fix(server): 未配置 root_api_key 时仅允许 localhost 绑定 #310

Merged qin-ctx merged 1 commit into `main` from `fix/localhost-bind-without-auth` on Feb 26

qin-ctx commented on Feb 26 Collaborator

Description

修复安全漏洞：当 `server.root_api_key` 未配置时，`resolve_identity()` 将所有请求解析为 `Role.ROOT`，结合默认绑定 `0.0.0.0`（所有网络接口），导致任何网络请求均可执行管理员操作。

本 PR 将默认绑定地址改为 `127.0.0.1`，并在启动阶段校验配置安全性：无认证 + 非 localhost 绑定时拒绝启动。

Related Issue

Fixes #302

Type of Change

- [x] Bug fix (non-breaking change that fixes an issue)
- [ ] New feature (non-breaking change that adds functionality)
- [ ] Breaking change (fix or feature that would cause existing functionality to not work as expected)
- [x] Documentation update
- [ ] Refactoring (no functional changes)
- [ ] Performance improvement
- [x] Test update

Changes Made

- **`openviking/server/config.py`**：默认 `host` 从 `0.0.0.0` 改为 `127.0.0.1`（`ServerConfig` 和 `load_server_config` 两处）；新增 `_is_localhost()` 辅助函数和 `validate_server_config()` 启动校验函数，无 key + 非 localhost 时调用 `sys.exit(1)` 并输出错误日志和修复建议
- **`openviking/server/app.py`**：`create_app()` 中加载 config 后调用 `validate_server_config()`；dev mode 日志从 `logger.info` 升级为 `logger.warning`，明确提示认证已禁用
- **`tests/server/test_auth.py`**：新增 6 个测试用例（含参数化共 10 个 case），覆盖 `_is_localhost` 和 `validate_server_config` 的各种场景
- **`docs/{en,zh}/guides/04-authentication.md`**：更新开发模式段落，示例 host 改为 `127.0.0.1`，添加安全说明

Testing

- [x] I have added tests that prove my fix is effective or that my feature works
- [x] New and existing unit tests pass locally with my changes
- [x] I have tested this on the following platforms:
  - [ ] Linux
  - [x] macOS
  - [ ] Windows

验证场景：

1. `pytest tests/server/test_auth.py` — 全部 22 个测试通过
2. `host: "0.0.0.0"` + 无 `root_api_key` → 服务器拒绝启动（`SystemExit`）
3. `host: "127.0.0.1"` + 无 `root_api_key` → 正常启动，输出 WARNING 日志
4. `host: "0.0.0.0"` + 有 `root_api_key` → 正常启动

Checklist

- [x] My code follows the project's coding style
- [x] I have performed a self-review of my code
- [x] I have commented my code, particularly in hard-to-understand areas
- [x] I have made corresponding changes to the documentation
- [x] My changes generate no new warnings
- [x] Any dependent changes have been merged and published

Additional Notes

- 现有测试 fixture 中 `ServerConfig()` 默认值改为 `127.0.0.1` 后，因属于 localhost 范围，校验自动通过，无需修改 conftest
- `auth.py` 中 `resolve_identity()` 逻辑保持不变，安全保护在启动阶段完成

`fix(server): 未配置 root_api_key 时仅允许 localhost 绑定` ··· ✓ `0251c70`

github-project-automation bot added this to **OpenViking project** on Feb 26

github-project-automation bot moved this to **Backlog** in **OpenViking project** on Feb 26

CLAassistant commented on Feb 26 • edited

CLA signed

All committers have signed the CLA.

zhoujh01 approved these changes on Feb 26

View reviewed changes

qin-ctx merged commit **`9e69113`** into `main` on Feb 26

5 of 6 checks passed

View details

qin-ctx deleted the `fix/localhost-bind-without-auth` branch 2 months ago

github-project-automation bot moved this from **Backlog** to **Done** in **OpenViking project** on Feb 26

Reviewers

zhoujh01

Assignees

No one assigned

Labels

None yet

Projects

OpenViking project

Status: Done +5 more

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

[Bug]: Missing `root_api_key` enables anonymous ROOT access (broken access control)

3 participants