llm-runtime Cheat Sheet

Quick reference for LLM file access and command execution

Commands

Command	Syntax	Example
Read File	`<open path>`	`<open main.go>`

Write File	`<write path>content</write>`	`<write config.yaml>`
		`port: 8080`
		`</write>`

Execute	`<exec command>`	`<exec go test ./...>`
Search	`<search query>`	`<search authentication>`

CLI Options

Option	Description	Default
`--root PATH`	Repository root directory	Dynamic repo in /tmp/dynamic-repo/
`--config FILE`	Config file path	./llm-runtime.config.yaml
`--exec-timeout`	Exec command timeout	30s
`--exec-memory`	Exec container memory	512m
`--io-timeout`	I/O operation timeout	10s
`--verbose`	Enable verbose output	false
`--reindex`	Rebuild search index	-

Default Whitelisted Commands

Category	Commands
Go	`go test, go build, go run, go mod tidy, go vet, go fmt`
Node.js	`npm test, npm run build, npm install, node`
Python	`python, python3, python -m pytest, pip install`
Build	`make, make test, make build, make clean`
Rust	`cargo build, cargo test, cargo run`
System	`ls, cat, grep, find, head, tail, wc`

Docker Setup

Task	Command
Build I/O container	`make build-io-image`
Check I/O image	`make check-io-image`
Pull exec container	`docker pull python-go:latest`

Verify images	`docker images | grep -E "llm-runtime-io|python-go"`
Clean Docker	`docker system prune -a`

Search Setup (Ollama)

Task	Command
Install Ollama (Linux)	`curl -fsSL https://ollama.com/install.sh | sh`
Pull embedding model	`ollama pull nomic-embed-text`
Build search index	`./llm-runtime --reindex`
Verify Ollama	`ollama list`

Common Errors

Error	Cause	Fix
`DOCKER_UNAVAILABLE`	Docker not running	Start Docker daemon
`EXEC_VALIDATION`	Command not whitelisted	Add to config whitelist
`EXEC_TIMEOUT`	Command too slow	Increase --exec-timeout
`READ_VALIDATION`	Path outside repo	Use relative paths
`SEARCH_FAILED`	Ollama not running	Start Ollama: ollama serve

Common Workflows

Code Analysis: `<search authentication>` → `<open internal/auth/auth.go>` **Make Changes:** `<open config.yaml>` → `<write config.yaml>...</write>` → `<exec go test ./...>` **Test & Build:** `<exec go test ./...>` → `<exec go build -o bin/app .>`

Dynamic Repository Isolation

By default, llm-runtime creates a temporary git repository in `/tmp/dynamic-repo/` for all operations. This prevents accidental modification of your working directories. Use `--root /path/to/repo` to operate on a specific directory. Set `KEEP_TEST_REPOS=true` to preserve dynamic repos for debugging.

Makefile Targets

Target	Description
`make build`	Build the binary
`make test`	Run tests
`make clean`	Remove build artifacts
`make build-io-image`	Build Docker I/O container
`make test-write`	Test write functionality
`make test-suite`	Run comprehensive test suite