MariaDB is a relational database solution deployed for secure data management across the network. In this topology, the Web_DB VM serves as the dedicated MariaDB server, and all other hosts requiring database access are strictly authenticated and authorized.

MariaDB Security Policy Overview

The MariaDB security policy in this environment is designed to enforce strong authentication, encrypt data in transit, restrict privileges, and harden the database server and its operating system configuration. Controls apply at every level: system, MariaDB configuration, network, and user access.

Hardening Measures for the MariaDB Server

- Only the designated Web_DB VM, configured with a static IP (`192.168.1.3`) inside the NAC network, runs the MariaDB server.
- The database service is installed using secure, up-to-date packages and is enabled to start automatically.
- Root accounts are protected via unix_socket authentication and are not allowed remote access.
- Anonymous users and test databases are removed, eliminating default and unnecessary access points.
- Data and log directories are relocated outside the system disk to a dedicated, restricted partition with strict permissions, handled only by a dedicated, non-interactive `mysql` user.
- The database process is sandboxed using systemd, with precise controls over accessible system paths, temporary space, and kernel resources.

Authentication, Authorization, and Encryption

- All client connections to MariaDB require SSL/TLS encryption with X509 certificates, ensuring secure and verifiable identities.
- Users are created with privilege separation: only authorized accounts are permitted, each assigned the minimum rights needed for their role (e.g., SELECT-only for web applications).
- Certificate management ensures that keys and client certs are protected—private keys are never stored on the database server, and permissions are set to restrict file access.
- The host, user, and privileges associated with every database account are reviewed and restricted to only necessary sources or services.

Connection Limits and Monitoring

- Maximum global and per-user connection limits are enforced to mitigate risk of denial-of-service or brute-force attacks.
- Privilege grants and access controls are adjusted and audited regularly; authentication relies only on securely managed X509 certificates.
- Regular validation of database status, privilege tables, and SSL connection logs supports operational monitoring and incident detection.

Operational Controls

- Immediate removal of temporary test accounts and client certificates after use, enforcing a clean security posture.
- Network and firewall controls ensure only authorized hosts within the DMZ or NAC networks may connect to MariaDB using encrypted channels.
- Secure transfer and import/export procedures are followed, and the database configuration is regularly validated for compliance with policy.

This security policy ensures MariaDB operates in a hardened, minimal trust environment: strong authentication and encryption are mandatory, privileges are separated by necessity, file and process-level controls prevent escalation, and regular monitoring enforces ongoing vigilance.