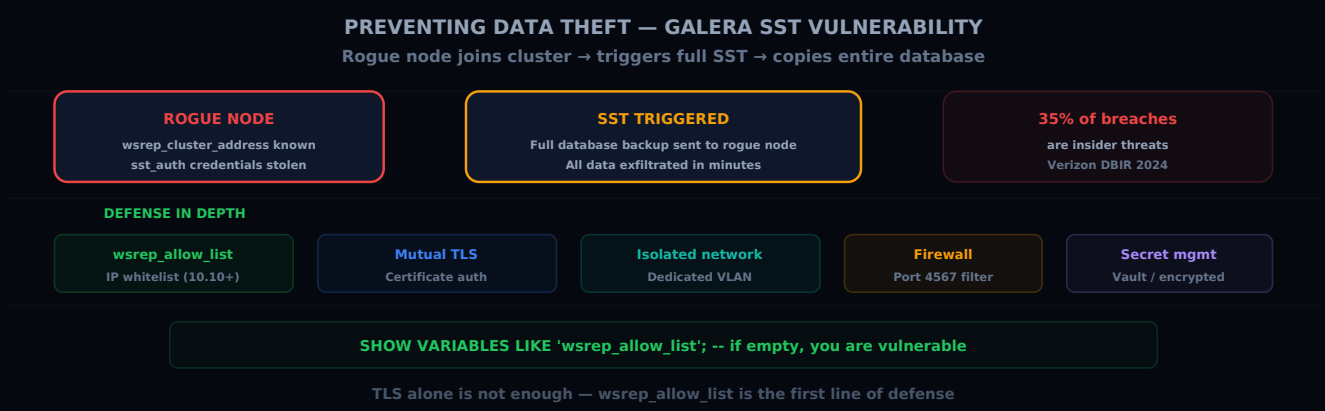
Предотвращение кражи данных: издание Galera

Sylvain ARBAUDIE · March 12, 2025

GALERA MARIADB SECURITY SST



Кошмарный сценарий

Представьте: злоумышленник настраивает сервер MariaDB с правильными параметрами wsrep, знает адрес кластера Galera и пароль SST. Он присоединяется к кластеру. Galera обнаруживает новый узел без данных и инициирует **State Snapshot Transfer (SST)** — полную передачу всех данных кластера на узел злоумышленника.

За несколько минут (или часов, в зависимости от размера базы) злоумышленник получает полную копию вашей базы данных. Без SQL-инъекций, без эксплуатации уязвимостей приложения. Просто JOIN к кластеру с правильными учётными данными.

Это не научная фантастика. Согласно отчёту Verizon 2024 об утечках данных, **35% нарушений данных связаны с внутренними угрозами** — сотрудниками, подрядчиками или лицами, имеющими легитимный доступ к инфраструктуре.

Как работает SST

State Snapshot Transfer — это механизм, с помощью которого Galera инициализирует новый узел. Когда узел присоединяется к кластеру без данных (или с данными, слишком устаревшими для инкрементального IST), кластер запускает SST:

1. Узел-донор (существующий участник кластера) выбирается
2. Донор выполняет полный бэкап (через mariabackup, rsync или mysqldump)
3. Бэкап отправляется присоединяющемуся узлу по сети
4. Присоединяющийся узел восстанавливает бэкап и входит в кластер

Проблема: **по умолчанию любой узел с правильной информацией о кластере может инициировать SST**. Нет белого списка, нет проверки идентичности присоединяющегося узла.

Минимальная конфигурация для атаки

Что нужно злоумышленнику:

```
[mysqld]
wsrep_cluster_address = gcomm://10.0.1.10,10.0.1.11,10.0.1.12
wsrep_sst_method = mariabackup
wsrep_sst_auth = sst_user:sst_password
```

Три элемента информации: адрес кластера, метод SST и учётные данные SST. Во многих организациях эта информация хранится в незашифрованных файлах конфигурации, открытых плейбуках Ansible или приватных Git-репозиториях.

Почему TLS недостаточно

«Но мы используем TLS для трафика Galera!» — это частое возражение. И оно недостаточно.

TLS шифрует трафик между узлами, но не обязательно проверяет идентичность присоединяющегося узла. Даже с TLS, если злоумышленник обладает сертификатом, подписанным той же CA (что часто бывает при внутренних развёртываниях с корпоративной PKI), он может присоединиться к кластеру.

Кроме того, многие развёртывания Galera не используют взаимную проверку сертификатов (mutual TLS). Они включают TLS для шифрования, но не для аутентификации.

Решение: wsrep_allow_list

Начиная с MariaDB 10.10, переменная `wsrep_allow_list` предлагает механизм белого списка IP для узлов, которым разрешено присоединяться к кластеру:

```
[mysqld]
wsrep_allow_list = 10.0.1.10,10.0.1.11,10.0.1.12
```

Только узлы, чей IP-адрес указан в списке, могут присоединиться к кластеру. Узел с IP, не входящим в список, будет отклонён, даже если он обладает правильными учётными данными SST и правильными TLS-сертификатами.

Это просто, эффективно и является первой линией защиты, которую должен иметь каждый кластер Galera.

Глубокая защита

Безопасность кластера Galera не основана на одном механизме. Вот подход глубокой защиты:

1. wsrep_allow_list — Сетевая фильтрация

```
wsrep_allow_list = 10.0.1.10,10.0.1.11,10.0.1.12
```

Ограничить IP-адреса, которым разрешено присоединяться к кластеру.

2. Взаимный TLS — Аутентификация узлов

```
wsrep_provider_options = "socket.ssl=yes;socket.ssl_key=/etc/mysql/ssl/server-
key.pem;socket.ssl_cert=/etc/mysql/ssl/server-cert.pem;socket.ssl_ca=/etc/mysql/ssl/ca.pem"
```

Каждый узел должен предъявить сертификат, подписанный CA кластера. Нет валидного сертификата = нет соединения.

3. Изолированная сеть — Сегментация

Трафик Galera (порты 4567, 4568, 4444) должен проходить по выделенной сети, изолированной от прикладной сети и сети управления. Рекомендуется выделенный VLAN или оверлейная сеть (WireGuard, IPsec).

4. Файрвол — Фильтрация портов

```
# iptables: разрешить только IP кластера на портах Galera
iptables -A INPUT -p tcp -s 10.0.1.10 --dport 4567 -j ACCEPT
iptables -A INPUT -p tcp -s 10.0.1.11 --dport 4567 -j ACCEPT
iptables -A INPUT -p tcp -s 10.0.1.12 --dport 4567 -j ACCEPT
iptables -A INPUT -p tcp --dport 4567 -j DROP
```

5. Шифрование учётных данных SST

Никогда не храните пароли SST в открытом виде в файлах конфигурации. Используйте менеджеры секретов (Vault, AWS Secrets Manager) или как минимум шифрование файлов конфигурации.

Аудит вашего кластера

Проверьте прямо сейчас состояние безопасности вашего кластера Galera:

```
-- Проверить, настроен ли wsrep_allow_list
SHOW VARIABLES LIKE 'wsrep_allow_list';

-- Проверить состояние TLS Galera
SHOW STATUS LIKE 'wsrep_connected';
SHOW VARIABLES LIKE 'wsrep_provider_options';

-- Список текущих узлов кластера
SELECT * FROM information_schema.WSREP_MEMBERSHIP;
```

Если `wsrep_allow_list` пуст, ваш кластер уязвим. Настройте его немедленно.

Заключение

Уязвимость SST в Galera — недооценённый вектор атаки. Неавторизованный узел может получить полную копию вашей базы данных, просто присоединившись к кластеру. Решение простое: `wsrep_allow_list` + взаимный TLS + изолированная сеть + файрвол.

35% утечек данных — внутренние угрозы. Защищён ли ваш кластер Galera?

Эта статья была первоначально опубликована на Medium.