HKUDS / **OpenHarness** Public

Code | Issues 10 | Pull requests 12 | Actions | Projects | Security and qua

Commit 438e373

Hinotoi-agent committed 4 days ago · ✓ 8 / 8

```
fix: keep bridge command local-only by default
```

main (#208)

1 parent 380bab4 commit 438e373

3 files changed +75 -1

Top

Filter files…

- src/openharness/commands
  - registry.py
- tests
  - test_commands
    - test_registry.py
  - test_ohmo
    - test_gateway.py

Search within code

src/openharness/commands/registry.py

```
@@ -1847,7 +1847,15 @@ async def _ship_handler(args: str, context:
CommandContext) -> CommandResult:
1847  1847      registry.register(SlashCommand("rewind", "Remove the latest conversation
turn(s)", _rewind_handler))
```

```
1848  1848        registry.register(SlashCommand("files", "List files in the current workspace", _files_handler))
1849  1849        registry.register(SlashCommand("init", "Initialize project OpenHarness files", _init_handler))
1850        -     registry.register(SlashCommand("bridge", "Inspect bridge helpers and spawn bridge sessions", _bridge_handler))
      1850  +     registry.register(
      1851  +         SlashCommand(
      1852  +             "bridge",
      1853  +             "Inspect bridge helpers and spawn bridge sessions",
      1854  +             _bridge_handler,
      1855  +             remote_invocable=False,
      1856  +             remote_admin_opt_in=True,
      1857  +         )
      1858  +     )
1851  1859        registry.register(SlashCommand("login", "Show auth status or store an API key", _login_handler))
1852  1860        registry.register(SlashCommand("logout", "Clear the stored API key", _logout_handler))
1853  1861        registry.register(SlashCommand("feedback", "Save CLI feedback to the local feedback log", _feedback_handler))
```

tests/test_commands/test_registry.py

```
@@ -130,6 +130,24 @@ async def test_reload_plugins_command_supports_explicit_remote_admin_opt_in(tmp_
130  130       assert getattr(command, "remote_admin_opt_in", False) is True
131  131
132  132
      133  + @pytest.mark.asyncio
      134  + async def test_bridge_command_is_marked_local_only(tmp_path: Path, monkeypatch):
      135  +     monkeypatch.setenv("OPENHARNESS_CONFIG_DIR", str(tmp_path / "config"))
      136  +     registry = create_default_command_registry()
      137  +     command, _ = registry.lookup("/bridge spawn id")
      138  +     assert command is not None
      139  +     assert command.remote_invocable is False
      140  +
      141  +
      142  + @pytest.mark.asyncio
```

```
      143 + async def test_bridge_command_supports_explicit_remote_admin_opt_in(tmp_path:
          Path, monkeypatch):
      144 +     monkeypatch.setenv("OPENHARNESS_CONFIG_DIR", str(tmp_path / "config"))
      145 +     registry = create_default_command_registry()
      146 +     command, _ = registry.lookup("/bridge spawn id")
      147 +     assert command is not None
      148 +     assert getattr(command, "remote_admin_opt_in", False) is True
      149 +
      150 +
  133 151   @pytest.mark.asyncio
  134 152   async def test_memory_show_rejects_path_traversal(tmp_path: Path, monkeypatch):
  135 153       monkeypatch.setenv("OPENHARNESS_CONFIG_DIR", str(tmp_path / "config"))
```

tests/test_ohmo/test_gateway.py

```
      @@ -464,6 +464,54 @@ async def fake_start_runtime(bundle):
  464 464       assert updates[-1].text == "/permissions is only available in the local
          OpenHarness UI."
  465 465
  466 466
      467 + @pytest.mark.asyncio
      468 + async def test_runtime_pool_blocks_bridge_spawn_from_remote_messages(tmp_path,
          monkeypatch):
      469 +     workspace = tmp_path / ".ohmo-home"
      470 +     initialize_workspace(workspace)
      471 +     handler_called = False
      472 +
      473 +     async def forbidden_bridge_handler(args, context):
      474 +         nonlocal handler_called
      475 +         handler_called = True
      476 +         return CommandResult(message="spawned")
      477 +
      478 +     async def fake_build_runtime(**kwargs):
      479 +         class FakeEngine:
      480 +             messages = []
      481 +             total_usage = UsageSnapshot()
      482 +
      483 +             def set_system_prompt(self, prompt):
      484 +                 return None
      485 +
```

```
+         command = SlashCommand(
+             "bridge",
+             "Inspect bridge helpers and spawn bridge sessions",
+             forbidden_bridge_handler,
+             remote_invocable=False,
+             remote_admin_opt_in=True,
+         )
+         return SimpleNamespace(
+             engine=FakeEngine(),
+             session_id="sess123",
+             current_settings=lambda: SimpleNamespace(model="gpt-5.4"),
+             commands=SimpleNamespace(lookup=lambda raw: (command, "spawn id")),
+         )
+
+     async def fake_start_runtime(bundle):
+         return None
+
+     monkeypatch.setattr("ohmo.gateway.runtime.build_runtime",
fake_build_runtime)
+     monkeypatch.setattr("ohmo.gateway.runtime.start_runtime",
fake_start_runtime)
+
+     pool = OhmoSessionRuntimePool(cwd=tmp_path, workspace=workspace,
provider_profile="codex")
+     message = InboundMessage(channel="feishu", sender_id="u1", chat_id="c1",
content="/bridge spawn id")
+     updates = [u async for u in pool.stream_message(message, "feishu:c1")]
+
+     assert handler_called is False
+     assert updates[-1].kind == "final"
+     assert updates[-1].text == "/bridge is only available in the local
OpenHarness UI."
+
+
 @pytest.mark.asyncio
 async def test_runtime_pool_allows_opted_in_remote_admin_commands(tmp_path,
monkeypatch, caplog):
     workspace = tmp_path / ".ohmo-home"
```

Comments 0

Please sign in to comment.