Translate

Search:

Home
Download
Cheat Sheet

Documentation
Quickstart
Installation
Tutorial
Features
Security
Performance
Advanced

Reference
Commands
Functions
• Aggregate • Window

Data Types
SQL Grammar
System Tables
Javadoc
PDF (2 MB)

Support
FAQ
Error Analyzer
Google Group

Appendix
History
License
Build
Links
MVStore
Architecture
Migration to 2.0

Securing your H2

Introduction

H2 is __not__ designed to be run in an adversarial environment. You should absolutely not expose your H2 server to untrusted connections.

Running H2 in embedded mode is the best choice - it is not externally exposed.

Network exposed

When running an H2 server in TCP mode, first prize is to run with it only listening to connections on localhost (i.e 127.0.0.1).

Second prize is running listening to restricted ports on a secured network.

If you expose H2 to the broader Internet, you can secure the connection with SSL, but this is a rather tricky thing to get right, between JVM bugs, certificates and choosing a decent cipher.

Alias / Stored procedures

Anything created with `CREATE ALIAS` can do anything the JVM can do, which includes reading/writing from the filesystem on the machine the JVM is running on.

Grants / Roles / Permissions

`GRANT / REVOKE` TODO

Encrypted storage

Encrypting your on-disk database will provide a small measure of security to your stored data. You should not assume that this is any kind of real security against a determined opponent however, since there are many repeated data structures that will allow someone with resources and time to extract the secret key.

Also the secret key is visible to anything that can read the memory of the process.