- `SYSTEM_VARIABLES_ADMIN`

  Affects the following operations and server behaviors:

  - Enables system variable changes at runtime:

    - Enables server configuration changes to global system variables with `SET GLOBAL` and `SET PERSIST`.

    - Enables server configuration changes to global system variables with `SET PERSIST_ONLY`, if the user also has `PERSIST_RO_VARIABLES_ADMIN`.

    - Enables setting restricted session system variables that require a special privilege. In effect, `SYSTEM_VARIABLES_ADMIN` implies `SESSION_VARIABLES_ADMIN` without explicitly granting `SESSION_VARIABLES_ADMIN`.

    See also Section 5.1.9.1, “System Variable Privileges”.

  - Enables changes to global transaction characteristics (see Section 13.3.7, “SET TRANSACTION Statement”).

- `TABLE_ENCRYPTION_ADMIN` (added in MySQL 8.0.16)

  Enables a user to override default encryption settings when `table_encryption_privilege_check` is enabled; see Defining an Encryption Default for Schemas and General Tablespaces.

- `VERSION_TOKEN_ADMIN`

  Enables execution of Version Tokens functions. This privilege is defined by the `version_tokens` plugin; see Section 5.6.6, “Version Tokens”.

- `XA_RECOVER_ADMIN`

  Enables execution of the `XA RECOVER` statement; see Section 13.3.8.1, “XA Transaction SQL Statements”.

  Prior to MySQL 8.0, any user could execute the `XA RECOVER` statement to discover the XID values for outstanding prepared XA transactions, possibly leading to commit or rollback of an XA transaction by a user other than the one who started it. In MySQL 8.0, `XA RECOVER` is permitted only to users who have the `XA_RECOVER_ADMIN` privilege, which is expected to be granted only to administrative users who have need for it. This might be the case, for example, for administrators of an XA application if it has crashed and it is necessary to find outstanding transactions started by the application so they can be rolled back. This privilege requirement prevents users from discovering the XID values for outstanding prepared XA transactions other than their own. It does not affect normal commit or rollback of an XA transaction because the user who started it knows its XID.

Privilege-Granting Guidelines

It is a good idea to grant to an account only those privileges that it needs. You should exercise particular caution in granting the `FILE` and administrative privileges:

- `FILE` can be abused to read into a database table any files that the MySQL server can read on the server host. This includes all world-readable files and files in the server's data directory. The table can then be accessed using `SELECT` to transfer its contents to the client host.

- `GRANT OPTION` enables users to give their privileges to other users. Two users that have different privileges and with the `GRANT OPTION` privilege are able to combine privileges.