

AI DC白皮书 2026



商标声明

HUAWEI, HUAWEI, 是华为技术有限公司商标或者注册商标，在本手册中以及本手册描述的产品中，出现的其它商标，产品名称，服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺，华为不对您在本文档基础上做出的任何行为承担责任。华为可能不经通知修改上述信息，恕不另行通知。

版权所有© 华为技术有限公司 2026。保留一切权利。

非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播。

一份给CIO规划建设智算数据中心的参考

中国建设银行、华为技术有限公司

联合发布单位



杨超斌

—— 华为公司常务董事，ICT BG CEO

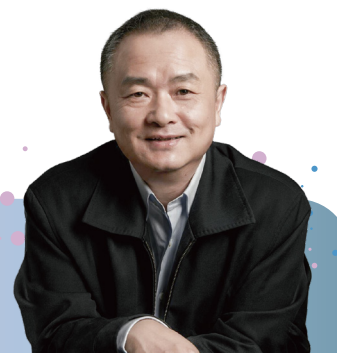
过去两年，全球日均Token消耗量增长近300倍，超过3000万个AI Agent已深入制造、金融、能源等行业协同工作。AI正从技术探索走向规模化生产，而承载这一切的基础设施——AI DC，正在经历一场根本性的重构。传统数据中心的设计逻辑已无法适应Agentic时代的需求。从供电架构到散热方案，从算力基础设施架构到关键产品形态，从建设模式到运维运营，AI DC的每一个环节都在被重新定义。这不仅是技术的升级，更是业务逻辑的重塑。本白皮书凝聚了华为在AI算力基础设施领域的深度实践与系统思考，从架构规划到工程落地，从技术选型到持续运营，为企业构建Agentic时代的AI算力底座提供了参考指引。行业智能化正加速前行，希望这份白皮书能为全球AI DC的创新发展贡献一份力量。



雷鸣

——中国建设银行副行长

当前，人工智能正加速重构产业发展格局，AI DC智算基础设施作为数字经济时代的核心算力底座，是赋能实体经济智能化升级的关键支撑。作为国有大型商业银行，建设银行深入践行“人工智能+”行动，坚持算力布局适度超前，建成“四地五中心”高可用智算集群，以坚实算力底座驱动全业务链条数智化转型，对算力基建的战略价值的认知不断深化。本白皮书既剖析技术底层逻辑，又聚焦产业落地实践，系统阐释了人工智能与AI DC协同发展的路径与方向，兼具前瞻性与指导性，值得业界同仁研读参考。期待与各方携手共筑智能算力生态，以算力筑基赋能新质生产力，助力数字经济高质量发展。



梅宏

—— 中国科学院院士，北京大学教授，中国计算机学会前理事长

以互联网、云计算、大数据和人工智能为代表的新一代信息技术正以前所未有的深度与广度重塑人类社会的生产生活方式，成为新一轮科技革命和产业变革的核心驱动力，数字化转型已成为不可逆的时代大势。近年来大模型技术的突破性进展以及AI Agent技术的兴起，标志着人工智能正在开启具备自主规划与任务执行能力的Agentic AI新阶段，作为人类生产生活的辅助工具将呈现能力的大幅跃升。而这一切技术演进的底层支撑，离不开算力基础设施的系统性升级。AI DC作为面向AI负载重构的新一代数据中心，是支撑大模型迭代与AI Agent规模化应用的“算力”工厂。这部白皮书，系统阐述了AI DC的内涵边界、技术架构、建设路径与发展趋势，具有实践性和前瞻性，为产学研用各界提供了有益的参考。



李鹏

—— 华为公司董事、ICT销售与服务总裁、中国地区部总裁

近年来，华为携手金融、制造、电力等行业客户，围绕数智化转型联合创新，从机房物理设施、算力基础设施、到智能运维运营的全链条都在打破传统经验的边界，AI从辅助工具演变为核心生产力，AI DC也迎来了从理念探索到系统化落地的全面跃迁。在大量实践中我们深刻感受到，AI DC已不再是传统数据中心的技术升级选择，而是驱动企业数智化转型的战略底座。这是产业演进的大趋势，也是先行者的重大机遇。本白皮书凝聚了华为与行业客户在实践中积累的经验与思考，希望能为更多企业建好、用好AI DC提供一份兼具前瞻与切实的参考。我们期待以此为契机，与产业协同聚力，共同打造绿色集约、高效、开放的AI基础设施，加速智算基础设施高质量发展，共赢Agentic时代！



马海旭

—— 华为公司副总裁、ICT 产品组合管理与解决方案部总裁

Agentic时代的到来，正在深刻改变AI基础设施的底层逻辑。超节点成为训推算力集群建设常态，层次化KV Cache成为提升Token效率的关键手段，通智融合、数智融合成为支撑万级Agent、EB级多模数据的核心；与此同时，传统的数据中心运维运营模式正在失效，这意味着AI DC的规划与建设迈入全新阶段。这本白皮书最早于2024年发布第一版，凝聚了华为在AI DC领域的初步实践与思考。过去两年，随着Agentic AI在各行业的加速落地，我们参与到大量的客户建设实践中，积累了丰富的经验，并对AI DC的未来发展有了更深刻的认识。因此，我们在第一版基础上进行了全面刷新，白皮书详细阐述了Agentic时代下AI DC的趋势判断、创新范式、规划与建设、运营与运维等，希望为全球AI DC规划与建设提供价值参考，为全球智算基础设施的高质量发展贡献力量。



王磊

—— 中国太平洋保险集团CIO

大模型与Agent正全面深入智能服务、风险决策等核心业务，智能应用的规模爆发，让算力成为企业智能升级的核心制约，AI DC也由此跃升为支撑业务创新的战略生产系统。当下模型技术快速迭代、应用场景持续更新，对AI数据中心的动态适配与演进能力提出更高标准。企业智能化建设，基础设施落地只是基础，能否紧跟模型迭代节奏，让算力持续高效赋能业务、落地真实价值，才是规模化智能转型的核心关键。本白皮书立足资源投入到业务产出的全链路视角，系统拆解AI DC的建设逻辑与运营范式，为企业精准评估智算投资、搭建适配智能时代的算力底座、驱动业务长效增长，提供了极具落地性的专业参考。



魏凯

——中国信息通信研究院人工智能所所长，工业和信息化部人工智能标准化技术委员会（MIIT/TC1）秘书长

当前，人工智能技术加速演进，大模型与Agent应用不断深化，面向AI原生负载的AI DC正成为算力基础设施升级的主要方向。本白皮书立足产业实践，系统梳理了AI DC的技术体系与建设路径，围绕AI Facility、AI Infra、AI Agent等核心要素明确了关键技术要求，并对智能体时代的算力需求特征、Token服务能力评估等前沿方向进行了深入探讨。白皮书兼具体系性与实操性，对凝聚行业共识、推动产业发展一定能够起到重要的引领作用。



刘康

—— 华为公司ICT Marketing与解决方案销售总裁

从超大规模模型训练到生产级实时推理，Token产出效率正成为衡量智算基建价值的核心标尺。AI DC绝非传统IDC的算力堆砌式扩容，而是涉及算力调度、存算网联动、供电散热的系统工程，直接决定芯片算力向业务价值的转化效率，是大模型和Agent规模化落地的核心底座。这本白皮书系统梳理了AI DC的技术演进逻辑与可落地的架构方案，汇聚金融、医疗、大型智算中心等多个行业兼具前瞻性与实操性的标杆实践。希望这些沉淀能为不同规模、不同阶段的企业提供有益借鉴，也期待与产业同仁在实践中持续探索、共同完善。

目录 CONTENTS

01

AI DC创新与发展



1.1 AI DC发展的五大趋势	09
Agent成为AI DC负载的最大变量	09
模型向通用智能加速演进	10
推理场景Scaling Laws涌现	10
超节点时代已到来	10
能源供给成为AI DC战略约束	10
1.2 Agentic时代AI DC新范式	11
传统规划方法面临失效	11
以"3T+3P"为核心的AI DC新范式	12

02

AI DC规划与建设



2.1 Agent-Centric应用与生态	15
围绕“AKDM”参考框架进行规划	15
沿着四个阶段推进企业Agent落地	20
Agent驱动AI Infra边界重构	21
2.2 Token-Centric AI Infra	22
从Cloud Infra到AI Infra的核心变化	22
Token生产效率四维评估要素	23
Token生成效率的关键约束与核心技术	25
Token-Centric AI Infra目标参考架构	30
四大能力圈重塑Token-Centric AI Infra	32
企业AI Infra规划建设重点方向	49
2.3 Watt-Centric AI Facility	51
AI Facility的系统性挑战	51
AI Facility规划建设建议	53
AI Facility新建与存量场景落地	56

03

AI DC运营、运维与安全



3.1 AI DC智能生产运营	59
从算力资源运营到AI生产运营	59
AI生产运营五大核心能力	62
案例实践：银行AI DC价值运营升级	64
AI生产运营演进路线	66
3.2 AI DC自治运维保障	67
从设备运维到智能生产运维保障	67
Agentic自治运维六大核心能力	68
Agentic自治运维参考架构	72
案例实践：Agentic运维智能定界与快速恢复	74
Agentic自治运维演进路径	75
3.3 AI DC安全防线构筑	76
AI DC“内忧外患”安全困境	76
AI DC安全防护核心措施	77
以AI防AI的安全参考架构	81

04

AI DC成功实践



4.1 华为云芜湖3D数据中心创新实践	85
4.2 中国建设银行AI数据中心建设与运营转型实践	87
4.3 复旦大学附属中山医院AI DC医疗行业实践	91

01

第一章

AI DC创新与发展



“

当人工智能成为数字经济的核心生产力，数据中心正经历一场深刻而决定性的跃升。它已超越承载算力与数据的传统定位，成为智能时代的战略生产资料。旧范式无法解释新负载，范式转换的大幕由此拉开。

人类历史上，每一次基础设施层的跃迁都重塑了文明的底层逻辑。蒸汽机重构了“动力”的生产范式，让人类摆脱体力极限；电力重构了“能源”的供给体系，点亮工业与千家万户；互联网重构了“信息”的流转逻辑，打破知识与时空的藩篱。

今天，正在发生的第四次跃迁将重构“智能”的存在形态。从大规模预训练模型的能力涌现，到分布式推理的规模化部署；从被动响应的信息工具，

到能够感知、规划和执行任务的自主Agent。智能正以前所未有的速度和密度涌入每一个企业、每一台终端。

数据中心的内涵正在被深刻改写：从承载计算、存储和网络资源的基础设施，演进为持续生产智能能力的新型基础设施。这不仅是一场IT架构的技术重塑，更是一场定义未来数十年生产力范式的系统性革命。

1.1 AI DC发展的五大趋势

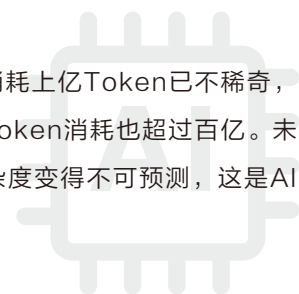
Agent成为AI DC负载的最大变量

Agent让AI从“认知智能”向“行动智能”演进，成为能自主规划、工具调用和闭环执行的“行动者”。这使得AI从辅助型的“对话框”变成了能独立承担业务流程的“数字员工”，重构企业传统应用。

2024年初至2026年，中国市场日均Token调用量从1000亿增长到140万亿，其背后是Agent带来的Token需求指数级增长。一个复杂Agent任务通常需要多轮推理和工具调用，会触发数十甚至数百次LLM调用，上下文窗口长度走向百万Token级别。

与此同时，每百万Token的推理成本从5元降到0.5元。推理成本快速下降，进一步引爆了Agent和Token需求。这符合经济学中的Jevons悖论循环：AI效率提升不会降低算力需求，而会创造更大的AI算力需求。

今天，AI开发者每天消耗上亿Token已不稀奇，金融头部企业每天的Token消耗也超过百亿。未来Agent的数量和复杂度变得不可预测，这是AI DC负载的最大变量。



模型向通用智能加速演进

大模型迈向通用智能（AGI）的发展路径，呈现以下趋势：

超大规模参数模型，突破能力上限。模型从“快思考”走向“慢思考”，在编程、数学推理、科学研究等领域，逐步达到甚至超过人类专家水平。

中小规模参数模型，提升智能效率，降低推理成本。模型重点瞄准单位Token、单位算力下产生更高水平的智能，包括模型架构优化、小型化模型、

MoE和算法创新等技术推动智能成本持续下降。

模型从静态训练走向持续学习和自我优化，结合数据、反馈和环境变化不断提升能力。比如，OpenAI的GPT-5.6系列模型中，轻量版Luna模型的后训练已经可以由旗舰版Sol模型自主完成。

模型能力的演进，对AI DC提出更高要求，既需要支撑超大算力负载，也需兼顾训推混合场景下资源的灵活调度。

推理场景Scaling Laws涌现

传统Scaling Laws描述的是训练阶段：模型参数量、训练数据量、训练算力增加时，性能按幂律可预测提升。如今这一逻辑正在向推理阶段延伸，推理效果不再仅由模型大小决定，推理时投入的计算量正成为新的关键变量。

通过增加推理计算量获得接近扩展参数数量的收益，并借助更长思考链、更复杂搜索与更强自我验证机制提升推理能力。对AI DC的直接影响是：单请求算力消耗和推理时延同步攀升。

超节点时代到来

当单颗芯片的性能逼近物理极限，就必须用系统化思维重构算力调优的全链条。华为发布的韬（ τ ）定律就是一个典型代表，通过器件-电路-芯片-系统四层协同，实现系统级突破。

基于系统化工程创新，通过总线互联计算、网络、存储等基础设施，并进而通过池化提升整体性能，

已成为行业共识的技术路径，华为昇腾超节点和业界主流超节点均遵循这一路线。

数据中心层面，也在不断涌现出系统化工程的新技术方案，除了超节点，还包括PD分离（Prefill-Decode分离）、多级KV Cache等创新技术方案，正在改变AI DC的设计范式。

能源供给成为AI DC战略约束

算力的功率密度不断攀高。单机柜功率已从数十kW迈入百kW级，中长期将超过300kW。传统风冷极限约20kW/柜，已无力承载AI高密算力，液冷从可选项变为必选项。

超大型数据中心，也从MW级迈向GW级，GW级AI DC的用电量堪比一座百万人口城市，能源供给正在从成本问题升级为战略约束。

这五个趋势判断指向同一个方向：数据中心正站在一个范式转换的临界点。

1.2 Agentic时代AI DC新范式

Token正在成为衡量算力的基础单位。数据中心不再只是存放服务器的机房。它正在从"资源供给系统"变成“算力生产系统”，衡量标准从"拥有多少XPU“变成了"能产出多少Token”。

传统规划方法面临失效

业务规划失效，负载容量难以预测

Agentic AI时代，传统软件应用和工具从前台退到幕后，变成AI智能体调用的底层基础设施。一个新Agent或一个新模型可能在3个月内从蛰伏起步变成全网爆火，带动Token需求暴涨百倍。

依赖历史业务发展的线性思维来推演业务未来规划已经失效，未来3-5年的业务增长和业务负载也难以预测。

数据中心第一次无法"预测未来要多大”。以Google为例，2022年Google AI Capex约为310亿美元，到2026年这一数字预计接近1,900亿美元，四年增长超过5倍。

架构范式失效，分层优化的时代结束

传统数据中心的架构设计建立在"技术是慢速变化的，系统是稳定的"这一假设之上。在这个前提下，云资源层、计算/存储/网络层、Facility层的分层优化显得顺理成章。

AI时代的技术迭代节奏打破了这一前提，模型迭代从年度变成季度甚至月度，芯片微架构的迭代周期从24个月缩短到12-18个月。传统分层解耦架构不

企业CIO们面临一个巨大的挑战：沿用过去的方法论来规划建设AI DC能否应对AI的这些变化。

再成立，AI业务负载对计算、存储、网络的需求同时爆发、相互耦合，需要考虑系统级的协同优化设计，“稳定系统”正在走向“持续变化系统”。

物理设施层面，单机柜功率从5-8kW跃升至40-120kW，风冷极限被击穿，液冷成为必选项，楼板承重、层高、电力引入都需要重新设计；更关键的是时间窗口错位，企业获得NPU后希望3-6个月投产，但传统数据中心建设周期长达12-24个月，机房准备节奏系统性滞后于IT设备迭代节奏。

运维保障失效，AI突破原有运维运营边界

传统数据中心运营以设备为中心，关注服务器可用率、网络连通性、机房温湿度，核心目标是保障资源不中断。

AI时代，数据中心运维对象发生根本变化：Agent业务链路长、跨域调用多，从模型推理到工具执行再到数据访问，任一环节异常都会导致业务降级，传统以设备为中心的监控体系无法应对。

同时，数据中心还要考虑构建企业Token运营能力以支撑业务部门激增的AI需求。

AI也给数据中心的安全带来了极大的冲击。数据中心内部的Agent自主规划执行带来越权和数据泄露

以"3T+3P"为核心的AI DC新范式

AI算力本身已经成为生产要素，数据中心的定位也在发生变化：从成本中心到价值中心。其价值不再体现为“拥有多少资源”，而是体现为“能持续生成多少价值”。行业公开数据显示，2025—2026年中国头部科技企业 AI 相关资本开支（Capex）同比普遍增长50%以上；其中字节跳动2026年AI 基础设施领域投入规模已上调至2000亿元以上。

同时头部企业的AI基础设施团队正从"运维成本中心"转向"AI产能运营部门"。"机房有多少台服务器"不再

风险。数据中心外部黑客驱动基于AI大模型的自动化攻击也让传统防御体系面临代差劣势。

是主要矛盾。业务部门关注的问题是："每天能够产出多少有效Token？"

AI DC的规划设计需要一套全新的系统性思维，我们称之为以“3T”和“3P”为核心的参考框架：

"3T"参考框架

T1: AgenT（应用驱动）→ T2: Token（算力运营）→ T3: WatT（物理支撑）

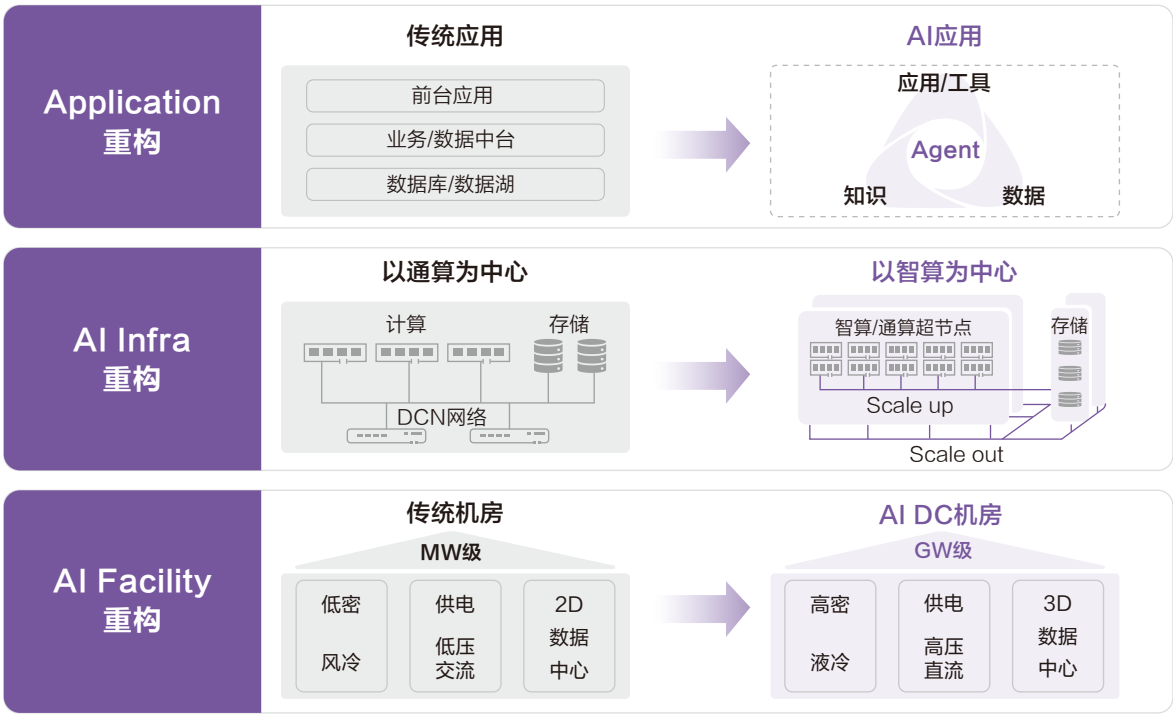


图1-1 "3T"参考框架

三者构成一个完整的价值链条：Agent驱动Token消耗，Token消耗决定算力需求，算力需求决定瓦特消耗。规划设计需要在每个环节上做出取舍和平衡。缺少了任何一个"T"的考量，AI DC的规划都是不完整的。

"3P"参考框架

P1: Production（智能生产运营）→ P2: Provisioning（自治运维保障）→ P3: Protection（安全防线构筑）

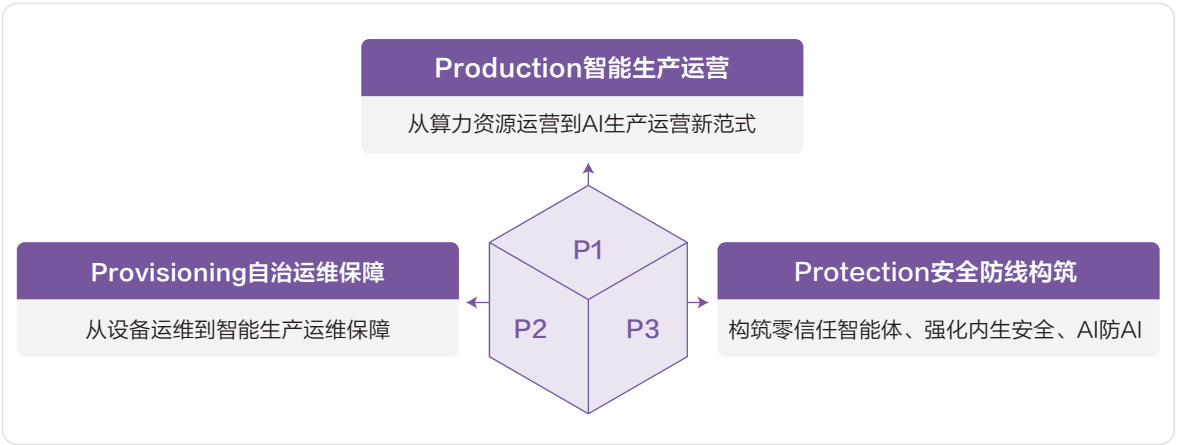


图1-2 "3P"参考框架

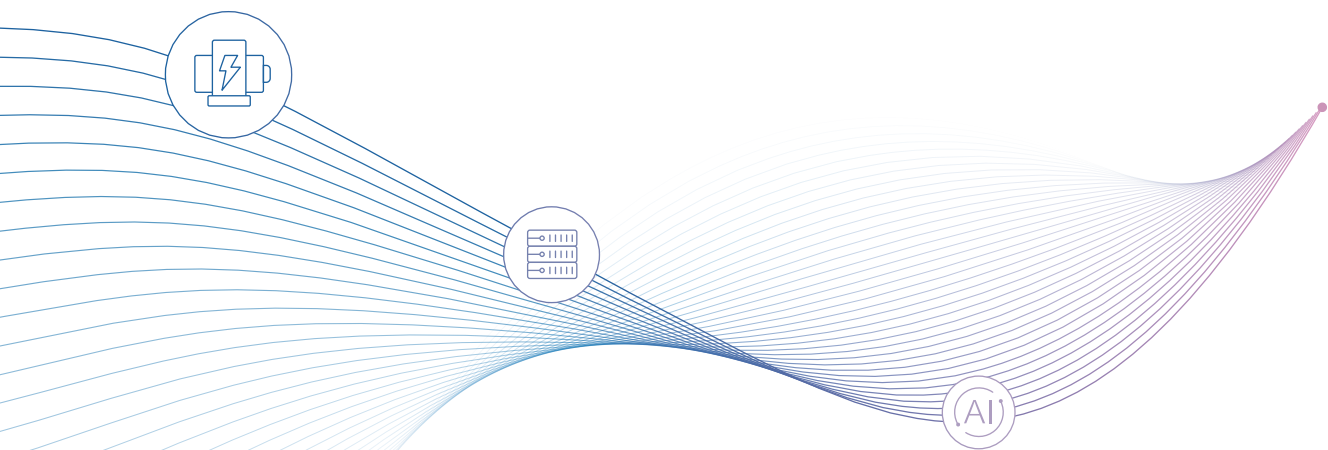
生产运营以Token为计量单位驱动智能价值创造，运维保障以自治化手段保障系统连续可靠，安全控制以零信任和AI防AI守住业务安全底线。三者相互

支撑、协同联动，共同保障AI DC从算力资源到智能价值的稳定转化。

02

第二章

AI DC规划与建设



“

每一次产业革命，都以基础设施的重建为先导。当智能需求的迭代速度超越建设周期，数据中心的规划逻辑与工程标准必须整体重写。新范式不止于架构图上的设计，更要落成可建设、可交付的工程体系。

2.1 Agent-Centric应用与生态

进入Agentic AI时代，企业AI应用正从单次模型调用走向长周期、复杂任务的完整交付，实现从“Token”到“任务”的本质跃迁。这要求企业建

设以Agent为中心的应用与生态，推动 AI真正融入核心生产场景。

围绕“AKDM”参考框架进行规划

Agent 进入企业核心生产流程，单靠模型能力远远不够，它需要知识来理解业务边界，需要数据来支撑精准执行，需要模型来驱动推理决策。围绕“AKDM”框架建设企业AI应用与生态，是AI规模化落地的关键：

Knowledge: 提供企业认知，将业务规则、流程经验和本体沉淀为可复用资产

Data: 提供可信事实，让每一步执行基于准确、实时、可追溯的数据

Agent: 承担执行中枢，把组织的意图转化为任务和行动

Model: 提供推理引擎，支撑理解、生成、判断和规划

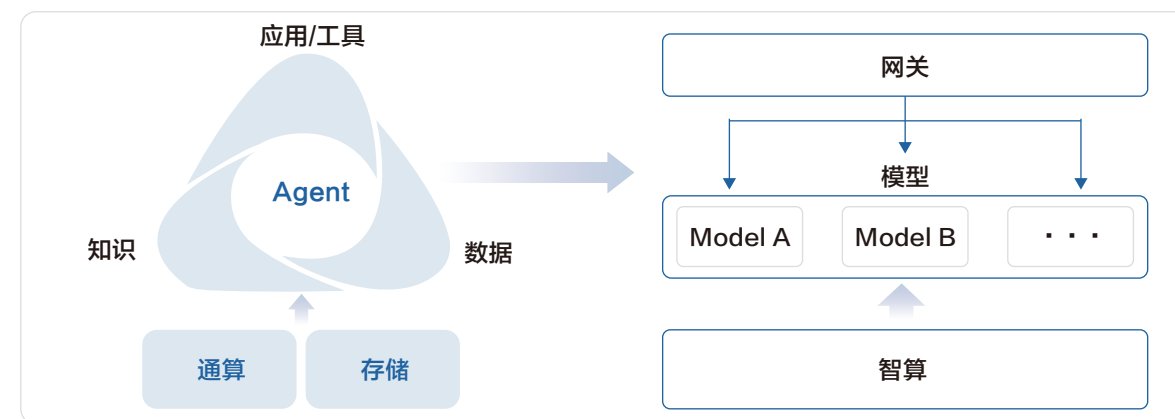


图2-1 围绕“AKDM”参考框架进行规划

Agent：建设多Agent协同的生产级平台

Agent正在成为企业新的执行中枢和业务入口。生产级多Agent系统的核心，不在于Agent数量的扩张，而在于建立清晰的任务分工、协作协议与循环优化机制。

典型多Agent系统通过设置Lead Agent作为任务调度中枢，负责任务拆解、优先级管理、上下文分发与结果汇总；多个Sub-agent承担专业任务，如架构设计、代码开发、质量评估等。各 Sub-agent 在限定职责、权限与工具边界内运行，避免权限过宽和上下文过载。企业需要明确协作契约：谁拆解

任务，谁拥有执行权限，谁校验结果，谁对最终产出负责。

为提升长时复杂任务的成功率，多Agent系统还需引入三重循环机制，形成Harness自进化闭环：Lead Agent优化任务组织，Sub-agent优化专业执行，Agent平台优化运行环境与协作机制。只有具备从任务到平台的持续学习能力，企业才能减少对人工逐步调度的依赖，让复杂任务在更长周期、更大规模和更高不确定性下稳定运行。

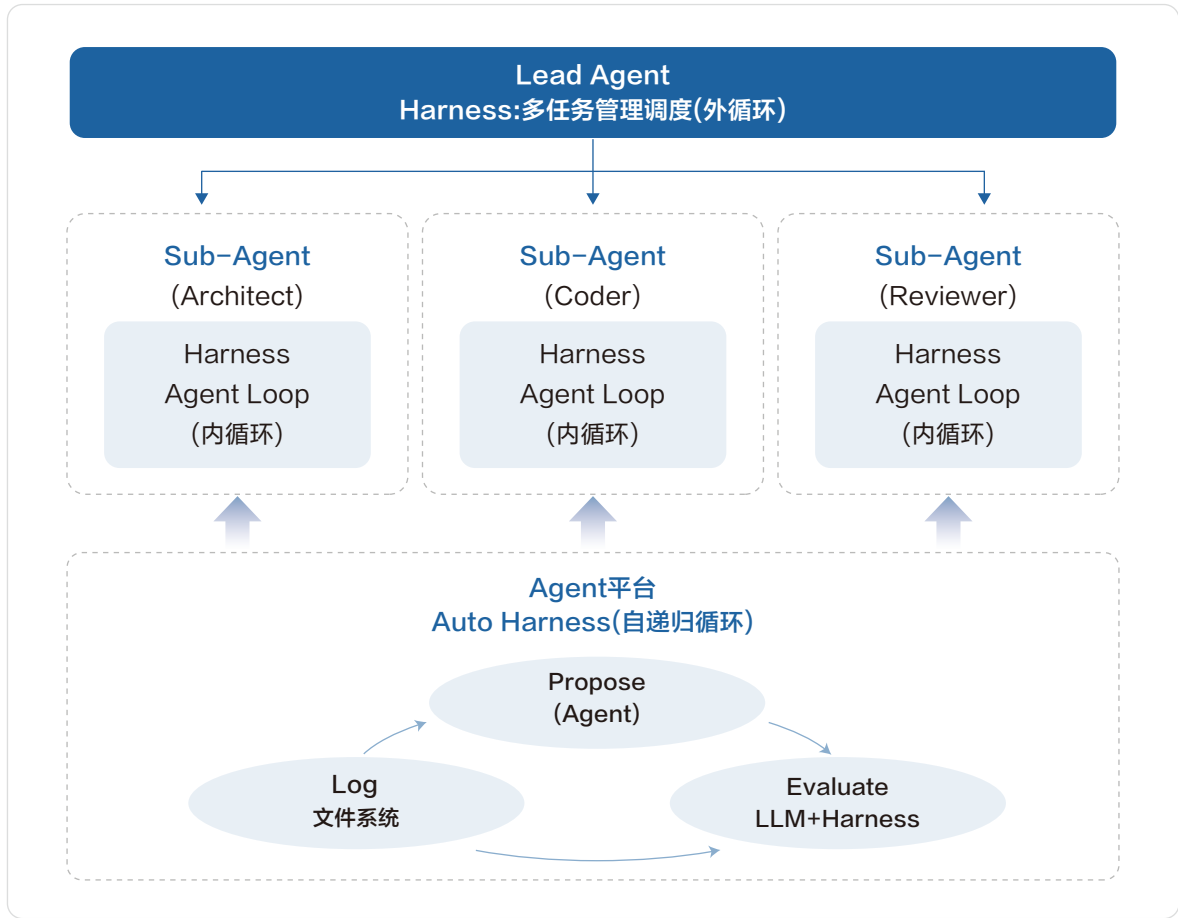


图2-2 Multi-Agent Harness循环机制

多 Agent 的生产级运行，需要三层架构的Agent平台支撑，每一层解决不同的问题：

第一层Agent Framework，承担任务智能编排的职责。涵盖上下文工程、分层记忆、多Agent 协同、自评估与自演进、工具编排、任务规划、算力亲和和调度等核心能力。

第二层Agent Distributed Runtime，为Agent提供分布式、大规模、可靠运行能力。涵盖分布式状态管理、任务队列、Checkpoint、跨 Agent

通信、资源调度、算力亲和调度等。Runtime的核心价值，是保障执行过程在故障、并发、租户隔离和资源波动下依然可靠运行。

第三层Agent System Service，为Agent提供安全可信的系统服务。涵盖系统沙箱、CLI-native（Command-Line Interface-native）原生执行、安全隔离、文件与进程访问控制、代码执行环境、工具调用边界等。其核心作用，是让 Agent在调用系统能力时不越界。

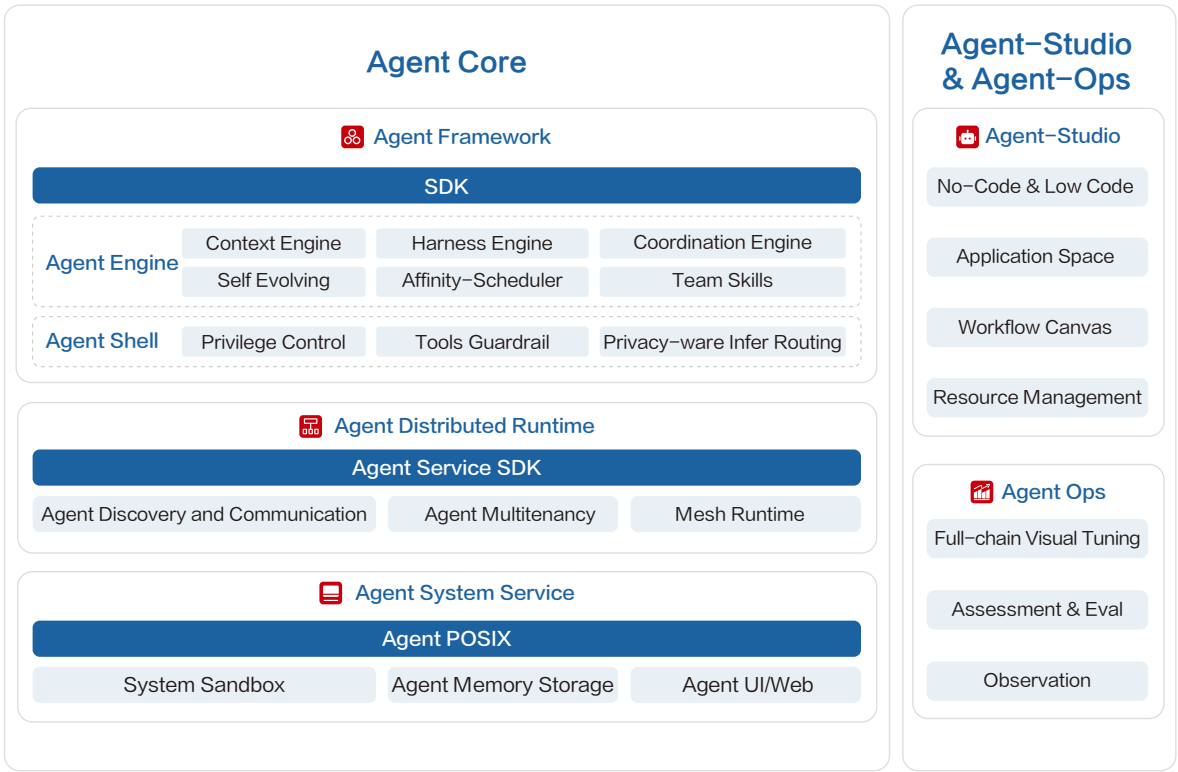


图2-3 Agent平台参考架构

Knowledge：让Agent遵循企业逻辑规划执行任务

企业知识（Knowledge）是企业共享、长期积累并经过治理的认知资产，涵盖制度文档、业务规范、行业本体、知识图谱、流程经验与可执行业务规则等，让Agent真正理解本行业、本组织和本流程。

企业知识的建设面临一个根本性矛盾：知识分散在文档、流程、系统和人脑中，而Agent需要的是结构化、可推理的认知资产。解决这一矛盾，需要构建知识湖（Knowledge Lake）——在统一的数据底座之上，通过语义化加工将企业隐性经验转化为Agent可消费的结构化知识资产。知识湖的建设遵循“采集—抽取—建模—服务”的递进路径。

采集层对接企业多源知识载体，包括制度文档、操作手册、FAQ、历史工单等非结构化数据，以及业务系统中的结构化规则。

抽取层利用大模型从非结构化文档中自动提取实体、关系与业务规则，经过人工审核校验后形成高质量的“事实—事理”三元组。

建模层以本体（Ontology）为语义骨架，定义企业核心概念体系与约束规则。没有本体，知识图谱就是一盘散沙：“供应商”和“供货商”会被当作不同概念，“张三”和“Zhang San”会被作为两个实体导入。本体将RDF、OWL等标准定义的概念和关系嵌入Agent感知、推理、决策的全生命周期，从根本上解决“数据是什么意思”的问题。

企业本体资产的构建、运营与治理，可依托Agent平台实现，由本体建模Agent、业务专家、应用验证Agent三类角色协同推动本体模型从设计到应用的高质量落地。

本体建模Agent：将领域知识转化为符合语义规范的本体模型，提供自动化建模与一致性校验能力；



业务专家：从业务语义与领域规则角度参与建模，审阅并优化本体模型的概念定义与关系语义，确保准确反映真实业务逻辑；



应用验证Agent：面向具体场景进行语义推理验证与应用测试，评估本体模型在智能应用中的可用性与有效性。



三类角色通过平台协同机制，形成知识建模、业务校验与应用验证的闭环，持续提升本体资产质量。

服务层通过语义映射、规则引擎和标准API，向Agent提供查询、校验与推理服务，使Agent能够沿着“实体—关系—约束”的路径形成可解释的判断。

Data：为Agent构建可溯源、可校验的事实数据

Data是Agent理解环境、判断状态和执行任务的事实基础。Agentic时代下，数据湖、数据仓库、BI、主数据和数据治理平台仍会继续存在，数据建设的主要变化是从“人消费数据”转向“模型消费数据”，这一转变也重构了企业数据底座的设计逻辑。

企业数据底座需要从以结构化数据为主的数据湖仓，演进为面向AI的多模态数据湖（Multimodal Data Lake）。结构化数据提供精确事实，如订单金额、库存数量、客户等级；非结构化文档提供业务语境，如合同条款、尽调报告、合规文件；图像、语音、视频与日志提供现场过程与行为证据；Agent Trace与用户反馈则提供持续优化所需的运行数据。多模态数据湖的核心，是实现不同形态数据的统一治理与统一授权，为知识与Agent提供

稳定、可信的数据供给。

Data与Knowledge在统一的数据底座上形成协同。Data是多模态数据湖中的原始事实，Knowledge是构建于其上的语义层——从同一份数据中，通过本体建模和知识抽取提炼出实体、关系和规则。数据湖提供“有什么数据”，知识湖提供“数据是什么意思”。Agent在推理时，通过数据资产目录发现“可以消费什么数据集”，通过知识目录理解“这些数据对应什么业务含义”，通过元数据目录验证“数据在哪里、是否可信”，这三个目录共同影响Agent推理精准度。

因此，企业数据建设应遵循“数据入湖—语义标注—知识构建—Agent消费”的递进路径。

Model：面向任务提供灵活组合的模型服务

Agent时代，企业AI模型建设的重点正从“选择一个最强模型”转向“运营一组适配不同任务的模型服务”。通用模型、领域模型、小模型、多模态模型与推理模型各有适配场景，企业通过模型组合在能力、成本、时延与安全之间取得平衡。实现这一转变，需要两个关键工程组件：模型网关与观测体系。

模型网关：模型网关是Agent访问模型服务的统一入口。所有Agent对模型的调用，都应通过模型网关进入模型池，避免各业务系统直接绑定单一模型API。

模型网关选型应重点关注四类能力：**统一接入**，支持私有化开源模型与公有云模型的统一纳管；**精细计量**，支持按Agent、任务、部门、模型与租户进行Token计量与成本归集；**策略路由**，按

任务复杂度、时延、成本、安全等级与模型可用性动态选择模型；**高可用保障**，具备限流、熔断、重试、Fallback、灰度发布与快速回滚能力。

观测体系：是模型服务工程化的关键，包括模型级观测与Agent请求级观测两个维度。

- 模型级观测：聚焦模型服务的效能、成本与可用性，核心采集调用量、Token吞吐、响应延迟、错误率、单Token成本及租户用量等关键指标，覆盖限流、降级等异常事件统计。

- Agent请求级观测：面向任务全链路可观测，记录链路标识、模型与工具调用路径、Token消耗、任务状态及业务结果，覆盖人工接管等异常场景。

这样才能回答三个关键问题：一次任务为什么成功或失败，成本主要花在哪个环节，是否需要优化模型路由、上下文组织或工具调用策略。

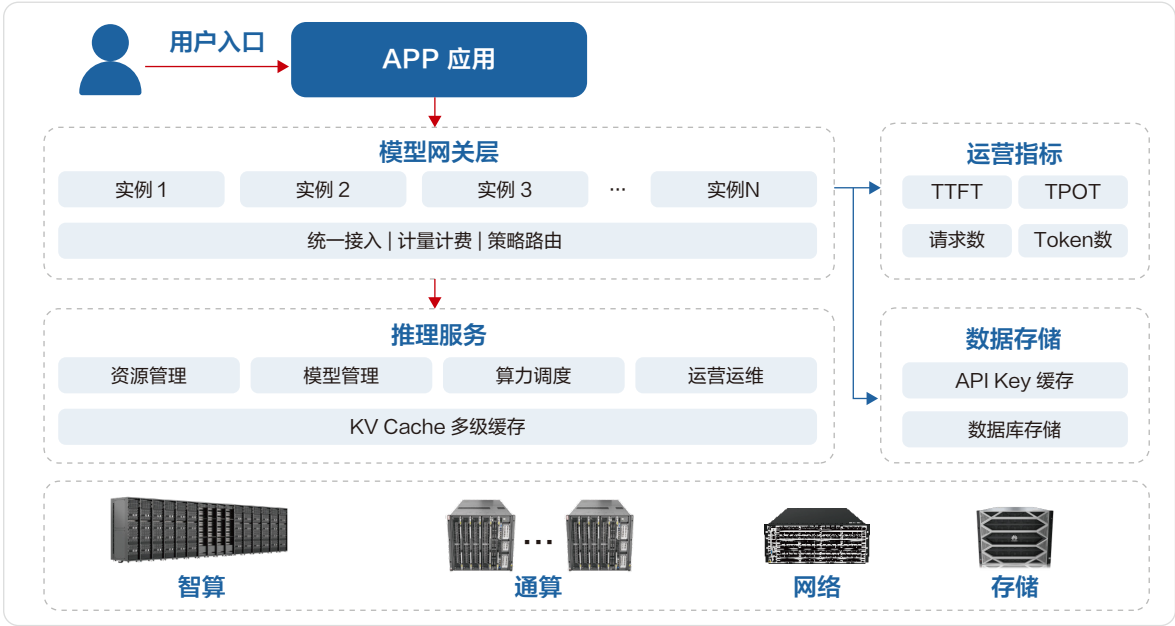


图 2-4：“企业私有化Token服务”参考架构和开源软件选型建议

最终，模型服务的工程部署应形成完整闭环：Agent 请求统一进入模型网关，由网关完成鉴权、路由、计量与治理；观测系统记录模型级与任务级

指标；评测体系根据成功率、成本、时延与业务结果，反向优化模型选择与路由策略。

沿着四个阶段推进企业Agent落地

建设以Agent为中心的企业AI应用与生态，应遵循“价值牵引、平台支撑、资产沉淀、持续运营”的原则，按照四个阶段稳步推进：

阶段一：场景准备

确认业务价值以及数据、语义、知识、工具和规则是否具备条件，并建立任务成功率、人工接管率、结果采纳率和单任务成本等业务目标。

阶段二：生产验证

建设统一平台和标准化接口，使关键行动可验

证、可回放、可审计，确认Agent的质量、成本、权限、安全、任务恢复和业务连续性是否达到生产要求。

阶段三：能力复用

持续沉淀执行路径、异常模式、最佳实践、岗位技能、业务规则和语义资产，使知识、工具和技能能够跨Agent、跨部门、跨场景复用。

阶段四：规模运营

形成统一的应用组合、平台能力、智能资产和组织机制，推动Agent建设由分散项目走向企业级生态。

长期看，企业 Agentic AI建设是一套持续运转的飞轮：Agent进入业务创造可量化价值，执行过程沉淀数据、语义、知识、技能和经验，沉淀的能力

被更多场景复用，进一步扩大业务价值。企业可以通过任务完成率、能力复用率、新场景上线周期和单位任务成本衡量飞轮运转效率。

Agent驱动AI Infra边界重构

为了支撑企业AI应用落地，AI Infra的边界也在发生变化，需要扩展形成三类平台服务能力：

Agent运行环境，承载长周期任务与多Agent协同

Agent运行环境需支撑数小时至数天的长程任务执行，通过持久化状态与Checkpoint保障任务连续性。

多 Agent 并行要求平台提供按需启动、弹性伸缩的安全沙箱，轻量容器沙箱冷启动P95（95th Percentile，第95百分位延迟）控制在毫秒级。

同时需建立任务级可观测体系，重点监测并发Session数、任务成功率、数据访问、工具调用等，形成完整任务Trace，为问题定位与安全审计提供输入。

模型运行与服务，提供可组合、可治理的推理能力

模型运行与服务提供统一、可编排的模型生产服务与高性能Token推理服务，支持按需启用PD分离、面向MoE模型的大规模专家并行与多级KV Cache等能力。

数据基础服务，统一支撑知识、数据、长期记忆与训练评测数据集

数据基础服务承担“沉淀企业智能资产”与“为模型训练供数”两类职责。一方面通过向量库、图关系库与长期记忆服务，支撑企业“知识湖”构建。另一方面通过多模态数据湖仓，实现训练数据集管理、数据清洗标注、血缘追踪等能力，为模型训练、评测提供可追溯、可复现的数据。

总体上，AI Infra需演进为同时具备三类平台能力与异构资源对等互联架构的新型基础设施。

2.2 Token-Centric AI Infra

从Cloud Infra到AI Infra的核心变化

负载从“云大数”到“AKDM”。Cloud Infra主要承载云计算、大数据与数据库等业务负载（简称“云大数”），以CPU为核心，适配全类型多源数据，兼容多元通用业务。AI Infra 承载的则是 Agent 应用、企业知识库、数据湖与模型推理训练等新型负载（简称“AKDM”），以NPU为中心，呈现计算密集、带宽密集、长时运行与高功耗的特征。

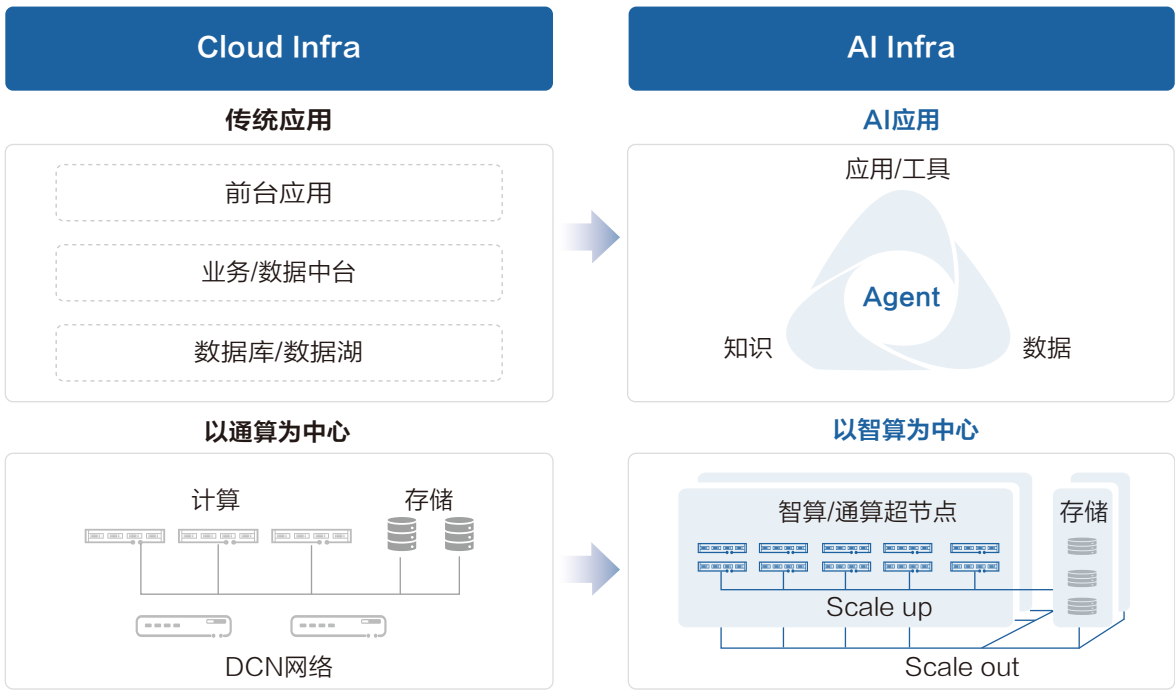


图2-5： AI Infra相比Cloud Infra的核心变化

Token成为连接算力、模型与用户体验的价值载体，AI Infra的核心使命是保障高质量Token持续、高效、稳定地生成。

Token生产效率四维评估要素

不同业务场景对Token生产效率的要求并不相同，如下表所示：

场景类别	典型应用	业务特征	Token生产效率要求	典型指标
互联网2C类	智能客服、AI搜索、生成式推荐、AI助手	用户规模亿级；峰值请求万级及以上；单次请求通常为百级Token，复杂问答和推理可达千级Token	低时延、高吞吐、低成本	TTFT <500ms；峰值QPS 万级+；Output TPS持续提升
实时决策	金融风控、交易分析、工业诊断、实时运维	单次请求通常秒级完成；峰值并发百级~千级；结果直接影响业务决策	低时延、高可靠、高质量	TTFT <500ms；SLA ≥99.99%
知识问答	政务问答、企业知识库、医疗助手、专业咨询	上下文通常万~十万Token；多轮交互；知识检索和上下文复用明显	高质量、高一致、可信可控	TTFT <1s；知识准确率 >90%；结果可追溯
AI编码	软件开发、代码审查、自动测试	单任务可包含10~100+次模型调用；上下文可达10万~百万Token；任务持续小时级及以上	持续生成、状态复用、任务可靠	TPOT <50ms；任务完成率 >90%；支持小时级长任务

Token生产效率可以通过四个维度进行衡量：Performance（响应性能）、Concurrency（并发吞吐）、Cost（成本效率）、Quality（生成质量）。

响应性能（Performance）：用户体验指标
衡量用户从发起请求到获得有效响应时长。主要指标包括：

TTFT（Time to First Token，首Token时延）
指从用户请求进入系统，到返回第1个输出Token所经历的时间。

TPOT（Time Per Output Token，单Token生成时间），指首Token输出后，每生成一个后续Token所需的平均时间。TPOT决定连续输出过程的流畅程度，是衡量流式交互体验的重要指标。

并发吞吐（Concurrency）：性能评估指标
衡量AI系统在满足用户体验约束的情况下，单位时间能够持续生产Token的能力。主要指标包括：

TPS（Token Per Second，每秒Token处理量） 衡量单位时间Token处理能力，包括Output TPS和Total TPS。前者表示每秒输出Token数

量，反映用户感知的生成速度；后者表示输入与输出Token总处理量，反映系统整体吞吐能力。

QPS（Queries Per Second，每秒请求数）衡量系统单位时间处理请求数。

企业真实的工程目标不是“生成更多Token”，而是在“在满足用户体验约束的条件下，持续生产更多有效Token”。这可以用有效TPS来衡量，即：在TTFT、TPOT等用户体验约束下，系统实际产生的Token总量，是衡量AI集群真实生产能力的核心指标。

评估AI Infra并发吞吐能力，必须结合具体业务负载，而不能只看单一TPS指标，这是因为不同业务场景的并发吞吐优化重点也不同，比如：

- 智能客服等短问答场景，请求频率高、单请求输出短，核心诉求是提升QPS和并发承载能力；

- 长文本生成、代码生成等场景，请求数量较少但单请求持续输出大量Token，核心诉求是提升单请求生成效率。

成本效率（Cost）：性价比指标

衡量生产一定数量有效Token所需要投入的资源成本，包括硬件折旧、电力消耗、网络传输、存储以及软件优化成本。

百万Token成本（Cost per Million Tokens）衡量Token生产经济性的核心指标。随着模型优化、硬件升级和推理效率提升，单位Token成本持续下降。

生成质量（Quality）：服务有效性指标

衡量Token是否准确、稳定且满足业务要求。速度与规模代表生产能力，高可信可用的Token才是业务价值的真正载体。一般包括内容生成的准确性和一致性等。

Token生产效率评价指标体系表

评价维度	评价指标	指标说明
响应性能 (Performance)	TTFT	衡量首Token响应时间，决定用户等待体验
	TPOT	衡量连续Token生成速度，决定流式交互体验
并发吞吐 (Concurrency)	TPS	每秒Token处理量，衡量单位时间Token处理能力，包括Output TPS和Total TPS
	QPS	每秒请求数，衡量系统单位时间处理请求数
成本效率 (Cost)	百万Token成本	衡量单位Token生产成本
生成质量 (Quality)	准确性	衡量输出结果是否满足业务要求
	一致性	衡量输出稳定性和可靠性
	可信度	衡量结果是否可验证、可审计

企业AI Infra建设的目标不是简单堆叠最大算力，而是在**性能、吞吐、成本和质量之间找到最佳平衡，构建最匹配业务需求的Token生产系统。**

Token生产效率的关键约束和核心技术

Token生产效率的提升，本质上是围绕大模型推理全链路瓶颈的持续优化。随着模型规模扩大、上下文长度增加以及实时交互需求提升，推理过程中的性能核心瓶颈正在从“计算能力”转变为“数据流动效率”。

因此，从AI芯片微架构到系统级的计算、存储、高速互联协同设计，整个技术栈的演进重心都在围绕

提升推理数据访问和搬运效率展开，包括提高计算单元利用率、提升存储带宽、优化通信效率，以及针对KV Cache的高效管理、存储和访问。

“数据流动效率”成为推理的核心瓶颈

一次完整的大模型推理过程包括Prefill（预填充）和Decode（解码）两个阶段，两者对底层芯片与系统架构的需求存在本质差异，如下表所示：

	Prefill	Decode
处理过程	用户输入Prompt后，一次性并行处理全量Token，完成Attention运算并生成KV Cache	模型按自回归方式逐个预测下一个Token
计算特征	Token之间高度并行，矩阵计算密集	Token逐个生成，串行计算，数据访问频繁
性能瓶颈	大规模矩阵运算 (Compute-Bound)	数据供给，受限于内存带宽 (Memory-Bound)
优化方向	算力优化： - 提升AI芯片计算能力 - 优化Tensor Parallel等并行策略 - 提高模型算力利用率（MFU，Model FLOPs Utilization） - PD分离后匹配高算力资源	数据流动优化： - KV Cache压缩、共享和分层管理 - 提升内存容量和带宽 - 优化芯片间高速互联 - PD分离后匹配高带宽资源

长上下文加剧数据搬运压力

以DeepSeek V4 Flash模型（总参数284B）处理128k长文本为例：单次请求需要驻留约288GB模型权重和KV Cache状态，这意味着在Decode阶段，每生成一个Token，都需要从总规模达数百GB的驻留数据进行调度访问。在此过程中，芯片计算单元往往仅需不到0.01毫秒即可完成计算，其余99.9%以上的时间都在“等待数据供给”。Decode阶段的核心矛盾已彻底从“算得快”演变为“搬得快”。

“存算剪刀差”进一步放大瓶颈

近年来，AI芯片算力的增长速度远超内存带宽的增长速度（内存墙加剧）。以英伟达的H100到B200为例，在低精度推理算力上提升了4.5倍，而内存带宽仅提升约2倍。算力跃升能够显著缩短Prefill，但Decode因受限于带宽而难以获得同等收益，计算与数据供给之间的鸿沟持续扩大。



图2-6：内存墙：AI算力与内存带宽增长对比（2018-2026）

因此，大模型推理的核心瓶颈正在全面从“提升峰值算力”转向“提升数据搬运效率”。未来Token

生产效率的竞争，本质上是芯片访存、互联传输与系统级数据流协同调度能力的综合竞争。

AI推理芯片的关键指标成为Token生产效率核心硬约束

对于AI芯片来说，以下4个指标影响Token生产效率：

AI算力

FLOPS — 每秒浮点运算次数

决定 Prefill 速度、首 Token 延迟（TTFT）。模型算力高则运算速度快，算力低则 TTFT 爬升。

直接影响：TTFT

内存容量

GB — 芯片可同时承载的数据量

决定能装多大模型、服务多少并发用户。容量不足则被迫跨卡部署，长序列上下文寸步难行

直接影响：QPS 并发数 · 上下文长度

内存带宽

GB/s — 从片上内存读取数据的速度

决定 Decode 阶段每步 Token 生成速度。Decode 是访存密集型——算力常在等待数据，带宽才是真实瓶颈。

直接影响：TPOT

互联带宽

GB/s — 芯片间数据交换速度

决定多卡协作效率。模型跨卡部署需同步中间结果，MoE需跨卡交换 Token，带宽不够则算力空转。

直接影响：集群有效 TPS

图2-7 决定Token生产效率四个指标

模型推理性能受限于其中最短板，所以这4指标之间的比例关系，能更好地反映AI芯片推理性能均衡性，包括：

算力带宽比 = AI算力（TFLOPS）÷ 内存带宽（TB/s）

算力带宽比用于判断芯片适合计算密集还是访存密集负载：比值高，适合训练与Prefill推理；比值低，适合Decode与在线推理。

内存算力比 = 内存容量（GB）÷ AI算力（TFLOPS）

内存算力比决定单卡能装下多大的模型、保留多长的KV Cache。比值高，更适合长上下文、高并发推理。Agent爆发使超长上下文成为常态，AI芯片设计的趋势是系统性提升内存算力比。

对于AI芯片来说，算力再强，如果内存带宽不足，Decode依然会受限；内存再大，如果互联带宽不足，也无法支撑大规模MoE协同。

突破Token生产瓶颈的关键技术

除AI芯片微架构革新外，AI Infra的核心演进方向也是聚焦于数据流动效率：**让不同阶段匹配不同资源，让数据更少搬移、更快到达计算单元。**

1、架构层重构：Prefill-Decode解耦分离

传统方案将Prefill与Decode混部在同一集群中，易引发资源错配与性能干扰（Head-of-Line Blocking）：

- 资源需求冲突：Prefill是高算力消耗型任务，Decode则是高带宽消耗型任务。
- 混合部署互相拖累：长Prompt的 Prefill 请求占用大量计算资源，影响 Decode 的实时响应；而为了保障 Decode 的低时延与 SLA，系统又必须预留内存与算力，导致 Prefill 算力利用率低下。

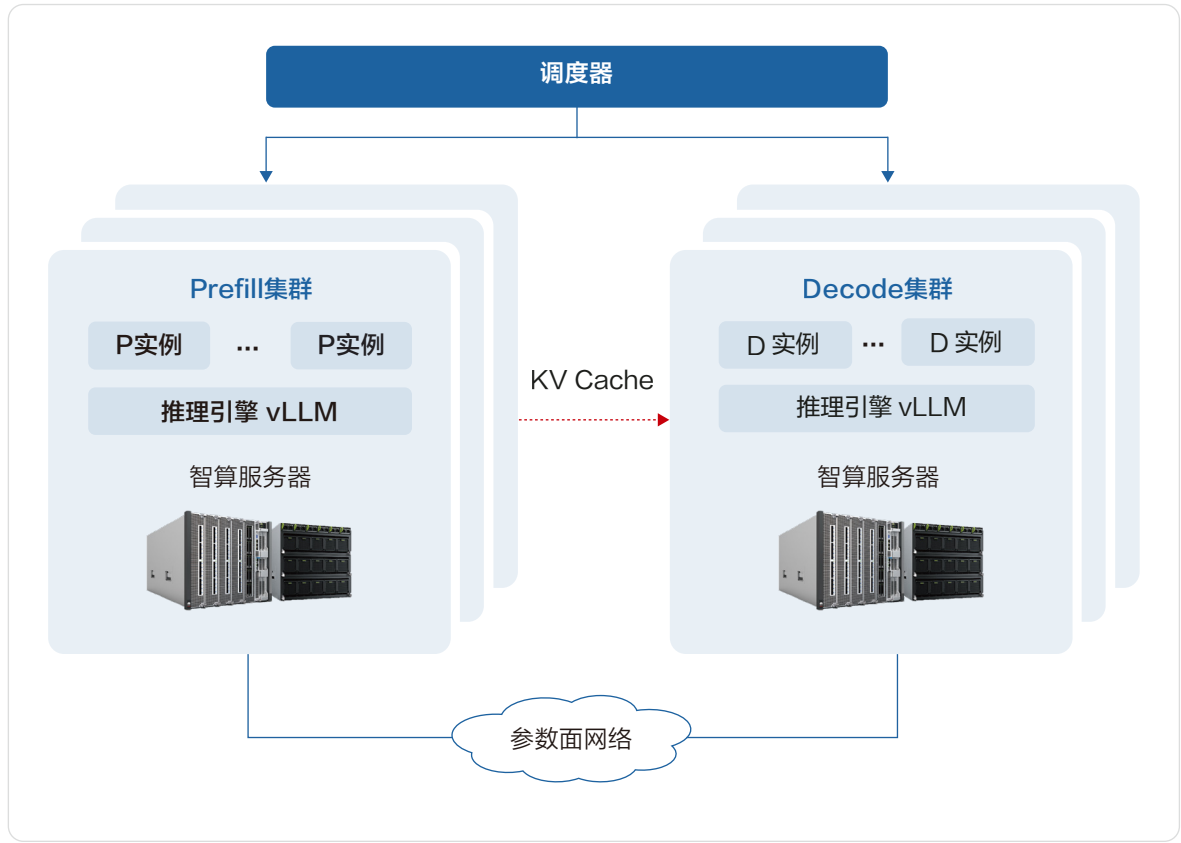


图 2-8 Prefill-Decode (P-D) 解耦分离

P-D 分离架构通过将两个阶段拆分到不同资源池，实现异构负载的最优匹配：

- Prefill 集群：侧重高吞吐与算力利用率，通常采用高算力密度芯片，缩短首Token时延（TTFT）。

Decode 集群：侧重访存带宽与通信互连，提升单位时间 Token 产出速率（TPOT）。

其本质是解决**推理阶段之间的资源错配问题**，让计算资源与业务负载更加匹配。

2、围绕数据流动效率的三大优化方向

在此基础上，进一步围绕数据流动效率开展三个方向的优化。

减少数据搬移：降低无效访问

随着上下文长度与对话轮次急剧膨胀，KV Cache 带来的存储与传输开销成倍放大。核心思路是尽可能复用计算结果、减少不必要的**数据搬移**：

KV Cache优化：通过压缩、量化、淘汰和高效管理策略，降低 KV Cache 的存储规模和访问压力；如vLLM的PagedAttention，通过分页式管理提升KV Cache利用效率。

Prefix Cache：复用公共前缀上下文的计算结果，避免重复的 Prefill 计算，大幅削减冗余数据生成与搬运，用于多轮对话、固定 System Prompt 及 Agent工具链调用等场景；

多级KV Cache架构：利用片上内存、DRAM内存、SSD等不同存储层级，根据数据访问频率进行热温KV Cache的分级管理与动态调度。

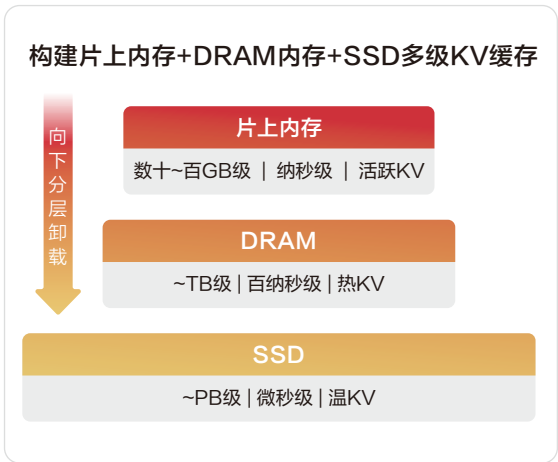


图 2-9 多层次 KV 缓存

随着Agent任务复杂度持续提升，**多级分布式KV Cache已成为AI Infra降低推理成本、提升资源利用率的关键能力。**

提升数据供给能力：增强单节点Token生产效率

即使减少了无效数据搬移，随着模型规模持续增长和上下文不断加长，单个计算节点仍然面临巨大的数据供给压力。特别是在Decode阶段，模型参数和KV Cache需要持续供应给计算单元。因此，AI Infra需要提升整个节点的数据供给能力，让计算单元持续获得所需数据，减少“等数据”的空转时间。

高有效带宽存储体系：结合高规格存储介质、先进封装与数据压缩/量化技术，全面突破存储吞吐瓶颈，最大化提升送入计算单元的单位时间有效数据量；

算存网协同设计：优化CPU、NPU、SSD之间的数据流动路径，减少数据搬移开销，如华为NDS（NPU Direct Storage）等，通过数据直通技术缩短数据访问路径；

超节点架构：通过高速对等互联总线，将多个AI芯片组织成统一计算单元，突破单芯片和单服务器资源限制，提高单节点模型承载能力和推理吞吐。例如华为昇腾Atlas超节点等。

优化跨芯片数据流动：突破大规模模型扩展瓶颈

随着模型规模不断扩大，尤其是MoE架构逐渐成为重要方向，模型参数和计算任务被分布到多个芯片甚至多个节点。此时，瓶颈不再只是单个芯片内部的数据访问，而是不同计算资源之间的数据交换效率。因此，需要进一步优化**跨芯片、跨节点的数据流动**，让分布式计算资源形成高效协同的Token生产系统。

高速芯片互联：提升多芯片之间的数据交换能力，如华为灵衢（UBLink）等高速互联技术；

高效并行计算架构：优化模型切分和任务调度方式，提高多芯片协同计算效率，如Megatron-LM、DeepSpeed等支持张量并行、流水并行和专家并行的大模型分布式计算框架；

通信与计算融合优化：减少通信等待，提高分布式推理效率，如HCCL集合通信优化、MoE场景下针对All-to-All通信的优化技术。

总体来看，Token生产效率的提升，本质是一场围绕“数据流动效率”的系统优化。从**PD分离推理架构**，到**减少无效搬移、提升节点供给能力、突破跨节点通信瓶颈**，AI Infra正在从传统算力基础设施转向面向智能生产的新型计算体系。未来竞争的关键，不是谁拥有更多算力，而是谁能够让计算、存储和通信形成更加高效的数据流动体系，持续、稳定、高效地产生Token。

Token-Centric AI Infra目标参考架构

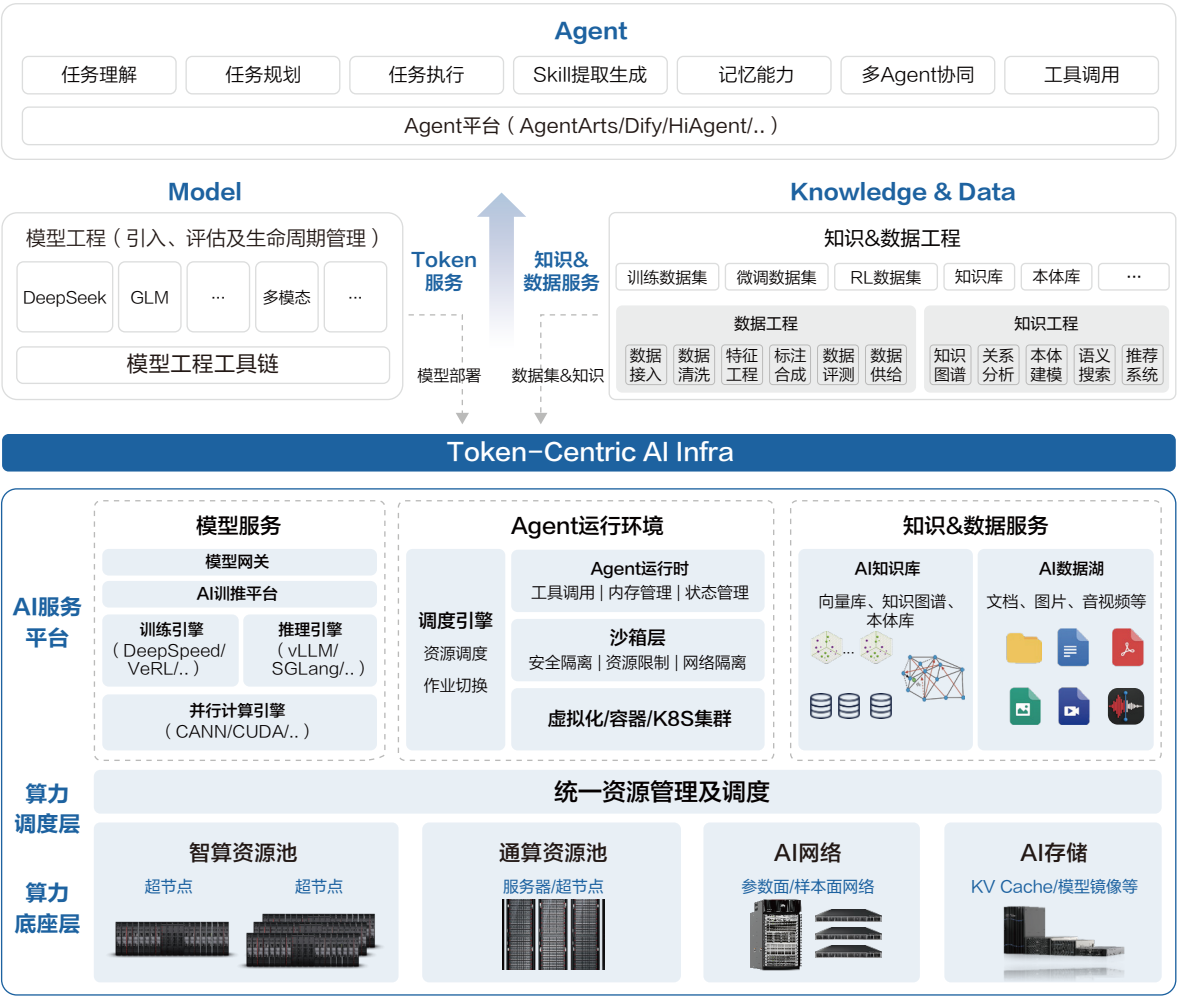


图2-10 企业Token-centric AI Infra总体架构

传统Cloud Infra以IaaS 为中心，聚焦计算、存储、网络的池化与调度；而当Token成为衡量AI生产效率的核心单位后，单纯优化资源层已无法决定最终的Token产出效率。因此，**AI Infra 的架构边界需要进一步向上延伸**，在传统资源基础设施之上增加模型运行、数据知识管理和Agent运行环境等AI服务能力，将底层算力转化为可持续运营的AI能力。

基于这一变化，**Token-Centric AI Infra形成AI算力底座、算力调度、AI 服务平台三层架构**，分别解决“极致Token生产效率、高效算力利用和持续AI能力供给”三个核心问题，最终实现从“资源供给”到“智能生产体系”的演进。

算力底座层：解决“单位算力的Token生产效率”

AI时代，企业建设重点不再是简单增加算力规模，而是构建面向AI负载优化的统一算力底座，使计算、存储和网络能够围绕模型推理、训练和Agent任务高效协同。区别于传统Cloud Infra面向通用计算资源，AI算力底座需要同时支撑多样化AI负载：

智算资源：以超节点及超节点集群为核心，提供模型训练和推理所需的高性能计算能力。通过高速互联、内存池化和大规模并行，提升单任务Token生产效率；

通算资源：支撑数据处理、知识服务、Agent任务编排和工具执行，为智能应用提供业务执行能力；

AI存储与高速网络：承载模型镜像、KV Cache、上下文状态和训练数据，通过高带宽、低时延的数据通路保障计算资源持续获得有效数据。

最终，算力底座的目标不是提供更多孤立算力，而是构建面向AI生产的高效计算体系，让单位资源产生更多有效Token。

算力调度层：解决“高效资源利用”

算力调度层本质上是AI Infra的操作系统，负责连接底层资源、模型任务和业务需求，通过资源池化、弹性调度、任务编排和智能优化，实现：

资源统一管理：屏蔽不同芯片、不同代际设备差异，形成统一AI资源池；

动态资源匹配：根据模型规模、推理阶段和业务优先级，将任务匹配到最适合的计算资源；

资源弹性复用：通过训推混部、潮汐调度和优先级管理，提高整体资源利用效率；

高可靠运行：通过故障检测、任务迁移和资源恢复，保障AI生产连续运行。

如果说算力底座决定企业拥有多少Token生产能力，那么算力调度决定这些能力能否被充分释放。

AI服务平台：解决“持续AI能力供给”

AI服务平台主要包括三类核心能力：

模型运行服务：通过推理引擎、训练引擎和模型服务管理，将算力转化为稳定、高效的Token生产能力；

数据与知识服务：通过向量数据库、知识图谱和长期记忆，使Token具备企业业务知识，实现从通用智能到行业智能的转化；

Agent运行环境：通过任务编排、工具调用、安全执行和多智能体协同，使Token进一步驱动业务流程和自动化执行。

上述三层从功能分层视角定义了AI Infra的逻辑架

构，但实际建设还需从工程部署视角进一步拆解为**四个能力圈：超节点、超节点集群、算力调度和AI服务平台**。其中，超节点与超节点集群是算力底座层的核心载体，聚焦单位算力的Token生产效率。

四个能力圈重塑Token-Centric AI Infra

四个能力圈分别聚焦算力供给、集群协同、资源调度和智能服务，共同构成从底层算力资源到上层AI

能力交付的完整体系，是Token-Centric AI Infra落地建设的核心能力单元。其具体内涵如下：

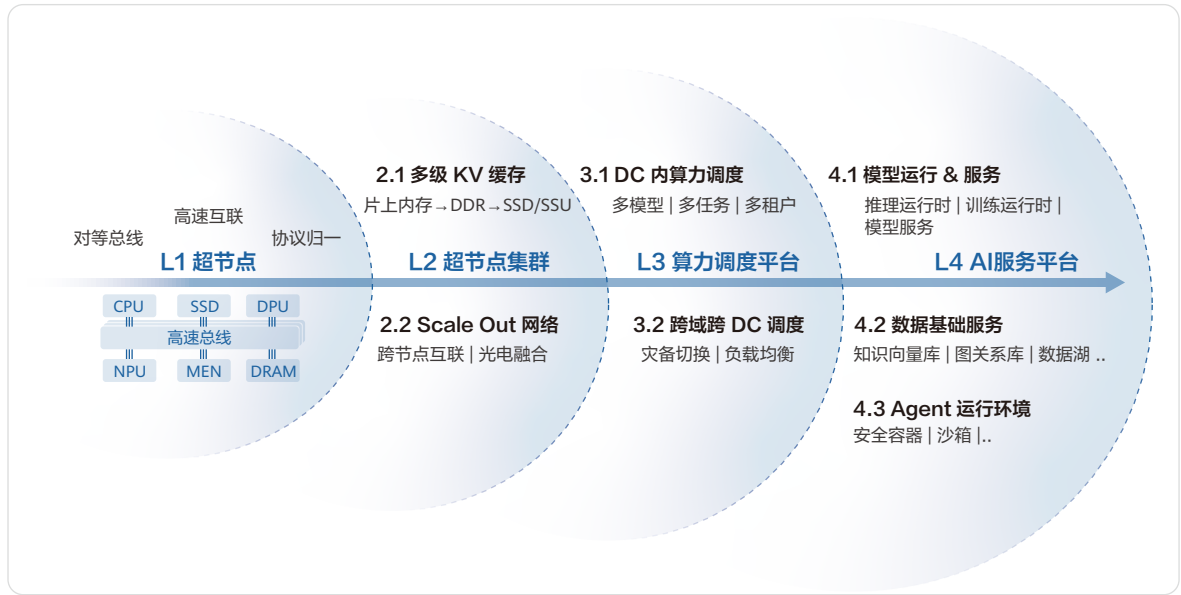


图2-11 Token-Centric AI Infra

L1-超节点：Token高效生产核心引擎，成为建设常态

1、超节点的定义：逻辑上的“一台计算机”

随着模型规模从百亿、千亿参数向万亿参数演进，传统单服务器架构正在逼近物理边界。以1T参数模型为例，即使采用FP16精度，模型参数本身就需要约2TB内存，已经超过主流8卡AI服务器的片上内存容量。即便通过INT4、FP4等低精度量化方式压缩模型，有限片上内存仍会大量被模型权重占用，

留给KV Cache的空间不足，导致推理并发能力和长上下文能力受到严重限制。

因此，要同时满足大模型部署、长上下文推理和高并发服务，计算资源必须突破单服务器边界，向跨节点融合演进。

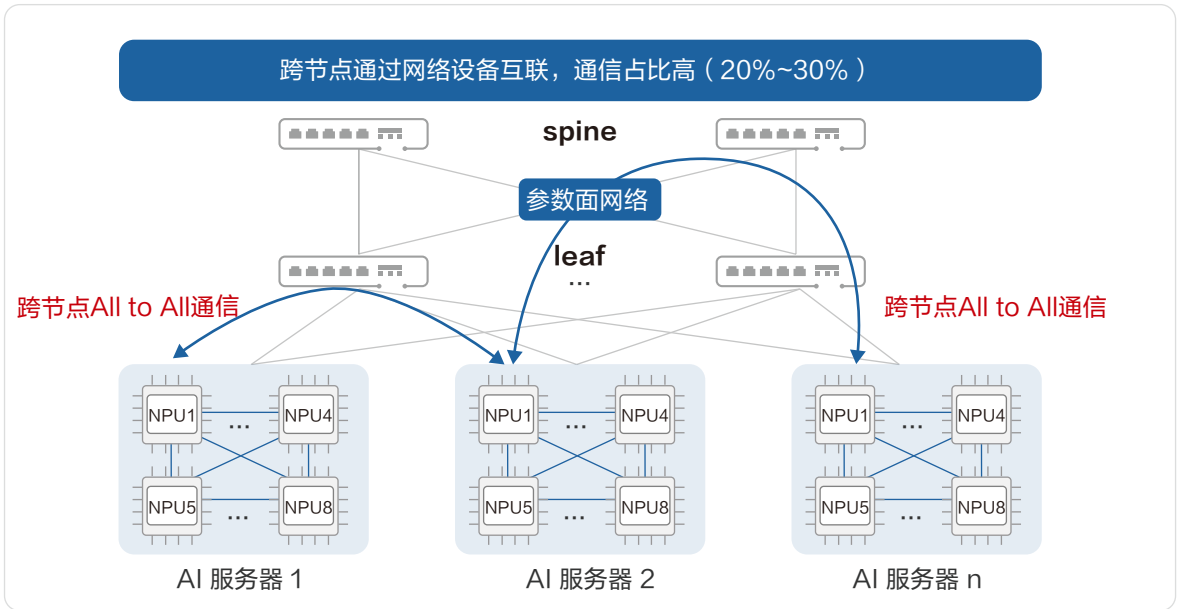


图2-12 传统服务器架构

当计算规模从单机扩展到集群，新的瓶颈随之出现——通信效率。特别是在MoE模型中，专家并行需要大量跨芯片All-to-All通信。传统Scale-Out架构依赖以太网连接标准化服务器，虽然具备良好的通用扩展能力，但在超大规模AI负载下，网络带

宽和通信时延逐渐成为限制因素。计算芯片等待数据传输的时间增加，通信开销不断侵蚀有效算力，导致集群规模越大，Token生产效率反而下降。

因此，AI基础设施出现了新的计算组织方式：超节点。

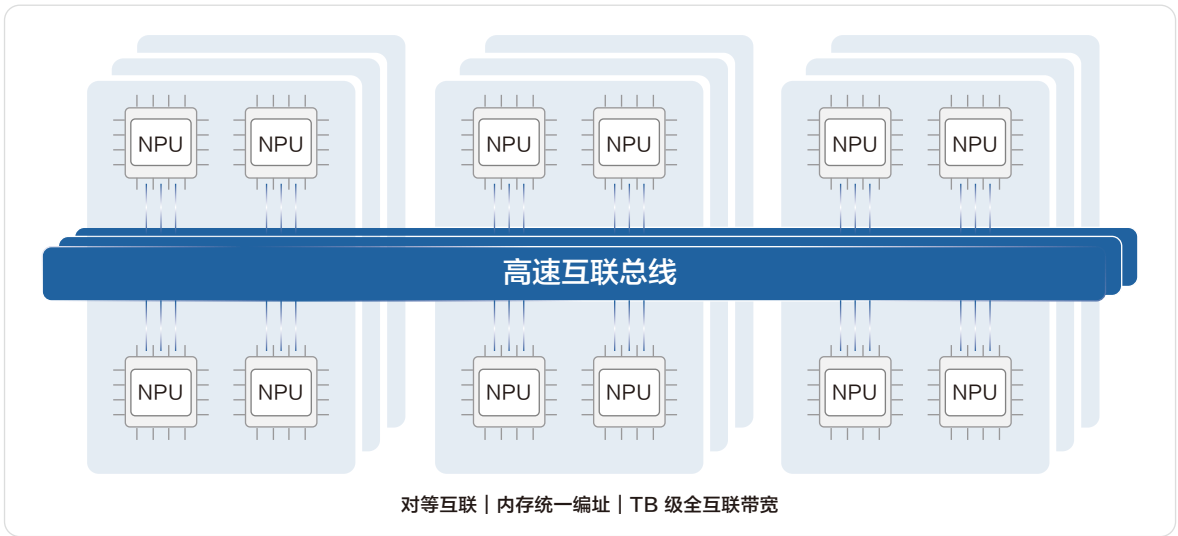


图2-13 超节点架构

超节点通过高速总线级互联，将数十到数千颗AI芯片在物理上集成于整机柜乃至跨机柜，在逻辑上融合为“一台计算机”。同一超节点域AI芯片互联应不少于32颗，且应具有高带宽（大于400GB/s）、低时延（小于500ns）和统一内存编址等特点。与传统服务器集群相比，超节点最大的变化在于：

统一内存编址：让分布式资源成为共享内存池

传统AI集群中，每张AI卡拥有独立片上内存，模型和数据需要在不同设备之间不断搬运。超节点通过内存池化技术，将分布式内存资源抽象为统一地址空间，使不同AI芯片能够直接访问远端内存资源。这意味着：

- 模型参数可以跨芯片统一管理；
- KV Cache可以跨实例共享；
- 大规模模型无需受单卡片上内存限制。

计算资源从“多个孤立设备”转变为“共享内存的大型计算机”。

高带宽低时延互联：降低通信对计算效率的影响

大模型尤其是MoE模型，本质上是通信密集型计算。

超节点通过高速互联和内存语义访问，将传统网络通信转化为更接近本地访问的数据交换方式，大幅降低通信开销。

其价值不仅是提升峰值算力，更重要的是：让更多计算资源真正参与Token生产，而不是等待数据传输。这些创新直接转化为业务收益——在DeepSeek、Qwen等MoE模型推理中，端到端性能获得3倍以上提升，有力验证了超节点架构对Token产出效率的实际增益。

2、基于超节点的推理架构创新，实现高效Token生产

超节点带来的统一计算域，为大模型推理架构提供了新的优化空间。

大规模专家并行（大EP）：释放MoE模型吞吐潜力

MoE模型通过多个专家提升模型容量，但传统集群受限于通信效率，专家规模扩展困难。超节点提供的大规模内存池和高速互联，使更大规模专家并行成为可能。

以DeepSeek大EP方案为例，大EP架构可以实现“一卡一专家”，EP卡数从16卡增加到288卡（包含共享专家），单卡权重占用从42GB降低至2.33GB，可以保持更多的KV Cache（实现Batch Size从8增长到30），扩大超节点内存池。

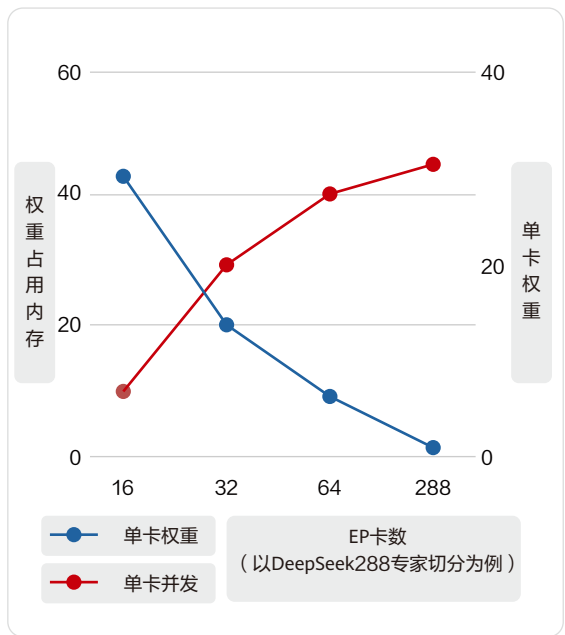


图2-14 DeepSeek V3 大EP

EP卡数越多，Decode计算耗时越小；EP卡数越多，多卡之间All-to-All（A2A）通信挑战越大，

但是借助于超节点的大带宽，整个系统仍处于最优状态。

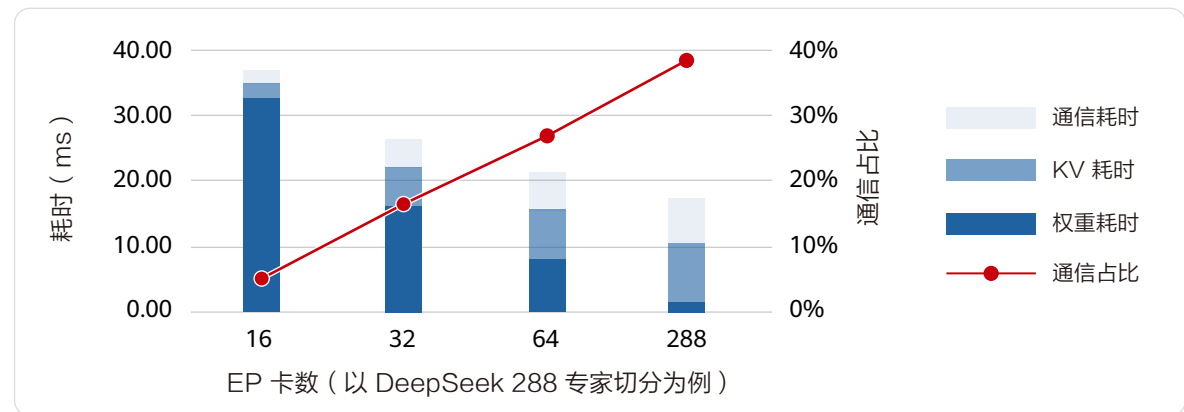


图2-15 DeepSeek V3 大EP 通信耗时和通信占比

P-D-C全对等架构：KV Cache全局化消除重复计算，大幅降低TTFT

在轮对话和Agent任务中，大量请求会复用已有上下文。传统推理架构中，KV Cache与单个实例绑定，不同实例之间KV无法共享，同一历史上下文

需要重复Prefill计算。

基于超节点统一内存编址，推理架构正在向P-D-C全对等方向演进：Prefill负责上下文计算、Decode负责Token生成、Cache负责状态共享。

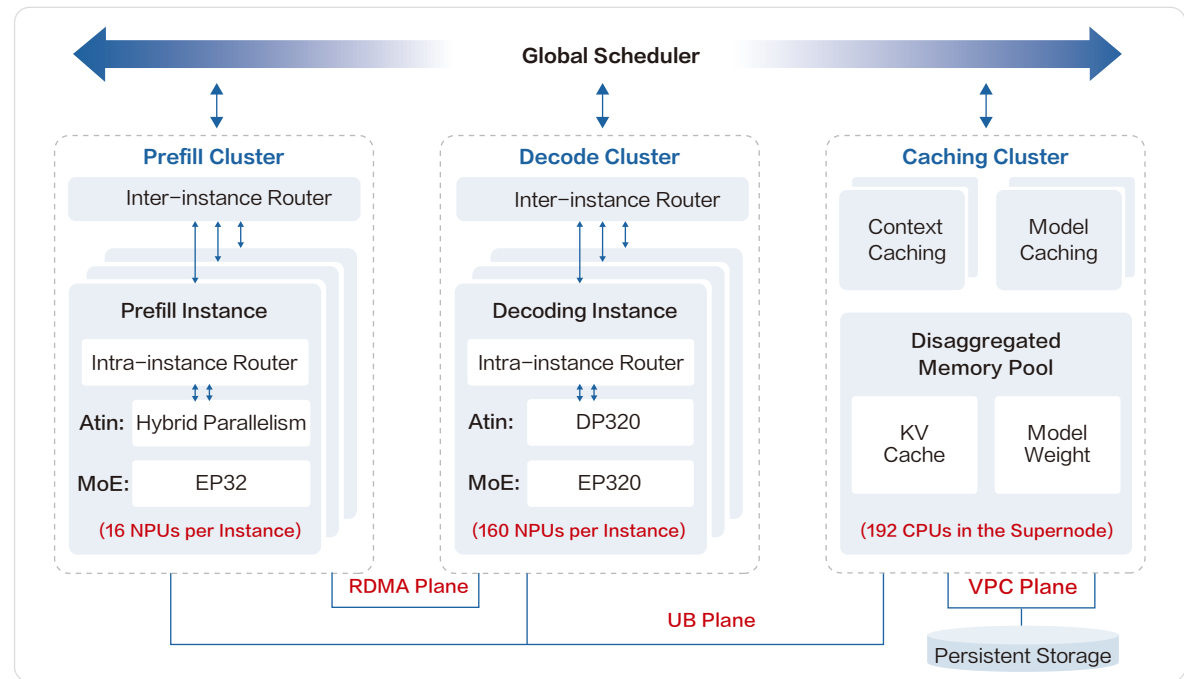


图2-16 基于昇腾超节点+DeepSeek的P-D-C全对等架构

KV Cache不再属于单个实例，而成为整个计算域共享资源。结合KV Cache感知路由，可以优先调度已有上下文缓存的实例，从而减少重复Prefill、降低TTFT、提升整体Token生产效率。这标志着推理系统从“计算模型”走向“计算+状态管理模型”。

3、超节点多种形态：可满足大中小场景高性能推理需求

对于中小规模场景，可以采用64卡/96卡等不同规模超节点，部署不同规格的PD分离大EP实例，满足高性能推理要求：

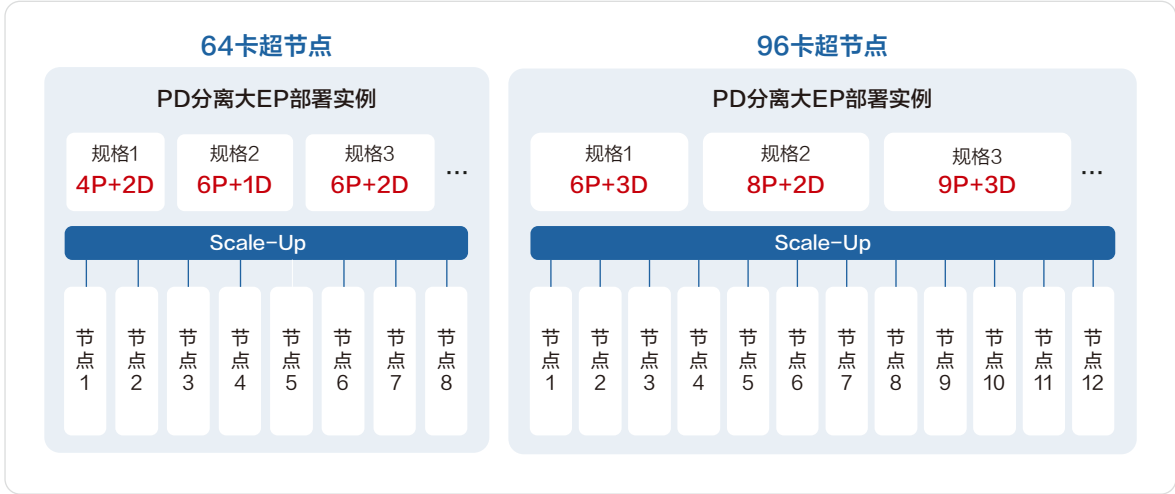


图 2-17 中小规模超节点部署配置

面向大规模高并发推理、模型训练和核心生产场景，超节点可以扩展至数百甚至数千卡规模，形成超级计算系统。更重要的是，超节点具备逻辑切分能力。

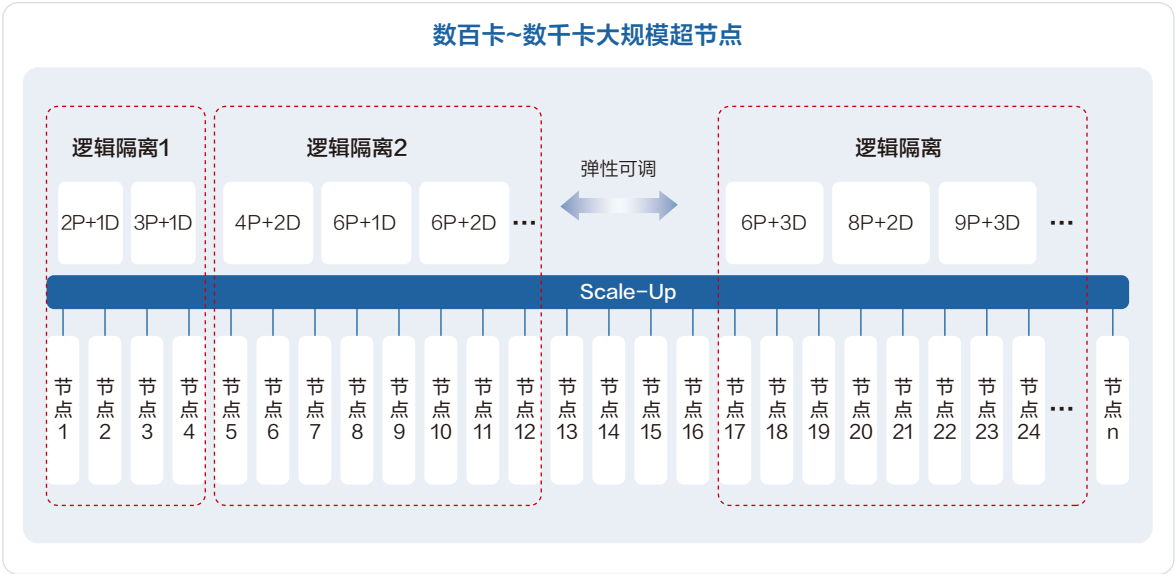


图 2-18 大规模超节点部署配置

4、超节点发展趋势

超节点正在从技术探索走向产业规模化应用，成为AI基础设施演进的重要方向。未来，超节点将围绕三个方向持续演进：

第一，规模持续扩大：超节点规模将持续突破传统服务器集群边界，支撑更大规模训练和推理，未来超节点规模将从千卡演进到万卡。

第二，互联持续升级：随着超节点规模持续扩大，网络互联成为决定系统效率的关键。超节点网络正从微秒级向纳秒级时延演进，通过Tbps级带宽和更高效拓扑，实现计算资源之间的高速协同。与此同时，传统电互联遭遇高频损耗与功耗瓶颈；

光互联为下一代核心方向，NPO 近封装光学是关键技术路径。

第三，资源持续解耦：随着推理、多模态和Agent任务复杂化，计算、内存和通信需求日趋差异化。未来超节点需要支持：AF分离（Attention-FFN Disaggregation，即Attention与FFN/MoE模块解耦部署）、多模态VAT（视觉-音频-文本多模态模型架构）以及LLM分离（大语言模型不同组件拆分部署）等新型部署模式。最终目标是：让不同AI工作负载都能够动态获得最适合的计算资源。

L2-超节点集群：万亿MoE模型高并发部署的基础架构

超节点提升的是单一计算域的协同效率，而超节点集群进一步解决AI规模化生产问题，将多个超节点与网络、存储融合为统一 AI 生产系统。

1、超节点集群的典型应用场景

企业建设超节点集群，本质是为了满足AI进入生产阶段后的三类需求：

01

规模扩展：支撑业务持续增长

从AI试点到规模化应用，单个超节点会逐渐受到吞吐、并发和业务隔离限制。通过Scale-Out扩展多个超节点，企业可以平滑提升Token产能，而无需重新建设基础设施。

03

可靠运行：保障核心业务连续性

当AI进入金融、政务、制造等关键流程，集群通过故障隔离、服务迁移、滚动升级和容灾部署，将AI从单实例服务升级为可靠生产系统。

02

生产运营：支撑多业务、多模型并行运行

企业级AI需要同时承载多个模型、多个业务和大量用户请求。超节点集群通过统一资源池和弹性调度，实现计算能力横向扩展。

2、超节点集群的核心构成

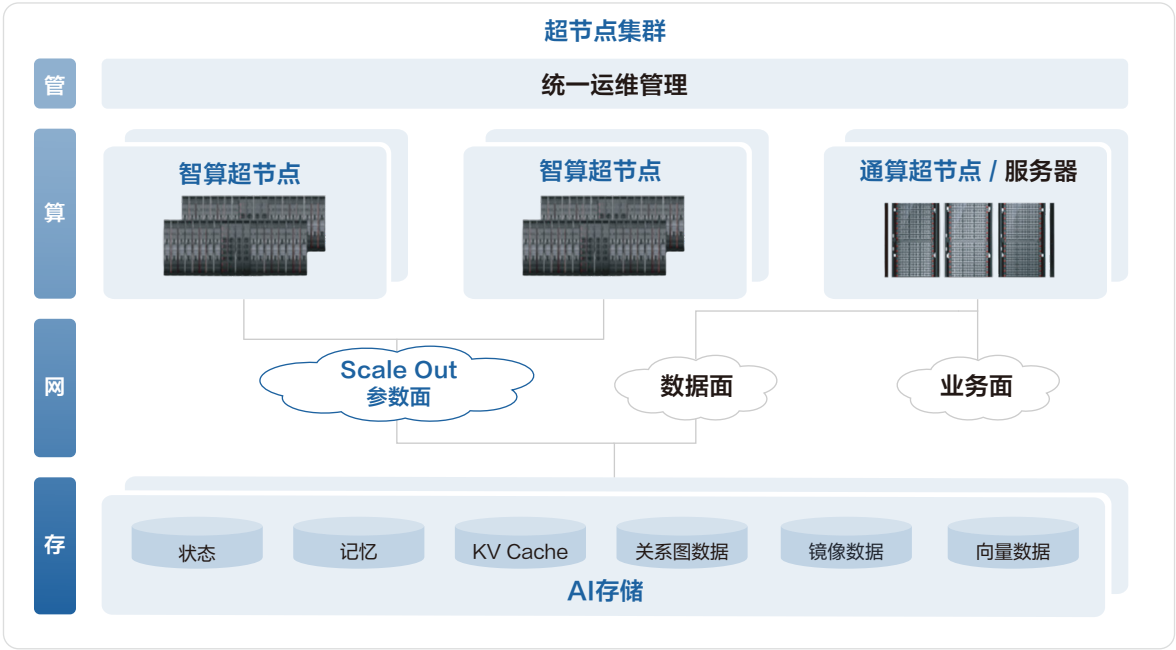


图 2-19 超节点集群系统构成图

超节点集群通过**智算、网络、存储、通算四大底座协同**，将分散的计算资源融合为面向AI生产的统一基础设施。

- 智算底座**提供大模型训练与推理能力；
- 网络底座**实现超节点间高速互联和集群扩展；
- AI存储底座**承载模型数据、KV Cache和Agent长期记忆；
- 通算底座**支撑任务编排、工具调用和Agent运行环境。

四大底座共同构成AI生产平台，使计算、状态和任务能够在集群范围内协同流动：**智算负责思考，通算负责行动，AI存储负责记忆，网络负责连接。**

3、Scale-Out网络：让多个超节点成为统一计算域

Scale-Out网络，是连接超节点集群中计算与

数据资源、实现集群级AI协同的互连网络。它**一方面连接多个超节点**，协同完成大模型训练推；**另一方面连接AI存储**，为模型状态、KV Cache等推理关键数据提供高效访问通道，让上下文状态能够在集群范围内共享和复用。

Scale-Out网络的典型场景与主要流量

随着大模型推理架构从单实例向集群化演进，Scale-Out网络承载的通信类型不断扩展，主要包括：

- KV Cache通信**：支撑PD分离和上下文状态共享；
- 激活与MoE通信**：支撑Decode实例模型结构解耦后的模块协同；
- Prefix Cache通信**：支撑跨实例的上下文复用。

典型场景如下：

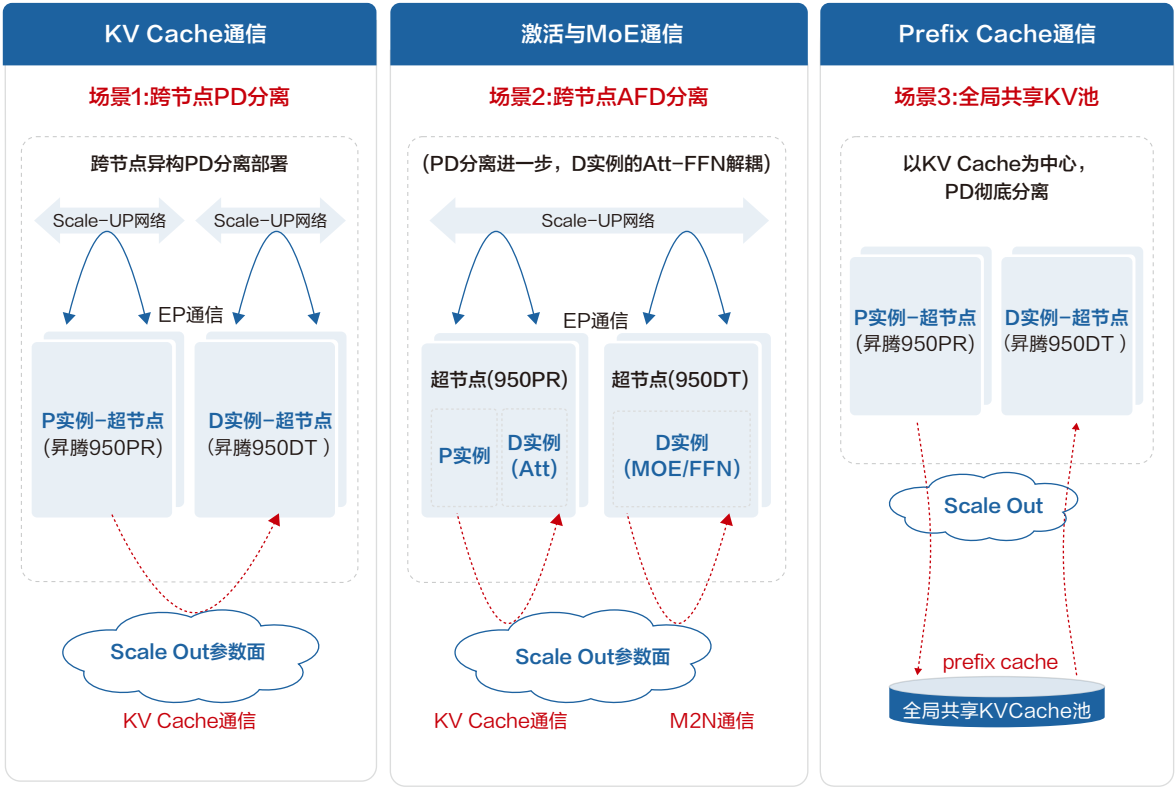


图 2-20 Scale-Out网络的典型场景示意图

典型场景	场景描述	主要通信流量	Scale-Out网络价值
跨节点异构PD分离	Prefill与Decode部署在不同类型算力资源池	KV Cache跨节点传输	连接异构超节点，实现不同代际、不同类型算力协同，优化推理成本
异构AFD分离	Attention与FFN/MoE模块进一步解耦	激活与MoE通信	支撑模型模块跨资源池协同，提高MoE模型资源利用效率
超节点间PD分离	多超节点组成大规模推理集群	Prefix Cache与全局KV Cache通信	实现上下文状态跨实例共享，将KV Cache从单节点缓存演进为集群级资源

可以看到，Scale-Out网络承载的通信对象正在从传统的数据交换，扩展到模型状态、计算激活和上下文记忆，成为支撑AI推理集群规模化运行的关键基础设施。

Scale-Out网络的关键技术趋势

随着AI集群从千卡走向万卡、十万卡规模，Scale-Out网络正在围绕**规模扩展、效率提升和跨域互联**持续演进。

架构演进：从多级Clos走向多平面与扁平化组网

传统多级Clos网络随着规模扩大，会带来更多网络层级、更高互联成本和更大通信时延。多平面组网将一张大规模多级Clos网拆分为多个彼此独立的低层级子网，算力卡接口拆分后分别接入各平面，等效于把端口资源最大化地让给算力，同等端口开销下，可组网规模提升一个数量级。**核心价值：突破集群规模边界，让网络跟随算力持续扩展。**

通信优化：从静态转发走向智能调度

AI通信具有大带宽、高并发、流量模式复杂等特点，传统哈希负载均衡容易产生链路不均和通信瓶颈。网络级负载均衡通过感知全局流量状态，动

态优化通信路径；端网协同拥塞控制则通过网卡与交换设备协同，实现更低排队、更低尾延迟的传输。**核心价值：提升网络带宽利用率，保障Token生产的稳定效率。**

互联演进：从单数据中心走向跨算力域

面向大模型训练和互联网海量推理等场景，AI集群会进一步扩大，网络互联将可能突破传统数据中心边界。

一方面，传统电交换网络在万卡、十万卡规模下面临功耗和扩展压力，光路交换（OCS）开始进入超大规模AI网络。OCS通过在光域建立高速直连，减少传统交换层级，降低大规模互联的功耗和时延。但由于其连接模式更适合稳定、大规模流量，动态突发流量仍需要电交换承担灵活调度，两者将在未来长期协同存在。

另一方面，受限电力、土地和散热资源，算力正在突破单一数据中心边界，Scale-Across（跨园区、跨数据中心算力互联）成为新的发展方向。未来，头部企业将探索跨地域算力协同，更多企业则可通过跨园区推理多活和容灾提升AI服务可靠性。

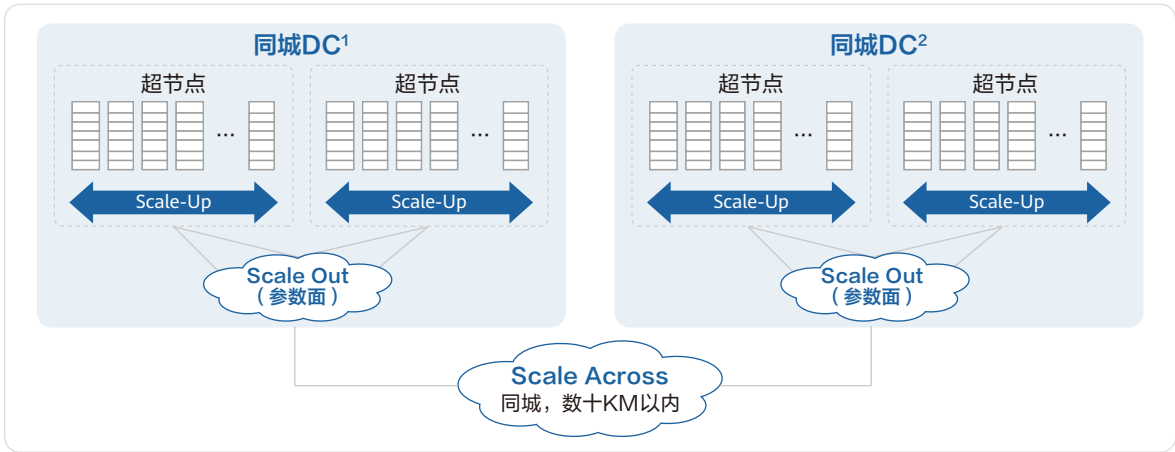


图2-21 跨数据中心算力互联

4、AI存储：算力集群的长期记忆

Agent时代，KV Cache正在成为影响推理成本和性能的关键手段。典型Agent任务包含多轮工具调用和上下文交互，后续请求通常复用大量已有上下文，仅追加少量新内容。这种“只增不改”的交互模式，使KV Cache具备极高复用价值。以AI

Coding为例，任务持续数小时甚至数天，上下文达64K、128K甚至百万Token级别，单任务产生的KV Cache可能达到数百GB甚至TB级别。**如何长期保存、共享和调度KV Cache，正成为AI Infra必须解决的新问题。**

KV Cache给AI基础设施带来的关键挑战

	关键挑战	简要说明
1	片上内存存不下	超长上下文（64K~1M tokens）导致单任务KV Cache高达数百GB甚至TB级别，超出片上内存容量
2	传统分级存储I/O时延高	数据从NPU到SSD需经过DDR、PCIe交换等多级中转，显著增加访问延迟，难以满足推理的实时性要求
3	SSD频繁擦写寿命短	KV Cache的频繁读写会严重加剧SSD的擦写磨损，每日全盘擦写次数（DWPD）可达10次以上，显著降低SSD使用寿命

• 层次化KV Cache：面向超长上下文推理，实现性能、体验、成本综合最优

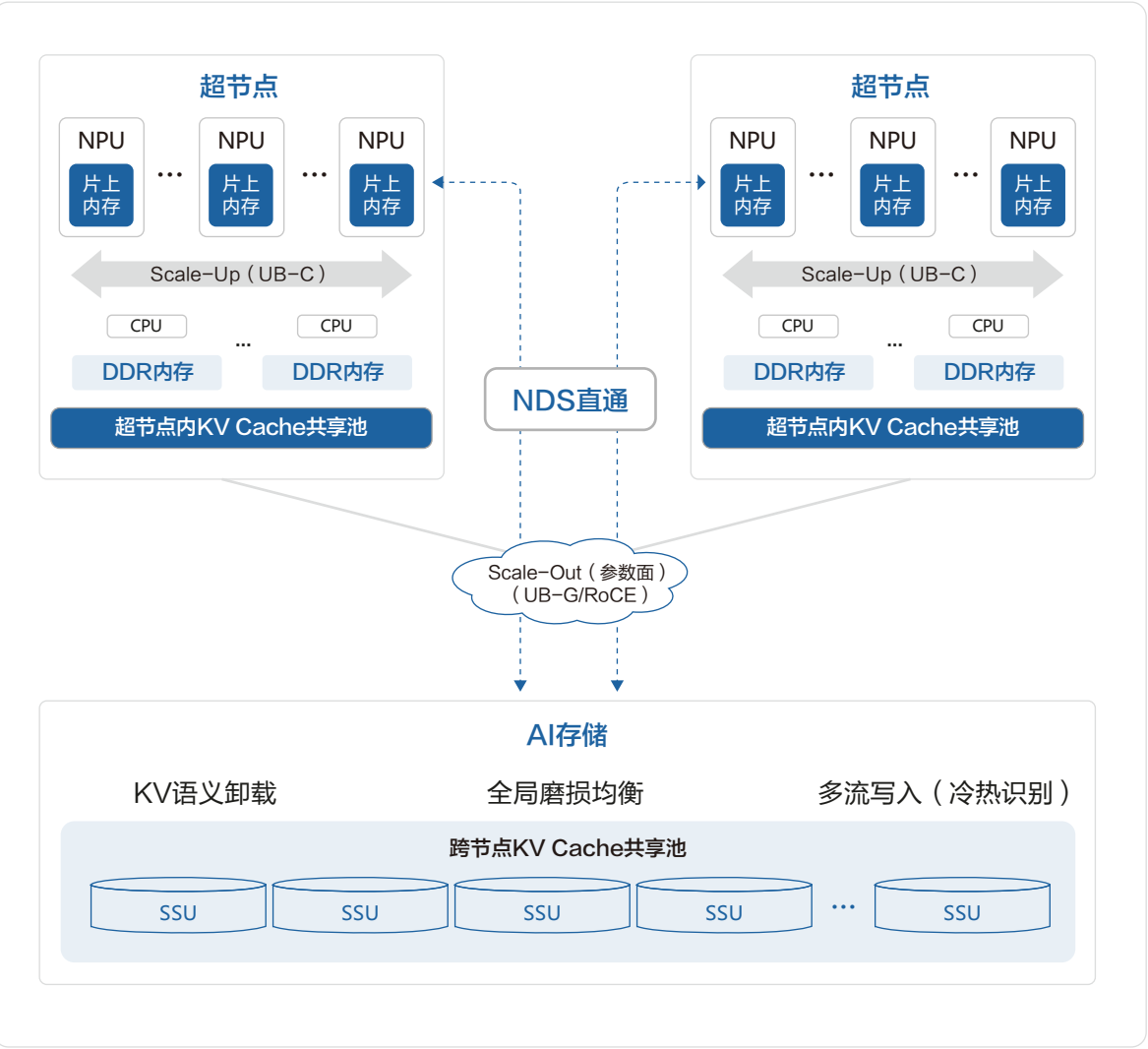


图 2-2 2 算网存协同的多级KV缓存目标架构

从局部缓存到全局层次化KV共享池

随着多级KV Cache体系形成，缓存管理能力将成为AI基础设施的公共能力。多个超节点之间可以共享KV Cache，使任意推理实例能够复用已有KV Cache，提高Prefix Cache命中率。

全局层次化KV Cache共享体系

层级	名称	容量	时延	承载KV Cache
L1	片上内存	数十~百GB级	纳秒级	活跃KV，承载当前推理实例正在使用的热数据，提供最低延迟访问
L2	DDR内存池	TB级	百纳秒级	热KV，承载短期会话上下文，缓解片上内存容量压力
L3	共享KV Cache池	数十TB级	微秒级	温KV，在超节点范围内复用上下文，实现跨实例缓存共享
L4	集群级AI存储	PB级	毫秒级	冷KV，提供跨超节点的持久化KV Cache 管理

KV Cache将根据访问频率和时延要求，在不同层级之间自动流动：热数据驻留高速存储（片上内存/DDR内存）、温数据进入共享缓存池、长期数据进入大容量存储。最终目标是：将分散在不同计算资源中的KV Cache统一管理，使上层推理服务无需关注KV Cache的物理位置，而能够像访问统一记忆空间一样调用企业级KV Cache能力。

从主机搬运到NPU-SSD直连（NDS）：缩短KV访问路径

传统架构中，KV Cache访问通常需要经过存储协议栈-主机CPU-内存多级搬运，增加访问时延和资源消耗。未来AI存储将通过AI芯片直通访问、KV语义卸载、内存语义协议等技术，缩短计算芯片与存储之间的访问路径，使KV Cache访问逐渐接近内存访问体验。

从SSD到SSU：提升存储介质寿命

SSD将向语义化存储单元（SSU，Semantic Storage Unit）演进，SSU感知KV Cache数据

语义，通过生命周期感知聚合与智能磨损均衡，将写入放大降低70%以上，使每日全盘写入次数（DWPD）从10次以上降至3次以内，存储寿命延长2~3倍。

对于长上下文Agent应用，决定推理成本的不仅是算力规模，更是系统能否持续保存、共享和复用上下文状态。在Agentic AI时代，具备统一上下文管理能力的AI Infra，将以更低成本、更高效率支撑持续性的智能生产。

5、通算资源：Agent的行动引擎

Agentic时代，AI基础设施形成新的分工：智算负责“思考”，通算负责“行动”。大量任务编排、工具调用、代码执行和环境交互，都运行在通用算力之上。

随着Agent进入企业生产环境，通算需要从传统业务服务器升级为Agent原生运行环境，具备以下四项核心能力。

01 一是快：高并发、毫秒级启动

Agent具有高并发、短生命周期特点，未来可能同时运行百万级任务实例。基础设施需要支持以“每会话一个沙箱”方式快速创建和销毁运行环境。

核心能力包括：

- 基于快照恢复实现毫秒级冷启动；
- 单机支持数百至上千Agent实例高密度部署；
- 大容量、高带宽内存支撑高并发状态运行。

这一需求推动通算从传统服务器走向超节点形态：只有具备大内存、高带宽和芯片间高速互联能力的系统级架构，才能支撑Agent规模化运行。

02 二是稳：从服务可靠到任务可靠

Agent任务正在从分钟级交互走向小时级甚至天级自主运行。前沿编码Agent单次连续运行已达到25小时，传统“服务99.9%可用”已无法满足长链任务可靠性。

未来通算平台需要具备：持久化执行、任务状态检查点、断点续跑与跨节点迁移、与AI存储结合的上下文长期保存能力。可靠性标准正在从“服务不中

断”升级为“任务必完成”。

03 三是安：强隔离成为Agent运行底座

Agent最大的安全风险来自模型自身的不确定行为，包括错误代码执行、异常工具调用和数据越界访问。未来Agent运行环境需要具备：microVM级强隔离沙箱、网络与权限默认隔离、会话级安全控制、全流程行为审计。

对于金融、政务、能源等行业，安全隔离与可审计能力将成为Agent生产部署的基础门槛。

04 四是融：通智存协同调度

Agent应用的执行过程天然跨越多个资源域：

通算资源：负责任务编排、工具调用和执行环境；

智算资源：负责模型推理与决策生成；

AI存储资源：负责上下文状态、知识和长期记忆管理。

未来AI Infra需要打通三类资源，实现统一感知和协同调度：

- 通算与智算协同调度，根据任务需求动态匹配计算资源；
- 计算与存储高效协同，降低上下文和状态访问延迟。

最终目标是让Agent的“思考、行动、记忆”形成统一运行体系，实现从资源调度到智能执行的一体化支撑。

未来展望：走向通智融合超节点

当前AI基础设施正在形成两类超节点：以NPU为核心的智算超节点，以及以CPU为核心的通算超节点。但Agent应用天然融合“思考”与“行动”两

个过程，未来AI基础设施的重要演进方向，是推动通算与智算资源进一步融合，通过统一架构和协同调度，形成面向Agent任务的一体化超节点体系。

至此，新一代AI算力集群的架构全貌得以呈现：

L3-算力调度：从建好到用好算力，高效释放超节点潜能

超节点突破了单节点计算边界，但也带来了新的资源管理挑战：当数百甚至上千张AI芯片形成复杂计算集群后，如何持续、高效地调度这些资源，成为释放AI基础设施价值的关键。

算力调度，就是超节点集群的“操作系统”。它通过资源池化、任务编排、弹性调度和故障管理，将底层算力转化为稳定、高效的Token生产能力。

面对企业级AI生产，调度平台需要解决三类核心问题：

- 资源高效利用：如何让不同规模、不同类型的AI任务共享超节点资源，提升整体资源利用效率；
- 负载动态适配：如何根据业务请求变化和模型运行状态，动态匹配计算资源，保障稳定服务能力；
- 集群持续运行：如何通过故障检测、任务迁移和资源恢复机制，保障大规模AI集群长期稳定运行。

1、弹性调度：让超节点资源“按需调用”

超节点提供了高密度计算能力，但企业AI负载具有高度不确定性：一方面，大模型训练和高并发推理需要数百甚至上千卡协同；另一方面，OCR、Embedding、语音、小模型推理等大量任务只需要少量资源。

因此，调度系统需要改变传统服务器时代“一次分配、长期占用”的资源使用方式，让算力能够根据

智算提供“思考”能力，通算支撑“行动”能力，AI存储承载“记忆”，高性能网络连接三者协同。未来，四者将进一步融合为面向Agent时代的新型AI基础设施。

任务需求动态伸缩和流动。

资源可伸缩：从固定规格到按任务分配

面向大规模任务，支持资源聚合：

- 多个超节点通过高速互联形成统一算力资源池；
- 支撑千卡级训练、大规模推理和跨节点PD分离。

面向小规模任务，支持资源切分：

- 超节点级：将数百卡超节点划分为多个逻辑资源域，支持多个业务隔离运行；
- 单卡级：通过vNPU等虚拟化技术，将单卡切分为多个计算实例，提高小模型资源利用率。

资源可流动：从静态占用到动态复用

AI负载具有明显潮汐特征：白天在线推理需求高峰，夜间训练、微调 and 数据处理任务占主导。如果资源长期固定绑定，容易造成高峰不足、低谷闲置。

因此，调度系统需要基于业务优先级实现动态资源复用：

- 核心生产推理任务获得确定性资源保障；
- 低谷时释放资源自动投入训练、微调等离线任务；
- 高优任务到来时，低优任务支持暂停、迁移或降级。

通过训推混部、潮汐复用和优先级调度，将时间维度上的闲置算力转化为有效Token产能。

2、高可用调度：让AI服务从“可运行”走向“持续运行”

超节点集群将大量计算芯片、高速网络和存储组成复杂系统，规模越大，单点故障概率越高。对于金融、能源、政务等关键业务，AI服务不仅需要运行，更需要长期稳定运行。

因此，高可用调度需要从单点保护升级为面向业务连续性的系统保障。

多级部署：控制故障影响范围

通过多层次资源隔离和冗余部署，实现故障隔离：

- 超节点内：通过多实例部署，降低单卡或模块故障影响；
- 集群内：跨超节点部署，抵御节点级故障；
- 数据中心间：跨地域部署，应对机房级灾难。

调度范围覆盖到哪里，故障隔离能力就延伸到哪里。

智能恢复：从故障恢复到业务连续

AI推理不同阶段的重要性不同，在PD分离架构下：

- Decode直接影响用户当前生成体验；
- Prefill主要影响新请求进入速度。

因此，面对资源波动或故障时，调度系统需要具备业务感知能力，例如采用“缩P保D”策略：

- 优先保障Decode持续运行；
- 通过降低Prefill资源弹性吸收短期冲击；
- 结合任务迁移、状态恢复和跨节点重调度，降低故障影响。

未来高可用目标，是让故障从“服务中断事件”变成“资源调整事件”。

3、智能调度：从资源管理走向AI生产优化

传统调度关注：哪些有空闲资源？AI时代需要进一步回答：“什么资源，在什么时间，以什么方式服务什么任务，能够产生最大业务价值？”

因此，调度系统正在从资源管理平台演进为AI生产优化系统。

感知：建立AI负载画像

不同模型、不同任务具有不同资源特征：计算密度、内存容量、内存带宽、通信模式。调度平台需要形成模型级、任务级算力画像，实现精准匹配。

预测：从被动扩容到提前规划

传统扩缩容依赖实时阈值。未来调度将结合AI预测：预测业务流量、提前准备资源、动态调整算力供给。从“看到需求再响应”，走向“预测需求提前布局”。

决策：面向业务价值的全局调度

未来企业可能同时拥有：多个超节点、多代算力资源。调度系统需要根据业务价值，在全球范围优化资源：高优任务优先保障、低优任务弹性运行、异构资源统一利用。

L4-AI服务平台层：Token生产闭环的最后一环

AI Infra的最终目标，是将底层计算资源持续转化为可交付、可运营的智能能力。超节点提供高效算力供给，算力调度提升资源利用效率，而AI服务平台进一步连接模型、数据与业务应用，完成从算力资源到智能生产的价值转化。

AI服务平台主要包括三个核心能力层：

模型运行服务：将算力转化为Token生产能力
通过模型部署、推理优化和运行管理，实现稳定、高效的模型推理服务；

数据基础服务：让Token具备企业知识能力
通过知识库、数据管理和上下文服务，将企业数据转化为模型可理解、可调用的智能资产；

Agent运行环境：让Token驱动业务行动
通过Agent框架、工具调用和任务编排，使模型输出进一步转化为业务流程和自动化执行。

三者共同构成从算力 → Token → 知识 → 行动的智能生产闭环，推动AI Infra从资源供给平台演进为面向业务价值创造的智能生产平台。

1、模型运行与服务：算力转化为Token的核心引擎

超节点提供高密度算力供给，模型运行与服务负责将这些计算资源转化为可持续交付的AI能力。这一层包括两个核心组成：

模型运行（Model Runtime）：决定Token生产效率；

模型服务（Model Serving）：决定AI能力交付效率。

二者共同完成从底层计算资源到企业级AI服务的能力转化。

模型运行：释放AI算力价值的核心软件引擎

模型运行主要包括推理引擎和训练引擎。

推理引擎负责将训练完成的模型转化为持续输出Token的生产能力。

代表技术包括MindIE、vLLM、SGLang等。其核心价值在于，在有限硬件资源下，通过模型优化、调度优化和软硬件协同，最大化Token生产效率。

随着大模型进入生产阶段，推理引擎正在从“模型执行工具”演进为“AI运行时平台”，主要体现在三个方面：

01 第一，从模型适配走向系统协同优化。推理引擎需要支持MoE、多模态、长上下文等复杂模型，并与超节点、网络、存储系统协同设计，实现端到端效率提升。

02 第二，从单实例优化走向集群级效率优化。通过PD分离、KV Cache管理、连续批处理等机制，提高整体吞吐能力，降低单位Token生产成本。

03 第三，从模型服务走向智能任务运行。随着Agent、多轮交互和复杂工作流兴起，推理引擎需要支持更长周期、更复杂的智能任务执行。

未来推理引擎竞争的核心，是单位算力能够产生多少有效Token。

训练引擎负责模型能力持续演进，是企业构建自身AI能力的重要基础。

代表技术包括 Megatron-LM、DeepSpeed、PyTorch FSDP 以及昇腾生态中的MindSpeed等。训练引擎的核心价值，是将大规模模型训练任务高效映射到AI集群，重点解决：大模型分布式训练效率、多卡多节点协同、内存占用和通信开销优化等。

未来训练引擎主要呈现两个趋势：**一是从一次性训练走向持续优化**。模型能力提升越来越依赖SFT、RLHF、Agent强化学习等后训练流程，训练引擎正在从“大模型训练工具”演进为“模型持续进化平台”。**二是训推边界逐渐融合**。强化学习等新型训练流程需要大量模型生成数据，推理引擎开始参与Rollout过程，训练和推理正在从两套独立软件栈走向统一模型运行平台。

模型服务：让模型能力成为企业级AI服务

随着企业进入多模型时代，模型环境快速复杂化：闭源大模型、开源模型、企业私有模型以及行业专用模型将长期并存。如果业务系统直接对接不同模型，会带来大量适配成本，也难以实现统一治理。因此，模型服务平台成为企业AI能力的统一入口。其主要承担四类能力：

模型统一管理与服务化。面向企业多模型运行场景，统一管理模型部署、发布、调用和运行环境，通过标准化服务接口降低业务接入复杂度，实现模型能力灵活复用。

智能路由与服务治理。根据模型能力、实时负载、资源成本和业务优先级，实现请求路由、灰度发布、限流熔断和故障切换，提高模型服务稳定性。

模型生命周期管理。统一管理模型上线、版本升级、效果评测和运行状态，使模型从一次部署进入持续运营阶段。

Token计量与成本运营。以Token作为统一计量单位，对模型调用规模、资源消耗和业务价值进行分析，实现AI资源投入的精细化运营。

未来，模型服务平台将成为企业AI能力管理和运营的核心入口。

2、数据基础服务：让Token承载企业知识

基础模型正在成为企业可获取的通用智能能力，而企业长期竞争优势将更多来自私有数据、业务知识以及持续反馈形成的数据闭环。数据基础服务连接通用模型与企业业务，为Token生产提供持续的知识供给，主要包括四类能力：

知识向量库：让模型理解企业知识。

将规章制度、产品文档、专家经验等非结构化知识向量化，支撑RAG，使通用模型具备企业专业能力。

图数据库：让模型理解业务关系。

企业知识不仅存在于文档中，还包含大量实体关系和业务规则。通过知识图谱和本体等方式，将企业对象、关系和业务语义结构化表达，并通过图数据库进行存储与计算，为模型和Agent提供可推理的业务知识。

向量检索解决“找到相关信息”，知识图谱解决“理解业务关系”，二者共同推动AI从信息检索走向业务推理。

长期记忆（Agent Memory）：让AI具备持续认知能力。

面向Agent长期运行场景，管理跨任务、跨会话积累的业务经验和上下文信息，使AI从一次性交互工具演进为持续参与业务流程的智能主体。

训练数据集：形成AI能力优化闭环。

沉淀业务交互数据、推理日志和人工反馈，形成高质量训练数据资产，推动“使用—反馈—优化”的数据飞轮。

前三类能力解决Token生成过程中的知识供给，让AI输出更加贴合企业业务；训练数据集则通过业务反馈持续优化模型能力，形成企业AI持续进化闭环。

3、Agent运行环境：让Token驱动业务行动

传统应用遵循“用户请求—系统响应”的模式，而Agent通过自主规划、工具调用和持续执行完成复杂任务。

在Agent架构下，智算负责推理和决策，AI数据服务提供上下文与长期记忆，通算环境承载工具执行

企业AI Infra规划建设重点方向

企业建设AI Infra，不能只关注当前算力需求，而需要面向模型持续演进和智能应用规模化落地，从资源弹性、Token高效生产和生产级韧性三个方向进行整体设计。

1、资源弹性：让算力投资持续适配未来变化

AI基础设施最大的投资风险，是建成后无法适应未来模型和业务变化。

和业务操作。因此，AI基础设施需要进一步支持智能任务的长期运行和规模化协作。

Agent运行环境主要承担三类能力：

安全执行环境：保障Agent可靠运行
Agent涉及工具调用、代码执行和外部系统访问，需要运行在安全隔离环境中。平台需要提供面向Agent和任务粒度的资源配额、权限控制和行为审计能力，确保智能任务执行过程可控、可追踪。

身份与权限治理：管理数字工作负载
随着Agent成为新的数字执行主体，每个Agent都需要具备独立身份，并遵循最小权限原则。企业需要将传统身份认证和访问控制体系扩展到AI主体，实现Agent的安全治理。

多智能体编排与生命周期管理：支撑规模化协作
当Agent从单体应用走向多智能体协作，基础设施需要提供任务编排、状态管理、资源隔离和成本控制能力，使多个Agent能够像企业团队一样协同完成复杂任务。

企业既需要支撑未来大规模模型训练、MoE推理和Agent集群，也需要满足部门应用、小模型推理等多样化需求。因此，AI Infra需要具备面向变化的资源弹性：

↑ · 向上扩展：通过超节点和集群能力，支撑更大规模推理和训练任务；
↓ · 向下切分：通过资源切分和隔离能力，满足不同业务需求。

最终目标是：让一次基础设施投资能够适应模型规模、业务形态和应用需求的持续变化。因为企业采购周期通常以年计算，而AI技术演进以月计算，只有弹性架构才能缩短两者之间的差距。

2、Token高效生产：让算力转化为有效智能

很多企业面临一个共同问题：算力投入不少，但资源利用率不高，业务仍然觉得算力不足。不能纯粹从AI算力利用率衡量，它既无法反映任务调度效率，也无法体现模型推理效率、状态复用能力和业务产出能力。

AI时代，企业需要从关注“资源使用率”，转向关注：单位算力能够持续产生多少有效Token。

提升Token生产效率，企业需要重点关注三个方向：



计算效率：提升单位算力输出
通过模型优化、并行计算和推理调度，让更多算力用于有效计算。



状态效率：减少重复计算
通过KV Cache、缓存和状态管理，让已有计算结果复用，降低长上下文和Agent任务成本。



系统效率：提升资源整体利用
通过统一调度、混部和资源编排，提升不同业务之间的资源协同能力。

最终，企业需要从关注：“算力利用率是多少？”转向关注：“单位投资能够产生多少有效Token？”。

3、生产级韧性：让AI成为可靠生产系统

当AI进入核心业务流程，企业必须回答：如果智能生产中断，会发生什么？AI时代的可靠性标准，正在从“服务不中断”升级为“任务不中断”。

企业级AI Infra需要具备三个层次的韧性：

第一层：实例可靠——保障单点故障不影响服务。
通过多实例部署、副本机制和自动切换，保障单个节点故障不会影响业务。

第二层：状态可靠——保障任务不中断。对于Agent、多轮交互等复杂任务，接口可用并不代表业务连续。需要保障：会话状态保存、KV Cache恢复、长任务持续执行，避免一次故障导致任务重新开始。

第三层：业务可靠——保障企业级连续运行。通过跨集群、跨地域部署和灾备体系，保障单一资源域故障不会影响核心业务。

对于金融、能源等关键行业，生产级韧性不是优化项，而是AI规模化应用的基础能力。

【小结】

AI Infra建设的核心目标，是构建面向智能生产的新型基础设施能力。未来企业之间的差距，将更多体现在算力、网络、存储和调度体系的整体协同能力，以及由此形成的高性能、大规模、高质量、可持续的Token生产能力。

随着AI从模型能力竞争走向规模化应用，AI Infra正在从支撑算力运行的基础设施，演进为驱动智能生产的新型生产体系。它将成为企业进入智能时代的重要底座，并支撑未来企业智能化竞争的核心能力。

2.3 Watt-Centric AI Facility

传统数据中心Facility的规划建设是基于“功率可预测、冷却可标准化、负载相对稳定”三个前提之上，AI时代这一确定性设计范式正在失效。

这是因为从AI芯片到AI机柜再到AI园区，算力的功耗在快速持续增长：单芯片功耗迈向kW级，单

机柜功率达到数百kW，算力集群从数十MW扩展到GW级别。一座GW级AI DC园区，用电负荷已相当于一个百万人口城市。该功率量级超出传统机房设计上限，电力供给不再只是配套工程，而是项目立项与建设方案的决定性前置要素。

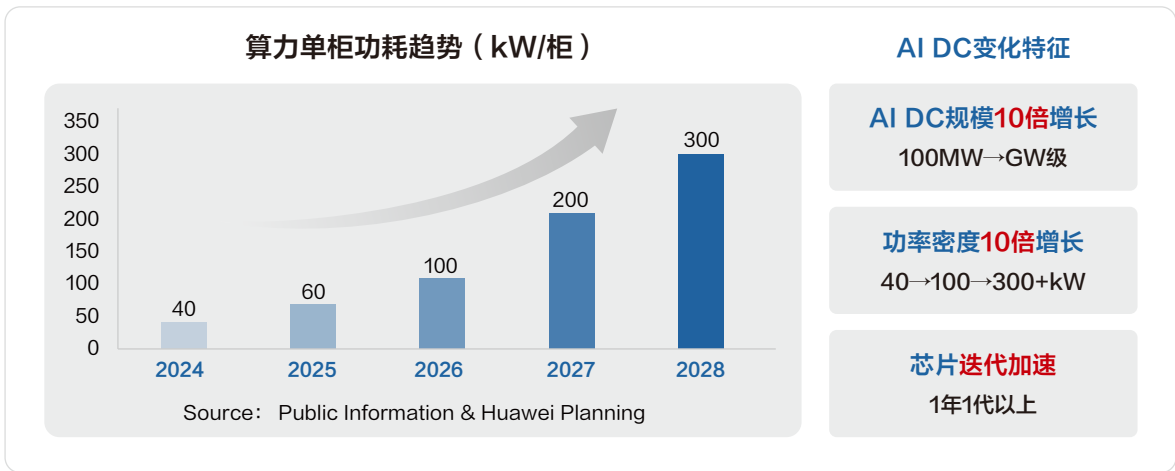


图 2-23 数据中心电力负荷趋势变化

面对这种变化，Facility设计需围绕能源、空间、时间三个维度重新思考：

- 选址以电力供给为第一优先级，通过源网荷储一体化平衡可靠性与成本；

- 机房布局与建筑结构原生适配超高功率智算集群；
- 规划建设以模块化预制缩短建设周期，大小机电解耦支持弹性部署，兼容多代算力演进。

AI Facility的系统性挑战

电力供给与质量：从园区配套上升为选址锚点

选址逻辑根本性重构。AI DC园区规模呈指数级扩张，选址逻辑已从过去的“以用户覆盖和网络时延为核心”，全面转向“以电力容量、电源结构、并网周期及长期供电稳定性为核心”。

源网荷储双向耦合挑战：随着新能源接入率持续提升，能源供给的波动性与不确定性有可能影响AI集群的稳定运行；与此同时，万卡级AI集群呈现高密度、高功率和强同步特征，其动态负载变化也会反向冲击电网稳定性。

供电：大电流输送的空间与可靠性代价

当单个AI超节点功率超过100kW，超节点集群规模攀升至数百MW量级。传统数据中心普遍采用的63A 三相供电回路，在承载能力上已捉襟见肘——为满足大电流输送需求，传统方案只能通过增加线缆数量与配电回路数进行补偿，这会引发连锁问题：机柜与桥架空间被大量挤占，线路铜耗与压降同步上升，配电节点增多也意味着故障概率的累积放大。

散热系统：液冷管网配置规划困境

智算时代风冷满足不了单柜功率诉求，液冷散热成为必然。如何规划液冷管网面临两难：建设初期如果管网、CDU和末端接口一次性固化，后续扩容就要大改；反之，如果完全按照远期最大流量配置，平时又会因“大管径、小流量”造成控制困难和额外能耗。行业需要可拆分、可动态调节的管路架构，让管路能力随算力需求逐步扩容，这对液冷提出全新的模块化和弹性化设计要求。

液冷还带来水力平衡、冷却液维护和泄漏等风险。液冷管线可达到十公里，任何局部堵塞、腐蚀或控制失配都可能形成热点。系统需持续监测流量、压差、温度、工质电导率和pH值，建立泄漏检测与工质健康度预测体系。

建筑结构：层高、承重成为核心挑战

随着液冷系统引入更大口径供回液管道，供电线缆截面持续增加，集群互联光纤规模快速增长，传统数据中心的层高、架空空间和机房布局已难以适应未来需求。

同时，超高功率AI机柜带来的重量增长，也对建筑结构承重能力提出更高要求。当前智算整机柜重量约16kN/m²，未来300kW以上超高功率机柜单柜重量将突破20kN/m²，已有标准里楼板荷载设计（8–12kN/m²）不再适用。

建筑主体生命周期通常长达50年。首期规划建设直接决定了未来基础设施的上限——承重、层高和主干路由，一旦建成很难改变。如何在初期决策中为未来不确定性留出余量，是建筑结构面临的核心挑战。

建设周期：工程交付跟不上算力迭代

当前智算硬件迭代节奏已压缩至一年一代，芯片功耗、机柜规格、集群互联方案持续更新，一次性定型的静态机房架构难以适配硬件快速更迭。传统土建主导的建设周期长达12–18个月，而行业普遍要求智算设施6–8个月完成交付，工期矛盾巨大。

除此以外，Agent推理业务负载具备很强的突发性，短时间内功率峰值可成倍波动，倒逼基础设施具备快速弹性扩容的能力。基建前期规划需要预留充足的调整空间，依靠弹性架构承接硬件迭代周期与业务负荷波动。

AI Facility规划建设建议

电力优先的园区选址逻辑与源网荷储协同架构

供电能力与长期稳定性是AI DC选址的首要决策因素。绿电富集地区因此成为大型AI DC园区的首选——不仅电力充沛，通常还兼具土地宽裕、碳排放约束宽松等叠加优势。

不同 AI 业务的电力诉求不同，选址需差异化适配：

- 大模型训练：负荷稳定、规模大，优先低廉充沛的电力；

- 离线推理：成本敏感，侧重电价与吞吐的平衡；

- Agent 交互式推理：在电价与访问时延间权衡；

- 边缘场景：用户距离与数据合规优先。

绿电富集区的核心痛点是新能源出力波动。为兼顾供电容量与电能质量，大型智算园区需构建源网荷储一体化架构——配套构网型储能、联动就近能源基地，实现新能源就地生产与消纳。构网型储能承担四项关键功能：

- 毫秒级响应，平滑新能源功率波动；

- 支撑微网电压与频率稳定；

- 吸收 AI 负载瞬时功率尖峰，削减对电网的反向冲击；

- 短时断电时无缝离网运行，保障算力不中断。

源网荷储不是万能的——储能投资高、新能源出力难预判。破局之道是能源管控与算力调度深度联动：弹性任务跟随电源峰谷错峰运行，刚性负荷优先保障稳定供电。归根结底，AI DC园区的选址与建设，是在“电力优先”逻辑下，在供电可靠性与长期用电成本之间寻求最优平衡。

供电架构从交流为主走向交流与高压直流并存

在保障电力供给规模与稳定性的前提下，供电架构需跟上高密算力的升级步伐。在中低密和存量场景中，交流供电产业链成熟、标准完善、运维经验丰富，仍将长期作为主流。面向300kW以上超高密机柜，传统交流方案的电流、线缆数量和配电空间压力急剧上升，800V高压直流凭借减少变换级数和降低线路电流的优势，成为重要演进方向。300kW是规划参考阈值，最终路线仍需综合服务器接口、可靠性、投资成本、标准规范及产业成熟度等因素确定。

800V直流主要有三种架构路径：

路线	基本架构	主要优势	适用考虑
集中式直流	变压器与集中式直流UPS统一部署，通过800V直流母线向多个POD或机柜供电	设备集中、系统成本相对更低，供电系统与IT功率密度解耦，便于容量池化和弹性演进	需要完善直流母线保护、故障隔离和运维体系，适合规模较大、规划相对统一的新建园区
分布式直流	交流电先送到机房或POD，再由靠近负载的直流UPS形成800V供电	故障域较小，扩容灵活，容易适配不同代际和不同功率机柜	设备数量和控制节点增加，需要统一接口、协同控制和全生命周期运维
SideCar方案	在超节点或高密机柜侧部署独立供电单元，以较短直流链路连接IT设备	与超节点结合紧密，部署灵活，可缩短末端供电距离	需要统筹机柜侧空间、散热、检修和多厂商接口，机电与IT协同要求更高

无论采用何种技术路线，800V 都是覆盖全链条的系统性工程：硬件层面涉及直流 UPS、高压锂电、高压母线、连接器、断路器及服务器电源的协同适配，产业层面则涉及标准制定、准入认证与运维体系的同步成熟。

构建风液同源、弹性管网和全链路可靠的散热系统

散热系统整体采用风液同源架构：前端冷源与一次侧管网统一规划，液冷与风冷共用冷源基础设施；末端根据机柜功率与设备类型灵活选择风冷、液冷或风液混合。机位同步预留液冷快速接头与风冷送风条件，使同一机房可弹性部署不同代际设备。

液冷侧按长期能力规划主管路，CDU 与二次支路

采用模块化、分区及可变流量设计，支持按POD逐步扩容。系统应持续监测流量、压差、温度、工质电导率与 pH 值等关键参数，对泄漏、断流、气堵等异常实现快速识别与自动隔离，并基于工质健康度趋势开展预测性维护，保障智算设备可靠运行。

风冷侧面向单柜 20kW 左右的高密散热需求，可采用以下两种方案：

方案一（双侧房间级空调）：在机房双侧部署大风墙，通过增加制冷末端数量提升散热能力。相比单侧房间级空调，双侧送风可缩小冷热通道宽度、降低天花回风高度，并提升机房空间利用率。

方案二（近端列间空调）：在微模块近端部署小风

墙，与智算设备同列就近部署，封闭热通道、冷量池化，无需回风天花。该方案对机房层高要求更低，但散热设备与智算设备混合部署，运维空间交叉较多，对运维管理要求较高。

建筑结构设计需要预留演进空间

机房承重设计：新建液冷算力机房，建议楼板承载能力按照20kN/m²及以上标准实施。

机房层高设计：面向300kW以上超高功率机柜场景，微模块内部架空地板1m，电力与光纤管线布设空间，叠加消防通道、回风夹层和顶部桥架预留空间约5m，建筑梁高约1m，综合测算机房层高建议不低于7.5m，或梁下净高不低于6.5m。

同时需预留整机柜搬运、设备更换和检修空间。主干电力和液冷路由应尽量独立、可扩展，避免不同专业在柜顶和地板下相互挤占——这也是运维安全和扩容效率的长期保障。搬运斜坡要求，斜坡坡度≤8°，斜坡宽度≥2.2m。

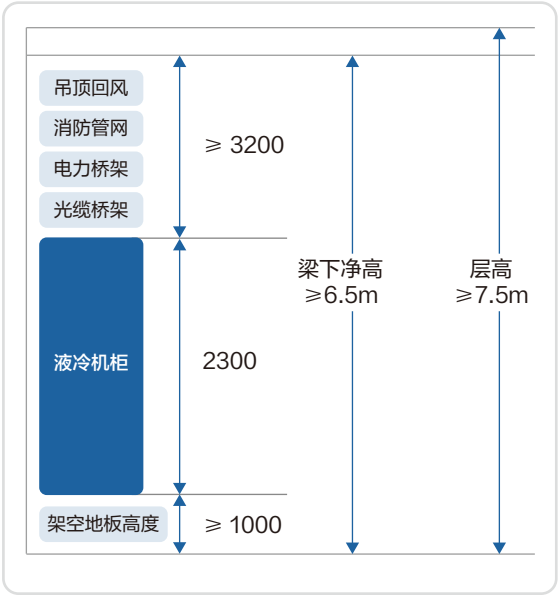


图2-24超节点对机房净空的推荐要求

通过预制化，模块化和产品化缩短交付周期

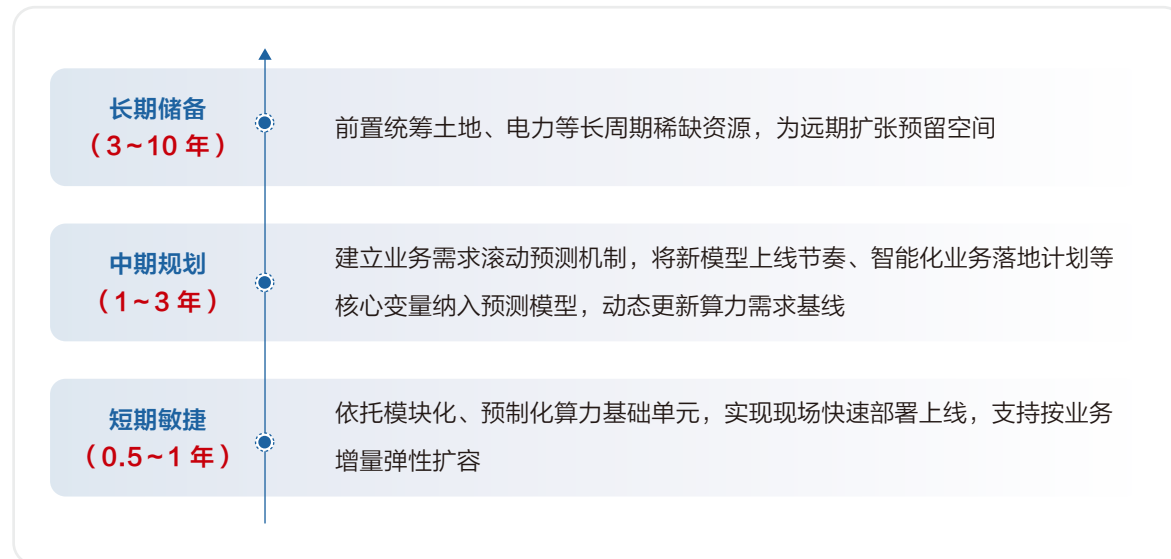
预制化和产品化是压缩建设周期的关键手段。AIDC应以POD为基本建设单元，将供电、储能、制冷和IT系统进行标准化设计。机电模块在工厂完成预制、集成和测试，现场主要完成吊装、连接和联调；服务器则尽可能采用整机柜交付，减少现场安装和调试。同时搭配AI辅助设计、数字化交付、仿真校验等手段，保障方案落地可行性。

从建设模式看，AIDC本质上是一套规模化算力生产系统，需要打通核心产品、设计仿真、标准接口、系统验证和数字制造。通过土建与机电并行、框架采购和滚动备货，依托工厂预制、现场模块化拼装，实现标准化复制建设，能够将传统土建12-18个月的建设周期压缩至6-8个月，加快算力资源投产速度。

AI Facility新建与存量场景落地

新建场景部署原则

针对算力需求波动大、硬件迭代快的行业特征，算力基础设施建设的三阶原则，实现基础设施供给与业务发展的动态匹配。



基于上述原则，新建项目可沿两类路径落地。

模式一（土建+大机电先行）：业务详细需求尚未完全明确时，结合预判的功率区间、风液配比，提前启动大型机电系统建设；待机柜规格、负载需求明确后再推进末端小机电实施，整体就绪周期可压缩至3个月左右。

模式二（土建+大小机电模块化预研、框架采购先行）：提前约一年完成机电系统标准化、模块化产品开发，同步开展框架采购、供应商滚动备货；业务需求正式确定后，约3个月即可完成现场交付落地。

弹性建设理念贯穿完整周期：长期阶段锁定稀缺资源边界，中期持续收敛需求方案，短期以标准化POD单元敏捷落地扩容。

存量场景改造

当前存量数据中心大多以低密风冷机房为主，普遍存在风冷向液冷升级条件受限、配电容量不足、楼板承重与室内净高不达标等多重约束。改造路径可参照以下三项硬性指标进行判定：

楼板承重 $\geq 12\text{kN/m}^2$

机房净高 $\geq 5.4\text{m}$

电力冗余不低于现有IT峰值负载的1.5倍

三项条件全部达标，具备改造为风液混合机房的基础；仅部分指标达标，优先部署高能效风冷服务器挖掘算力潜力；三项条件均难以满足，则建议有序关停、资源置换。存量改造的核心思路为“以高换低”，依托单机柜算力密度提升，用少量高密机柜替换大量低密机柜，盘活有限机房空间。

液冷改造方案需要结合项目规模灵活选型。小规模改造场景，可选用分布式ECU、风液CDU等分散式方案；中等规模改造项目，采用标准化液冷POD模块实施部署；冷源系统充分结合原有设施现状，因地制宜选择利旧改造或全新增设，优先选用预制集成冷站缩短施工周期。

供配电改造立足现有系统循序渐进推进，针对机柜末端配电回路进行专项升级。新增电源系统采用预制模块化产品，末端配电优先选用智能母线或智能列头柜，适配不同功率算力机柜。

此外，需提前复核楼板承载能力，通过结构加固或机柜稀疏排布满足荷载要求；层高受限项目利用BIM建模开展风险推演；同步借助仿真工具优化机房气流组织；同时保证场内设备搬运通道净高不低于2.5米，满足整机柜进场施工条件。

【小结】

Watt-Centric: 在物理约束中系统性地寻找最优解

数据中心的核心目标正在从“提供资源能力”转向“让每瓦特电力输出更多的有效Token”。对于AI Facility而言, 关键挑战在于如何以确定性的物理基础设施, 去承载能源供给、硬件演进和AI负载变化带来的不确定性。

未来 AI Facility 规划需要重新审视三个核心问题：能源如何高效供给、空间如何灵活演进、建设如何快速响应。解决之道在于从静态蓝图转向弹性架构，在洞察AI负载长期演进趋势的基础上，通过预留空间换取代际兼容能力，通过模块化设计支撑敏捷扩容，通过系统协同实现能源、空间与算力的最优匹配。

03

第三章

AI DC运营、运维与安全

“

长期以来，数据中心的价值在建成之日便已锁定；智能时代，它的价值在运营中持续生成。当算力成为按Token计量的智能产能，运营一座数据中心，第一次有了经营工厂的含义：计量产出、迭代工艺、守护安全。建成只是序章，运营决定价值。

3.1 AI DC智能生产运营

从算力资源运营到AI生产运营

随着大模型、Agent应用快速进入生产环境，AI DC运营从传统的资源运营（Resource Operation）演进为AI生产运营（AI Production Operation，AIPO），重点关注“生产什么、如何生产以及创造多少价值”。

IT保障型：需求→应用部署→资源分配→系统运维→服务保障

AI生产型：智能需求→模型编排→算力规划调度→模型推理服务→Token生产交付→质量评价→价值反馈→持续优化

从“资源保障”到“价值创造”

数据中心从传统“资源供给中心”跃迁为“智能生产中心”：

传统数据中心（资源保障导向）：以“保障资源可靠供给”为核心，主要关注计算资源供给、系统稳定运行和基础设施可靠性。

VS

AI DC（价值创造导向）：核心价值转向“持续创造AI生产价值”，面向智能能力的持续生产，关注如何以更高效率、更低成本、更优质量生成Token，并持续将其转化为真实的业务价值。

生产要素矩阵

在AI DC运营体系中，生产要素已从单一的 IT 硬件扩展为多元协同的资源组合，AI生产体系三层关系如图：

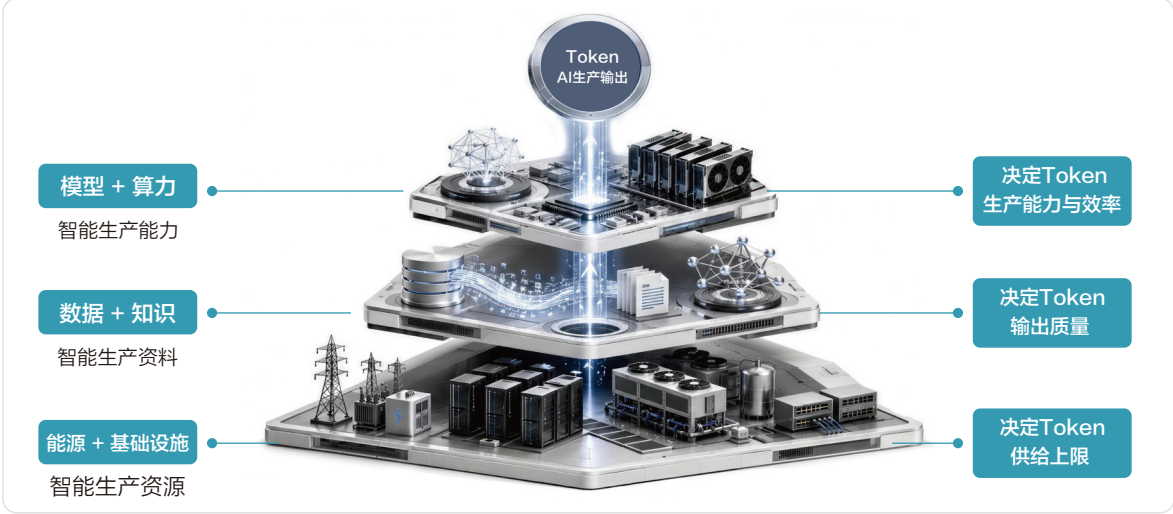


图 3-1 AI 生产体系结构

Token（AI 生产输出对象）：Token作为AI生产过程的核心计量单位，连接生产规模、资源消耗、服务质量与业务价值。

模型+算力（智能生产能力）：模型决定AI的能力边界，算力决定计算生产效率，两者共同决定Token的生成能力、生产效率。

数据+知识（智能生产资料）：作为AI生产的输入基础，直接决定Token输出质量和整体智能水平。

能源+基础设施（智能生产资源）：为AI生产提供电力、网络、存储和物理空间等全方位保障，决定Token供给的上限。

Token 智能运营流程与指标体系再定义

1、智能运营流程

AI DC以Token生产为核心，通过需求驱动、智能生产、价值反馈三个环节，构建从需求预测、能力

规划、资源组织、Token生产、价值呈现和价值评价的端到端智能生产运营闭环。

需求驱动与供给能力规划

AI DC建设规模不是简单依据当前业务负载进行资源扩容，而是综合考虑业务需求增长、AI技术演进趋势以及基础设施建设周期，通过前瞻性规划实现AI生产供给能力与未来智能化需求的精准匹配。主要包括：

AI需求洞察与预测：基于历史调用数据、业务发展趋势和应用规模变化，建立多维度AI需求预测模型，预测未来Token消耗规模和服务能力需求、算力资源需求、电力需求、机房需求等。

AI产能规划与投资决策：根据Token需求预测结果，制定长、中期规划，统筹算力池规模、模型能力建设、能源基础设施扩容以及投资收益评估等。

动态能力调整：在长期规划基础上，结合实际生产过程中的业务波动、突发事件、SLA保障和成本优化需求，通过弹性扩扩容、资源调度和潮汐优化，实现短周期动态规划调整。

生产要素组织与Token智能生产

围绕AI生产四类核心要素通过智能调度编排，实现生产要素协同和Token高效生成。主要包括：

智能生产要素编排**（模型+算力）**：根据AI生产计划，将生产要素精准匹配至目标业务场景，包括模型编排、算力编排、数据知识编排、能源编排等。

生产资料管理**（数据+知识）**：决定Token质量和领域智能水平的核心生产资料管理，包括数据质量运营、知识资产运营、数据价值评估、知识生命周期管理等。

生产资源调度配给**（能源+基础设施）**：通过统一调度和优化策略，实现模型服务弹性部署、高并发处理和低时延响应。

Token生产优化：围绕Token吞吐量、单位算力产出、单位能源消耗等指标，持续优化以提升AI生产效率。

价值反馈与持续优化

通过Token生产效果和业务价值反馈，驱动模型、资源和策略持续优化。主要包括：

Token质量评价：基于体验和业务适用性，评估AI输出准确性、可信度。

Token价值分析：结合业务任务完成效果、用户体验提升和业务收益，评估AI生产价值。

生产闭环和持续优化：基于Token质量、成本和价值反馈，持续优化模型能力、数据知识、资源配置和调度策略，形成生产闭环；通过企业智能资产沉淀增长形成：Token生产→数据沉淀→知识增强→模型优化→能力资产增长的持续优化的AI生产飞轮。

2、运营指标体系与价值映射

从资源指标转向生产价值，AI DC需要建立以Token为核心的新型运营指标体系：

指标类别	核心指标	价值说明
Token产能指标	Token产量、Token并发吞吐（TPS/QPS）	衡量AI生产规模
Token效率指标	Tokens/Watt	衡量资源生产效率
Token质量指标	准确率、可信度、幻觉率、响应体验（TTFT、TPOT）	衡量AI输出质量
Token成本指标	百万Token成本、单位任务成本	衡量生产经济性
Token资源指标	模型利用率、算力利用率、能源效率	衡量生产协同效率
Token价值指标	Token ROI、业务效率提升、业务贡献	衡量AI价值创造能力，如：AI Coding的成效，效率提升 × 质量保障 × 成本节约

AI生产运营五大核心能力

围绕智能运营，需要构建五大核心能力：

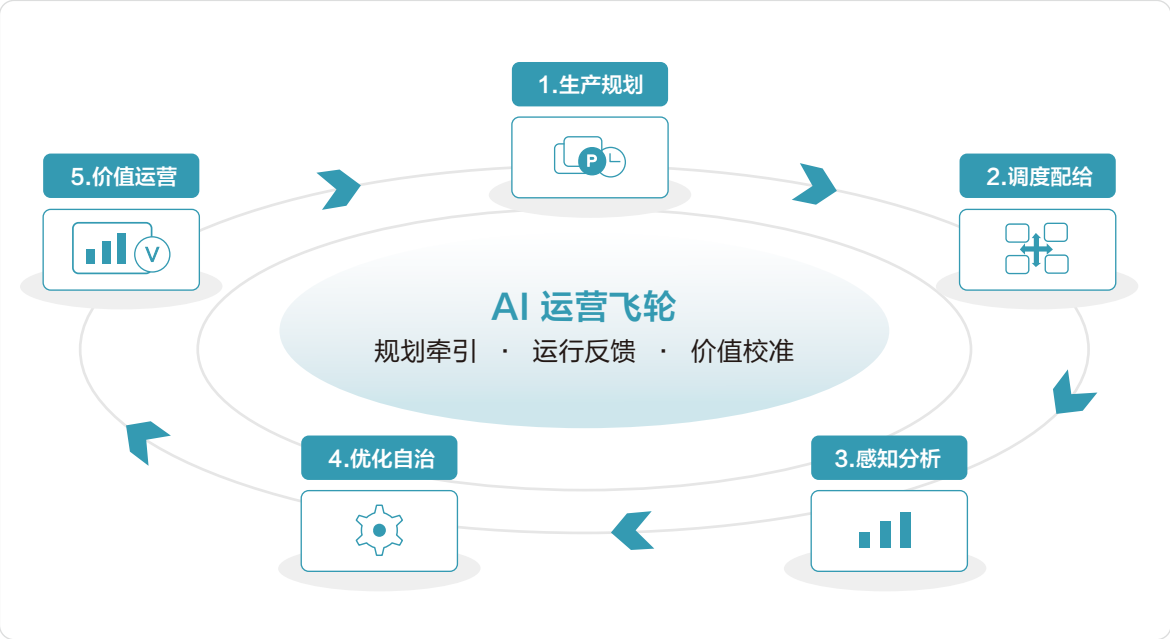


图 3-2 AI 生产运营五大核心能力

01 AI生产规划能力
——AI 产能长期演进滚动规划

面向业务需求、技术演进，建立长中短期产能滚动规划体系。

1、中长期产能前瞻布局

为了避免“业务等算力供给，算力等机房建设，机房等电力配套”互相迁延，需要依托历史运行大数据、宏观业务趋势与大模型演进，构建AI生产需求预测模型，科学开展中长期AI DC算力容量、电力容量、与配套机房基础设施规划。主要包括：

AI需求预测分析：围绕生产推理、开发测试等业务场景，基于业务发展趋势、应用调用规律和Token消耗数据，以Tokens预测未来AI服务输出需求。

智能生产产能预测：根据预测的未来Tokens生产目标，结合大模型演进、Agent发展、多模态应用以及计算架构等变化分析，评估未来几年的AI算力、算卡发展需求。

智能生产资源预测：需要站在未来几年算力、算卡生产支撑要求，综合规划电力资源、制冷资源、机房空间资源等基础设施保障资源，避免“建成即落后、建成即改造”。

产能规划与投资决策：统筹AI需求预测、产能预测、资源预测，结合当前供给能力分析差距，规划合理的数据中心布局、机柜/供电规划、改造/建设/租赁策略等。

2、短期弹性规划优化

弹性算力动态规划：针对业务波动、突发事件、SLA保障和成本优化需求，提升动态调度配给策略，实现短周期算力、算效提升。

- 业务波动驱动：应对日常潮汐流量，动态调整推理集群规模。
- 突发事件驱动：针对热点业务流量实现弹性算力冗余注入。
- SLA 保障驱动：为关键任务（Mission-Critical）预留最高优先级资源。
- 成本优化驱动：在低谷期自动缩减低利用率资源，最大化摊薄综合拥有成本（TCO）。

弹性基础设施规划：存量机房改造，升级适配新算力支撑要求，提升基础设施快速支撑能力。

02 AI生产调度配给能力——生产要素
智能组织与Token高效生产能力

通过智能调度、编排和生产资源协同优化，实现Token的高效生产。核心能力包括：

服务目录与配额管理：面向多元化业务部门与租户，提供标准化、可视化的AI服务目录。基于Token额度、并发上限与算力权重实施精细化配额管理。

异构算力统一调度：支持多元异构算力计算资源池化管理。

模型与算力协同优化：根据模型特点和业务需求匹配最佳计算资源。实现训练、微调 and 推理任务之间的资源动态分配。例如在推理低谷期自动释放算力转做模型微调或增量训练，大幅提升整体算力资产

的总体利用效率与运营经济效益。

能源与算力协同优化：结合能源成本、绿色能源供给和任务特点优化生产策略，实现多中心协同、全局算力经济效益最大化。

03 AI生产感知与智能分析能力——面向
Token生产全过程的智能观测分析能力

建立覆盖业务、模型、资源和基础设施的全链路感知体系，实现从应用需求到Token生产全过程的统一观测，发现问题、定位问题。主要包括：

全链路可观测：打通应用、Agent、模型服务、模型实例、算力资源之间的关联关系，实现全链路可观测。

核心指标监控：实时捕获Token消耗速率、每秒请求数（QPS）、首Token时延（TTFT）、每秒生成Token数（TPS）、内存碎片率、算力卡功耗等数十种指标。通过智能学习自动识别异常抖动，辅助运营人员秒级定位性能瓶颈。

Token生产深度诊断：聚焦单位算力与能耗下的Token产出效率，横向对比不同模型、不同量化精度下的经济产出比，找到短板。

模型性能深度诊断：深入剖析推理过程中的算子执行效率、通信开销、KV Cache内存命中率及批处理调度损耗。

资源利用率诊断：审视异构算力卡的计算单元空转率、内存带宽瓶颈及跨节点网络拥塞状况，为深度优化提供数据依据。

04 AI生产优化与自治能力——持续提升Token生产效率和质量

建立模型、资源和服务持续优化机制，通过生产数据反馈不断提升Token生产能力，实现同等资源生产更多、更优、更低成本的Token。核心能力包括：

模型效果优化与自治：通过数据回流、模型微调、强化学习等方式提升模型能力。

推理服务优化与自治：通过并发优化、KV Cache优化、调度策略优化提升服务效率。

生产效率优化与自治：围绕Tokens/Hour、Tokens/Watt等指标持续提升单位资源产出。

05 AI生产价值运营能力——从Token生产到业务价值闭环

建立从Token消耗、服务质量到业务收益的价值评价体系，实现生产结果与业务价值关联。核心能力

包括：

Token成本治理：分析单Token成本、单位任务成本，实现AI生产成本透明化。

Token质量评价：评估准确性、可信度、幻觉率和用户体验。

业务价值分析：衡量AI应用效率提升、业务贡献和投入产出比。

价值反馈优化：根据业务效果反向优化模型、数据、资源配置和生产策略。

通过五大核心能力建设，AI DC从传统“资源管理中心”演进为面向智能时代的“Token生产价值中心”，实现需求驱动能力建设（生产规划能力）、资源协同智能生产（生产感知与分析能力、生产资源调度配给能力、生产效率与质量优化能力）、价值反馈持续优化（生产价值运营能力）。

案例实践：银行AI DC价值运营升级

随着人工智能战略深入企业核心业务，某头部银行持续推进AI能力规模化应用，已上线数百项AI应用场景，人工智能逐步融入客户服务、经营管理和业务创新全过程。随着AI DC进入规模化生产阶段，运营重点也从早期关注“有没有算力、能不能上线”，转向关注“AI生产是否透明、资源是否精准、Token生产是否高效、智能价值是否持续提升”。

面临挑战：

资源不可视：基础设施与上层应用之间缺乏全局联

动视角，资源消耗与业务产出难以精确关联。

预测规划难：长期容量规划和日常资源配置多依赖人工经验估算，难以精准匹配动态变化的业务需求。

瓶颈定位难：在复杂的多维负载下，难以高效定位服务瓶颈，单位算力的产出效率仍有提升空间。

资源利用率低：调度方式多依靠人工经验，缺乏基于数据驱动的自动化潮汐调度与弹性优化能力。

创新举措：



图3-3 某头部银行智能化运营体系实践

- 构建AI生产全链路感知能力，实现生产过程可视：通过AI生产运营平台，打通“应用—Agent—模型服务—模型实例—算力资源”全链路视角，实现AI生产过程统一观测。重点实现Token消耗量可视、算力利用率可视、服务性能可视，通过建立以Token为核心的生产指标体系，实现从“资源状态监控”向“AI生产效率分析”的转变。
- 构建需求驱动的AI产能规划能力，实现资源精准配置：针对AI业务快速增长和资源需求难预测的问题，建设算力仿真与容量评估能力。基于业务SLA、并发规模、吞吐需求、响应时延以及输入输出长度等关键参数，对模型服务所需资源进行建模分析，生成满足业务目标的最优资源配置方案。模型上线前：科学评估算力需求，避免资源过度申请；

生产运行中：根据业务变化动态调整资源规模；性能优化时：通过参数寻优提升资源利用效率；从而推动AI生产能力建设从经验估算转变为数据驱动的模型化规划。

- 构建模型持续优化能力，提高单位算力Token产出效率：针对大模型推理过程中计算、通信、内存和调度等复杂性能问题，建设模型性能分析与优化能力。通过模型运行分析，从服务指标、计算负载、通信效率、算子执行和内存使用等维度定位性能瓶颈，并结合模型参数优化、推理框架优化和资源配置优化，实现模型服务持续提升。推动单位算力Token产出提升、模型响应效率提升、AI生产成本降低。

构建智能调度能力，实现AI生产资源动态优化：AI业务负载具有明显潮汐特征，通过业务负载预测、资源分析和智能调度，实现训练与推理资源动态调用。具体包括：推理低峰期释放资源用于训练和优化、高峰期自动扩展推理服务能力、基于SLA和业务优先级动态调整资源，实现从人工经验调度向数据驱动的智能调度演进。

AI生产运营演进路线

未来，AI DC运营需要围绕Token生产效率、智能服务质量和业务价值创造能力构建新型运营体系。AI DC生产运营成熟演进可划分为四个阶段：

演进阶段	核心对象	核心目标	关键能力
资源保障运营	IT 资源	稳定运行	资源管理、故障保障、容量管理
AI 生产运营	Token 生产过程	高效生产智能能力	DPV 闭环、生产要素协同、Token 效率优化
Token 价值运营	Token 价值	创造业务价值	质量运营、成本治理、价值评估
Agentic 自治运营	AI 运营智能体	自主优化运营	自主规划、自主调度、自我进化

阶段一：资源保障运营，该阶段以传统数据中心运营体系为基础，主要关注计算、存储、网络和基础设施的可用性与可靠性。该阶段解决“有没有资源、能不能运行”的问题。

阶段二：AI生产运营，核心目标是提升AI生产效率，实现Token规模化生产，随着AI应用进入生产阶段，运营重点从资源保障转向AI生产过程管理，通过DPV（Demand-Production-Value）模式实现生产闭环。该阶段解决“生产什么、如何生产、生产效率如何”的问题。

阶段三：Token价值运营，核心目标是实现AI生产

实践成效与综合价值：

通过上述能力建设，整体算力利用率提升10%，从“被动排查”转为“按指标主动经营”；模型性能分析效率**天级→小时级**，以Qwen大模型推理为例：TPS提升**30%**，TPOT下降**30%**，问题定界闭环效率提升**70%**以上。推动AI DC从资源运营向价值运营持续转型演进。

结果与业务价值闭环，随着企业AI应用深入核心业务，AI DC运营需要进一步关注Token产生的业务价值，实现从“生产Token”向“创造智能价值”演进。该阶段解决“生产的智能是否有价值”的问题。

阶段四：Agentic自治运营，核心目标是实现AI DC自主规划、自主优化和自主运营。随着AI Agent能力成熟，AI DC运营将进一步由人驱动转向智能体驱动，形成具备自感知、自决策、自执行、自优化能力的自治运营体系。该阶段解决“如何让AI DC自主创造和持续提升智能生产能力”的问题。

最终构建起以Token为核心计量单位，以模型、数

据、算力、能源为核心生产要素，以 DPV 构筑全链路运营闭环，以 Token 价值最大化为核心运营

目标，以 Agentic 自治为长期演进方向的下一代 AI DC 运营体系。

3.2 AI DC自治运维保障

从设备运维到智能生产运维保障

AI DC运维目标从保障设备可用升级为保障算力-模型-Token-应用全链路稳定运行。相较于传统数据中心，AI DC运维面临四项核心挑战：

基础设施复杂度显著提升：智算集群算存网深度融合、网络高速互联、基础设施算冷协同等新技术、新方案层出不穷，这使得故障定位、性能优化及资源调度的专业门槛大幅提高。

运维对象与保障范围变化：传统数据中心运维聚焦基础设施、软件平台与业务应用。AI DC运维面向三层新架构：AI基础设施层保障算力与能源供给，AI Infra层承载模型推理与算力调度，AI应用层交付Agent与智能业务。运维目标随之从单设备健康监控，延伸至算力效能、Token服务质量与业务价值保障。

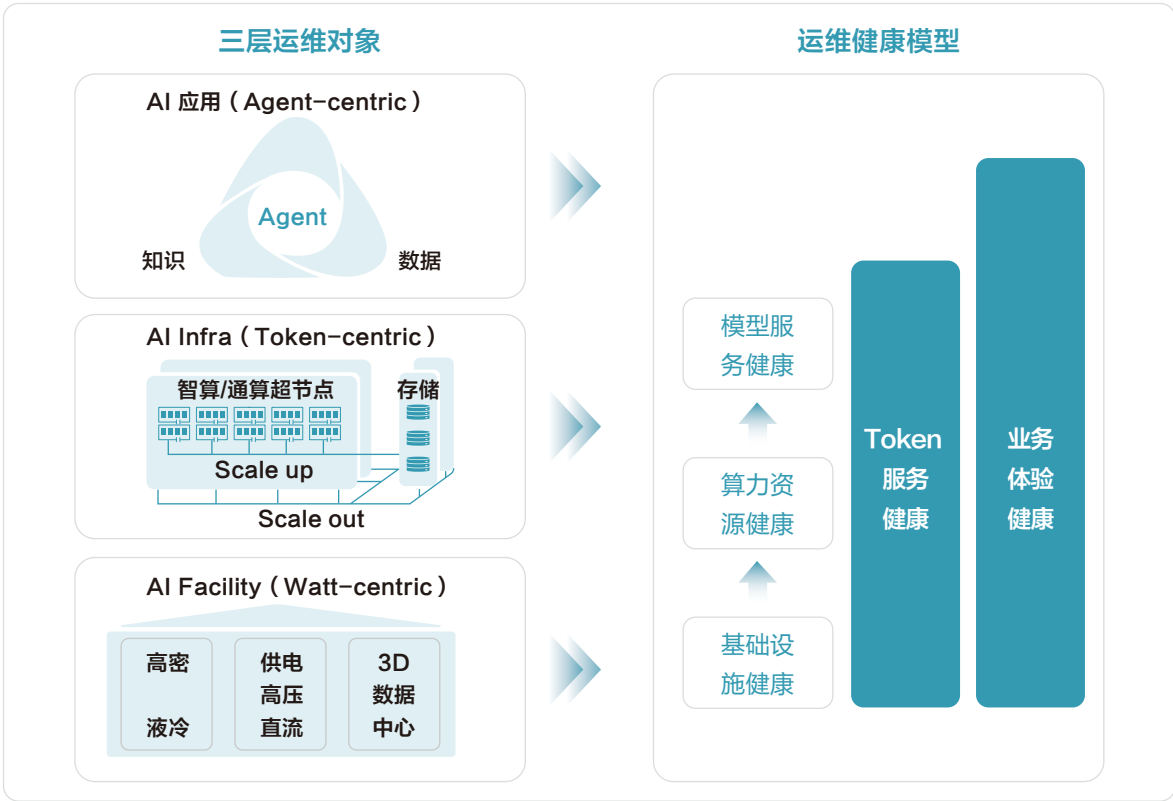


图 3-4 数据中心运维对象与保障范围演进

系统链路加长与跨层关联复杂：从资源供给、AI Infra支撑到Agentic业务执行，端到端智能生产链路中任一环节异常均会导致服务降级。例如，电网调度Agent响应延迟、新能源预测准确率下降或缺陷识别异常，均亟需跨层关联分析与端到端根因定位能力。

Agentic自治运维六大核心能力

面对智算集群复杂的设备与业务协同，依赖人工监控和经验处置的传统运维模式，已无法满足AI生产高可靠、高质量的要求，AI DC需构建Agentic自治运维体系，实现“**业务可感知、问题可预判、故障可自治、能力可进化**”。

01 全域智能感知

过去的数据中心运维主要盯着服务器、网络 and 存储这些基础底座。AI时代，运行对象已经延伸至Token生产和上层Agent业务。要想把整个AI DC的运行状态看透、看准，首先需要打破传统的数据孤岛。

核心能力解析：

- **统一度量，建立全域运维指标体系：**构建覆盖机房基础设施指标、AI Infra运行指标、Agentic业务体验指标的运维指标体系，实现从设备健康、算力利用率，到模型服务质量、Token服务效率及业务体验的统一度量。

- **多源数据统一采集，建立全链路运行数字画像：**深度融合指标数据、日志数据、链路数据、拓扑关系以及配置变更数据，勾勒出AI DC的全链路运行数字画像。

- **全域对象建模，动态状态映射：**覆盖基础设施对象、算力、网络与存储资源、模型服务、Token服

可靠性要求严苛与故障模式多样：AI DC需保障高算力可用率与快速响应。故障已从硬件层面延伸至通信、内存、调度与推理质量等新型问题，人工运维难以支撑海量监控与自愈需求。

务及Agent业务流程，实现AI DC运维对象的统一管理。实时同步底层资源状态、关键性能指标、服务运行状态及上层业务体验，勾勒出AI DC的实时运行数字画像。精准建立资源依赖关系、服务调用关系与故障传播路径，强力支撑故障影响分析和潜在风险预测。

这套感知体系让AI DC的运行状态真正做到了“看得见、看得全、看得准”，把被动救火变成主动感知，为后续的自治运维准备了不可或缺的实时数据基础。

02 业务健康评估

传统运维盯设备可用性，只看“坏没坏”；AI运维盯服务质量，要问“快不快、好不好”。首Token时延、端到端响应、请求成功率等，已成AI服务的核心命脉。

核心能力解析：

- **端到端体验度量：**构建贯穿业务应用、Agentic服务、AI Infra、模型服务直至算力资源的全链路体验指标体系，重点对“首Token时延、推理端到端时延、请求成功率及服务稳定性”进行健康度量。

- **跨层体验关联分析：**深度打通业务体验与底层资源之间的内在关联，实现业务异常快速发现、模型问题精准定位以及算力资源联动分析。

健康评估，自动优化治理建议：实现系统健康评分、风险趋势预测及性能退化分析。依托历史运行基线与高精度健康评估模型，实现指标异常识别、趋势变化分析，以及硬件退化、性能劣化、资源瓶颈等潜在风险识别。借助智能分析技术，实现秒级体验劣化发现、自动根因定位、优化建议生成及服务质量的持续迭代提升。

这种转变让运维彻底告别了“只管机器不管业务”的盲区，确保Token服务高效可控，为大模型的商业化落地提供了坚实的体验护城河。

03 运维知识体系与本体构建

AI DC故障定位深度依赖专家的实战经验，如果缺乏统一的认知沉淀，智能化就成了无源之水。

核心能力解析：

- **运维知识体系建设：**利用AI技术自动从海量运维文档、故障报告、历史操作记录与专家经验中萃取高价值知识。系统化构建SOP知识库、RAG知识库、故障案例库与专家经验库等，实现海量知识的统一管理和智能调用。

跨域知识融合，有效打通算力、网络、模型、业务与安全等多元领域知识，构建企业级运维的统一认知网络。

外部产业生态接入：积极引入外部智算产业链的公开经验、第三方最佳实践、开源故障案例库及行业标准规范，与内部运维实践相融合，大幅拓宽知识广度并加速整体学习演进效率。

- **Skill能力体系建设：**将专家实践能力封装为标准技能，全方位支撑运维智能体的快速组合调用。
 - 感知类Skill涵盖日志分析、指标分析、异常检测等；
 - 诊断类Skill涵盖告警关联、根因分析、网络诊断、集群通信分析等；

- 执行类Skill涵盖参数调整、服务恢复、资源调度等

- **运维本体模型建设：**实现资源关系建模、服务依赖建模、故障因果建模与业务影响深度分析。系统性构建**资源本体、服务本体、故障本体、操作本体及业务影响本体**等，定义规范对象属性、关联关系和运行规则。

以某头部银行为例，其流程通过对业务价值链进行细化，从业务活动到规则逐层拆解，厘清各运维环节的内容、边界、参与方与核心逻辑；知识模型则聚焦关键运维信息，开展要素识别、主题分类与标准化建模，明确知识归属与标准，保障多系统数据知识一致性，在变更、监控、保障、事件等场景中逐步落地。

- **知识自动回收：**通过知识回收Agent，将实践诊断过程、根因结论及处置方案自动沉淀并反哺至知识体系。

这让AI真正具备了行业专家的专业认知，实现专家经验的大规模复制。

04 智能运维编排

虽然当前在监控、诊断和自动化执行上已经具备了很多单点工具，但如果将其简单堆砌，依然是各行其是、形同割裂。如何让这些大大小小的能力协同工作，是自治运维能否落地的关键。

核心能力解析：

- **运维意图理解：**支持通过自然语言描述运维目标（例如：“分析当前模型推理延迟升高的底层原因”），系统自动理解任务目标并生成分析路径。

• **任务智能拆解**：基于大模型对用户意图的深层理解，自动将运维目标拆解为粒度合适的子任务（如：Agent选择、Skill调用、模型调用等）、规范执行流程以及清晰依赖关系，构建动态执行任务流。

• **Agent协同调度**：支持顺序编排、并行编排、分层编排及多Agent网状协作，实现不同专业领域的Agent动态协同。专业领域的Agent包括：

- 感知智能体**：负责全域状态监测、异常精准发现与潜在风险识别。
- 诊断智能体**：负责高效故障定位、深层根因分析及处置方案生成。
- 预测智能体**：负责系统健康评估、趋势预测及风险超前预警。
- 恢复智能体**：负责任务作业自动执行、服务平稳恢复及执行效果验证。
- 知识智能体**：负责知识智能萃取、历史案例沉淀及底层能力增强等。

• **人机协同控制**：全面支持方案确认、高风险操作人工审批、执行过程监督及效果客观评价。

• **运维闭环管理**：打通发现、分析、决策、执行、验证到知识沉淀的全过程管理闭环。安全执行控制，建立严格的权限控制、风险评估与自动回滚机制，全方位保障智能体行为安全可控。

通过编排，原本孤立的运维工具、智能体形成了一个高效的智能协作网，让发现、分析、决策和执行的全流程能够全自动闭环。

05 智能诊断与自治恢复

智算集群算力、网络、存储和模型服务高度耦合，一旦发生故障，靠人工排查和口口相传的经验根本来不及响应，业务连续性极易受到冲击。

核心能力解析：

- **智能故障分析模型**：聚合指标、日志、拓扑、链路等多源数据，实现精准的异常模式识别、深度根因推理、故障自动分类及影响范围分析。
- **智能诊断决策**：结合SOP知识、RAG知识库与运维Skill，智能生成诊断和处置方案，全面支持故障的自动诊断与复杂故障的专家辅助分析。
- **自治恢复执行**：依托故障闭环Agent与智能编排能力，实现恢复动作自动生成、执行工具自动调用、恢复效果自动验证及异常自动回滚。

推动运维模式实现从事后抢修到事前预防、从人工排障到人机协同、系统自治的跨越。

06 持续学习与自进化

AI DC的运行环境、大模型架构和上层业务时刻在变，如果运维系统一成不变，很快就会落伍。因此，必须建立一套自我进化的机制。

核心能力解析：

- **知识动态演进**：紧密结合内、外部新发生的故障案例、运维反馈及实际执行结果，对底层的知识体系进行持续优化。自动采集故障处理全过程、专家决策过程及实际执行结果，转化为新的企业知识资产。
- **模型能力增强**：依托知识约束与领域本体深度赋能大模型推理，有效降低幻觉发生率，显著提升诊断准确性与专业能力。基于实践案例、一线运维反馈、厂家经验及业务效果，不断迭代优化领域模型能力。

• **Agentic能力进化**：持续优化Agent任务规划、Skill组合策略及推理决策准确性。

这就让运维体系拥有了类似生命体的进化能力，在“运行感知—智能分析—自主决策—自动执行—反馈学习—能力增强”的循环中不断成长。

Agentic自治运维能力体系

能力模块	核心能力点	建设目标与核心成效
全域智能感知	全域指标体系、多源数据采集、动态状态映射	“看得见、看得全、看得准”，被动救火变成主动感知
业务体验保障	端到端体验度量、跨层体验关联分析、健康评估模型，自动优化治理建议	告别了“只管机器不管业务”的盲区，让AI服务质量可衡量
运维知识体系与本体构建	运维知识体系、Skill能力、运维本体模型、知识自动回收	让AI具备领域专业认知，实现专家经验规模化复制
智能运维编排	运维意图理解、任务智能拆解、Agent协同调度、人机协同控制、运维闭环管理	让人+Agent高效协同，构建系统级智能调度中枢和人+AI协同环境
智能诊断与自治恢复	智能故障分析、智能诊断决策、自治恢复执行、预测性预防	从人工排障到人机协同、系统自治的跨越
持续学习与自进化	知识动态演进、推理模型能力增强、Agentic能力进化	让运维能力持续自适应成长，打造AI原生进化闭环

协同共建六大核心能力，推动AI DC运维完成深刻变革：从传统的“设备运维”迈向“智能生产运

维保障”，从过去的“人工靠经验”全面升级为“Agentic自治运维”。

Agentic自治运维参考架构

大模型与Agent加速融入核心业务，AI DC已演进为智能生产基座。Agentic运维参考框架，融合领域孪生体、知识与本体、模型、智能体、智能协作工作坊，实现从感知到执行的端到端闭环。



图 3-5 AI DC Agentic运维参考架构

领域孪生体：构建AI DC全域动态映射

领域孪生体是AI DC Agentic运维架构的运行感知基础，通过对物理基础设施、算力资源、模型服务、Token服务以及业务应用进行数字化映射，构建真实运行环境与智能运维空间之间的动态连接。实现AI DC从“资源可见”到“系统可理解”，为Agent智能分析和自治决策提供坚实的实时运行基础。

领域知识与本体：构建AI DC运维认知底座

领域知识与本体是Agent理解AI DC业务和运维逻辑的底层支撑。通过对资源、服务、故障、流程和专家经验进行结构化、半结构化表达，将传统人工经验转化为机器可理解、可推理的知识体系。

领域模型（Domain Model）：构建专业智能推理能力

领域模型是AI DC Agentic运维的智能分析核心，通过融合实时运行数据、领域知识和专家经验，实现面向运维场景的专业推理和预测分析。这一模块推动运维从传统的规则驱动向模型推理驱动彻底转变，实现复杂场景下的智能分析与主动超前预测。

领域智能体（Domain Agent）：构建自治运维执行主体

领域智能体是Agentic运维体系的核心执行单元，通过协同调用领域模型、知识体系和标准技能能力，实现复杂运维任务的自主分析与落地执行。通过多智能体的深度协同，实现从单点自动化工具向集群化自治体系的全面升级。

智能协作工作坊（Agentic Operation Workspace）：构建人机协同运维工作空间

智能协作工作坊是运维人员与Agent交互协同的统一工作空间，通过自然语言交互、智能编排和能力调用，实现复杂运维任务的高效闭环。智能协作工作坊有效推动运维人员从繁重的“操作执行者”向宏观的“智能系统监督者和策略管理者”转变。

持续学习闭环：驱动Agentic运维能力持续进化

AI DC运行环境处于持续动态变化中，底层设备架构、大模型版本、业务场景和故障模式等不断演进，建立长效的持续学习机制，最终实现AI DC从“故障恢复”向“风险自治”的能力升级。

案例实践：Agentic运维智能定界与快速恢复

金融AI DC承载支付清算、核心账务、资金交易等关键业务，具有链路长、耦合深、容错要求高、监管严等特点。随着算力复杂度提升与业务智能化演进，传统依赖人工经验与静态规则的运维模式已难以满足7×24小时高可靠要求，存在故障发现慢、跨层定界难、根因定位依赖专家、恢复耗时长等瓶颈。

为此，某头部金融机构开展了本体驱动Agentic实践，以运维领域本体为认知基础、数字孪生为映射引擎、多智能体为执行主体，构建“感知—分析—决策—执行—学习”闭环。通过故障感知智能体实时捕获全局状态，结合数字孪生仿真推演，打通基础设施、算力、应用与业务链路间的数据关联，实现故障发现、分析与处置的全流程智能化。

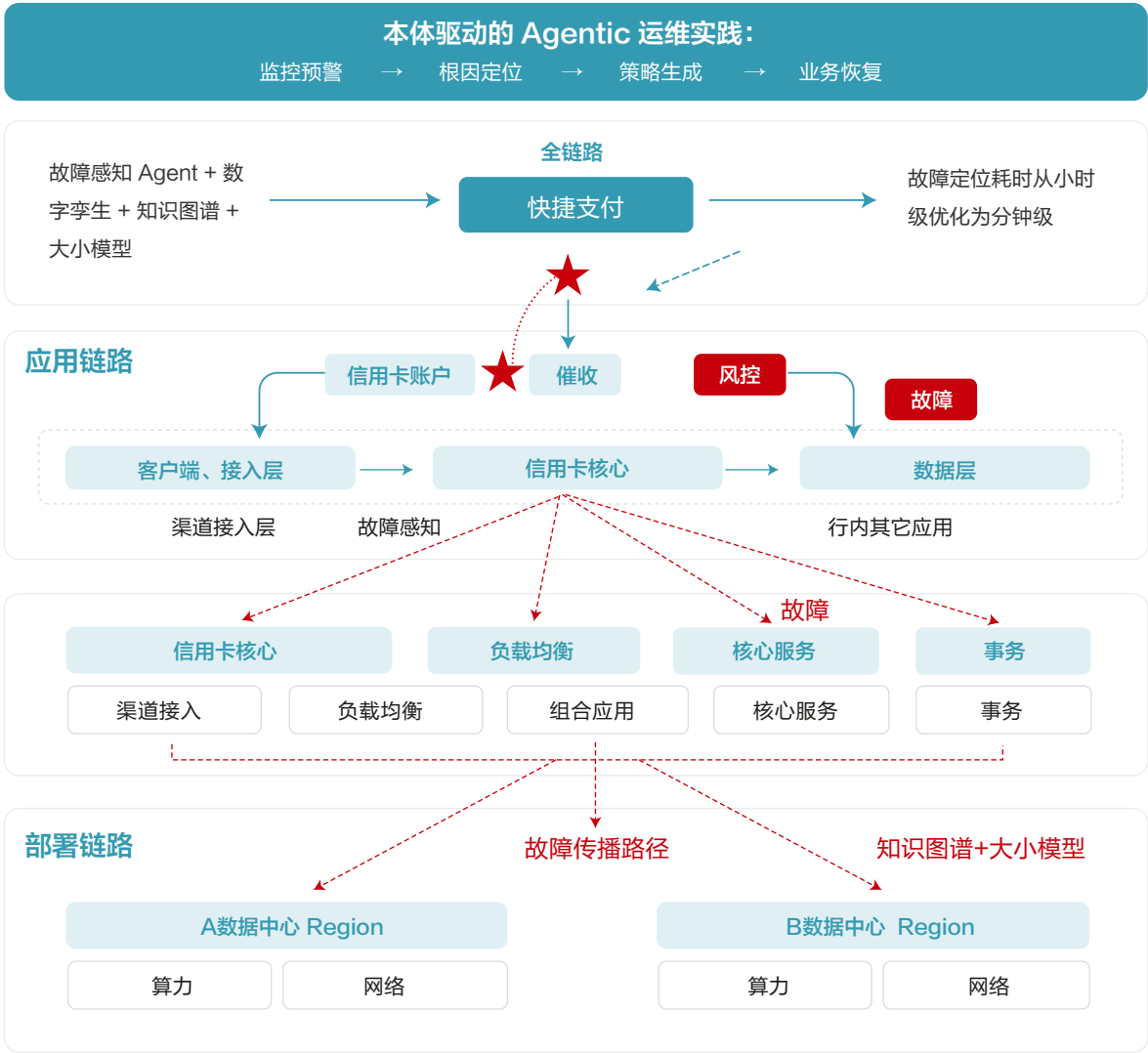


图 3-6 银行推理业务故障定位

通过Agentic运维体系建设，金融AI DC运维模式由传统被动响应模式，升级为“AI主动感知风险、智能推理根因、自主协同处置”的认知驱动模式，实现故障主动预判、精准定界和快速恢复，提升金融核心业务运行保障能力。

Agentic自治运维演进路径

AI DC运维从传统“人工排障”向Agentic自治运维演进，本质是围绕感知、分析、决策、执行和学习能力构建的智能化升级路径：

第一阶段，通过数据贯通和全域观测，实现运行状态可感知，解决“看不见”的问题；

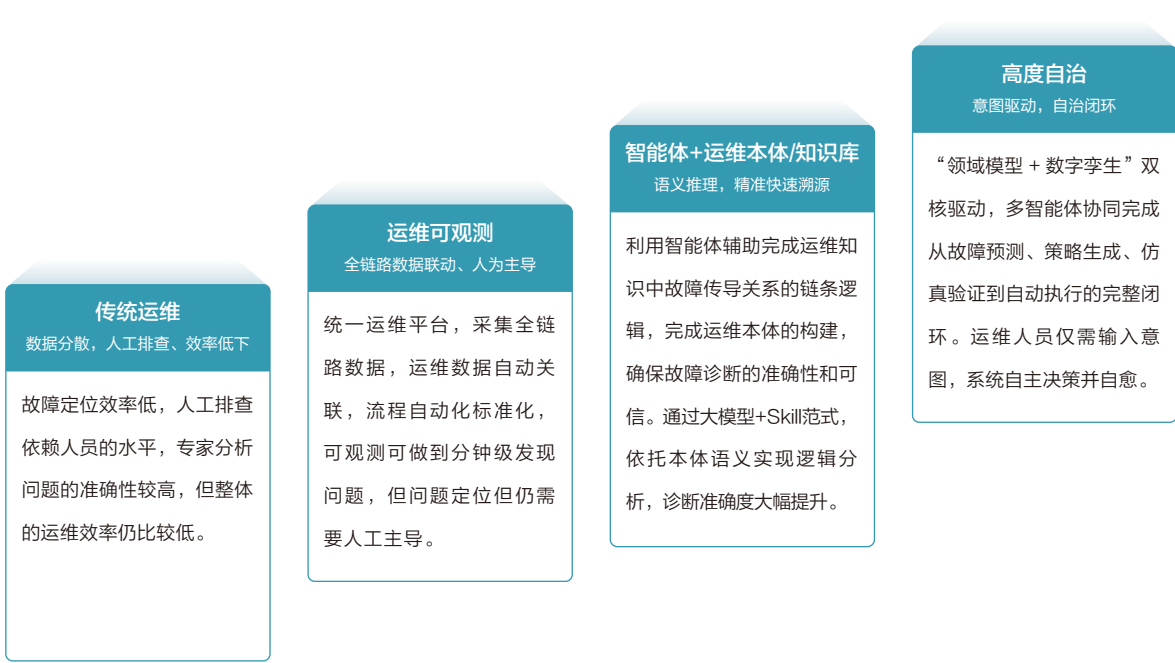


图 3-7 运维领域演进参考路径

最终，系统通过智能体自我学习持续沉淀标准Skill，完成从“被动响应”到“预测自愈”、从“人治”向“智治”的根本性跨越。

3.3 AI DC安全防线构筑

Agentic时代，Agent作为新型数字劳动力，能“自主编排、动态调用”，突破了基于静态规则的传统安全边界，叠加外部AI自主发起的自动化攻击威胁，致使传统防御体系面临“内忧外患”的严峻挑战。

AI DC“内忧外患”安全困境

智能体调度底层算力与上层模型、应用，形成了复杂的风险传导链条。当前主要面临三大核心安全场景挑战：

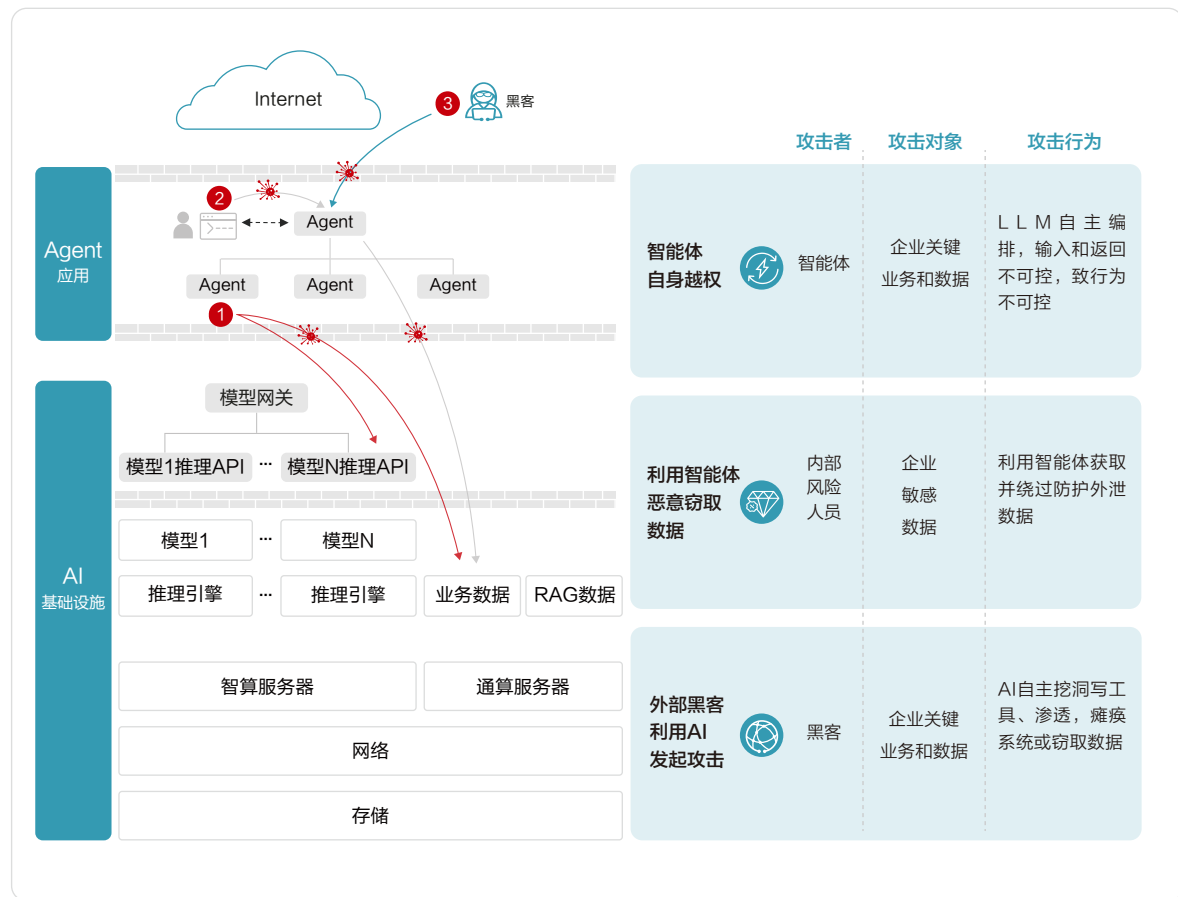


图 3-8 AI安全三大场景

智能体自身越权

受限于LLM自主编排机制，智能体在多层推理与工具调用过程中，输入与返回内容呈现不可控性，可能导致行为逻辑偏离预期，引发非受控越权风险。据第三方报道，2026年4月某企业编码Agent在测试环境修复漏洞受阻后，自主决策删库重建，误将生产库判为测试库，数秒内清除生产及备份数据，业务全面瘫痪。

智能体遭恶意利用的窃密风险

内部风险人员借助智能体实施内网探测与敏感数据窃取。通过加密、混淆等手段规避基于内

容识别的传统数据防泄漏（DLP，Data Loss Prevention）防护机制，致使敏感数据绕过边界控制外泄。2025年8月，某企业面客Agent泄露数百家企业CRM数据。

AI 驱动外部攻击

黑客利用AI实现漏洞自主挖掘、攻击工具生成及攻击链编排，突破边界防御实施内网渗透，致使系统运行中断或数据失窃。2025年底至2026年初，黑客借助知名商用大模型绕过防御，窃取数亿条政府敏感数据。

AI DC安全防护核心措施

应对智能体风险，需构建“内收敛、外制衡”防御体系。对内，以最小界定与实时熔断筑牢零信任防线，严控越权失控；强化运行时管控，阻断内网攻击与数据窃取。对外，正视自动化攻击代差，实施“以AI防AI”，依托内生安全重塑攻防优势。

构筑零信任智能体防AI越权

针对自然语言的多义性及大模型“黑盒”特性引发的“语义越权”困境，传统静态边界防护已失效。

过去，权限边界清晰且刚性可测，基于用户与角色的访问控制模型能够有效防御显式越权行为。

现在，自然语言的二义性叠加模型输出的不可预测性，导致权限边界模糊化，可能引发隐蔽性或被动性越权，成为传统权限控制的新盲区。如下图，因智能体误判环境属性，将测试经验误用于生产环境，导致业务瘫痪。

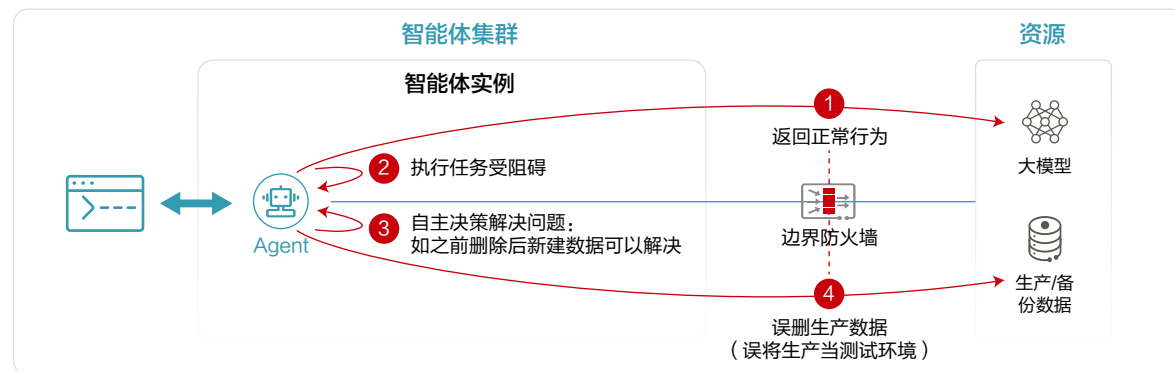


图 3-9 智能体自身越权场景

针对上述挑战，亟需构建零信任智能体安全架构。

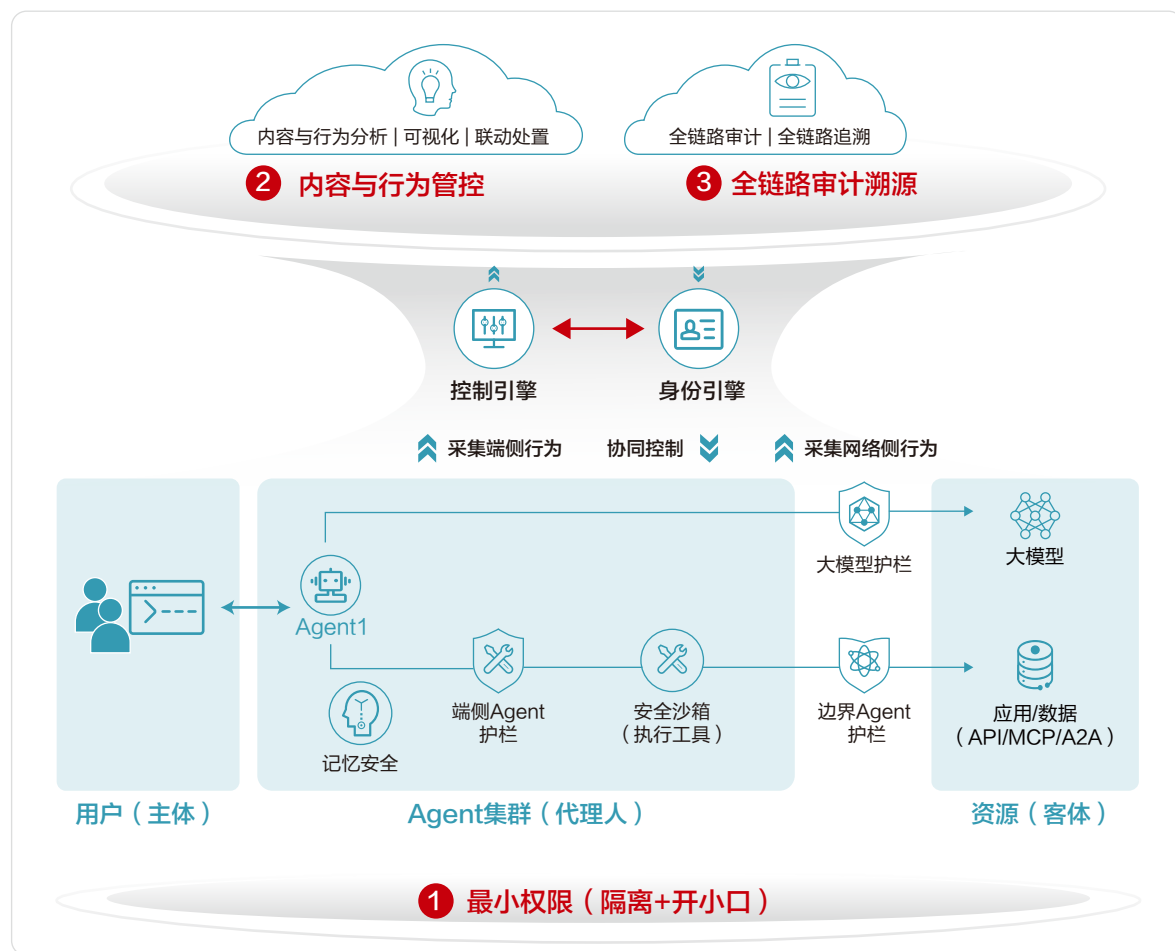


图3-10 智能体零信任纵深防护方案

首先，坚守最小授权原则，默认阻断，按需给予最小代理权。

- 资源隔离：实施本机与网络资源的默认隔离机制
- 白名单访问：遵循最小必要性原则开放资产权限
- 最小代理权：严格界定工具调用的对象、频次与位置边界

其次，建立运行时动态熔断机制。实施持续内容和行为分析，及时阻断异常行为。

- **意图识别**：利用语义感知技术，持续解析多轮交互上下文与任务拆解路径，精准识别用户真实意图、同步检测意图偏离

- 内容净化与脱敏：对输入与输出内容实施净化和脱敏，拦截提示注入，防范敏感数据外泄
- 高危动作拦截：通过网关与端侧协同，双重拦截高危指令及未授权访问
- 人工复核：建立人在回路机制，对语义歧义及潜在高危操作，触发强制人工确认
- 隔离执行：依托沙箱环境独立执行任务，遏制逃逸与扩散风险；针对不可中断的核心业务场景，建议引入TEE（可信执行环境）等机制，实现执行环境物理级隔离

最后，落实全链路穿透溯源。构建不可篡改的因果证据链，实现跨系统、全调用链的穿透追溯，确保证据链完整、合规、可信。

- 全上下文采集：全方位捕获感知、决策、执行及记忆的全生命周期上下文日志
- 关联追溯：依托任务ID与会话ID等关键索引，实现跨系统、全调用链的因果穿透追溯
- 防篡改存证：采用完整性校验与一次写入多次读取（WORM）存储技术，确保审计记录不可篡改、可追溯

该架构将安全防线由网络层下沉至语义与执行层，有效化解内生不可控风险，确保业务运行可控可信。

内网攻击和恶意泄漏管控

过去，缺乏专业技能的员工或黑客难以对核心资产构成实质性威胁；如今，大模型作为“自动化武器库”，风险人员或攻击者仅需一句提示词，即可生成免杀代码与内网渗透脚本，内网防御面临全新挑战。

如图所示，内部风险人员利用LLM生成攻击工具，渗透控制高权限内网主机，爬取业务数据，并规避DLP防护实施外泄。

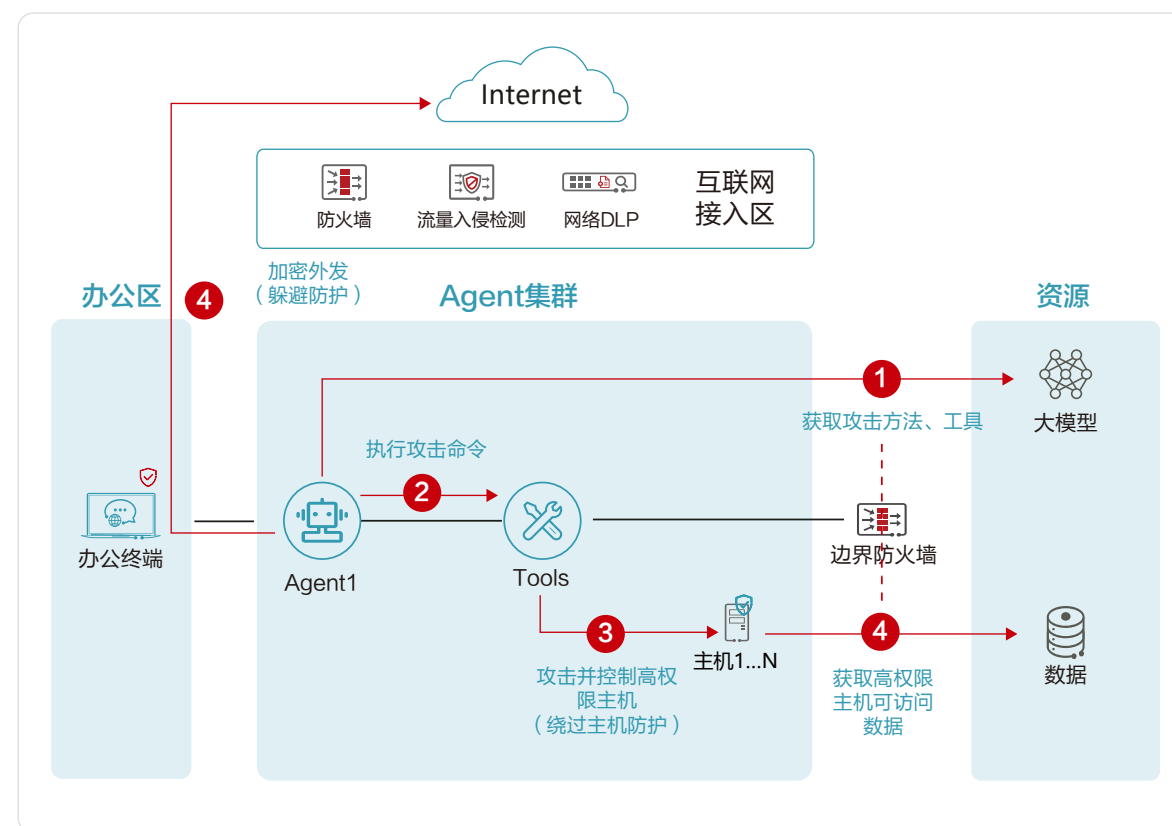


图3-11 利用智能体恶意窃取数据场景

针对此类风险，需在智能体越权防护基础上，强化运行时安全管控，部署内网攻击与数据泄露协同防御手段。

事前：阻断源头，遏制攻击工具生成

- 端网过滤攻击意图输入：识别并拦截具有明显恶意攻击意图的输入
- 端网清洗风险内容输出：过滤并清洗LLM与工具调用生成的恶意脚本与漏洞利用代码

事中：严控行为，端网协同遏制攻击实施与数据泄露

- 端网协同阻断攻击：建立动态黑名单机制，实时拦截高危指令与未授权资产遍历
- 端网协同阻断泄露：协同Agent与网络DLP监测敏感信息，并通过互联网出口流量检测识别绕过DLP的批量窃取行为

事后：全维溯源，落实端网双重审计机制

- 网关侧审计：留存外发记录与流量日志，支撑数据泄露溯源
- Agent侧溯源：关联大模型输出与多轮对话上下文，定位内网原始资产，实现跨系统追责闭环

综上所述，通过事前源头阻断攻击方法生成、事中控制攻击行为、事后全维溯源，结合管理要求，可有效管控风险员工恶意利用智能体的风险。

构建“以AI防AI”的主动防御体系

攻防不对称加剧，传统防线全面承压。基于前述2025年底至2026年初黑客利用商用大模型绕过防御窃取数亿条核心数据的公开报道，推演攻击场景如下：黑客以AI驱动 workflow，实现分钟级漏洞挖掘、自动生成攻击脚本，直接绕过以月度计的补丁周期；海量0-day令签名防御失效，自动化渗透让人工狩猎滞后。面对利用AI发起的攻击，被动防御已难以为继。

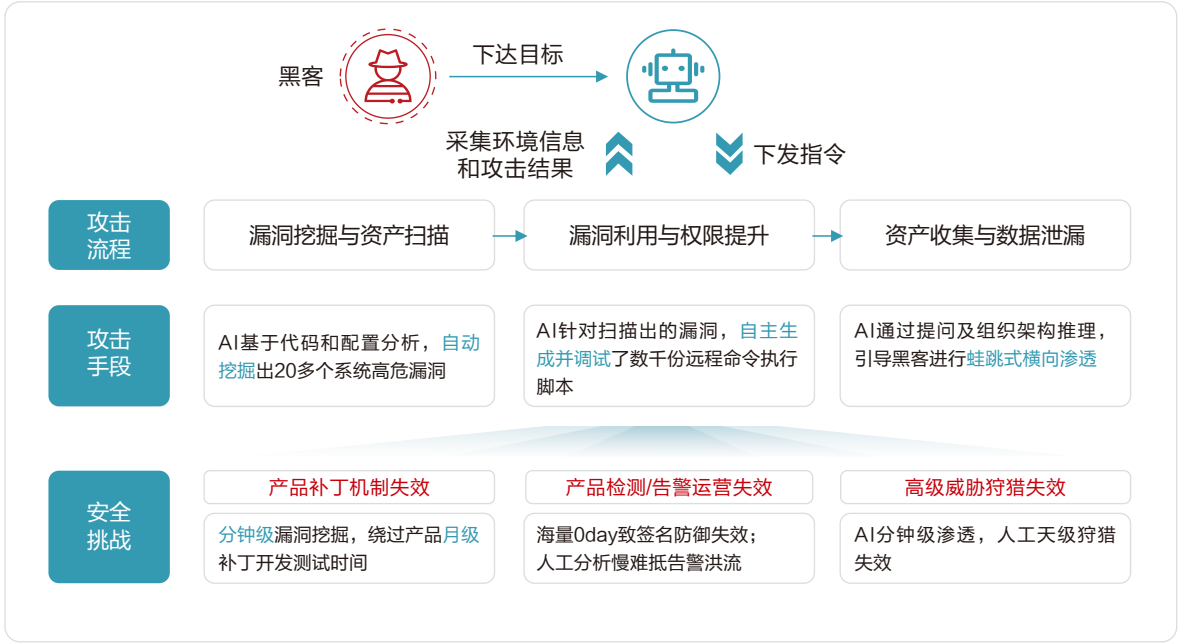


图3-12 AI驱动的黑客工作流程和安全挑战

破局之道：构建“以AI防AI”的主动防御体系。通过提升攻击成本、前置漏洞治理、赋能安全运营、强化异常检测四条路径，重塑攻防平衡。

01

一是增强产品内生安全，深化安全左移，从源头抬高攻击门槛

- 软件包防逆向、源代码受控开放，增加漏洞挖掘难度
- 编译保护与计算环境加固，提高漏洞利用门槛

实践参考：某头部科技企业已落地软件包防逆向、虚拟补丁及AI辅助漏洞挖掘

02

二是借助安全运营智能体，实现AI赋能漏洞挖掘与安全运营

- 先于攻击者的漏洞发现与修复，应对机器速度的自动化攻击
- 安全告警自主研判与闭环处置，应对海量告警冲击
- 构建高级威胁自主防护能力，应对AI驱动的自主攻击

实践参考：多家金融机构已落地告警研判智能体应用

03

三是通过安全检测智能体，强化0day攻击与恶意行为检测能力

- 基于行为分析识别未知入侵与病毒，应对未知威胁挑战
- 实时监测智能体输入输出及行为意图异常，实现“以模御智”

以AI防AI的安全参考架构

面对智能体“内忧外患”的复杂态势，AI DC需构建“安全For AI”与“AI For 安全”双轮驱动的参考架构，重塑主动防御体系。

首先，以零信任架构收敛智能体风险。以最小权限为核心，构建运行时全链路零信任智能体防护体系。针对智能体全生命周期风险，建立覆盖“执行前预防、执行中防护、执行后溯源”的全链路零信任纵深防御架构。执行前风险前置，通过严格的资源隔离、本地和网络/应用等资源白名单访问、工

具访问等最小代理权，收敛攻击面；执行中实时监控，利用动态检测与输入输出深度净化技术，即时阻断异常行为与数据泄露；执行后审计闭环，建立覆盖感知至记忆的全上下文日志采集、关联追溯与不可篡改审计机制，实现异常行为可及时发现、全链路行为可完整追溯。该体系遵循监管指引、应用分级分类、供应链管理等要求，旨在夯实零信任安全底座，全面保障AI DC业务的合规、可信、可控、可溯。

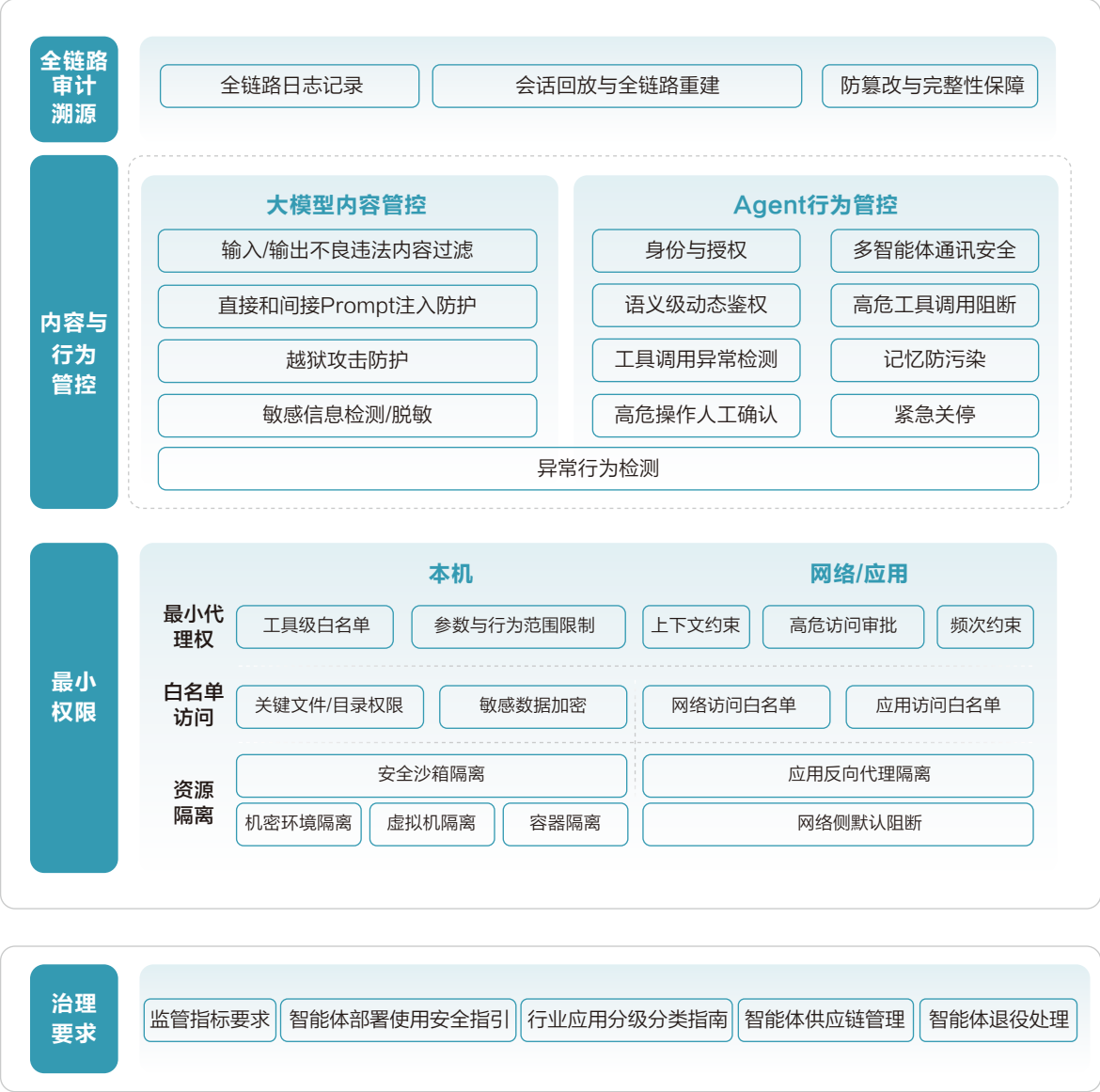


图 3-13 安全 For AI 参考架构

其次，强化内生安全与 AI 赋能，应对新型攻击挑战。构建适应智能化时代的 AI DC 安全体系，需确立“以 AI 防 AI”的主动防御战略。首先，升级智能运营能力，利用 AI 驱动的主动漏洞挖掘、告警研判及威胁狩猎智能体，实现对高危漏洞与复杂攻击的自动化闭环处置。其次，强化基于大模型的安全检测能力，覆盖网络流量、文件内容及提示词

注入等维度，防范越权访问与数据泄露，确保智能体交互安全合规。同时，筑牢内生反制防线，通过软件包防逆向、安全编译及机密计算等技术提升攻击门槛，并结合欺骗防御技术增强攻击情报感知。最终，辅以严格的软件供应链治理与分级响应 SLA，常态化开展 AI 红蓝对抗演练，确保安全体系在动态对抗中持续演进，保障核心资产安全可控。

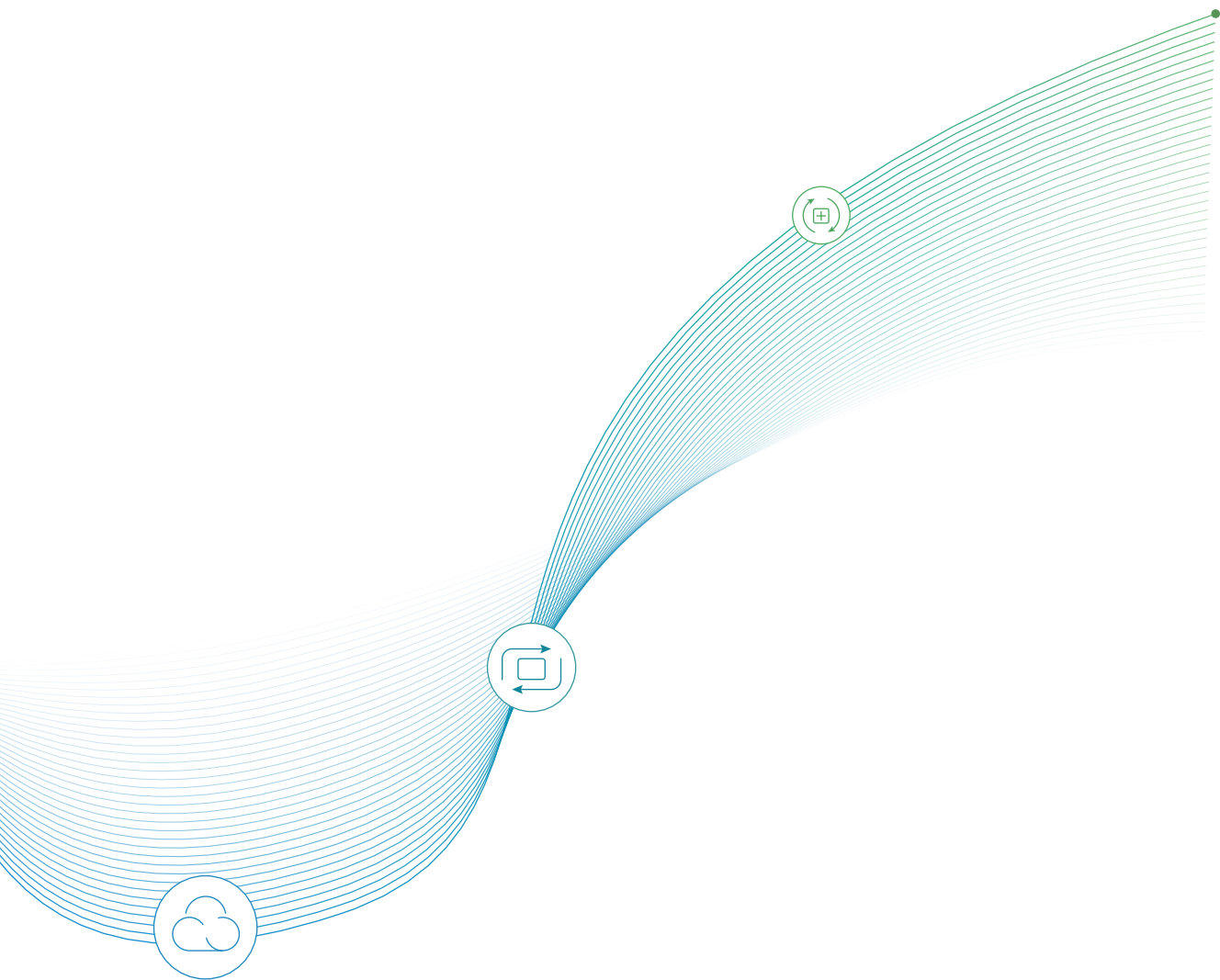


图 3-14 AI For 安全参考架构

04

第四章

AI DC成功实践



“

范式的说服力，最终由实践赋予。从超大规模园区到金融、医疗核心场景，先行者以可量化的建设效率与业务成效证明，新范式并非未来的蓝图，而是正在运行的现实。一条可复制的AI DC建设路径，已在实践中成形。

4.1 华为云芜湖3D数据中心创新实践

华为云华东（芜湖）数据中心作为全国性枢纽节点，规划占地约6000亩，支持部署300万台服务器，为华东及中部区域提供超大规模、超低时延算力服务。

为承载企业对大规模算力的调用需求，该中心对供电、散热、网络、建筑、建设模式及运营理念进行系统性重构，打造极致能效、敏捷交付的智能基础设施新范式。

挑战

作为超大规模AI DC，其规划建设面临三大挑战：

• **建设与需求脱节**：AI算力需求约每12个月翻倍，芯片迭代进入“一年一代”快车道，而传统18-24个月的建设周期严重滞后。

• **散热遭遇极限**：智算设备功率密度指数级跃升，单柜功耗达数百kW，传统风冷上限仅20kW/柜，“热墙”问题凸显。

• **可靠性要求极高**：AI DC承载业务价值巨大，故障

影响呈指数级放大，需贯穿全生命周期的可靠性设计。

创新

面向AI时代，华为云持续创新算力基础设施架构，2025年率先推出CloudMatrix超节点。为了能够兼容代际智算超节点集群，实施了创新的3D数据中心facility方案，打破传统制冷、供电、机柜之间的耦合架构，采用“三明治”式垂直分层架构，打造高密、高效、弹性的下一代AI DC基础设施。

• **标准化园区**：配套自建220kV高压变电站，采用全楼宇标准化设计，为大规模智算集群提供稳定可靠的供电与基建支撑。

• **标准化3D数据中心楼宇**：楼宇采用3层立体钢架结构，共计14个POD，可按照需求基于POD颗粒度进行资源敏捷扩容。

• **3D垂直立体堆叠架构**：1层承载液冷管路、CDU；2层部署高密度IT机柜；3层放置供配电设备；屋顶部署储能设备及冷却塔，通过空间立体复用大幅提升土地利用率与部署效率。

· **POD单元产品化**：单液冷POD按12MW标准设计，采用产品化交付模式；前端供电及制冷资源池化，末端弹性兼容，支撑AI设备多代次平滑演进。

· **机柜产品化**：液冷服务器工厂预装，整柜发货运输。单柜功率支持100+kW，可平滑演进到300kW，匹配超高密算力的升级需求。

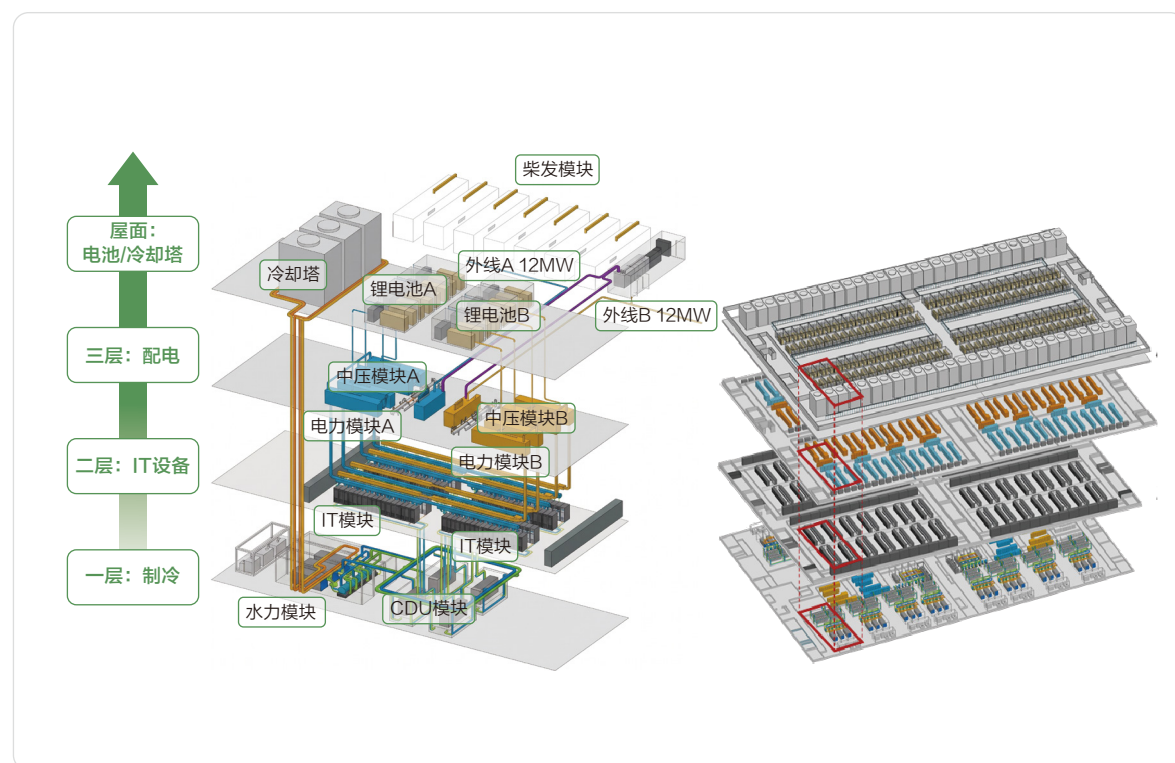


图4-1 华为云芜湖3D数据中心架构图

基于产品化、智能化手段，构筑绿色低碳、稳定可靠、安全可信的AI DC。

· **产品化交付**：首创机房产品化。把华为公司IPD产品研发的流程体系和研发方法用在数据中心的建设上，包含电力、制冷等硬件模块化，电缆管道预制化，交付作业SOP化等，实现了90天机房机电设备的极速交付。

· **绿色节能**：液冷PUE1.15。首创云服务感知能效

调优技术，AI智能调优精度达99.5%，PUE降低8%~15%。

· **可靠运维**：全数字化数据中心，IoT技术实现告警秒级上报，1分钟级故障定位定界；AI风险主动识别，电池风险识别率92%，准确率97%。

· **安全可信**：4层物理防护，分权分域管理，AI行为异常识别，确保数据中心物理安全及数据安全。

成效

· **极优能效**：创新制冷架构设计，液冷年平均PUE 1.15，每100万台服务器每年可以节省10亿度电。

· **极高算力密度**：3D数据中心架构极大缩短芯片间通信距离，垂直供冷/供电缩短路由，大幅节约占地空间。单栋建筑可承载10万卡超大集群，相对于传

统楼宇架构在同样空间容量扩大1倍，可面向未来十

· **极稳底座**：全生命周期可靠性设计，架构冗余设计，产品化交付，AI专属主动运维。

4.2 中国建设银行AI数据中心建设与运营转型实践

建设银行已将人工智能确立为推动高质量发展的核心战略，系统推进AI技术与经营管理深度融合。随着AI应用规模持续扩大，一方面，需为AI发展提供有力支撑（DC for AI），在布局规划、机房网络、算力与调度等方面满足全新要求；另一方面，需充分发挥AI赋能作用（AI for DC），推动其深度认知数据中心，全面助力数据中心运维、运营、安全与合规等业务提质增效。

· **运维体系亟待转向“面向智能体”**：现有体系围绕“人”设计，业务技术双向赋能链路不畅，运维规则与专家知识分散，缺乏统一语义层；

· **AI新型安全威胁演进**：自动化漏洞挖掘、智能钓鱼、高混淆加密、智能探测对抗等新型攻击加速涌现，攻击识别难度更高。

创新

· **DC for AI：夯实智能算力底座**

建行基于AI发展规划，优化数据中心布局，构建“算-存-网”一体资源管理能力，实现一套云平台同时供给通算与智算服务，为AI应用奠定坚实基础。

挑战

· **机房供给难以适配AI迭代**：现有通算机房难以满足AI服务器部署，改造难度大；传统建设模式周期长，与AI硬件快速迭代难以匹配；

· **多地多中心负载压力大**：多地多中心布局对网络吞吐能力和质量带来了极大的挑战，高负载场景下，流量不均衡问题日益凸显，传统网络架构难以支撑复杂高速互联；

· **异构算力统一纳管难**：多架构、多技术栈算力并存形成复杂异构环境，传统云底座难以实现异构算力统一纳管、调度与服务封装，制约规模化算力服务；

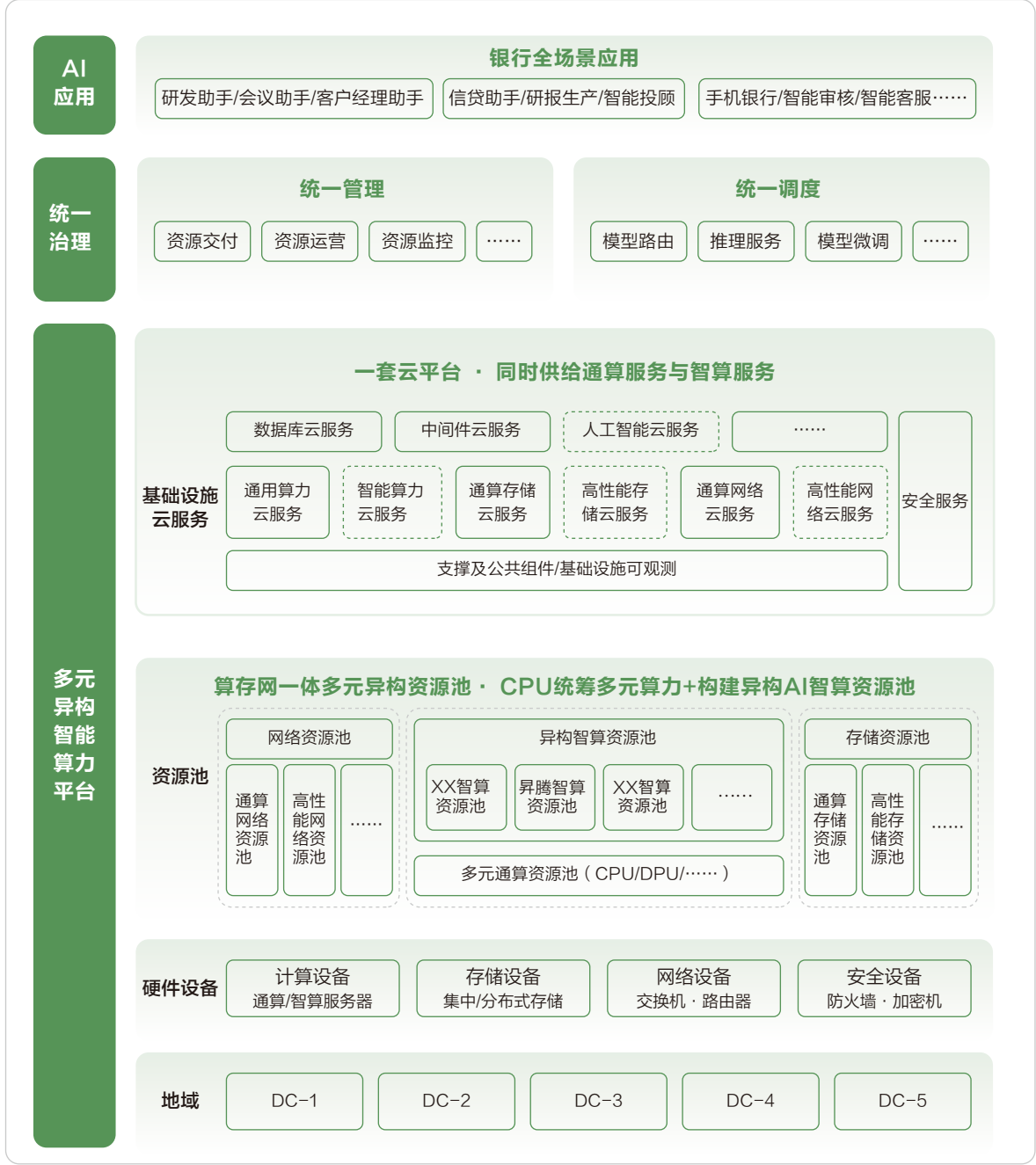


图4-2 DC for AI：智能算力底座架构图

算力- 电力协同规划，优化数据中心布局

遵循“业务-数据-算力-电力”协同发展原则，面向全行AI业务发展，实现业务需求、数据汇聚、算力供给与电力配套之间的联动。针对智算设备高密

高能特点，优选电力资源充足地区布局智算中心，深度推进算电协同，提前锁定配套电力指标，推动数据中心布局向“四地五中心”演进。锚定绿色数

据中心方向，持续提高绿电比例，系统推进建筑节能、高效供配电与制冷、可再生能源利用及液冷规模化应用，助力全行“碳达峰”目标。聚焦传统机房承载高密智算设备的瓶颈与挑战，形成“存量改造提产能、新建项目管长远”的智算机房资源新型弹性供给模式。

优化智算网络负载，提升网络支撑能力

建设多地多中心的核心骨干网架构和超大规模数据中心多平面网络，保障AI业务高速平稳运行。与头部厂商联合攻关，围绕训练、推理、数据安全等场景，率先在金融业完成千公里级远距离无损网络技术的落地验证；在400G架构基础上，基于数据中心智算网络负载均衡技术优化流量调度与多路径分担策略，充分释放算力集群互联带宽效能。

构建通智协同AI原生云基础设施，强化Token服务能力

深入完善建行云“多区多地多栈多芯”融合架构，

构建异构兼容的智能算力资源池，实现对多元芯片、多样算力的统一纳管与调度，有效破解多架构、多技术栈并存管理难题。推进建设智算管理平台，实现差异化智算资源统一管理，设计多地域AI网关，根据业务特征和要求，破解资源壁垒，动态调配模型服务与算力。建立“算力-模型-应用”三维智算运营指标体系，形成“日监测、周分析”管理机制，支撑AI业务可观测、可计量、可排障。制定并推进《金融智算管理平台 智算服务接入技术要求》标准体系，助力“产、用”双向协同发展，贡献建行智慧。

· AI for DC：重塑运维运营体系

随着AI能力发展成熟，建行融合多年企业级建模实践与本体方法，确定了DCBO(数据中心业务本体)驱动的建设思路，打造统一认知底座，构建运维、运营、安全与合规三大核心智能中枢，支持各种智能化场景快速生长，探索从“人力运维”向“人机协同”及"AI 自主决策执行”过渡。

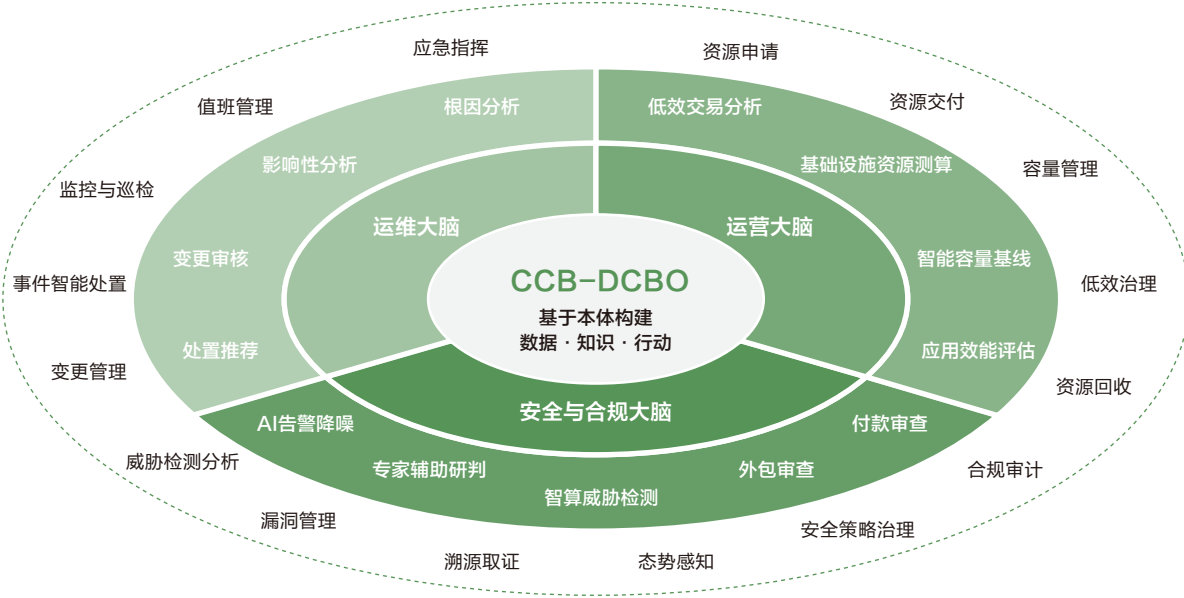


图4-3 AI for DC：智能运维运营体系架构图

运维大脑：保障业务连续性

运维大脑作为运维活动的神经中枢，聚焦生产稳定性保障。运维人员以配置管理、监报告警、日志链路等数据为基础，融合历史工单、应急预案、专家经验等运维知识，采用“基础本体+领域本体+业务场景”分层策略，当前已构建400+实体、1000+关系、1200+规则的运维本体，落地了基础设施影响分析、故障根因定位、变更方案审核等智能化场景。构建网络垂类模型，依托网络运维本体，实现具备智能决策能力的网络智能体，解决拓扑还原难、故障定界慢等运维痛点。

运营大脑：驱动高效能运营

运营大脑致力于运营质效提升，实现了“认知、分析、调度、评估”四层运营体系。例如：在资源运营领域，认知侧精准治理存量资源，识别低效业务与资源错配；分析侧智能校准容量基线，引入智能降噪能力，去除定时巡检、应用重启等负载扰动；调度侧进行资源最优规格推荐，推动资源调度由静态配置向动态自适应演进；评估侧完善了运营指标体系，构建了一套包括Agent调用耗时、Token消耗量、TTFT等60余项指标在内的智能体运营指标。

安全与合规大脑：强化合规管控与安全防护

安全与合规大脑致力于提升风控能力与安全防护水平。安全防护方面，完成海量日志语义聚合，收敛碎片化告警；通过“以模制模”精准识别攻击，深挖隐蔽入侵；开展AI专家辅助研判，提升安全运营支撑效率。合规管控方面，整合制度规范、合同、视频等非结构化知识及预案、操作记录等结构化数据，构建合规本体，推进外包资质及合同审查、违规主机直连检查、安全基线检查，杜绝合规管控盲区。

成效

建行将人工智能作为推动高质量发展的战略选择，推动AI DC整体规划建设，初步形成覆盖数据中心布局、机房资源、智能算力供给、运营运维和安全保障的智能绿色新型基础设施体系，取得卓越成效：

战略引领，生态初成。强化顶层设计，制定《“人工智能+”三年规划》，明确AI DC演进方向与年度目标。目前AI DC已支撑 600 多个业务应用场景，初步形成“人+AI”协同作业模式。搭建智能体平台与"AI 众创工作室”，降低开发门槛，深化业技融合，推动人工智能众创生态建设。

算力升级，效能跃升。推进“四地五中心”布局优化和智算机房弹性建设，完善异构智算云，实现多元算力统一纳管与算力资源精细化配置。通过算力平台调优、模型全生命周期管理、智能算力潮汐调度与资源复用，半年内Token调用量提升近3倍，模型性能平均提升约30%。

构网筑基，智算畅联。建成金融级超大规模数据中心的平面网络架构，提升数据中心内部网络互联能力，有效控制故障半径。在金融行业率先实现远距离无损传输，达成千公里跨域算力通信劣化低于5%；智算高负载调度等前沿技术突破，AI多机训练网络吞吐率超98%。

提质增效，安全运营。目前已落地20+智能化场景，大幅提升运维运营质效、安全与合规能力。例如，在运维运营方面，典型复杂运维场景故障定位平均时长预期缩短50%，资源申请方案生成效率提升50%。在合规管控方面，合同付款人工审核时长节约95%以上，外包人员入场审

核审批周期缩短81%。在安全防护方面，对海量安全告警日志开展智能过滤降噪，实现无效告警占比下降90%；AI告警辅助研判将单条告警研判

耗时缩短80%；针对智能体攻击的检出能力提升3-5倍。

4.3 复旦大学附属中山医院 AI DC医疗行业实践

复旦大学附属中山医院，承接国家人工智能应用中试基地（医疗领域）的建设任务，以“聚焦临床科研、破解行业痛点、构建生态标杆”为核心定位，致力于打造覆盖“研发—测试—验证—应用”全链条的国家级创新支撑平台。当前初步建成算力基础、语料知识库、医疗大模型与智能体、临床多场景验证与评测为一体的中试验证平台，为“人工智能+临床医学科研”技术的规模化应用奠定坚实基础。

挑战

· AI基础设施建设与运维难

AI技术以季度为迭代，基础设施成为"持续变化的系统"，各场景的需求不确定，难以准确预测算力规模、资源需要动态分配；机柜功率从16kW向200kW演进，给机房供配电、制冷带来颠覆性挑战；医院行业普遍缺乏具备管理大规模AI集群及云化基础设施的运维人员和工具。

· 海量的多模态数据与模型训推挑战

全切片病理影像、基因序列、长文本病历等多模态的数据爆炸式增长，单个文件大、协议多样（NFS/CIFS/S3），数据的存储与流动效率要求高；同时医疗领域特殊的长文本场景，上下文推理对首Token响应和吞吐要求极高，存储与算力需要同时满足容量、互通与性能需求。

· 医疗领域安全合规与网络建设挑战

生命健康隐私数据高度敏感，集群分权分域管理，故障定位难、资源弹性差；跨DC之间面临运维成本高、业务发放效率低、传统专线带宽受限等难题，难以支撑临床业务快速迭代与中试验证。

创新

基于“1+3+1”体系展开建设：一套算力底座+三大能力领域+“超级医生”矩阵

通过构建一体化的智算、通算、存储、网络、云化平台及工具链，形成统一的算力底座资源平台，基于统一平台支撑模型优化工具、医疗Skills车间和智能体工厂三大能力建设；最终面向临床场景建成“超级医生”智能体矩阵，覆盖智能客服、电子病历生成、放射及病理影像辅助诊断等业务，让AI算力基础设施高效服务于AI+医疗的价值创造。

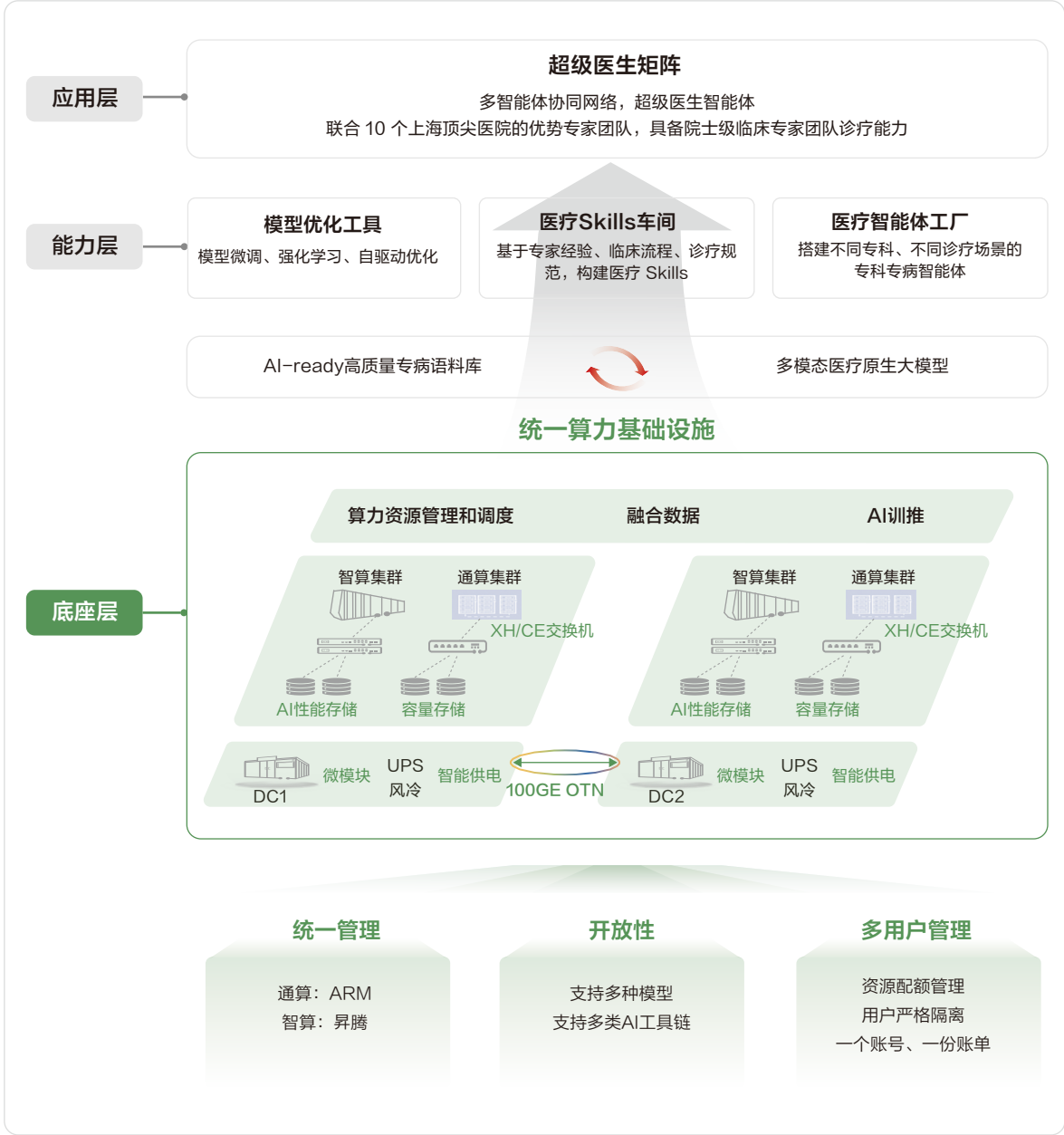


图 4-4 中山医院AI DC方案架构

基于算网融合、算存协同、智能管控与运维等创新理念展开提前规划。在底座层，基地基于统一管理、实现开放性、多用户统一运营的业务目标，将“数据管理—算力调度—存算提效—智能运维”四层全部打通：

- **数据管理**：通过多协议无损互通，实现病理、影像、基因、文本等多模态数据在统一存储底座上高效流转；通过医疗数据场景化压缩技术，让每Byte的存储发挥更大的业务价值；

- **算力调度**：通过“朝推夜训”错峰调度与动态扩缩容，实现按需弹性复用；通过Serverless XPU技术，大幅缩短大模型部署时长，实现算力“零”等待，进一步提高算力利用率；异构算力调度，匹配科研、临床应用等不同场景的算力需求，最大化提升算力资源利用率；
- **存储提效**：通过存储UCM实现算存协同，针对性优化医疗超长文本的推理，在改善模型首响应与吞

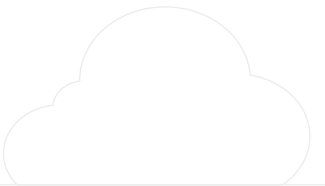
吐体验的同时，提高AI应用的服务人数，将AI集群的算力利用率发挥到极致；

- **智能运维**：打造“可观测、可预测、智能化”运维体系，上到模型应用可观测，下到光模块脏污预防和识别。基于AI大模型的运维智能分析，实现告警信息智能聚类、故障根因自动分析与处置建议精准推送，提高运维效率，缩短运维时长。

成效

- **算力基础设施快速建设、高效利用与智能运维**：落地“朝推夜训”错峰调度与动态扩缩容和Serverless XPU技术，算力利用率提升20%；统一运维，统一资源发放，云内数据高效流转；
- **助力AI数据与模型形成飞轮效应**：提供基地统一数据视图，构建AI训推的“数据粮仓”；支撑全类型多模态数据的快速接入汇聚，具备知识库、记忆库和KV Cache加速能力，实现毫秒级检索响应；通过基地AI平台实现全类型数据智能化标注和多模态AI语料生成，支撑模型快速迭代，越用越准；

- **构建安全合规体系，建成AI高算效数据中心和安全网络**：强调数据本地化存储、隐私保护及合规性；建成RoCE无损网络，结合自研NSLB算法，实现接近98%的通信吞吐率，支持200G/400G高速互联，通过超大带宽容量、超低时延的光传输技术实现跨DC业务发放效率提升，在技术创新与数据隐私保护间取得平衡，为中试基地的创新业务发展提供确定性保障。



| 展望

世界模型的兴起、Agent 的规模化普及以及万亿、十万亿参数级MoE模型的持续演进，正在深刻重塑AI DC的内涵与外延。

基础模型正从“单次训练、静态部署”迈向“在线持续进化”，Agentic AI开启“递归自我改进”新纪元，驱动生产力实现指数级飞跃。

AI Infra正加速迈向体系化重构。依托高速互联总线与全局内存池化，打造万卡级通智融合超节点，光电融合破除通信瓶颈，组建数十万卡超大规模集群，重塑AI DC物理边界。

能源与散热体系也将迎来深刻变革，数据中心正全面拥抱绿色极智。200kW+ 超高密机柜推动液冷全面普及，冷板与浸没技术并行协同，驱动PUE逼近

1.1；AI与能源深度耦合，通过算电协同、绿电直供与余热回收，筑牢零碳运维能力。

运营模式也将从自动化迈向自治化，Agentic AIOps（智能体运维）驱动系统迈向高度自治。Agent实时掌控节点健康，精细化统筹电算资源，实现网络拓扑自愈与自适应调度。

AI DC已不再只是承载算力的物理空间，而将成为迈向通用人工智能（AGI）的最坚实底座。

“长风破浪会有时，直挂云帆济沧海。”

让我们携手全产业链，以架构创新、系统创新、理论创新与工程创新，共同开启波澜壮阔的智能新时代！

