



DATABLAU · DAM

数据治理智能体

产品模块用户手册

版本 9.1.2

目录

01	数据治理智能体
02	快速开始
03	后台管理
04	智能体模板
05	人工审批与协作
06	上下文检查与发布
07	数据智能空间
08	数据智能空间端到端治理
09	核心治理能力
10	初始化
11	模型服务
12	例程编排与运行
13	精灵设计与发布
14	精灵与例程

数据治理智能体

“数据治理智能体”是对外统一名称，英文名为 DIG；DAM 界面模块名称为“数据智能治理”。DIG 是对 DAM 传统数据治理能力的 AI 增强：以智能体辅助各阶段治理工作，并将治理后的资产语义和知识组织为可对外提供的上下文。DIG 不替代原有治理模块、审批或数据权限。无相应 License 时，DAM 右下角 AI 对话入口及相关 AI 页面不可见。

DIG 如何参与治理

DAM 保存元数据、标准、质量规则、安全分类与级别以及资产目录等治理对象。DIG 根据用户提出的目标调用这些能力，形成建议并把经确认的结果落入对应模块。使用 DIG 前，仍需准备可以访问的对象、业务规则和相应权限。

可以从 DAM 当前数据源、表或资产详情唤起 AI 对话，处理一个明确任务；也可以在 DIG 创建数据智能空间，长期组织一个业务范围内的资产、文档和治理流程。

选择使用方式

你要完成的工作	使用入口	开始阅读
给一张表补齐业务名称和描述	DAM 的 AI 对话或对象详情治理入口	快速开始
围绕业务域组织持续治理	数据智能空间	创建空间并组织治理
从治理现状分析到持续治理和上下文发布	数据智能空间端到端治理	端到端治理
将治理成果用于 AI 查询	空间的上下文管理和发布阶段	上下文质量与发布
审核标准、分类分级等建议	我的审批单	人工审批与协作
沉淀可重复的治理动作和流程	配置管理 → 治理精灵	精灵、例程与执行诊断
配置模型和可调用工具	配置管理	初始化设置、模型服务、后台管理

两个空间阶段

智能治理（DG by AI）：用 AI 辅助原有数据治理工作。把待治理资产和文档加入空间，使用空间专属智能体或例程开展元数据补齐、标准、质量、安全和资产整理，并审核结果。

上下文对外赋能 (DG for AI)： 让已治理的结果为 AI 应用提供依据。将资产语义、标准、血缘和知识文件组织为可信上下文，检查质量后通过空间 Agent 或 MCP 提供查询能力；这不等于向外部直接交付底层业务数据。

这两个阶段在工作区中对应“开始、数据治理、上下文管理、发布”四个步骤。治理阶段是否结束取决于实际结果，不以对话结束或执行次数判断。

核心对象

对象	作用	与其他对象的关系
智能体	理解目标并组织执行	使用模型、工具、Skill、精灵和例程
智能体模板	保存不可直接执行的配置快照	已发布模板用于创建空间专属实例；后续调整不自动覆盖实例
Skill	封装可复用的任务说明与执行方法	指导智能体如何完成一类任务；本身不是数据源或审批人
治理精灵	承担一个明确的原子任务	定义输入、执行工具和输出，可独立测试
例程	按确定流程组合精灵	负责节点顺序、参数映射与失败处理
数据智能空间	组织业务范围、文档和阶段智能体	承接治理，再提供治理后的上下文

MCP（Model Context Protocol，模型上下文协议）用于通过约定的工具接口连接智能体与外部能力。在 DIG 中要区分两个方向：配置 MCP 服务是让 DIG 调用外部工具；发布空间 MCP 是让外部 AI 应用使用该空间开放的上下文能力。两者的服务地址、授权与可见范围分别配置，不能互相代替。

按职责阅读

数据管家先阅读[快速开始](#)和[核心治理能力](#)；需要组织完整闭环时阅读[端到端治理](#)；审批人阅读[人工审批](#)；空间负责人阅读[空间操作与上下文发布](#)；管理员阅读[初始化](#)、[模板管理](#)及[后台管理](#)。这些是建议的职责分工，实际角色和权限由组织配置。

精灵设计者应先阅读[精灵设计与发布](#)，流程设计者再阅读[例程编排与运行](#)。

使用边界

模型输出需要结合企业规范和实际数据核对。高置信度、任务成功状态或对话中的“已完成”均不能替代对 DAM 实际结果的检查。不同部署可用的智能体、模板和工具由管理员配置，示例名称不代表所有环境均已内置。

数据治理智能体快速开始

DIG 的对外产品名称是“数据治理智能体”，DAM 中的模块名称是“数据智能治理”。本指南以“为一张表补齐业务元数据”为例，带你完成进入对话、选择范围、生成建议、人工审批和结果核对。示例任务需要替换为自己有权处理的表。

使用前提

- 环境已部署并启用 DIG，相应 License 已生效。
- 当前用户具有 DIG 入口和目标治理对象的数据权限。
- 管理员已配置可用的模型、智能体及其工具能力。
- 已明确治理目标、对象范围、参考规范和验收方式。
- 上传内容不含未经授权的敏感信息。

未启用 DIG 时，DAM 右下角 AI 对话图标及相关 AI 页面不可见。客户可自定义角色和功能权限，因此本手册用职责描述使用者，不把角色名称写成系统固定值。

如果环境尚未配置可用智能体，请管理员先完成[初始化设置](#)。如果要长期组织一个业务域的治理，可以随后[创建数据智能空间](#)。

第一步 选择进入方式

从 DAM 右下角 AI 图标打开对话框；从表或资产详情页的魔法棒或治理入口发起时，系统会带入当前对象上下文。进入后仍需检查对象和所属系统。

要使用 DIG 独立工作区，可在 DAM 右上角用户菜单选择“切换DIG”。返回 DAM 时，在 DIG 左下角用户菜单选择“切换 DAM”。





第二步 认识入口并新建会话

AI 对话框

AI 对话框是日常发起治理任务的主要入口。对话框底部可提供以下操作，实际可见项取决于权限：

- 对话 / 计划。
- 新建会话。
- 选择智能体。
- 查看用户进程。
- 进入我的审批单。
- 管理我的提示词。
- 上传或引用文件。
- 会话历史。



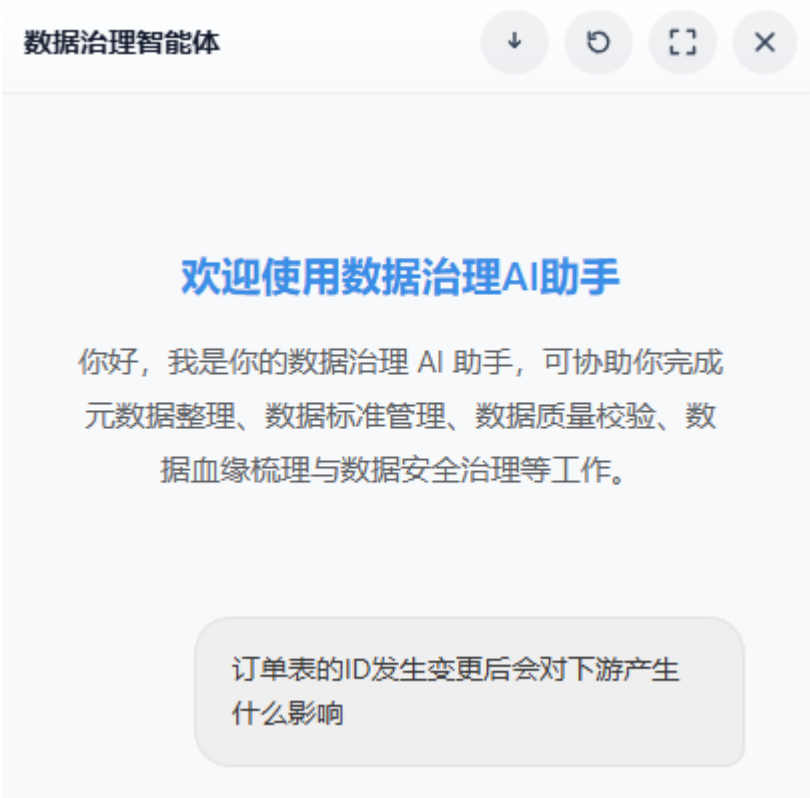
[查看对话框原图](#)。管理员配置智能体和资源时使用 DIG 主导航的“配置管理”。

治理看板

治理看板包含 AI 治理统计指标、近五天核心治理 workflow 审批完成率趋势，以及历史 AI 治理任务统计和实时执行列表。统计与审批状态用于跟踪进展，实际治理结果仍应回到 DAM 对象核对。

新建会话

- 1. 在 DAM 打开右下角 AI 对话框。
- 2. 选择新建会话。
- 3. 从可用列表选择与任务匹配的智能体。
- 4. 输入治理目标、对象范围、参考依据、限制条件和期望结果。
- 5. 需要文档依据时上传文件，或从已授权文件中选择。
- 6. 提交请求并观察执行过程。
- 7. 检查建议范围和异常提示，再进入审批处理。



一个可执行的请求应说明：

要素	应说明的内容
目标	补齐、生成、检查、核标还是盘点
范围	数据源、表、字段、主题域或其他对象
依据	企业制度、已发布标准或业务背景
约束	需要跳过的对象、命名规则或阈值要求
验收	人工审核时如何判断建议可用

需要引用 DAM 对象时，优先使用界面提供的对象选择能力，并核对对象所属系统和环境。仅在提示词中手写名称可能选中错误的同名对象。

第三步 提交一项有明确范围的任务

进入你有权处理的表详情，通过治理入口带入表对象。先核对表名、所属系统和字段清单，再从“我的提示词”选择中文补全提示，替换其中的业务背景和范围。

也可以使用以下示例表达任务：

text

请检查当前选择的这张表，只对缺少中文名称或业务描述的字段提出补齐建议。

依据我提供的业务说明，保留已有且准确的描述。

请列出对象、原值、建议值和理由。无法确定的含义请说明缺少什么依据。

需要修改的数据请交由人工确认。

这是示例提示，不是系统固定规则。提交前确认没有使用“所有数据源”等超出预期的范围。其他任务的输入要求见[核心治理能力](#)。

会话标识与状态

会话 Key 由智能体标识和用户名组成，同一 Key 下只有一个会话处于 ACTIVE。每个对话实例有独立 Session ID；其他历史会话为 CLOSED。向管理员报告问题时，可提供会话标识以及发生时间。

状态	含义	用户操作
ACTIVE	会话可继续交互或仍有活动上下文	继续提问前核对当前对象和文件
CLOSED	会话已关闭	需要继续时从历史会话重新激活或新建会话

重新激活历史会话不会自动证明其中的文件、规范和对象仍然有效。继续任务前应重新核对引用资料的生效状态和对象范围。

上传和复用文件

1. 在会话中选择上传文件，或进入用户文件选择已有文件。
2. 检查文件名称、来源、用途和可见范围。
3. 上传后在提示中明确本次任务要引用的文件及章节。
4. 查看生成结果是否正确采用文件内容。

复用文件前检查版本、生效日期、权限和敏感信息。文件仅提供上下文，不会替代业务人员对制度适用性的判断。

从 DAM 发起治理

在支持 DIG 的 DAM 页面，可通过魔法棒或相应治理入口选择对象并发起任务。入口会把当前对象带入治理上下文，但用户仍应确认范围、所属系统和任务类型。批量对象应先用少量样本验证。

第四步 查看执行过程

提交后关注智能体调用步骤、当前进度、处理对象、未处理项和错误信息。用户进程用于查看本人任务的执行情况。若任务长时间无进展，不要重复提交相同大任务，应记录会话标识并由管理员检查模型和工具服务。

AI 生成内容是待审核建议，不是已发布结果。所有治理结果都应进入人工审批。

第五步 审核并回到 DAM 检查

1. 从对话框打开“我的审批单”，找到本次任务。
2. 逐项比较原值和建议值。涉及业务含义时，对照业务说明，而不是仅看置信度。
3. 修改、通过或拒绝建议，必要时填写原因。
4. 返回原表详情，核对中文名称和业务描述是否与通过的内容一致。
5. 对未处理字段补充背景后再次生成建议。不要重复提交已成功修改的范围。

完整审批操作见[人工审批与协作](#)。完成这个小任务后，再逐步扩大范围或使用[数据智能空间](#)组织多项治理任务。

完成检查

- 会话使用了正确的智能体和治理对象。
- 引用文件和规范仍然有效。
- 处理对象与输入范围一致，跳过项和失败项可解释。
- 建议已进入人工审批，没有被直接当作发布结果。
- 会话、进程、文件和审批单能够相互追溯。

常见问题

看不到 DIG 入口

请管理员检查部署、License、功能权限和模块入口。仅有 DAM 账号不代表具备 DIG 权限。

历史会话无法继续

检查会话状态，尝试从历史记录重新激活。若依赖的智能体、文件或对象权限已变化，应新建会话并重新选择有效上下文。

建议范围不正确

停止后续审批，重新选择对象并明确系统、环境、表或字段范围。必要时将大任务拆成多个小任务。

相关文档

- [核心治理能力](#)
- [人工审批与协作](#)
- [DIG 后台管理](#)

数据治理智能体后台管理

本指南供管理员维护智能体及其可复用资源。统一入口为 DIG 主导航“配置管理”；先核对当前智能体，再维护属于该智能体的模型、工具、Skill、文件和治理能力。

配置关系

 text

智能体

— 模型

— MCP 服务

— 内部服务

— Skill

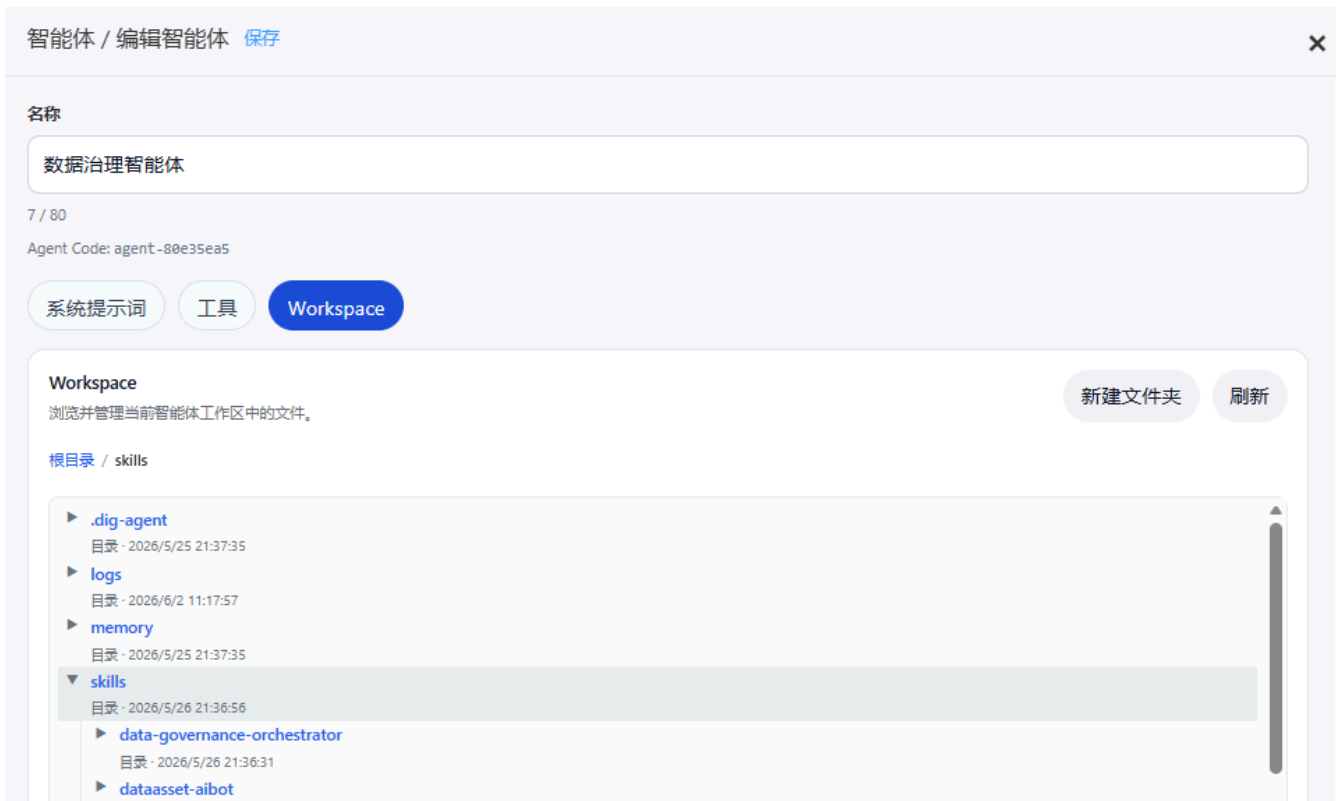
— 提示词与参数

— Workspace

精灵完成单一治理动作，例程编排多个精灵，用户文件提供受控上下文。

管理员应遵循最小权限原则，只为智能体配置完成职责所需的模型和工具。

智能体管理



创建或导入智能体

1. 进入“配置管理 → 智能体”，选择“添加智能体”或“导入智能体”。
2. 填写智能体名称，在系统提示词中说明职责、允许处理的数据范围和输出要求。
3. 选择已批准的模型。
4. 配置系统提示词和必要参数。
5. 绑定完成任务所需的工具、内部服务和 Skill。
6. 按需配置 Workspace。
7. 使用非敏感样本进行测试。
8. 保存并按页面提供的发布流程开放使用。新建会话后核对是否可以选择该智能体。

导入智能体时应检查包的来源、依赖服务、权限和提示词，不能直接把测试环境配置发布给用户。

智能体模板

模板是不可执行的配置快照，分为“数据治理智能体模板”和“业务查询智能体模板”。已实例化的智能体与模板相互隔离，模板更新不会自动覆盖实例，例程调度也不随模板复制。完整步骤见[创建和发布智能体模板](#)。

测试与发布

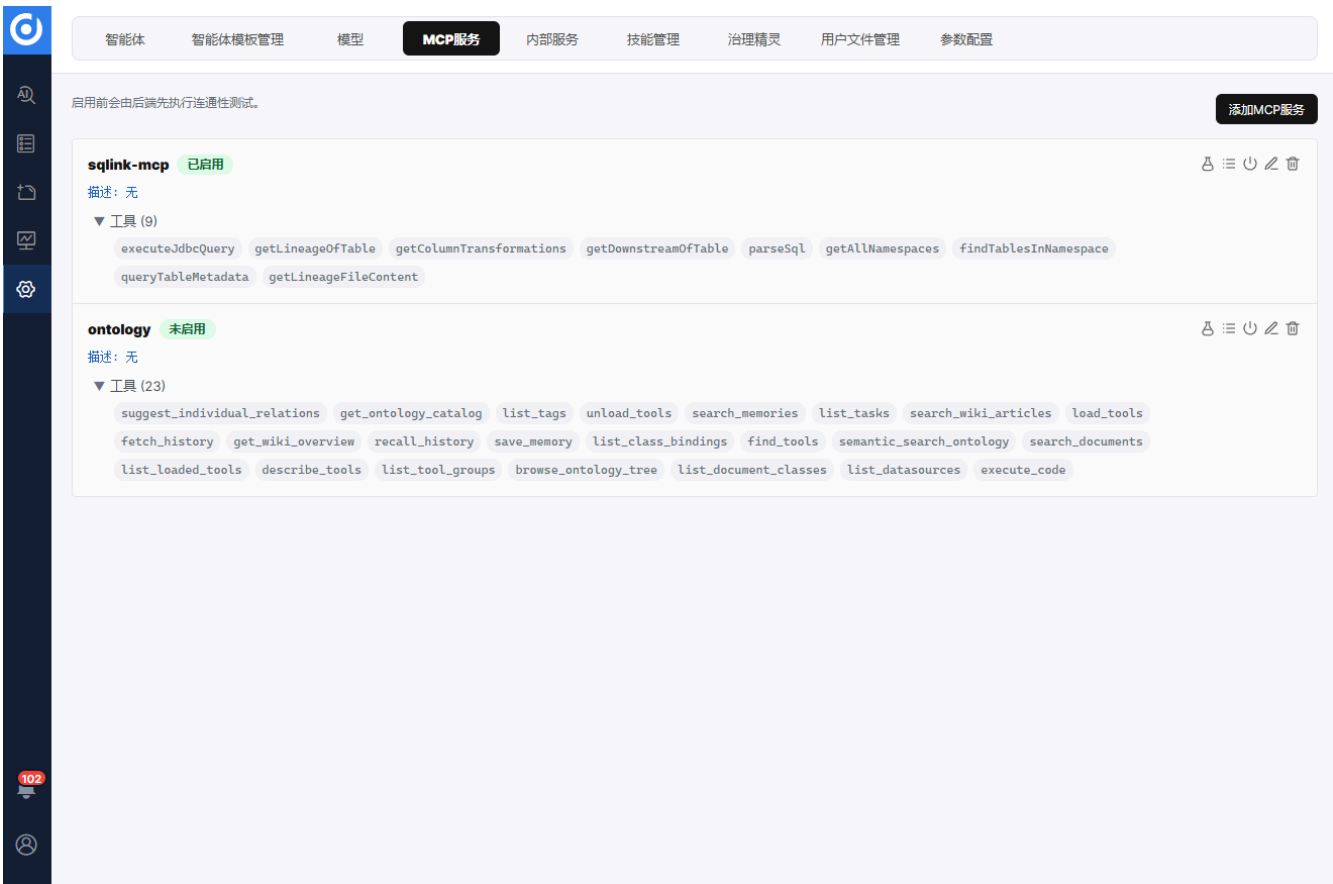
测试应覆盖正常输入、空输入、错误对象、超大范围、权限不足和服务不可用。发布前确认结果进入人工审批，且智能体不会向无权用户暴露工具或数据。

模型管理

进入“配置管理 → 大模型配置”维护共享模型配置，按 LLM 或 Text Embedding 类型设置参数。当前页面要求连接测试通过后才能保存，向量模型还需核对实际向量维度。具体字段、[大模型参数建议](#)、模型发现、复制及排查见[模型服务](#)。

连接可达不等于模型能够正确调用治理工具。保存后还需在目标智能体中验证小范围任务，并区分默认模型与默认智能体。

MCP 管理



MCP 服务用于让 DIG 调用其他应用的工具。进入“配置管理 → MCP服务”，选择“添加MCP服务”后填写以下字段：

智能体

启用前会由后端先执行

sqlink-mcp 未启

描述: 无

工具 (9)

ontology 未启

描述: 无

工具 (0)

添加 MCP 服务

名称

服务地址

连接模式

Streamable HTTP

连接超时 (毫秒)

30000

自定义设置 JSON

{ }

请求头 JSON

{ }

描述

测试 查看详情 取消 保存

添加 MCP 服务

添加 MCP 服务

[查看 MCP 表单原图](#)。图中地址和服务名称仅为当前环境示例。

字段	用途与填写要求
名称	在 MCP 列表中识别服务的名称。
服务地址	DIG Server 可以访问的 MCP Server 地址。
连接模式	当前表单提供 Streamable HTTP 和 SSE，按服务端协议选择。
连接超时 (毫秒)	单次连接测试的超时时间，页面提供默认值；按网络和服务响应情况调整。
自定义设置 JSON	服务端要求的附加设置；必须使用合法 JSON。
请求头 JSON	服务端要求的请求头；认证信息应按企业安全规范管理，不放入截图或普通提示词。
描述	记录服务用途和适用智能体。

单击“测试”检查连通性，再保存。列表中的“工具（数量）”用于查看服务暴露的工具，“查看详情”用于核对工具定义；启用前系统还会由后端执行连通性测试。测试成功只表示服务可达，不代表返回内容正确，也不表示所有用户都有权执行全部工具。删除或停用前检查依赖的智能体、Skill 和精灵。

内部服务

进入“配置管理 → 内部服务”。页面支持“上传 YAML”批量导入，也支持“添加内部服务”逐条定义。逐条添加时填写：

字段	含义
名称	在内部服务列表中显示的名称。
目标应用	接口所属的 DAM 或其他应用。
描述	说明用途、数据范围和风险。
服务接口	接口的声明或标识。
服务路径	实际调用路径。
方法名称	底层接口的方法名称。
参数 JSON	接口输入参数定义。

保存后页面会立即生效。内部服务通过底层程序接口提供能力，无需为每个接口另建 MCP 或命令行程序。导入或添加前检查接口用途、输入输出、身份传递和写操作风险；导入后以最小样本验证调用结果。

创建、修改、发布或删除类服务应比只读查询设置更严格的授权和审批。快速调用用于测试或受控执行，不能绕过业务权限。

Skill 管理

Skill 封装可复用的治理步骤。配置内容可包括：

- 适用范围和职责说明。
- 提示词及其 Markdown 预览。
- Skill 包路径和依赖接口。
- 可调用工具与输入输出约束。
- 测试用例和预期结果。

进入“配置管理 → 技能管理”，先选择作用域：

- **智能体**：保存在当前智能体工作目录，进入会话后按配置启用；可扫描工作区、上传 ZIP 或单击“添加 Agent 技能”。添加表单至少包含“Skill 编码”“名称”和“内容”，已有 Skill 还可切换“智能体默认启用”。
- **全局**：管理系统可用 Skill，单击“添加 Skill”维护编码、名称和内容，再编辑、删除或查看详情。
- **用户**：维护当前用户自己的 Skill，作用范围不等于全局 Skill。

编辑提示词后使用 Markdown 预览检查格式，核对 Jar、Python 包等依赖路径和 DAM 接口，再测试典型输入与失败情况。默认 Skill 优先复用，确有定制需求时再修改。定制 Skill 调用需要用户身份的接口时，使用运行时 `${session.token}` 引用，不写入固定 Token。

治理精灵

进入“配置管理 → 治理精灵”，选择当前智能体，在精灵、例程和执行历史之间切换。精灵只处理一个明确任务，例程组织步骤、参数传递和失败策略。具体操作见[配置治理精灵和例程](#)。

用户文件

用户文件为会话和治理任务提供上下文。管理员可管理全部用户文件，普通用户管理本人文件；具体权限边界以当前环境为准。

进入“配置管理 → 用户文件管理”，选择当前智能体并查看文件列表。可编辑内容、引用到 AI 对话、下载、重命名或删除。新会话可继续引用已上传文件，无需重复上传。删除或替换前确认是否仍被会话、智能体或任务引用，避免历史任务失去依据。

参数管理

进入“配置管理 → 参数配置”。系统参数由运行时提供；全局参数和“我的参数”是静态配置，在分发 Skill 和调用提示词时替换。全局与个人参数支持新增、编辑、复制、删除和预览。

系统参数示例包括 {workspace.dir}（智能体工具目录）和 {usr.name}（当前用户名称）。全局 baseUrl 和用户身份的配置见[初始化设置](#)。复制含认证信息的参数时应确认目标用户和用途；预览时不要把真实认证值放进截图或反馈文件。

常用提示词

常用提示词用于复用成熟的任务表达，可在界面维护或按支持格式导入。提示词应包含目标、输入范围、规则、限制和输出要求。导入后预览格式并用样本验证，再提供给用户。

提示词不是权限控制手段，不能依赖文本指令阻止未授权的数据访问或写入操作。

上线前检查

- 智能体只对授权用户可见。
- 模型、MCP 和内部服务连接正常，失败信息可定位。
- 每个智能体只绑定完成职责所需的工具和 Skill。
- 对会写入 DAM 的治理结果，已按企业审批策略确认是人工审批、批量审批还是允许自动通过；不要把“审批页面可用”误写成所有任务都强制人工审批。
- 用户文件和参数的可见范围符合数据安全要求。
- 凭据未出现在页面、日志、提示词和导出文件中。
- 配置变更、测试和发布具有审计记录。

常见问题

配置保存后似乎没有生效。 先核对当前智能体和实际对话使用的智能体是否一致，再检查依赖服务与参数。模板和空间实例隔离，更新模板不会修改既有实例。

模型测试成功，但治理任务失败。 继续检查 DAM 根地址、用户身份和工具调用日志。模型、MCP、内部服务是不同的连接环节。

新会话找不到原文件。 检查登录用户、当前智能体和文件列表，确认没有删除、替换或引用错误文件。

相关文档

- [开始使用 DIG](#)
- [核心治理能力](#)
- [人工审批与协作](#)
- [系统管理](#)

智能体模板

智能体模板是不可执行的配置快照，用于复制已经整理好的智能体能力。创建数据智能空间时，空间使用模板生成专属智能体，而不是直接在模板上运行任务。

选择模板类型

进入“配置管理 → 智能体模板管理”，选择适合阶段的分区。

模板类型	用途	后续使用位置
数据治理智能体模板	组织治理能力、精灵和例程	空间的数据治理阶段
业务查询智能体模板	查询和解释已治理资产及知识	空间的上下文使用阶段



查看模板列表原图。截图中的实例名称和修订标识为演示内容，不是必须使用的模板名称。

创建前准备

先在智能体管理准备来源智能体，并验证模型、系统提示词、MCP、Skill、精灵和例程。模板发布不是连通性测试，也不会修复来源配置中的错误。

创建草稿

1. 在对应模板分区单击“新建模板”。
2. 选择“创建来源智能体”。这是用于复制配置的普通智能体。
3. 填写“模板名称”和“描述”，说明适用业务和能力边界。
4. 单击“创建草稿”。
5. 打开草稿，依次核对基本信息、系统提示词、MCP、Skill、精灵和例程。

系统复制来源智能体的系统提示词、MCP、Skill、精灵和例程配置，**不会复制例程调度**。精灵和例程在模板中以只读快照展示。

发布模板

1. 完成草稿配置的检查。
2. 回到模板列表，核对 Skill 数量和工具数量是否符合预期。
3. 单击该模板的“发布”。
4. 检查状态是否为“已发布”，以及最后编辑时间、修订记录是否符合本次操作。
5. 到空间创建入口检查模板是否出现在正确类型的选择列表。

模板列表中的“版本”表示模板自身配置修订，不是产品版本号。

编辑与发布新修订

在列表单击“编辑”，修改可配置内容并保存，再回列表发布。模板后续发布新修订不会自动改变已经创建的智能体或数据智能空间。

推广修改前，建议用新模板建立测试实例，检查原有任务是否还能得到预期结果。已有实例需要独立管理其配置；重新加载页面不会将其升级为最新模板。

实例化后的调度

由于例程调度没有随模板复制，需在目标智能体实例中单独配置和启用。检查实际触发时间及执行历史，不能因为模板中存在例程就认定空间已有周期任务。

删除模板前检查

确认该模板不再用于新建空间，并核对是否仍有使用者依赖它。删除模板不会改变已实例化的智能体，但会使后续无法从该模板创建实例。

常见问题

现象	排查方法
创建空间时找不到模板	检查模板类型及“已发布”状态
模板无法直接对话	模板是快照，需要实例化为智能体或空间
来源智能体改了，模板没有变化	检查是否重新整理模板并发布，不把快照当实时连接
模板更新后旧空间没变化	属于实例隔离机制，应检查目标实例配置
例程存在但没有定时执行	到目标实例检查调度；模板不复制调度

相关文档

- 创建空间并组织治理
- 精灵、例程与执行诊断
- 初始化设置

DIG 人工审批与协作

DIG 生成的治理内容是否进入人工审批，取决于治理任务和企业配置。对分类分级、标准、元数据等会影响治理结果的任务，建议默认进入审批；如果管理员配置了批量或自动通过策略，应在发布前明确适用范围。只要进入审批单，审批人就必须核对业务事实、治理规范和目标对象，并在提交前修改或拒绝不可靠建议。



进入审批单

1. 从 DIG 导航选择“我的消息”，打开待处理的审批请求；也可以从 AI 对话或治理任务入口进入。
2. 在审批列表中使用搜索框，或打开“筛选”按字段输入包含关键字的条件。多个字段同时生效。
3. 打开目标审批单，确认审批单名称、类型、编号、总行数和待审核数量。
4. 在“待审核”“已通过”“已拒绝”页签之间切换，检查当前处理状态。

状态筛选反映审批处理状态，不代表目标 DAM 模块中的发布或执行状态。审批通过后仍应到目标模块检查结果。

阅读审批详情

审批详情通常按清单和逐行查看组织：列表显示资产、分类目录或标准、结果字段、置信度和选择理由；单击“查看”可打开“逐行审批”，完整查看当前行属性并编辑文本框。审批页还提供“全部通过”“全部拒绝”“全部重置”“导出”和“提交”，并显示总行数、待审核、已通过、已拒绝及进度。

审核时至少确认：

- 对象属于正确的系统、环境和资产域。
- 修改前内容与当前 DAM 数据一致。
- 修改后内容符合企业制度和业务事实。
- 建议没有与已发布内容重复或冲突。
- 生成理由能够解释建议，不包含虚构依据。
- 变更不会越过当前审批人的职责范围。

修改、通过和拒绝

- **修改**：建议方向正确但内容需要纠正时，在逐行审批窗口编辑字段后再决定。
- **通过**：确认建议完整、准确且符合适用规范后逐行通过，或对已筛选的同类记录批量通过。
- **拒绝**：对象、依据或内容不正确时逐行拒绝，或批量拒绝明显不适用的记录，并保留原因。

逐行审批支持“连续模式”：通过当前行后自动进入当前页下一行；关闭连续模式则停留在当前行。已审批但尚未提交的行可以重置，已经提交的结果只能查看。完成逐行处理后，单击“提交”才会提交整张审批单。



[查看逐行审批帮助原图](#)。快捷键只对尚未提交的待审核行有效。

修改或拒绝理由应指出问题所在，例如对象范围错误、定义与现行制度冲突或技术规格不兼容。不要只写“错误”或“不合适”。

审批置信度

页面可能提供审批置信度、排序或逐条得分，帮助审批人优先检查不确定建议。置信度不能替代业务判断；高分建议仍可能因上下文缺失而错误，低分建议也可能包含有效线索。

批量处理

1. 筛选到同一治理任务、同类对象和相同规则范围。
2. 检查记录总数、异常项和低置信建议。
3. 打开若干明细，比较前后差异和生成理由。
4. 排除需要逐条判断的高风险对象。
5. 对确认范围执行批量通过或拒绝。
6. 操作后检查成功、失败和未处理数量。

分类分级、标准发布、关键质量规则或大范围元数据变更应提高抽样比例，必要时逐条审批。不要仅根据分数批量通过。

审批记录与反馈闭环

已通过和已拒绝列表用于追溯历史处理。对被修改或拒绝的建议，审批理由应反馈到后续治理规则、提示词或智能体优化中。完整闭环为：

1. 用户提出治理目标。
2. DIG 生成待审核建议。
3. 审批人比较前后内容并修改、通过或拒绝。
4. 结果进入相应 DAM 模块的后续流程。
5. 用户在目标模块检查实际状态。
6. 管理员根据重复问题优化配置。

自动通过不应作为本手册的默认策略。即使环境提供相关策略，也应由产品、治理和风险责任人确认任务范围、抽样比例和回退方式，并在审批列表中检查是否仍有待处理记录。

结果验证

- 审批单对应正确的会话、任务和对象。

- 审批决定与修改内容、理由一致。
- 批量范围未包含异常或范围外记录。
- 目标 DAM 模块中可查到审批后的结果或后续状态。
- 审批记录保留操作者、时间和必要变更信息。

常见问题

看不到审批单

检查当前账号的功能权限、数据范围和审批参与者配置，并确认生成任务已经进入审批阶段。

修改前内容与 DAM 不一致

停止审批，检查对象是否选错、数据是否被并发修改，以及审批单是否基于过期上下文。确认后重新生成或按流程处理冲突。

批量操作部分失败

记录失败对象和错误信息，检查数据权限、对象状态和并发变更。只重试确认失败的记录，避免重复处理成功项。

相关文档

- [开始使用 DIG](#)
- [核心治理能力](#)
- [DIG 后台管理](#)

上下文检查与发布

空间治理完成后，将已治理资产及知识组织为 AI 可使用的“上下文”：即回答问题时可引用的资产语义、标准、血缘和审核后文档，而不是底层业务数据的自动交付。这个阶段关注语义和知识是否可信、使用范围是否明确，以及查询智能体能否正确解释资产。

从治理进入上下文

先完成[空间治理与结果核对](#)，再进入工作区“上下文管理”。确认空间内的未审批建议、失败任务和业务争议都有处理结论。查询能力应基于已确认的结果。

组织上下文范围

可用上下文包括：

- 数据资产及其中文名称、业务描述和标准。
- 血缘、上下游依赖及相关影响关系。
- 已整理的指标、报表等资产。
- 审核后的业务文档、数据字典和规范。

先按使用者要回答的问题确定范围，再排除无关或过期内容。发布资产描述、语义或知识能力不等于已经批准对外提供底层业务数据。

检查 Context 质量报告

进入上下文阶段后查看 Context（上下文）质量报告。它按资产数量、语义、标准、血缘和分类分级等维度提示材料是否足以支撑查询，不是模型回答正确率，也不是数据质量规则执行报告。以下指标帮助定位需要返回治理阶段处理的内容。

检查维度	要回答的问题	不足时的处理方向
资产数量	应纳入的对象是否齐全，有无多余对象	调整空间范围
中文语义完整度	用户能否理解表和字段的业务含义	补齐业务元数据并审核
标准覆盖	关键字段是否关联正确标准	检查落标与核标结果
血缘覆盖	能否解释数据来源与流向	核对元数据血缘或 SQLink 解析结果
分类分级	对外使用前是否明确敏感性和等级	完成分类分级及安全复核

本手册不设统一的通过分数。结合报告、实际任务和组织要求判断是否适合发布；统计完整度不能证明每一条定义都正确。

配置并验证查询智能体

查询阶段使用由“业务查询智能体模板”形成的空间实例，与治理阶段智能体职责不同。检查所选模板、模型和查询工具是否适合空间内的上下文。

在发布前选择可核对的样例问题，例如：

- 1. 询问一张已治理表的业务用途，核对中文名称、描述和责任信息。
- 2. 询问一个字段适用的数据标准，核对标准是否实际存在且关联正确。
- 3. 询问一个对象的数据来源，到血缘页面核对路径。
- 4. 询问空间中没有的信息，检查是否明确说明缺少依据。

这些是建议的验收方法。回答中出现看似合理但无出处的定义时，应修正上下文或工具配置后再验证。

选择发布形式

“空间 Agent”供使用者以自然语言询问空间内已授权的资产和知识；“空间 MCP”将相应能力作为工具提供给外部 AI 应用。二者使用同一空间治理成果，但调用方式和访问授权需要分别核对。这里的空间 MCP 与管理员在 DIG 中配置的外部 MCP 服务方向相反。

形式	使用者	能力说明
空间 Agent	人员或集成的 AI 应用	通过自然语言使用空间上下文查询和解释资产
空间 MCP	外部 AI Agent	通过标准化工具使用空间中的资产、语义、血缘及知识能力

在工作区“发布”阶段检查当前可用的发布设置，确认访问对象和范围后再发布。客户端配置使用页面实际提供的接入信息；不要照抄来源截图中的服务地址。

发布后的核对

- 授权使用者能够访问相应能力。
- 返回内容只涉及允许使用的空间上下文。
- 查询结果可追溯到实际资产或已审核文件。
- 未授权对象或缺少依据的问题没有被伪造为确定答案。
- 资产、规则或文件变更后重新检查 Context 质量及查询结果。

常见问题

治理已完成，质量报告仍显示缺口。 核对缺口对象是否属于本次治理范围、建议是否已经审批，以及 DAM 实际结果是否已更新。空间内“执行成功”不等于所有质量维度都完成。

查询智能体答非所问。 检查查询阶段所用模板、选中的上下文和引用文件，确认没有误用治理智能体或其他空间的实例。

外部 Agent 无法使用 MCP。 检查发布状态、访问范围、客户端接入信息和网络可达性。不要把“DIG 调用外部 MCP”的配置与“空间向外发布 MCP”混为一谈。

相关文档

- [创建空间并组织治理](#)
- [智能体模板管理](#)
- [后台管理](#)

数据智能空间

数据智能空间把一个业务目标需要的数据资产、资料和治理能力集中到同一工作区。完成本任务后，你将有一个明确数据范围、专属治理智能体和可追溯治理结果的空间，并可以继续检查上下文质量。

本页的“母本”指创建空间时选用的系统 Agent 或已发布模板，用来生成空间专属智能体实例；“实例”是该空间实际运行的配置副本。母本后续变更不会自动修改已有空间实例。“空间上下文”指本轮允许智能体参考的资产与文档范围，不等于源数据库数据已被复制到空间。

开始前准备

- 明确一个范围有限的治理目标，例如“示例客户表业务描述补齐”。这是示例名称，请替换为自己的任务。
- 确认可查看和治理目标数据源、表或其他资产。
- 管理员已准备可用的系统数据治理 Agent；在部分环境中，该 Agent 由已发布模板实例化。创建向导会显示当前账号可选的母本。
- 已准备适用的业务文档和规范，并明确结果审核人。

空间范围只组织本次任务的上下文，不自动授予源数据访问权限。

第一步 进入空间目录

在 DIG 主导航选择“数据智能空间”。通过“全部”“我的”“共享”切换可见范围，按空间名称搜索，或用“空间排序”调整展示顺序。目录支持网格视图和列表视图。

“我的空间”用于查看自己创建或有管理权限的空间；“共享空间”展示自己可以访问的共享空间。找不到空间时，先检查范围和搜索条件，再确认共享权限。

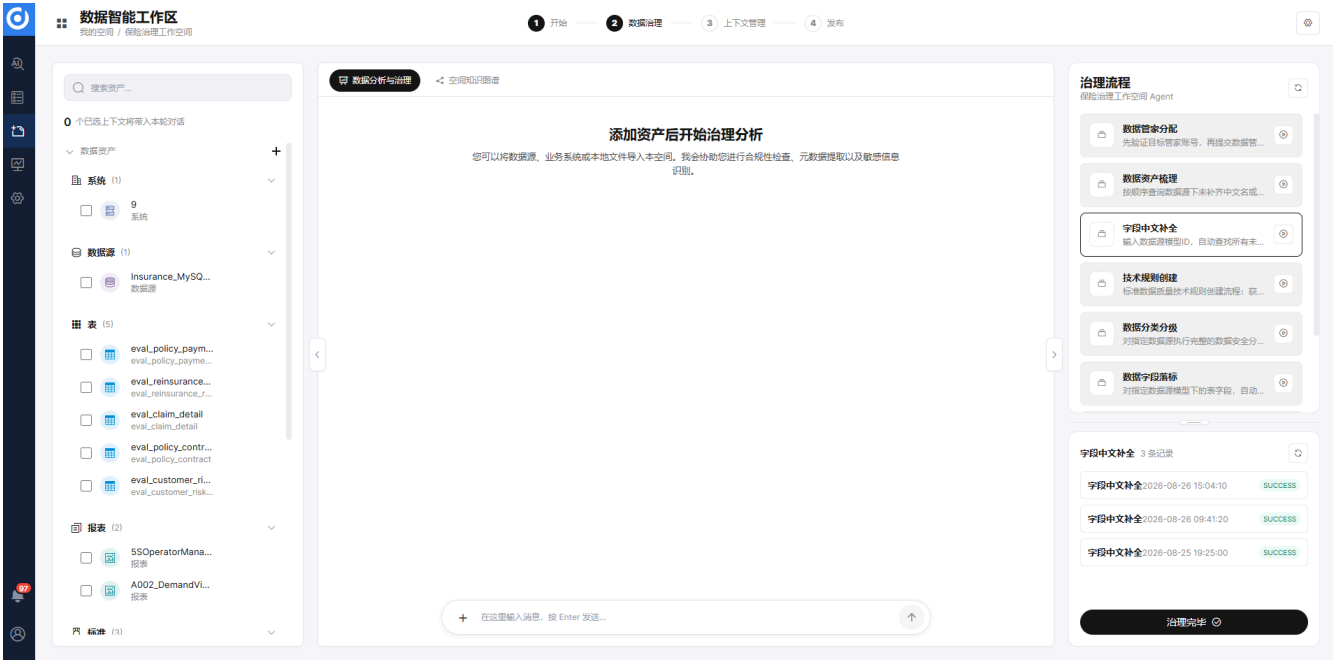
第二步 选择母本并建立空间

1. 单击“创建治理空间”。
2. 在“开始”步骤填写“名称”和“描述”。名称表达业务域和治理目标，描述说明范围与验收要求。
3. 在“选择数据治理Agent”区域选择一个可用的系统 Agent；需要建立母本时，单击“去模板管理创建”。通过展开项检查其职责和能力。
4. 确认选择的 Agent 适合本次任务后，单击“确认并继续”。未完成选择时该按钮不可用。
5. 进入工作区后核对空间名称及当前专属 Agent，再配置待治理对象。

系统根据所选母本复制空间专属智能体。不要因母本已更新就假定现有空间已经使用新的配置。

第三步 添加资产和文档

工作区按“开始 → 数据治理 → 上下文管理 → 发布”显示进度。在“数据治理”阶段，左侧组织资产，中间进行对话或查看空间知识图谱，右侧显示可用治理流程及执行记录。



[查看工作区原图](#)。图中的空间、资产和流程仅为界面示例，操作时应选择实际业务对象。

1. 使用资产区域的添加入口，将需要治理的系统、数据源、表或其他对象加入空间。
2. 用资产搜索缩小范围，检查同名对象的来源。
3. 勾选本轮任务所需的对象。注意已加入空间和已选为本轮对话上下文是两个不同状态。
4. 按需添加业务说明、数据字典和标准规范；确认其适用于当前对象。
5. 在发起任务前检查选中数量和对象清单。

第四步 开展治理

可以直接在对话框中描述任务，也可以选择右侧已经配置好的治理流程。第一次使用建议从一张表或少量字段开始。

对话示例（仅为示例，不会自动执行）：

请检查我选中的示例表，只对缺少中文名称或业务描述的字段提出补齐建议。
参考空间中的业务术语说明，保留已有且准确的人工描述。
请列出对象、原值、建议值和理由，并将需要修改的结果交给人工确认。

执行例程时先阅读输入参数的含义。空间中的流程来自所用模板或实例配置，名称和数量不是固定的。详见[精灵与例程](#)。

第五步 审核并检查落地结果

- 1. 查看执行记录，区分成功、失败和未处理对象。
- 2. 打开[我的审批单](#)，检查前后差异及理由。
- 3. 修改、通过或拒绝建议，并记录必要原因。
- 4. 回到对应 DAM 模块，核对实际属性、规则或目录结果。
- 5. 检查是否仍有待审批、失败和需要补充业务解释的记录。

第六步 转入上下文管理

完成本轮治理后，通过工作区的“治理完毕”进入下一阶段，按照[上下文质量与发布](#)组织可供查询的数据和知识。

治理完毕表示进入下一阶段，不代表系统已代替负责人确认所有治理目标。转入前应核对未完成事项和实际结果。

完成检查

检查项	应看到的结果
空间范围	资产来源正确，选中对象符合本轮任务
空间智能体	使用合适母本的独立实例，依赖能力可用
治理执行	记录可查询，失败和未处理项有原因
审核与落地	建议已处理，DAM 中能核对实际结果
后续使用	可以按目标范围整理上下文，尚未误发布范围外内容

常见问题

没有可选母本。 请管理员检查当前账号可见的系统 Agent；如果组织通过模板管理 Agent，再到“配置管理 → 智能体模板管理”检查模板类型及发布状态。普通智能体和模板是不同对象。

已经加入资产，对话仍未使用它。 检查是否勾选为本轮上下文，以及对象访问权限和本轮提示中的目标范围。

模板改了，空间行为没变化。 这是实例隔离机制。需要调整空间实例或使用适用模板建立新实例，不能依靠重新打开页面更新配置。

看不到共享空间。 检查范围筛选、搜索条件和当前账号是否在共享范围内。

数据智能空间端到端治理

通过 DAM 的 AI 对话可以快速处理一项明确的治理任务；当治理对象较多、需要持续跟踪变化，或需要把规范和治理结果沉淀为可复用上下文时，应进入 DIG 创建数据智能空间。数据智能空间将“发现问题、组织输入、执行治理、检查结果和发布上下文”放在同一个可追溯的工作区中。

本页描述的是 DIG 的完整治理路径，不表示 DAM 内置了一个固定的自动化流程。实际可用的智能体、治理精灵、例程、知识图谱和发布方式由 License、管理员配置及当前用户权限决定。

DAM 对话与 DIG 空间如何选择

任务特征	推荐入口	结果管理方式
单个表、字段或一次性问题	DAM 中的 AI 对话框	生成建议后进入审批，并回到对应 DAM 模块核对
一个业务域包含多类对象和参考文档	DIG 数据智能空间	以空间为边界持续治理，记录资产、文档、执行和验收状态
需要监测元数据变化并重复执行	空间治理例程和调度	变化触发治理任务，结果仍须按配置进入审核与核对
治理结果要供其他 AI 应用查询	空间“上下文管理”与“发布”	先完成质量检查，再发布空间 Agent 或空间 MCP

第一步 进入 DIG 并分析治理现状

1. 直接进入 DIG 平台，或在 DAM 用户菜单选择“切换 DIG”。返回 DAM 时使用 DIG 用户菜单中的“切换 DAM”。
2. 在 DIG 首页通过 AI 对话分析当前数据治理平台的现状，例如元数据覆盖、业务语义完整度、标准关联、血缘和分类分级情况。
3. 明确本轮治理目标、业务范围、验收标准和责任人。不要只输入“治理全部数据”等无法验收的目标。
4. 查询待治理的数据源、表、字段、报表或其他元数据对象，将确认后的对象加入治理清单。

AI 的分析结果是治理范围和优先级建议，不是已经完成的治理结果。加入清单前应核对对象来源、所属系统、Schema 以及当前用户的访问权限。

第二步 创建数据智能空间

1. 在 DIG 的“数据智能空间”中创建空间，使用业务域和治理目标命名，并填写范围、负责人和验收要求。
2. 将治理清单中的数据源、表、字段或其他对象作为空间的治理输入。

- 3. 在空间中补充治理所需的文档，例如治理要求、数据标准、命名规范、业务制度、指标口径和验收说明。
- 4. 进入“数据治理”阶段前，检查资产和文档是否来自正确的系统、版本是否有效、访问范围是否合适。

空间中的对象和文档只是本轮治理的上下文，不会自动复制源数据库数据，也不会替代源系统、DAM 或文档服务器的权限控制。空间的创建与详细资产操作见[数据智能空间](#)。

第三步 使用治理例程执行治理

在空间右侧选择适用的治理例程（治理精灵）并指定本轮治理对象和参考文档。例程由多个治理精灵按顺序组成，可能覆盖元数据补齐、标准匹配、质量规则、安全分类或资产整理等任务。

- **立即执行**：适合首次验证、范围较小或需要人工观察过程的任务。建议先用少量对象试运行。
- **调度执行**：适合按固定周期重复治理的任务。设置频率、对象范围、失败处理和通知责任人后，再启用调度。
- **主动治理**：可监测空间中数据源等对象的元数据变化，在发现变化后发起配置好的治理任务。主动发起不代表自动通过审批或自动发布结果。

执行前检查输入参数、例程版本、治理对象数量和审批责任人；执行后区分成功、失败、跳过和待审核对象。例程编排和运行规则见[精灵与例程](#)及[例程编排与运行](#)。

第四步 在空间中持续了解治理进度

治理过程中可以使用以下能力交叉核对进度，不应只看一个总进度百分比：

能力	用途	核对重点
空间 AI 对话	询问对象状态、未完成项和下一步建议	回答是否引用了当前空间对象和有效文档
治理图谱	查看对象、标准、质量、安全和治理任务之间的关系	关系是否来自已确认的资产和治理结果
资产画像	汇总单个资产的语义、责任、质量和使用信息	画像缺口是否需要返回相应 DAM 模块补齐
业务血缘	了解来源、流向和影响范围	血缘是否已采集、解析且经过业务复核

发现对象缺失、语义不完整或关系不可信时，应暂停后续发布，回到元数据、标准、质量、安全或血缘模块处理，再重新检查空间上下文。

第五步 检查治理结果与积分卡

在空间中查看治理执行记录、待审批事项和治理积分卡，按组织设定的目标评估本轮治理是否达到预期。积分卡用于汇总完成度和缺口，不是对业务数据质量的单一结论。

至少检查：

1. 治理清单中的对象是否全部有处理结论，失败和跳过项是否有原因。
2. 建议是否完成必要的人工审核，并已在 DAM 对应模块中落地。
3. 关键对象的业务语义、标准、血缘、质量和安全信息是否足以支持目标场景。
4. 空间 AI 的抽样问答是否能引用正确对象和文档；对于空间外或缺少依据的问题，是否明确返回无依据。
5. 仍存在缺口时，是否已明确下一轮范围、责任人和验收时间。

只有在治理结果、上下文质量和访问范围均得到确认后，才进入发布阶段。不要把“例程执行成功”或“积分卡达到某个分数”直接等同于业务负责人已经验收。

第六步 发布空间知识库并对外赋能

治理达到预期后，在空间的“上下文管理”中整理已确认的资产语义、标准、血缘和审核后文档，然后进入“发布”：

1. 选择需要提供的上下文范围，排除无关、过期或未审核内容。
2. 验证查询智能体对典型问题的回答、引用依据和越权边界。
3. 将空间知识库发布为可供外部 AI 应用调用的 MCP，或按需要提供空间 Agent。
4. 为发布能力配置访问对象、授权范围和客户端接入信息，并记录发布版本。
5. 当源对象、标准、权限或文档发生变化时，重新检查上下文质量和已发布能力。

空间 MCP 提供的是经治理的资产语义、知识和关系上下文，不等于直接开放底层业务数据。DIG 调用外部 MCP 与空间向外发布 MCP 是两个相反方向的配置，不能混用。详细发布检查见[上下文检查与发布](#)。

完成标准

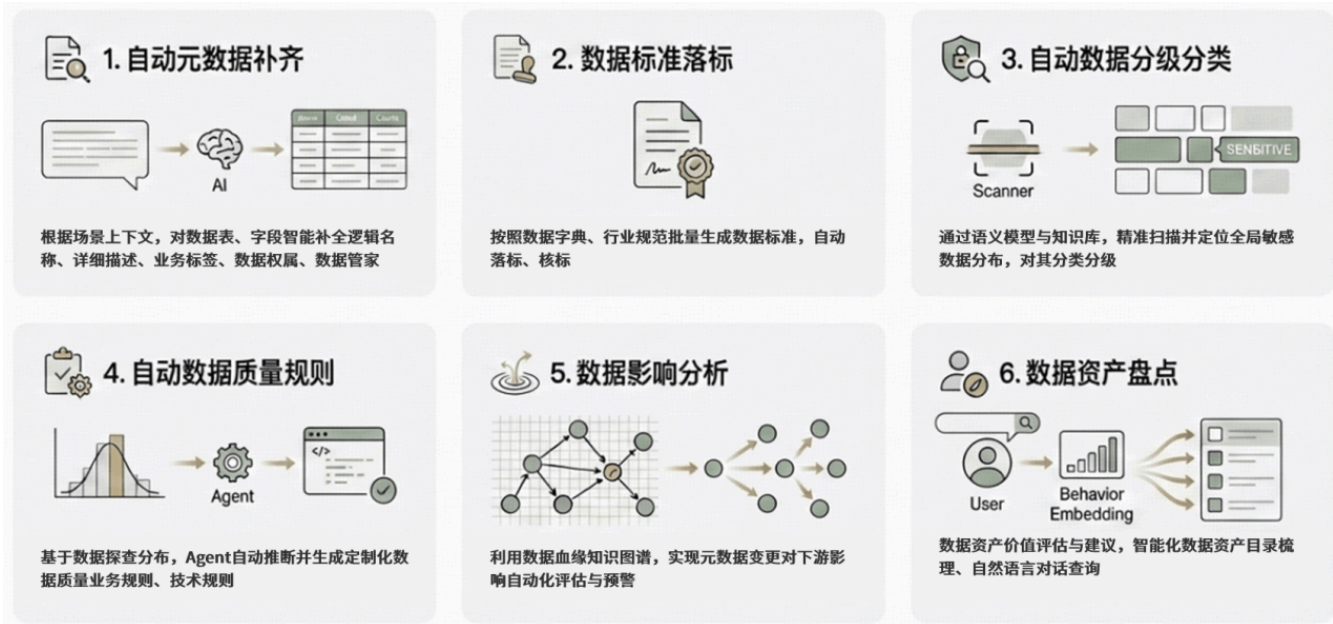
- 治理对象来源和范围清楚，空间内资产与文档可追溯。
- 例程执行、调度或变化触发记录完整，失败和未处理项有结论。
- 关键治理结果已审核，并能在 DAM 对应模块中核对。
- 治理图谱、资产画像、业务血缘和积分卡反映的是已确认的结果。
- 发布的空间 Agent 或 MCP 仅包含经过检查、授权范围内的上下文。
- 后续变更有重新治理、重新检查和重新发布的责任人及计划。

相关文档

- [数据治理智能体概述](#)
- [数据治理智能体快速开始](#)
- [数据智能空间](#)
- [核心治理能力](#)
- [上下文检查与发布](#)
- [人工审批与协作](#)

核心治理能力

DIG 通过会话理解目标，调用已配置的 DAM 能力形成建议，再交由人员审核。实际可用能力取决于 License、智能体、模型、Skill、MCP、内部服务和当前用户权限。



元数据补齐

功能说明

为表或字段生成中文名、业务描述等候选内容，适合处理已完成采集但业务属性不完整的元数据。

输入准备

- 目标数据源、表或字段范围。
- 所属业务域和对象用途。
- 企业术语、语言和命名规则。
- 已确认的相似对象或参考资料。

操作与审核

1. 选择元数据补齐智能体和目标对象。
2. 说明需要补齐的属性及命名限制。
3. 生成后检查未处理对象和异常。
4. 在审批单比较原值和建议值，修改后通过或拒绝。

审核时确认说明不是物理名称的机械改写，同类对象没有被错误套用相同描述。通过后在元数据模块检查属性是否进入后续流程。

数据标准生成

功能说明

根据业务域、字段语义和企业规范生成候选数据标准。候选标准不等于已发布标准。

输入准备

- 数据域和适用范围。
- 标准类型、命名与编码规则。
- 业务定义、数据类型、长度和值域要求。
- 现有标准目录和去重范围。

操作与审核

1. 选择标准生成能力并限定对象范围。
2. 引用当前有效的标准制度或模板。
3. 生成候选标准并检查重复项。
4. 审核定义、技术规格和适用范围。
5. 通过后按数据标准模块的发布流程处理。

重点检查标准定义是否可执行、是否与已有标准重复，以及类型、长度和值域能否用于实际字段。

质量规则生成

功能说明

根据数据结构和业务要求生成候选业务规则与技术规则，用于辅助建立质量检查。

输入准备

- 目标表、字段和数据结构。
- 业务校验要求与质量维度。
- 值域、阈值、空值和唯一性等约束。
- 规则执行范围和责任人。

操作与审核

生成后检查业务规则与技术规则是否正确关联，表达式能否在目标数据源执行，阈值是否有业务依据。审批通过后到数据质量模块确认规则配置、任务和执行状态，不把自然语言建议当作已运行规则。

分类分级

功能说明

依据企业分类目录、分级规则和数据用途，为表或字段提出分类与级别建议。

输入准备

- 当前有效的分类目录和分级体系。
- 数据对象、业务用途和使用场景。
- 适用的法规、制度和例外规则。

操作与审核

1. 选择数据范围和分类分级能力。
2. 指定使用的分类目录与分级体系。
3. 生成建议并优先查看敏感或高等级对象。
4. 由数据安全责任人核对漏判、误判和级别依据。
5. 审批后在数据安全模块验证结果。

落标与核标

功能说明

落标用于把元数据字段与适用的数据标准建立候选匹配；核标用于检查已有匹配是否仍然合理。

输入准备

- 已发布且当前适用的数据标准。
- 字段中文名、英文名、描述和技术属性。
- 匹配范围和需排除的对象。

操作与审核

选择对象后发起落标或核标，检查候选标准、匹配理由和置信信息。重点复核低置信建议、技术类型不兼容、已废弃标准以及缺少业务语义的字段。通过后在数据标准或元数据相关页面检查实际匹配状态。

数据资产盘点

功能说明

辅助识别和整理候选资产，为后续编目、责任确认和发布提供输入。

输入准备

- 盘点系统、业务域和对象范围。
- 企业的资产定义与目录分类。
- 已知负责人、业务用途和价值信息。

操作与审核

1. 选择盘点范围和资产视角。
2. 提供资产口径与目录规则。
3. 查看候选资产及缺失信息。
4. 由业务和资产责任人确认归属、名称、价值与开放范围。
5. 审批后进入数据资产目录的正式管理流程。

DIG 不替代资产责任认定，也不自动决定资产发布范围。

主动治理

“主动治理”指后台常驻任务在发现元数据变化后按配置发起治理，而不是等待用户在对话框提出每项请求。它以持续任务发现问题并产生待审批事项；“主动”不表示建议可以跳过人工审核自动发布。



由系统管理员启用 Nacos 中的常驻主动治理任务开关。任务在后台监听元数据变更，按业务元数据补齐、落标、分类分级、资产梳理的顺序串行治理，并产生审批单。启用前核对数据源、智能体配置和审批责任；具体开关由实际部署配置提供，不在会话中猜测参数名称。

运行后检查元数据变更与生成任务是否对应，再检查建议和审批结果。若建议量异常增加，先检查来源及配置变化，避免直接批量通过。

主动治理的完整周期是发现问题、生成建议、人工审批、目标模块验证和规则优化，不能跳过人工确认。

血缘辅助

功能说明

血缘辅助可用于 SQL 解析失败分析、算子业务解释和影响分析总结。它使用可用的 SQL、血缘和元数据上下文帮助理解问题。

操作与审核

在 SQLink 血缘空间，将鼠标移动到失败或部分成功 SQL 文件的状态栏，在失败对话框选择“智能生成预处理”激活 AI 对话。发送请求后检查生成并加入任务的预处理脚本，比较原文和处理后内容，再重新解析。生成脚本不代表解析或链路已经正确。

解释算子时，在算子窗口单击魔法棒激活 AI 对话。询问影响范围时提供明确的目标对象和变更要求，再对照 SQLink 实际节点、关系及计算代码核对。自然语言总结不能替代血缘事实。

通用完成检查

- 输入范围与实际处理对象一致。
- 引用规范是当前有效且适用于该业务域的资料。
- 未处理项、失败项和低置信建议均有结论。
- 审批人具备对应领域知识和数据权限。
- 审批后的结果已在目标 DAM 模块中验证。
- 会话、审批意见和目标结果能够相互追溯。

异常处理

现象	处理建议
建议与规范明显不符	检查引用文件、提示要求和智能体配置，拒绝错误建议
处理范围过大或超时	缩小对象范围，用样本验证后分批执行
大量对象未处理	检查对象权限、元数据完整性和工具调用错误
同类错误反复出现	汇总审批反馈，由管理员优化提示、Skill 或服务配置

相关文档

- 开始使用 DIG
- 人工审批与协作
- DIG 后台管理
- SQLink 数据血缘

初始化数据治理智能体

本页供管理员准备模型、DAM 连接参数、用户身份、智能体及模板，使用户能够从 DAM 发起治理对话并创建数据智能空间。日常使用者如果已有可用智能体，可以直接进入[快速开始](#)。

配置顺序

顺序	工作	完成后检查
1	配置大模型并设置默认模型	连接测试成功，测试请求能返回结果
2	设置全局 baseUrl	智能体能访问正确的 DAM 环境
3	配置用户访问身份	调用使用当前用户获授权的身份
4	导入治理和资产查询智能体	列表可见，模型和工具配置正确
5	准备常用提示词	用户能够按任务选择并替换示例范围
6	发布两类智能体模板	空间创建及后续查询阶段有可选模板

配置模型

- 从模型服务负责人取得通信协议、Base URL、模型名称及认证信息。
- 进入“配置管理 → 大模型配置”。
- 添加模型，填写服务提供方给出的参数。
- 测试连接并配置默认模型。
- 用少量非敏感的任务输入验证响应内容，再用于治理。

“提供商”用于选择通信协议，不能只凭模型品牌推断。API 密钥只在指定认证字段填写，不放入普通提示词或截图。模型发现、LLM/Embedding 参数和连接测试要求见[模型服务配置](#)。

设置 DAM 根地址

进入“配置管理 → 参数配置”的全局参数，配置 baseUrl，其值为智能体可访问的 DAM 根地址。

text

参数名称：baseUrl
示例值：https://dam.example.com

该地址仅为示例，应替换为管理员确认的实际环境地址。不要将 DIG 页面地址、完整业务页面路由或另一个测试环境地址误填为 DAM 根地址。

配置用户身份

来源操作流程为：在 DAM“个人工作台 → Token管理”取得有效用户 Token，再到 DIG“配置管理 → 参数配置”的个人参数区域配置相应认证信息。Token 应属于执行任务的用户，不应共用他人的管理员身份。

用户自定义智能体使用官方 Skill 时，还需核对 Skill 提示词所要求的会话身份引用。来源要求使用系统参数 `${session.token}`。这是运行时身份引用，不是应填入手册示例的真实令牌。

静态个人认证参数与运行时会话参数用途不同。若身份无效，检查 Token 是否仍有效、用户权限是否足够以及相应参数是否被当前智能体使用，不要把真实 Token 贴入对话中排查。

导入智能体

1. 进入“配置管理 → 智能体”。
2. 选择“导入智能体”，使用实施人员交付的治理智能体或资产查询智能体包。
3. 修改为能说明职责的名称。
4. 检查系统提示词、模型、MCP、Skill 和依赖工具。
5. 按需设置默认智能体。嵌入式对话使用此默认配置。
6. 新建测试会话验证对象查询和建议生成，再开放给用户。

导入包内的地址或路径可能来自其他环境，导入完成后必须核对。不要仅以导入成功判断所有能力可用。

准备提示词与模板

管理员可导入中文补全、分类分级、标准创建、系统落标、规则创建、资产梳理等常用提示词。用户从“我的提示词”引用后，应替换对象范围和业务约束，避免原样提交演示场景。

最后按[创建和发布智能体模板](#)分别准备数据治理智能体模板与业务查询智能体模板。普通智能体可用不等于模板已经发布。

初始化验收

- DAM 用户能够打开 AI 对话，且选择或默认使用预期智能体。
- 智能体可查询当前用户有权访问的测试对象。
- 一项小范围治理建议可进入人工审核，并能在 DAM 核对结果。
- 空间创建页可以选择已发布的治理模板。

- 查询阶段具备合适的业务查询模板。
- 当前用户的身份、文件与实例配置没有误用其他用户或环境的资源。

排查顺序

无法运行时依次检查 License 与功能权限、模型连接、baseUrl、用户身份、当前智能体、工具和 Skill 依赖。模型连接成功只证明模型服务可用，不能证明 DAM 身份和治理工具也已配置成功。

模型服务

模型配置是可供智能体复用的共享资源。管理员先配置服务和连接，再由智能体选择所需模型；模型能返回响应与治理任务能正确调用 DAM 是不同的验收步骤。

本页的 **LLM**（Large Language Model，大语言模型）用于理解和生成文本；**Text Embedding**（文本向量化模型）把文本转换为数值向量，供语义检索等环节使用，不负责直接生成对话答案。“最大 Token 数”约束模型处理或输出的文本单元数量，不等同于中文字数；“向量维度”是向量中数值的个数，必须与服务实际返回一致。

使用前准备

从模型服务负责人取得通信协议、服务基础 URL、服务端模型标识及所需认证信息。确认 DIG 服务能够访问该地址，并明确使用对话生成模型还是向量模型。不要把网页聊天地址当作模型 API 基础 URL。

新建模型配置

1. 进入 DIG“配置管理 → 大模型配置”，单击“添加模型”。
2. 填写“配置名称”，选择“模型类型”和“提供商”。提供商表示通信协议，不仅是模型品牌。
3. 填写“基础 URL”，按服务要求填写 API Key。
4. 页面会尝试发现模型名称；也可单击“发现模型”。从返回列表选择目标模型，或在发现失败时手动填写准确的服务端模型名。
5. 根据模型类型填写专用参数，按需选择“设为系统默认模型”。
6. 单击“测试连接”，确认通过后再“保存”。当前页面明确要求先通过连接测试才能保存。
7. 返回列表核对配置名称、提供商和模型标识，再在所需智能体中选择并验证。

不需要保存时使用“取消”或“关闭”。仅发现到模型名称，不等于完成连接测试，也不表示该模型适合治理任务。

大模型参数建议

DIG 的治理效果高度依赖底层大语言模型（LLM）的配置。以下是面向数据治理场景的通用建议，适用于大多数生产环境。实际取值仍需遵守模型服务的上下文窗口、输出长度和参数范围限制。

参数名称	推荐值	说明
模型名称	DeepSeek-V4-Pro、Kimi K2.6、GLM-5.1、Qwen3.6	优先选择支持长上下文（≥128K）和中文优化的模型
Temperature	0.1 ~ 0.3	治理任务需要稳定、可复现的输出，避免过高温度带来随机性
Top P	0.9 ~ 1.0	保持适度的词汇多样性，避免过度截断
Max Tokens	4096 ~ 8192	保证长提示词和输出内容不被截断，尤其适用于批量资产治理
Frequency Penalty	0.0 ~ 0.2	减少重复生成相同内容，建议设置较低值
Presence Penalty	0.0 ~ 0.2	鼓励引入新主题，建议设置较低值
Stop Sequences	无需配置	除非需要强制结束输出，一般不设置
System Prompt（系统提示词）	见系统提示词示例	用于固化角色身份和输出格式约束

硬件与部署建议

本地部署模型时，可按下表作为起始配置，再根据模型规模、并发量和上下文长度进行压测：

资源项	建议配置
GPU	至少 1 × A100（40 GB）或 2 × 4090（24 GB）
内存	≥ 32 GB
存储	≥ 200 GB SSD，用于模型缓存与日志
网络	低延迟访问大模型、DAM 数据库和元数据服务

模型选择对照

以下模型是按治理任务整理的示例，具体可用性、版本和服务能力以实际提供商为准：

使用场景	推荐模型	原因
元数据补齐、标准生成	Qwen 3.7、DeepSeek V4、Kimi 2.5、GLM 5.1	中文语义理解较强，输出稳定
血缘解析、代码解读	Claude 3.5 Sonnet	代码理解能力较强，适合 SQL 和 ETL 解释
分类分级、敏感数据识别	文心一言 4.0	内置安全与合规语义能力
低成本或测试环境	GPT-3.5-Turbo、通义千问-Turbo	成本可控，适合非核心任务

以上是通用建议。上线前应根据治理任务类型、数据量、响应速度和服务成本进行调优，并通过已获准的小范围任务验证结果。

两类模型的区别

模型类型	表单中的专用设置	配置重点
LLM 模型	温度、最大 Token 数	根据模型服务约束和任务要求设置，不把页面初始值当作统一推荐值
Text Embedding 模型	向量维度	必须与模型实际返回的向量长度一致；不能用生成模型的 Token 上限代替

切换模型类型后，核对表单中变化的参数。已有资源依赖某个向量模型时，调整模型或向量维度前先检查相应依赖和重建要求，不把它当作仅修改显示名称。

字段说明

字段	含义与核对方法
配置名称	供管理员和智能体配置者识别，建议体现用途和服务来源
模型类型	选择 LLM 或 Text Embedding，决定专用参数
提供商	选择与模型服务匹配的通信协议
基础 URL	服务实际 API 根地址；核对路径和网络可达性
API Key	页面标为可选，但模型服务要求认证时仍需填写有效凭据
发现的模型名称	服务发现返回的候选项，应与本次目标一致
手动填写模型名	发现不可用时填写服务端可识别的标识，不使用随意命名的显示名称
默认模型	设为系统默认模型；与“智能体”页面的默认智能体是不同配置
温度	LLM 的采样参数，按任务和服务支持范围设置
最大 Token 数	LLM 配置中的长度参数，需遵守所选服务的限制
向量维度	Embedding 返回向量的长度，必须与实际服务一致

凭据只填写在相应认证字段，不写入系统提示词、普通参数说明、截图或反馈记录。

编辑、复制与删除

模型列表提供“编辑”“复制”“删除”。编辑前核对配置名称和被使用的范围；修改地址、模型名或认证后重新测试连接。复制后应使用能区分用途的名称，并核对复制来的服务参数，不把来源环境直接用于另一环境。

删除前确认没有智能体或其他资源仍需要此模型。共享配置的变更可能影响多个使用方，应先在已获准的小范围任务验证，再扩大使用。

验证是否可用于治理

1. 在[智能体管理](#)中核对所选模型。
2. 新建测试会话，以一个已知、获准的对象提出范围明确的查询或建议任务。
3. 检查模型响应、工具调用和错误信息，而不只检查文本是否流畅。
4. 涉及治理建议时，按[人工审批](#)核对建议，并返回 DAM 检查实际结果。
5. 如果连接测试通过但工具调用失败，继续检查 DAM 根地址、用户身份和工具依赖，参见[初始化](#)。

常见问题

现象	排查顺序
发现模型为空或失败	基础 URL 与网络 → 通信协议 → 服务是否提供模型发现 → 手动模型标识是否正确
测试连接认证失败	API Key 是否需要、是否有效、是否获准访问目标模型
无法保存	先查看连接测试及表单校验提示，不能跳过测试前置条件
向量调用结果不匹配	核对实际向量长度与配置维度，检查所选模型类型
测试成功但会话仍用另一模型	检查当前智能体和会话实际配置，不混淆默认模型与默认智能体
文本响应正常但治理无结果	检查工具服务、baseUrl、身份参数及人工审批状态

例程编排与运行

例程把多个精灵组合为可复用的治理流程，负责节点顺序、输入输出映射、失败策略和运行记录。例程不改变精灵本身的职责；同一个精灵可以被多个例程复用。

规划例程

先画出业务任务的输入、处理步骤和验收结果，再在页面中创建节点。每个节点只选择一个精灵，并写清本节点完成的动作。独立的只读检查可以并行；存在数据依赖或写入依赖时使用串行连接。

规划项	说明
入口参数	例程调用者必须提供的对象、空间或筛选条件
节点	对一个精灵的一次调用
参数映射	入口参数或上游输出如何传给下游节点
依赖	节点执行前必须完成的节点
失败策略	当前节点失败后继续执行或终止例程
结果	供调用方查看或供后续节点使用的结构化输出

创建和编排

1. 进入“配置管理 → 治理精灵 → 例程”，创建例程并填写稳定编码、名称和描述。
2. 定义入口参数，说明每个参数的类型、必填性和业务范围。
3. 添加精灵节点，为节点填写可识别的步骤名称。
4. 选择精灵，核对该精灵的输入参数和权限依赖。
5. 将入口参数或上游输出映射到节点输入；逐项检查名称、类型和空值处理。
6. 按业务依赖连接节点。只有互不依赖的节点才安排并行。
7. 配置失败策略。关键写入或审批前置检查通常应终止，非关键统计节点才考虑继续。
8. 保存后运行测试，检查完整路径、分支和异常路径。

连接执行箭头不代表参数已经映射。每个节点都要单独检查输入来源，尤其是数组、对象和上游空结果。

测试与发布

至少使用正常输入、空结果、缺失必填项、工具不可用和部分节点失败五组样例。测试时同时检查节点顺序、参数内容和业务结果。对会修改元数据、标准、质量、安全或资产的精灵，发布前应设置人工确认或审批边界。

发布后不要直接修改正在使用的例程定义。若环境支持版本或复制，应先复制为新配置，完成回归后再切换调用方。例程模板、空间实例和调度配置分别维护，发布模板不会自动覆盖已经创建的空间实例。

调度和运行记录

例程可由空间、智能体调用或按部署提供的调度入口运行。调度频率、启停状态和首次运行时间应在实际环境中单独确认。执行历史中应检查：

- 例程输入和最终状态。
- 每个节点的开始结束时间、输入输出和工具调用。
- 失败节点及异常消息。
- 继续策略是否导致后续节点使用了不完整结果。
- 写入型节点是否产生了预期的待审批记录或治理变更。

节点诊断

现象	可能原因	处理建议
例程未启动	调度未启用、入口参数为空或实例未发布	先查实例、发布状态和入口参数
某节点跳过	上游失败且策略为终止，或条件未满足	查看上游节点状态和分支条件
节点反复失败	工具服务、权限或输入结构错误	单独运行该精灵并比对输入 Schema
节点成功但结果为空	对象范围无匹配，或上游输出字段映射错误	查看节点实际输入和查询范围
下游结果不完整	并行节点尚未汇总，或继续策略忽略失败	增加汇总节点并显式处理失败结果

与其他 DIG 对象的关系

智能体负责理解目标并选择能力；精灵执行原子任务；例程固化顺序和映射；数据智能空间承载业务范围、文档和治理阶段；智能体模板保存可复用配置。它们的名称和权限并不互相替代。

相关文档

- [精灵设计与发布](#)
- [精灵与例程总览](#)
- [创建和发布智能体模板](#)
- [在空间中组织治理](#)

精灵设计与发布

精灵是数据治理智能体中可复用的原子能力。它应当只承担一个边界清楚的任务，例如查询对象、补充描述、检查标准关联或生成待审核建议。需要多个步骤、条件和结果传递时，应使用[例程](#)编排精灵。

设计前准备

开始前明确以下内容：

项目	需要明确的内容
任务边界	精灵完成什么，不处理什么
输入	对象标识、空间、数据范围和必填参数
输出	文本、结构化结果、建议或待审批变更
工具	DAM 内部服务、MCP、命令或 Skill
权限	查询权限、写入权限和审批要求
失败处理	参数缺失、工具不可用或结果为空时的返回方式

不要把“治理整个系统”作为一个精灵的职责。过大的职责会导致参数、权限和结果难以验收。

创建精灵

进入“配置管理 → 治理精灵”，选择目标智能体后创建精灵。根据页面实际字段填写编码、名称、描述和提示词。编码应长期稳定，名称用于列表展示，描述应说明适用对象和结果。

输入参数

为每个参数定义名称、类型、是否必填、默认值和业务含义。提示词中的变量必须与参数名称一致；对象 ID、名称和展示文本不要混作同一参数。对数组或对象参数，明确每个成员的结构和允许为空的条件。

提示词与边界

提示词至少写清：

- 任务目标和处理范围。
- 参数如何解释，以及没有参数时怎样返回。
- 应调用的工具和调用顺序。

- 4. 输出字段、格式和证据要求。
- 5. 发现冲突、权限不足或无法确认时如何报告。

提示词不能替代工具权限，也不能把模型的推断写成已完成的 DAM 操作。

工具绑定

精灵可以按部署配置使用 DAM 工具、MCP、内部服务、命令或 Skill。只绑定完成任务所需的工具，并逐项检查服务地址、连接模式、请求头、超时和参数 JSON。工具测试通过只表示连接可用，还需要用真实对象验证返回内容。

测试与验收

使用受控样本至少测试四类输入：正常对象、缺失必填参数、空结果和工具失败。检查输入是否被正确映射、工具是否调用了预期对象、输出字段是否稳定，以及是否产生了不应有的写入。涉及标准、质量、安全或资产变更时，默认先输出建议并交由人工审批。

保存、启用和发布

保存前复核编码、输入 Schema、工具和提示词的对应关系。启用状态控制精灵是否可调用；“作为工具暴露”会影响其他智能体或例程是否能够发现它。发布前记录当前配置、测试样例和已知限制，避免直接覆盖正在使用的配置。

不同环境可能提供版本、复制、导入 ZIP 或从 Skill 扫描生成等入口。导入或自动生成后仍须人工检查内容、依赖和权限，不能以生成成功作为验收结论。

常见问题

现象	排查顺序
精灵列表为空	确认已选择正确的智能体，并检查当前账号的配置权限
参数未替换	对照输入参数名称、提示词变量和例程映射
工具连接失败	检查地址、连接模式、请求头、超时和服务端日志
返回内容不稳定	收紧输出 Schema，减少无关工具，并增加边界条件
任务显示成功但对象未改变	核对精灵是否只有查询权限，以及结果是否需要人工审批

相关文档

- [例程编排与运行](#)
- [精灵与例程总览](#)
- [后台管理](#)

精灵与例程

治理精灵（Governance Sprite）完成一个边界明确的原子任务，例如查询元数据或获取标准。例程（Routine）将多个精灵按确定的业务逻辑组合成可复用流程。精灵本身并不等同于周期运行的主动治理任务。

阅读配置时还需区分：**输入参数 Schema** 是精灵输入的名称、类型和约束说明，不是数据库 Schema；**参数映射**是把例程入口或上一步输出填给后续精灵的输入；**工具**才是实际读取或修改外部对象的执行接口。仅有提示词或执行箭头，不代表参数和工具已经可用。

进入管理页

进入“配置管理 → 治理精灵”，先选择“当前智能体”。页面包含“精灵”“例程”“执行历史”三个分区。没有选择智能体时，页面会提示选择要配置的智能体。

资源属于当前智能体，查不到已有精灵或例程时应先核对选择，不要立即重新创建同名对象。

设计一个精灵

需要逐项配置输入 Schema、工具和发布边界时，参阅[精灵设计与发布](#)。

先写清任务边界，再配置页面。一个精灵需要有明确输入、执行工具和可供下游使用的输出。

配置	用途	检查重点
编码、名称、描述	稳定标识并说明任务	名称不能掩盖多个不同职责
模板提示词	说明目标、边界、输出及异常处理	引用参数与输入 Schema 一致
输入参数 Schema	定义参数名称、类型及说明	必填项、默认值和对象范围有明确含义
当前模型	执行必要的理解或转换	与任务所需能力相匹配
MCP、内部服务或 Command Line	分别通过协议工具、DAM 内部接口或命令行提供执行能力	只绑定该任务必需的能力，并核对权限与运行环境
启用、作为工具暴露	控制精灵是否可用及调用方式	发布前核对调用范围

编辑精灵

编码

find_all_objects

名称

查询数据源下所有没有补齐中文名的对象

描述

这个用来查询一个数据源下所有没有中文名或者描述的元数据列表

模板提示词

你应该使用以下命令来获取所有没有中文名的对象列表
java -jar \${workspace.dir}/tools/datablau-metadata-cli.jar findObjectsWithoutLogicalName \
--baseUrl \${custom.baseUrl} \
--token <token> \
--modelId {{modelId}}\
--category table view \

输入参数 Schema (JSON)

定义这个 Sprite 需要哪些输入参数。模板里可以直接使用类似 `{{name}}` 的占位符。

modelId

数据源的ID

添加参数

当前模型

Select

MCP 绑定

☐ sqlink-mcp

内部服务绑定

☐ user_get_details

[查看精灵编辑原图](#)。图中的命令和资源仅为界面示例；实际执行应使用已配置并验证的工具。

创建与测试精灵

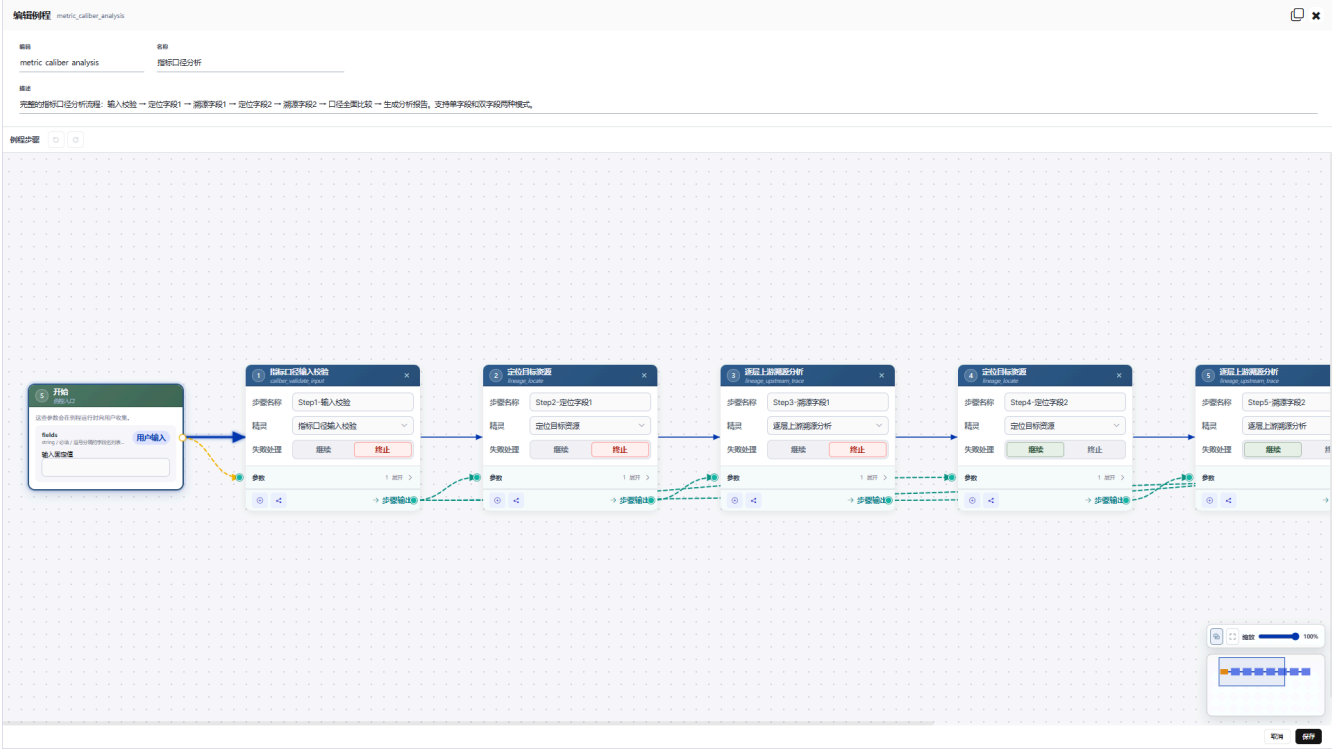
1. 在“精灵”分区创建精灵，填写编码、名称和描述。
2. 编写模板提示词，明确只完成哪一件事，以及不能处理时怎样报告。
3. 配置输入参数。提示词中类似 `{{name}}` 的占位符必须与实际参数名一致。
4. 选择模型并绑定工具。
5. 配置启用状态和是否作为工具暴露。
6. 使用受控样本检查输入、输出和工具结果，再保存可用配置。

精灵也可以通过 AI 从已有 Skill、治理对话或过程提炼。生成后仍需检查职责、参数和工具依赖，不能把生成成功作为可运行证明。

设计例程

需要配置入口参数、节点映射、失败策略和执行诊断时，参阅[例程编排与运行](#)。

例程负责流程，精灵负责节点能力。先确定输入和期望输出，再安排步骤。例如，只读的“对象检查”流程可以先定位元数据，再分别检查描述和标准关联，最后汇总缺口。这是设计示例，不表示环境中已内置该例程。



[查看例程画布原图](#)。图中指标口径分析仅展示画布操作，节点名称取决于实际配置。

编排步骤

1. 在“例程”分区创建例程，填写编码、名称、描述和入口参数。
2. 添加精灵节点，为每个节点填写清楚的步骤名称。
3. 选择该节点执行的精灵。
4. 将入口参数或上游输出映射到节点输入。
5. 按业务依赖连接步骤。后一步需要前一步输出时使用串行；彼此独立的下游任务才适合并行。
6. 为各节点配置失败处理：“继续”或“终止”。关键写入步骤通常应终止，避免在错误输入上继续执行。
7. 使用画布的参数关系显示、缩放、撤销和重做检查流程。
8. 测试完整路径，保存后按环境提供的发布流程开放调用。

注意区分执行顺序和参数传递：连接了执行箭头并不自动证明所有必需参数都完成映射。检查每一个下游输入都有正确来源。

调度与模板关系

例程调度属于具体智能体实例。创建模板时复制精灵和例程配置，但不复制调度。空间实例需要周期执行时，在实例中单独配置，并核对首次实际触发记录。

查看执行历史

切换到“执行历史”，找到目标精灵或例程记录。例程应继续下钻到节点，检查输入、输出、状态、工具调用结果和失败原因。

现象	优先核对
列表为空	当前智能体是否正确，是否执行过任务
节点缺少参数	入口参数、占位符名称和上游输出映射
工具调用失败	模型、MCP、内部服务或命令执行环境的可用性
有些节点未执行	上游失败策略是否为终止，是否存在依赖
流程成功但业务结果不对	对象范围、节点输出语义与 DAM 实际记录

验收建议

分别测试正常输入、缺失必填参数、服务不可用及部分节点失败。对会修改 DAM 数据的节点保留人工确认，并在实际模块核对结果。执行日志中的成功只说明该次调用完成，业务验收仍应检查是否修改了正确对象和属性。

相关文档

- 后台管理
- 创建和发布智能体模板
- 在空间中使用治理流程