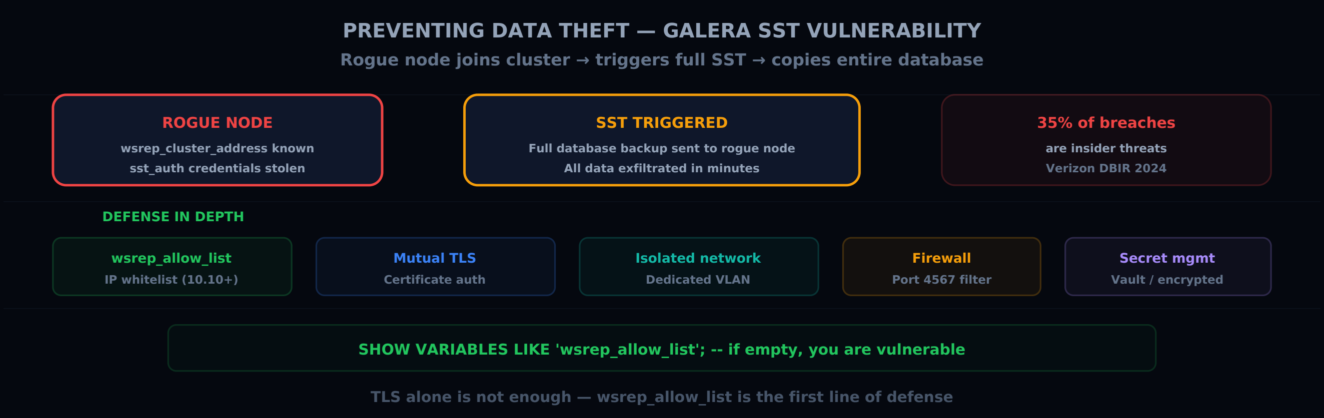
[illegible]Galera [illegible]

Sylvain ARBAUDIE · 2025[illegible]3[illegible]12[illegible]

GALERA MARIADB SECURITY SST



[illegible]

[illegible] MariaDB [illegible] wsrep [illegible] **State Snapshot Transfer [illegible] SST** [illegible] Galera [illegible] SQL [illegible] JOIN[illegible]

[illegible] 2024 [illegible] **35%** Verizon [illegible]

SST [illegible]

State Snapshot Transfer [illegible] Galera [illegible] IST[illegible] SST[illegible]

1. [illegible]
2. [illegible] mariabackup[illegible]rsync [illegible] mysqldump[illegible]
3. [illegible]
4. [illegible]

[illegible]**SST**

[illegible]

[illegible]

```
[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
```

三条信息：集群地址、SST 方法和 SST 凭据。在许多组织中，这些信息存储在未加密的配置文件、明文的 Ansible playbook 或私有 Git 仓库中。

为什么 **TLS** 还不够

"但我们对 Galera 流量使用了 TLS！"——这是一个常见的反驳。但这是不够的。

TLS 加密了节点之间的流量，但不一定能验证加入节点的身份。即使使用了 TLS，如果攻击者拥有由相同 CA 签发的证书（在使用企业 PKI 的内部部署中通常如此），他们仍然可以加入集群。

此外，许多 Galera 部署不使用双向证书验证（mutual TLS）。它们启用 TLS 进行加密，但不进行身份验证。

解决方案：**wsrep_allow_list**

从 MariaDB 10.10[illegible] `wsrep_allow_list` 变量提供了一个 IP 白名单机制，用于限制允许加入集群的节点：

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

只有 IP 地址在列表中的节点才能加入。即使拥有有效的 SST 凭据和 TLS 证书，IP 不在列表中的节点也会被拒绝。

这很简单、有效，是每个 Galera 集群都应该配置的第一道防线。

纵深防御

Galera 集群的安全不依赖于单一机制。以下是纵深防御方法：

1. wsrep_allow_list——网络过滤

限制允许加入集群的 IP。

2. 双向 **TLS——**节点认证

每个节点必须出示由集群 CA 签发的证书。

3. 隔离网络**——**网段划分

Galera 流量（端口 4567、4568、4444）应在专用网络上传输，与应用程序和管理网络隔离。

4. 防火墙——端口过滤

```
# iptables: 仅允许集群 IP 访问 Galera 端口
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. 加密的 SST 凭据

永远不要以明文存储 SST 密码。使用密钥管理器（Vault、AWS Secrets Manager）或至少使用配置文件加密。

审计您的集群

立即检查您的 Galera 集群安全状况：

```
SHOW VARIABLES LIKE 'wsrep_allow_list';
SHOW VARIABLES LIKE 'wsrep_provider_options';
SELECT * FROM information_schema.WSREP_MEMBERSHIP;
```

如`wsrep_allow_list` 为空，您的集群存在漏洞。请立即配置。

结论

Galera SST 漏洞[illegible]个被低估的攻击向量。[illegible]经[illegible]权[illegible]节点[illegible]通过[illegible]入集群[illegible]可[illegible]取您数[illegible]库的完整副本。修复方法很简单：

35% 的数据泄露是内部威胁。您的 Galera 集群是否受到保护？

本文最初[illegible]表于[illegible]。