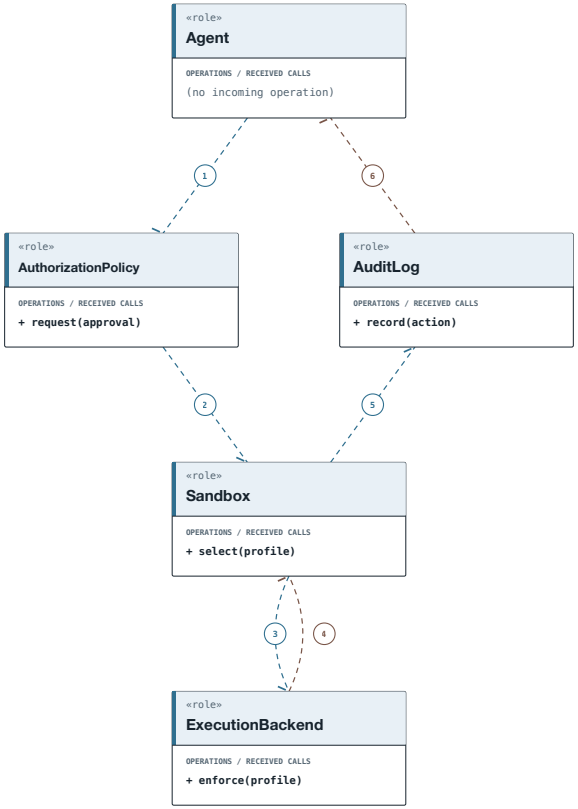
P23 Layered permission and sandbox

Primitive / UML CLASS VIEW / ANALYTICAL MODEL

Combine policy decisions with execution isolation.

UML CLASS VIEW

dashed arrow: call dependency · brown: return/failure · analytical, not an observed trace



POINTCUT / PATTERN INTERFACE

CONTEXT	A tool action is evaluated by policy and executed in a controlled environment.
TRIGGER	A privileged operation or command is dispatched.
STRUCTURE	Authorization decision, sandbox profile, environment adapter, and enforcement point.
EFFECT	The effective capability equals the authorized capability, including filesystem and network.

CONTRACT / REQUIRED BEHAVIOR

REQUIRES	Requested operation and active environment policy are both observable.
ENSURES	Any difference between approval and enforcement fails closed or asks for escalation.
INVARIANT	A policy decision cannot be bypassed by switching sandbox or transport backend.
VIOLATION	Enforcement errors deny execution and preserve actionable diagnostics.

RELATIONSHIPS / ANALYTICAL CALLS

number · caller → callee · message

1 Agent → AuthorizationPolicy request(approval)
2 AuthorizationPolicy → Sandbox select(profile)
3 Sandbox → ExecutionBackend enforce(profile)
4 ExecutionBackend ↩ Sandbox return(result)
5 Sandbox → AuditLog record(action)
6 AuditLog ↩ Agent report(denial_or_error)

VARIATION / TEST / NEGATIVE CONTROL

VARIATION	OS sandbox, container, mount policy, network rules, and approval mode.
TEST_OBLIGATION	Test each backend, denied write/network, cross-backend parity, and escape attempts.
NEGATIVE_CONTROL	A prompt warning without execution enforcement is not a sandbox.