلا

بعضاً موجهل لعجت ةفاضم ةقبط لك . ةربخو آتقو MariaDB ةمدقتملا بلصتلا اليمع بلطتت فاشتكالل ةيلباق رثك أو أطب أو

لجج نكلو ، (لحس م اذو) أنصح م نوكت نأ سيل فدهلا . فيط وه لب ، ةيئاثل ةلاح سيل نمألا لهسأ فده يلإ مجاهملا لقتني شيحب ةيفاك ةجردب أفلكم موجهلا

طسوتم يلعل لصلألا يف ةلاقملا هذه رشن م