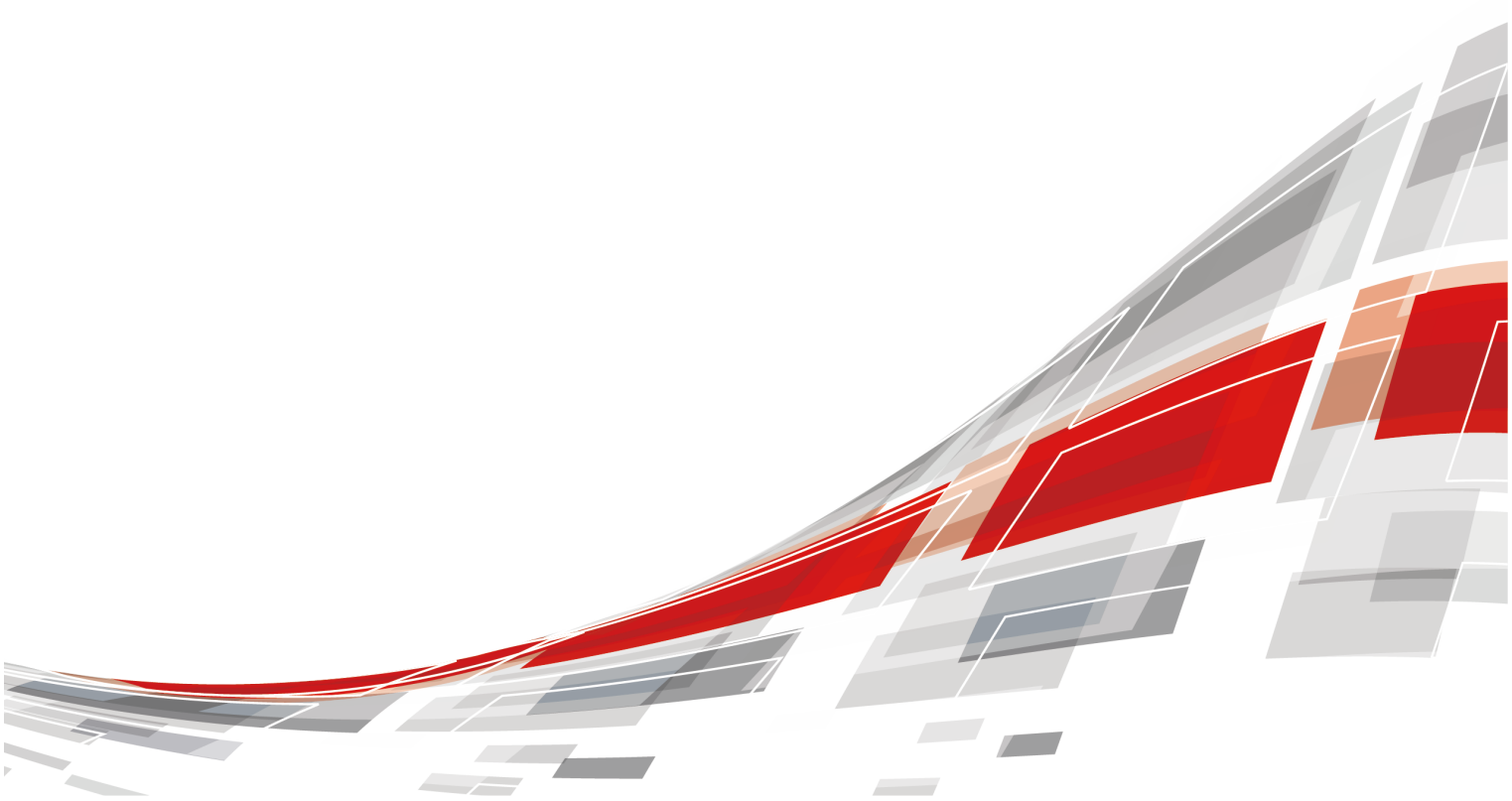
FusionOS 26

技术白皮书

文档版本 01

发布日期 2026-06-30



超聚变数字技术股份有限公司

版权所有 © 超聚变数字技术股份有限公司 2026。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

FUSION 和其他超聚变商标均为超聚变数字技术股份有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

本文中，只是为了描述的简洁和方便理解，用“xFusion”指代“xFusion Digital Technologies Co., Ltd.”，这并不代表“xFusion”还可以具备其它含义。基于本文中单独提及或描述的“xFusion”，不能用于“xFusion Digital Technologies Co., Ltd.”之外的理解或表达，超聚变数字技术股份有限公司也不承担因单独使用“xFusion”所带来的其它任何法律责任。

您购买的产品、服务或特性等应受超聚变数字技术股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，超聚变数字技术股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

超聚变数字技术股份有限公司

地址： 河南自贸试验区郑州片区（郑东）龙湖内环北路99号 邮编：450000

网址： https://www.xfusion.com

前言

概述

本文档详细介绍超聚变服务器操作系统FusionOS (以下简称FusionOS) 26的产品特性、技术指标以及主要功能与服务等内容，让用户对FusionOS 26有一个深入细致的了解。

读者对象

本文档主要适用于售前工程师、技术服务人员等。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。
	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

 版权所有 © 超聚变数字技术股份有限公司

修改记录

文档版本	发布日期	修改说明
01	2026-06-30	第一次正式发布。

 版权所有 © 超聚变数字技术股份有限公司

目 录

前言 ii
1 简介 1
2 产业技术背景 2
3 产品概述 3
3.1 产品定位与核心理念 3
3.2 版本生命周期 3
3.3 代际演进 4
3.4 新增能力 4
4 系统架构总览 7
4.1 总体架构 7
4.2 架构全景说明 9
5 核心技术能力 10
5.1 安全可信引擎（xSec） 10
5.1.1 安全可信引擎特性介绍 14
5.2 xAI 加速引擎 15
5.2.1 xAI 加速引擎特性介绍 17
5.3 虚拟化引擎（xVirt） 18
5.3.1 虚拟化引擎特性介绍 19
5.4 实时计算引擎（xRT） 20
5.4.1 实时计算引擎特性介绍 21
5.5 智能交互入口（OSPilot） 22
5.6 可靠性与维测增强 24
5.6.1 可靠性与维测特性介绍 26
6 技术规格 28
6.1 平台与组件规格 28
6.2 技术能力规格 29
6.3 生态兼容与适配 32
7 持续服务与支持 33
7.1 版本生命周期 33
7.2 技术服务 33

 版权所有 © 超聚变数字技术股份有限公司

8 附录.....35
8.1 术语表.....35

 版权所有 © 超聚变数字技术股份有限公司

1 简介

FusionOS 26是超聚变数字技术股份有限公司面向数据中心及边缘延伸场景打造的新一代企业级服务器操作系统。本产品以安全可信、AI原生、生态统一、供应连续为核心设计理念，基于Linux 6.6 LTS内核构建，面向通用计算、虚拟化与云基础设施、AI推理与智能计算、边缘计算、高可靠关键业务等多种部署场景，提供统一的操作系统底座支撑。

 版权所有 © 超聚变数字技术股份有限公司

2 产业技术背景

操作系统作为数字基础设施的核心底座，正面临多重结构性技术挑战的交织冲击。这些挑战不是孤立的单点问题，而是共同构成了新一代服务器操作系统必须回应的技术背景。

- 供应链连续性风险加剧

  开源软件供应链正从偶发性风险演变为系统性攻击面。2024年xz-utils后门事件首次证明，攻击者可通过长期社会工程学渗透获取基础设施级组件的维护权限并植入后门，几乎波及所有主流Linux发行版。此后攻击迅速工业化——2025年新增恶意开源包超过45万个；2026年，攻击者利用构建流水线信任链以合法签名身份发布恶意版本，绕过现有检测机制。供应链的可信治理能力是操作系统产品的生存前提。

- 安全威胁向纵深演进

  攻击手段从传统网络渗透向供应链投毒、固件级植入、内存级攻击等纵深方向持续演进。与此同时，AI正在根本性地改变攻防节奏——2026年初，AI模型在无人类介入的条件下，数小时内自主完成了针对主流操作系统内核的完整漏洞利用链构建；同期，Google威胁情报团队首次确认AI生成的零日漏洞已被用于实际攻击活动。漏洞从发现到武器化的周期正从数周急剧压缩至小时级，操作系统的安全要求已从"功能合规"上升为"架构内生"。

- AI规模化部署重塑OS能力需求

  大模型、智能体和多模态应用正从试验验证走向规模化部署，算力需求呈爆发式增长。在高端AI芯片供给受限的背景下，操作系统层面的异构算力编排、推理引擎优化和内核轻量化成为释放算效的关键路径。同时，AI也在反向重塑操作系统自身——智能化运维、意图驱动的系统管理正在成为新一代OS的基本能力预期。

- 多场景碎片化与运维复杂度攀升

  企业IT基础设施正从单一数据中心向"数据中心+边缘+云"的混合架构演进，操作系统需要在通用计算、虚拟化、AI推理、边缘部署、实时控制等多种场景间保持统一底座的一致性，同时提供场景化的定向增强。场景碎片化叠加基础设施规模增长，使得传统手工运维的模式难以为继，系统自身的可观测性、自动化运维和智能诊断能力成为刚性需求。

FusionOS 26的架构设计正是对上述四重挑战的系统性回应。

 版权所有 © 超聚变数字技术股份有限公司

3 产品概述

3.1 产品定位与核心理念
3.2 版本生命周期
3.3 代际演进
3.4 新增能力

3.1 产品定位与核心理念

- FusionOS 26定位为面向AI时代的新一代安全可信数据中心操作系统。产品以安全可信、AI原生、生态统一、供应连续四大核心支柱为设计主线，基于Linux 6.6 LTS内核构建，重点面向通用计算、虚拟化与云基础设施、AI推理与智能计算等数据中心核心场景，并向边缘延伸场景进行能力扩展。
- 在架构层面，FusionOS 26采用"统一底座+四大引擎+一个智能交互入口"的核心架构体系。统一底座为上层各引擎提供共用的基础能力，涵盖内核与异构硬件适配、基础运行时环境、资源隔离与调度编排以及贯穿各层的安全基础设施。四大引擎——xSec安全可信引擎、xAI加速引擎、xVirt虚拟化引擎、xRT实时引擎——建立在统一底座之上，分别面向安全、AI、虚拟化和实时场景形成定向增强。OSPilot原生系统级智能体作为统一交互与编排入口，将自然语言、命令行和标准接口请求转化为受控的系统任务，推动系统从传统被动响应式运维向意图驱动的智能化运维演进。可靠性与维测体系横贯各层，保证系统在长期运行、升级演进和故障处置过程中的连续性与可恢复性。
- FusionOS 26聚焦数据中心场景下的安全、轻量、AI原生差异化定位：通过安全可信架构实现纵深防护，通过xAI加速引擎释放异构算力，通过虚拟化与资源编排能力提升资源利用效率，通过OSPilot智能体重塑运维范式，形成从底层内核到上层智能的全栈差异化能力体系。

3.2 版本生命周期

FusionOS 26采用13年全生命周期维护策略，划分为标准支持阶段（5年）、扩展支持阶段（5年）和安全支持阶段（3年）三个阶段，维护范围从全功能更新逐步收敛至关键安全漏洞修复。13年的维护承诺覆盖企业级关键业务系统的典型硬件生命周期，各阶段的详细维护范围见**7.1 版本生命周期**。

 版权所有 © 超聚变数字技术股份有限公司

3.3 代际演进

FusionOS 26相较FusionOS 23实现了架构理念、内核基线、核心能力的全面代际跃迁。以下从关键维度对比两代产品的技术演进：

维度	FusionOS 23	FusionOS 26	演进说明
内核版本	Linux 5.10 LTS	Linux 6.6 LTS	内核跨越两个大版本，获得更完善的硬件支持、性能优化和安全特性
架构理念	四大引擎	统一底座+四大引擎+智能入口	从功能特性导向演进为架构驱动的系统化设计
安全体系	xSec安全框架（安全使能服务）	xSec安全可信引擎（安全中心+主动免疫+安全使能服务，10维度安全功能体系）	从组件拼装式安全升级为内生纵深安全架构
AI能力	xTuning性能加速	Wings自研推理引擎+xTuning性能加速+OSPilot智能体	从零到全栈AI原生，覆盖推理加速、系统调优和智能交互
虚拟化	xVirt虚拟化引擎	xVirt虚拟化引擎（含宿主机-虚拟机协同、平台集成）	从基础虚拟化支持升级为引擎级虚拟化能力体系
实时能力	xRT实时引擎（混合部署+跨OS通信）	xRT实时引擎2.0（实时扩展+混合部署+跨OS通信）	新增实时计算场景支持能力
运维模式	CLI+传统运维工具	OSPilot意图驱动运维（自然语言+CLI+API三位一体）	从命令驱动到意图驱动的范式跃迁
供应链治理	中心仓源码托管+常规开源组件管理	全链路SBOM+供应链检测+中心仓源码托管	从被动依赖上游到主动治理供应链全链路
生命周期	13年	13年	产品生命周期整体时间13年

3.4 新增能力

FusionOS 26在四大引擎与智能交互入口上推出了一系列新增能力，覆盖安全可信、AI加速、虚拟化、实时计算、智能运维、可靠性维测等方向。下表按引擎分组给出版本新增能力的索引，各项能力的详细技术说明参见第5章对应小节。

 版权所有 © 超聚变数字技术股份有限公司

引擎归属	新增特性	一句话价值
xSec	eFilter流量过滤引擎	用单一内核态高性能过滤引擎统一替代多策略栈，简化运维并降低开销
xSec	innersafer鲲鹏全栈主动免疫	软硬协同主动免疫，从硬件度量到运行时策略形成内生安全闭环
xSec	mcage内存精细化管控	内核内存非法访问检测与隔离，补齐内核态内存安全短板
xSec	mguard内存安全守护模块	用户态进程内存越界/释放后使用实时检测，无需重编译即可启用
xSec	trirole三权分立	系统/安全/审计三管理员职责分离，满足等保2.0三权分立要求
xSec	xSec安全中心	目标层→服务层→策略层→机制层统一管控闭环，等保/涉密/金融策略一键落地
xAI	Wings高性能推理引擎	OS原生轻量推理运行时，边缘/数据中心通用
xAI	xTuning-ops特定芯片定向优化算子库	针对国产NPU/GPU的算子级垂直调优，释放硬件算力上限
xAI	CXL共享内存统一管理	跨节点内存池化与统一寻址，突破单节点内存容量上限
xAI	TCMU性能增强	用户态存储后端IO通路优化，降低存储抽象层CPU与延迟开销
xAI	智能调度器	面向AI负载特征的感知式调度，提升训练/推理资源利用率
xAI	跨NUMA场景下代码页副本	减少跨NUMA代码页访问开销，提升AI算子执行局部性
xAI	面向AI场景的内存管理优化	大页/异构内存精细化管理，降低AI任务TLB miss与内存抖动
xAI	AIOS软件生态扩展能力	AI生态运行时与依赖统一治理，加速AI应用上手与部署
xVirt	xVirt-top虚拟化性能统计工具	VM/vCPU/线程级性能实时观测，top-like命令简化虚拟化运维
xVirt	xVirt-vna虚拟化节点代理	节点级虚拟化资源协同代理，为云管平台提供统一接入面
xRT	实时应用性能调优工具集	端到端调度抖动收敛至300μs以内，工业级确定性低延迟保障

 版权所有 © 超聚变数字技术股份有限公司

引擎归属	新增特性	一句话价值
xRT	实时引擎2.0 —— 混合虚拟化	100K数据通信时延<1ms，xRT节点上Windows等异构VM共存
xRT	实时引擎2.0 —— 容器化实时管控体系	MicRun容器运行时+nerdctl标准命令，容器创建延时<2s，实时与通用容器统一管理
OSPilot	OSPilot系统级智能体	OS原生AI助手，以自然语言完成运维/排障/调优，显著降低运维门槛
DFX	inband-sysinfo带内硬件管理服务	通过OS带内通道获取硬件信息，无需外接BMC即可完成关键硬件状态采集
DFX	remoteTrig远程主机故障诊断信息收集	中心节点远程触发受控主机故障现场采集与回传
DFX	SCSI细粒度错误处理框架	LUN/Target/Host三层分级隔离，避免单点故障引发全局重置
DFX	snapshot进程快照	用户态进程级快照，支撑故障复盘与冷热迁移
DFX	内核热升级	kexec机制下保留关键会话与内存状态完成内核版本切换，业务不中断
DFX	内核栈实时监控工具	关键路径内核栈实时采样，异常栈帧主动告警
DFX	免卸载实时增量快照	业务不停机的实时增量数据保护

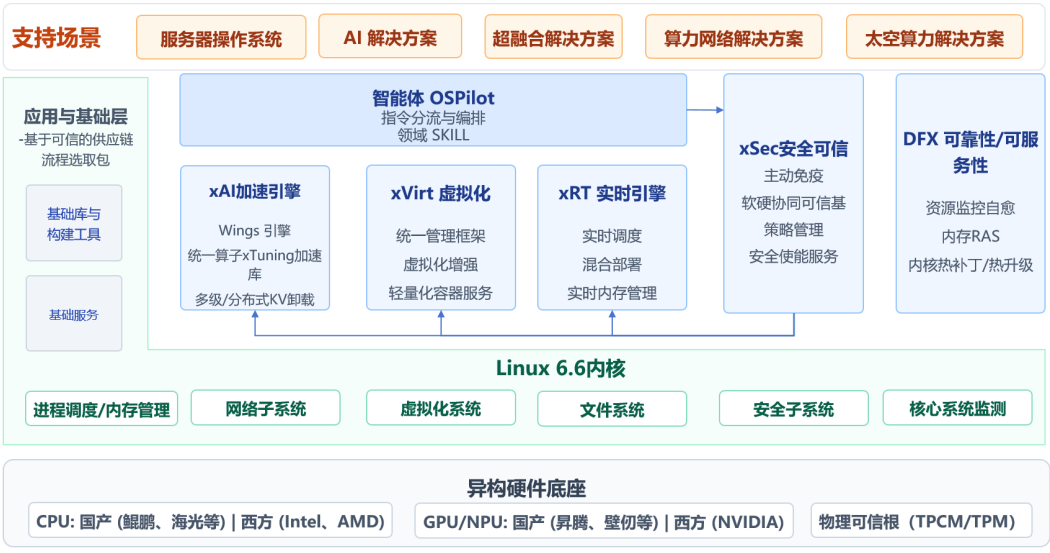
 版权所有 © 超聚变数字技术股份有限公司

4 系统架构总览

4.1 总体架构
4.2 架构全景说明

4.1 总体架构

FusionOS 26采用"统一底座+四大引擎+一个智能交互入口"的总体架构。架构以分层解耦为基础，安全作为内建属性贯穿全栈，各引擎共享底层机制但面向场景独立演进，在保持Linux生态兼容的前提下形成差异化能力体系。可靠性与维测体系横贯各层。



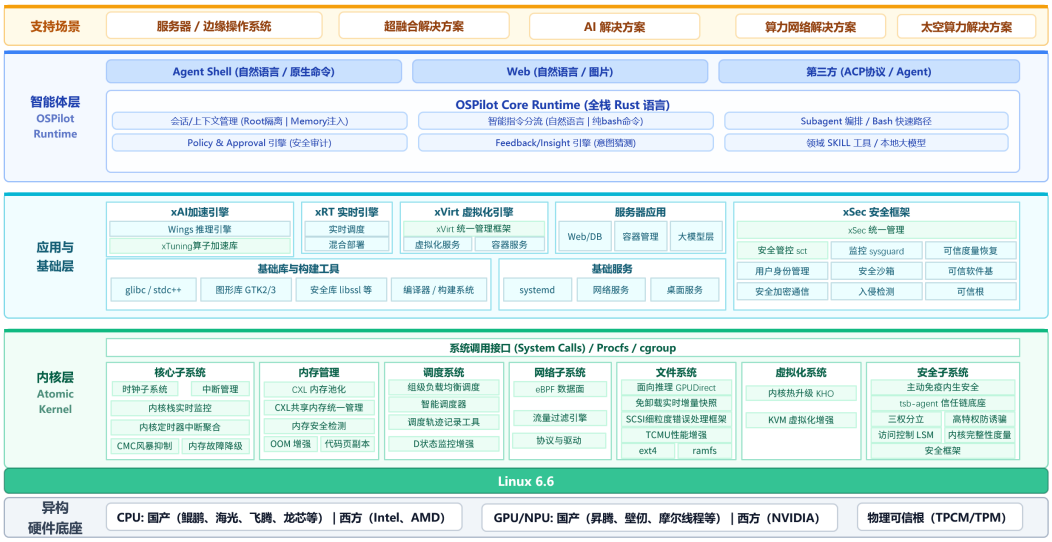
- 统一底座为上层各引擎提供共用的基础能力。
  - 在硬件适配层，系统完整兼容国产（鲲鹏、海光、昇腾等）与国际主流（Intel、AMD、NVIDIA等）全系列算力芯片，屏蔽底层硬件差异，为上层提供一致的运行环境。同时，基于TPM/TPCM等硬件组件的物理可信根能力，构建安全可信的底层基础。在内核层，基于Linux 6.6 LTS内核，针对数据中心核心负载进行内核精简与配置优化——对与目标场景相关性较低或维护价值有限的内核模块进行有序收敛，优先保留与算力承载、基础服务运行密切相关的驱动与功能，在收敛攻击面的同时保持主流生态兼容性。

 版权所有 © 超聚变数字技术股份有限公司

  - 在基础运行时层，提供系统库、包管理、容器运行时、资源隔离与调度编排等共性能力，为四大引擎和上层应用提供统一的运行基础。安全基础设施贯穿统一底座各层，从内核安全机制到系统级安全服务形成连续的安全支撑。
- 四大引擎建立在统一底座之上，分别面向安全、AI、虚拟化和实时四个方向形成定向增强，各引擎共享底层机制但独立演进：
  - xSec安全可信引擎：将可信根、策略编排、运行防护与安全使能能力组织为统一闭环，构建从硬件可信根到应用运行时的全链路可信保护体系。
  - xAI加速引擎：围绕自研Wings推理引擎提供深度学习推理优化，xTuning性能加速框架面向国产NPU/GPU进行垂直调优，形成从算子到存储通路的全栈AI加速能力。
  - xVirt虚拟化引擎：基于KVM虚拟化增强，打通虚拟化层与物理加速器的协同，提供统一虚拟化管理框架，支撑计算、存储、网络的一体化融合。
  - xRT实时引擎：提供实时调度与混合部署能力，支持实时容器与实时通信路径，保障关键业务的确定性低延迟。
- OSPilot智能交互入口作为FusionOS原生的系统级智能体，将自然语言、命令行和标准API请求统一为受控的系统任务入口。
  - OSPilot采用全栈Rust构建，常驻内存小于15MB，可无感融入生产环境。对于简单确定性操作，通过Bash快捷路径直接执行，零推理开销；仅在意图复杂时启用模型推理。其安全机制与xSec深度协同，从执行层沙箱隔离、权限层高危指令审批、输入层上下文防注入到恢复层快照回滚，建立四层执行边界。
  - OSPilot所依赖的本地轻量模型基于Wings引擎在CPU端实现超低延迟推理，使系统级智能体能够在涉密生产环境中本地部署和运行。
- 可靠性与维测体系横贯统一底座和各引擎。
  - 系统围绕四条主线构建可靠性能力：
    - 以运行态观测和异常事件采集提升故障可见性；
    - 以细粒度隔离将故障限制在最小影响域内；
    - 以内核热补丁、热升级和故障回退保障业务连续性；
    - 以快照、日志和诊断采集支撑问题追溯和持续改进。
  - 可靠性机制与安全可信、DFX维测增强、供应连续性和OSPilot统一管理入口深度协同，形成完整的可靠性保障闭环。

 版权所有 © 超聚变数字技术股份有限公司

4.2 架构全景说明



从整体架构视角看，FusionOS 26的各层级和组件之间形成清晰的职责分工与协同关系：

架构层级	职责定位	核心组成
异构硬件底座	屏蔽底层硬件差异，提供统一算力承载	国产+国际主流CPU/GPU/NPU全系列适配
内核层	提供经过场景化精简和配置优化的内核基础能力	Linux 6.6 LTS内核，进程调度、内存管理、文件系统、网络协议栈、设备驱动
基础运行时层	提供系统库、包管理、容器运行时等共性运行环境	Glibc、systemd、RPM/DNF、容器引擎、资源隔离与调度
引擎层	面向安全、AI、虚拟化、实时四个方向的定向增强	xSec、xAI（Wings+xTuning）、xVirt、xRT
智能交互入口	统一承接用户与系统的交互、编排和管控	OSPilot智能体（自然语言+CLI+API三位一体）
可靠性与维测	横贯各层的可靠性与维测保障	故障感知、隔离恢复、热补丁/热升级、诊断采集
供应链连续性（纵向贯穿）	保障从源码到镜像分发全链路的可信治理	全链路SBOM、供应链检测、中心仓源码托管、内源开发体系

统一底座提供共性能力、引擎承载场景增强、入口完成统一编排、可靠性与维测体系贯穿全局——这一架构使系统既具备差异化能力，又保持长期演进所需的稳定性和工程可治理性。

版权所有 © 超聚变数字技术股份有限公司

5 核心技术能力

5.1 安全可信引擎（xSec）
5.2 xAI加速引擎
5.3 虚拟化引擎（xVirt）
5.4 实时计算引擎（xRT）
5.5 智能交互入口（OSPilot）
5.6 可靠性与维测增强

5.1 安全可信引擎（xSec）

传统操作系统的安全能力通常以独立组件形式散落在系统各层——防火墙、SELinux、审计各管各的，缺少统一的管控和编排手段。管理员要落地一套完整的安全策略，往往需要逐一配置多个组件，操作繁琐、容易遗漏，且各组件之间缺乏联动。

xSec将操作系统已有的和新增的安全能力组织为一个可统一管理、可策略编排、可持续验证的安全框架。整个框架建立在物理可信根和软硬协同可信基之上，由三大支柱协同构成：xSec主动免疫负责安全防护执行，xSec安全中心负责策略管控，xSec安全使能服务负责能力对外输出。安全中心通过策略层的机制调用驱动机制层执行具体安全操作。



 版权所有 © 超聚变数字技术股份有限公司

- 物理可信根与软硬协同可信基

  整个框架的信任起点是物理可信根（TPM/TPCM）。在此之上，xSec软硬协同可信基通过可信软件基、可信软件栈和软硬协同机制，将硬件信任向上延伸，建立从开机上电到操作系统运行的完整信任链。启动阶段通过可信启动对引导加载器、内核、initramfs逐级度量；运行阶段通过对关键文件和可执行程序持续度量校验；检测到异常时，可回退到已知安全状态。可信基为上层三大支柱提供共同的信任锚点。

- xSec主动免疫

  主动免疫是xSec的核心执行面，建立在软硬协同可信基之上，按四个阶段构建递进式安全防护。

  - 主动约束

    从源头收窄权限和行为边界，在攻击发生之前降低系统暴露面。系统将管理职责拆分为系统管理员、安全管理员、审计管理员三个角色，互相制约，防止单一账户权限过大。在资源访问层面，通过完整性标识与强访问控制约束进程对文件、设备等资源的操作行为。应用可信管控和文件可信管控进一步将可信验证从系统层延伸到应用和数据层，确保只有经过验证的应用和文件才能在系统中运行和使用。

  - 主动保护

    在约束基础上，对运行中的关键资源建立持续防护。关键组件防护确保内核、系统服务等核心组件在运行时不被篡改或替换。高特权防诱骗防止攻击者利用高权限进程的信任关系实施提权攻击。进程防杀保障关键守护进程和安全服务在遭受恶意终止时能够自动恢复。外设端口安全管理对USB、串口等物理接口实施访问控制，阻断通过物理接口引入的威胁。

  - 主动检测

    在约束和保护的基础上，持续发现已经渗入或正在发生的异常行为。漏洞管理平台对系统组件进行持续的漏洞扫描和风险评估。内存安全检测（mcage）在运行时监控内核内存的非法访问和异常操作。安全SHELL资源隔离为管理会话提供独立的资源边界，防止会话间的信息泄露和横向渗透。系统端口可信跟踪与治理持续监控网络端口的开放状态和服务绑定情况，发现异常端口占用和未授权服务。

  - 主动恢复

    检测到安全异常后，将系统恢复到已知可信状态。文件可信恢复基于可信基线对被篡改的关键文件进行自动修复。可信恢复在系统级别提供从可信启动链到运行时状态的完整恢复路径，确保恢复后的系统处于经过验证的可信状态。

    四个阶段形成"约束→保护→检测→恢复"的完整闭环——先收窄攻击面，再保护关键资源，同时持续检测异常，发现问题后快速恢复到可信状态。

- xSec安全中心（策略管理）

  安全中心是xSec的管控面，负责将安全意图转化为可执行的策略并驱动机制层落地。

  安全中心采用目标层→服务层→策略层的三层结构：管理员在目标层声明安全意图（例如“等保2.0”），服务层将其拆解为有序的原子策略序列，经依赖分析、冲突检测和执行排序后，策略层通过机制调用驱动下游机制层执行具体安全操作，执行结果逐层回传形成闭环。复杂安全目标可以"一键落地"，降低配置门槛和人为出错概率；策略与机制解耦，新增安全功能只需注册新策略，不影响已有配置。

- 安全功能体系（机制层）

 版权所有 © 超聚变数字技术股份有限公司

机制层是安全能力的实际执行载体，对接安全中心策略层的机制调用。FusionOS 26在机制层构建了10个安全功能维度，覆盖从网络边界到系统运维的完整安全面：

序号	功能维度	防护目标	关键机制
维度1	边界防御	在系统暴露面构建第一道防线	主机防火墙（iptables/nftables/eFilter）、端口可信跟踪与治理、可信信道（SSL/TLS）、SYN Cookie防护
维度2	认证与权限控制	确认访问者身份并控制访问权限	PAM模块化认证框架（口令鉴别、多因素认证、失败锁定、超时断连）、统一身份认证、自主访问控制（DAC+ACL）
维度3	强制访问控制	基于系统策略强制执行访问控制	SELinux（BLP模型）、IAC（BIBA模型）、三权分立、Linux Capabilities最小授权、应用白名单
维度4	数据保护	保护数据在存储和传输中的保密性与完整性	进程通信完整性、块设备完整性校验、文件扩展属性保护（EVM）、日志记录完整性、文件系统/块设备加密（ecryptfs/dm-crypt+LUKS）、客体重用清零
维度5	内核内存安全	防止内核内存被非法访问、篡改或利用	页表隔离（KPTI）、SMAP/SMEP硬件隔离、地址空间随机化（KASLR）、SLAB空闲链保护、内核模块签名、mcage内存安全检测
维度6	可信保护	建立从硬件到应用的信任链	安全启动、可信启动（TPCM/TPM/TCM PCR度量）、IMA完整性度量、可信计算3.0

 版权所有 © 超聚变数字技术股份有限公司

序号	功能维度	防护目标	关键机制
维度7	安全检测与响应	持续监控、检测和响应安全事件	内核审计（kauditd+auditd）、RAS硬件错误日志、系统容错（systemd+sysguard+watchdog联动）、高特权防诱骗、进程防杀、AIDE入侵检测
维度8	安全隔离	隔离进程和资源，遏制攻击扩散	命名空间、控制组（cgroups v2）、沙箱（seccomp-bpf）、容器（Docker/containerd）、虚拟化（KVM+QEMU）、安全SHELL资源隔离
维度9	安全使能服务	将安全能力以标准化接口向上层开放	多元异构可信根框架（TPM/virtCCA统一接口）、内核Crypto框架（国际+国密算法）、OpenSSL密码库、内核IPsec、根CA证书集成
维度10	安全部署与运维	保障系统全生命周期的部署和运维安全	安全安装与最小化安装、安全加固工具、签名校验升级、内核热补丁（livepatch）、可信恢复、系统备份与恢复（LVM快照）

机制层与xSec主动免疫四个阶段是同一套安全能力在不同视角下的组织方式——主动免疫回答"按什么顺序防护"，机制层回答"用什么手段实现"。两者通过安全中心的策略管控链路统一编排，形成体系化的安全防护能力。

- xSec安全使能服务

  安全使能服务将主动免疫和机制层的安全能力向外输出：SDK用于上层业务集成安全能力；原子服务将认证、校验、检测、防护、恢复等能力封装为可独立调用、可灵活组合的服务单元；接口适配确保安全接口在系统版本升级过程中保持稳定。

- 安全和合规认证

  FusionOS 26的安全体系面向国内主流认证标准进行设计：

认证/合规项	目标等级	当前状态
网络安全专用产品认证	四级	申请中
商用密码产品认证	二级	申请中

 版权所有 © 超聚变数字技术股份有限公司

认证/合规项	目标等级	当前状态
中文编码认证	符合GB18030-2022标准	申请中

典型应用场景

xSec作为基础安全架构横贯所有部署场景。

- 在政务和金融等等保合规场景中，xSec安全中心的策略管理能力支持安全目标一键落地，降低合规配置的复杂度和人为出错概率。
- 在边缘和涉密环境中，xSec配合最小化安装和安全启动，将系统攻击面收敛到最小范围，同时通过IMA运行时度量持续验证关键文件完整性。在多租户虚拟化场景中，xSec主动免疫的主动约束和主动保护机制为租户间的资源边界提供系统级保障。

5.1.1 安全可信引擎特性介绍

xSec在FusionOS 26版本重点强化了主动免疫纵深防护、安全策略自动化编排（安全中心目标-服务-策略三层管控）等能力，同时完成了全量安全特性在6.6 LTS内核上的适配增强。

- innersafer鲲鹏全栈主动免疫

  通用安全软件以独立组件叠加在系统之上，缺乏与硬件信任根的协同，难以应对供应链攻击与权限滥用。innersafer基于鲲鹏TPCM/TCM硬件可信根，自下而上构建可信计算基（TCB）、可信安全基（TSB）、可信软件栈（TSS）三层信任链。运行时提供启动镜像静态度量、关键文件动态度量与可信恢复、cgroup会话级资源隔离、shell会话独立等多维度主动防护，并通过白名单基线工具与xSec安全中心联动。从硬件度量到运行时策略形成闭环，抑制供应链攻击与未知代码执行。

- xSec安全中心

  操作系统内置的防火墙、SELinux、IMA、审计等安全功能各自独立管理，落地安全防护目标时管理员需逐个组件配置，易遗漏、难审计。xSec安全中心采用四层资源模型——Target（安全目标）、Profile（策略集）、Policy（原子策略）、Mechanism（安全机制），将"想要的安全状态"转化为对安全机制的有序调用。每个会话经生命周期管理，支持原子化提交与失败回滚；多个Profile灵活组合定义同一Target，实现"安全目标一键达成"与"客户化定制"并存。CLI+Daemon前后端分离架构便于自动化集成，全流程留下审计记录，将分散配置压缩为目标导向的策略选择。

  FusionOS 26在xSec体系上还继承并向6.6 LTS内核完成适配增强了多项能力：cfraud高特权防诱骗（防止root账户被钓鱼脚本诱骗执行）、cups安全水印增强（打印输出嵌入身份水印防泄密）、IAC完整性访问控制（文件/进程完整性度量与访问控制）、sct安全管控工具（一站式物理端口管控）、livepatchadm内核热补丁管理（不停机修复内核漏洞）、killshield进程防杀（关键业务进程防止误杀、恶意杀）、xSec安全使能服务（安全能力SDK/API统一输出）。

- mcage内存精细化管控

  内核模块的内存越界、释放后使用、双重释放等问题往往直接导致系统崩溃，KASAN等开发态工具开销过大不适合生产长期开启。mcage为每个内核模块建立独立内存管理域，在分配内存块两端填充红区字节检测越界，以模块为单位记录分配、释放元数据，覆盖OOB（越界）、UAF（释放后使用）、DF（双重释放）

 版权所有 © 超聚变数字技术股份有限公司

三类典型异常。mcage支持最多10个模块同时纳管，每个模块独立配置告警阈值，通过/proc/mcage接口提供实时内存统计查询。性能开销低、可生产环境长期开启，将内核模块内存问题从崩溃后回溯压缩到运行时即时定位，显著降低运维排障成本。

- mguard内存安全守护模块

  用户态进程的缓冲区溢出、释放后使用等内存漏洞是生产业务崩溃的主要原因，AddressSanitizer等传统工具需重编译应用且性能损耗高，难以在已上线业务上部署。mguard在分配内存页前后插入"左右守护页"（ABABA交错模式），通过页表级权限将守护页设为禁止访问，应用越界或释放后再访问则立即触发硬件异常，并通过die_notifier将调用栈与时间戳记录到日志。mguard覆盖OOB、UAF、DF、守护页越界四类检测，无需重编译应用即可启用，可在生产环境中直接开启对关键业务进程的内存防护。该机制将内存安全从"漏洞被利用后修复"前置到"非法访问立即拦截"，显著提升关键业务可用性。

- trirole三权分立

  传统Linux的root账户集中几乎全部权限，单一口令泄露即可导致系统完全沦陷，且不满足等保2.0标准中"系统、安全、审计三权分立"的强制要求。trirole基于LSM框架实现三类管理员的职责分离——sysadm负责日常运维、secadm负责安全策略配置、auditadm独占访问审计日志，三者权限互不交叉。通过权限映射哈希表与DAC特权消除机制拦截越权访问，并对/var/log审计目录独立保护防止管理员篡改自身行为日志。trirole将root超级权限拆解为可审计的多角色操作，单点账户泄露不再意味着系统完全失守，满足GB/T 20272等保2.0三权分立合规项，为政务、金融、涉密场景测评提供原生支撑。

- eFilter流量过滤引擎

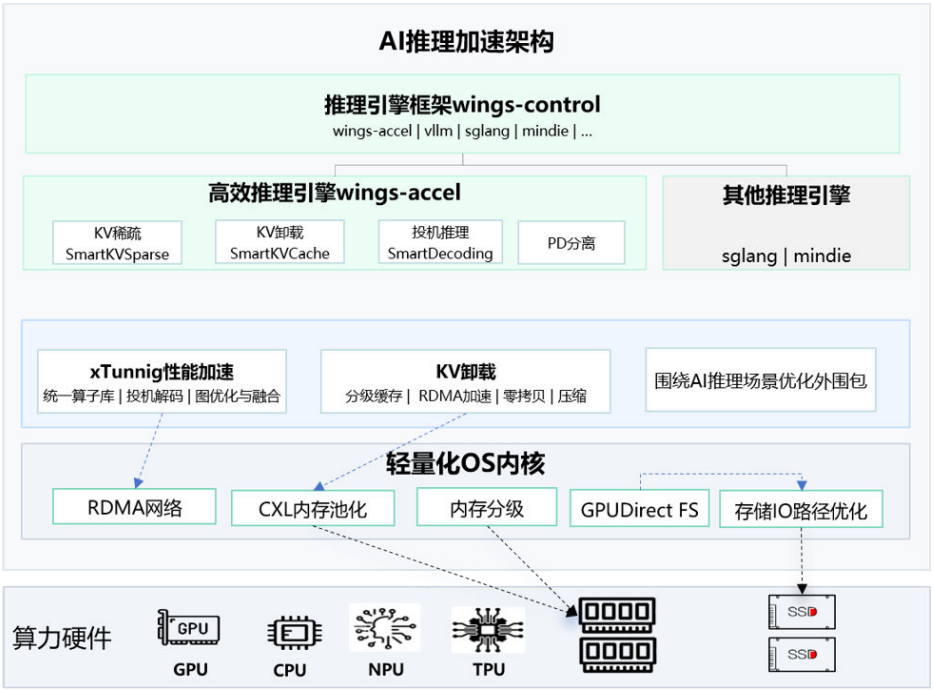
  传统iptables在虚拟化场景下存在覆盖盲区——虚拟机vNIC接入OVS网桥后无法被iptables规则触达，VM间东西向流量缺乏统一防护。eFilter基于eBPF构建内核态高性能流量过滤引擎，在每个网口的XDP入向钩子和TC出向钩子两点挂载eBPF程序，采用PERCPU_ARRAY类型BPF map消除多核同步开销。eFilter支持五元组（源/目IP、协议、源/目端口）精确匹配，每方向最多100条规则，提供实时丢包统计和pcap抓包能力。物理网口与vNIC的过滤策略统一到一套机制下，消除虚拟化网络的防护盲区，可视化的流量拦截数据加速网络故障诊断。

5.2 xAI 加速引擎

随着大模型从训练走向规模化推理部署，数据中心正的负载特征逐步在发生变化。AI负载与传统计算负载有本质差异：计算侧需要CPU、GPU、NPU等多类算力协同；内存侧对显存容量和带宽高度敏感；IO侧需要存储与加速器之间更短的数据路径。传统操作系统围绕CPU构建的资源管理模型，在面对这类异构、数据密集型负载时力不从心。

xAI在FusionOS 26版本已实现Wings自研推理引擎（多后端适配、轻量部署、OSPilot推理支撑）和xTuning算子加速库（国产NPU/GPU垂直调优、Kernel Launch优化），KV cache部署与缓存优化和GPUDirect文件系统在后续版本中规划落地，同时完成了已有AI支撑特性在6.6 LTS内核上的适配增强。

 版权所有 © 超聚变数字技术股份有限公司



- Wings推理引擎

  Wings是FusionOS 26自研的轻量级深度学习推理引擎，定位为操作系统原生的推理运行时。Wings直接运行在操作系统层，能够感知底层硬件拓扑和系统资源状态，在推理调度中做出更精准的资源决策。Wings通过统一的算子抽象层对接昇腾NPU、NVIDIA GPU、Intel CPU等多种计算后端，业务代码无需针对不同硬件做适配修改。

  Wings同时是OSPilot系统级智能体的核心推理基础设施。OSPilot所依赖的本地轻量模型基于Wings引擎在CPU端实现超低延迟推理，使智能体能够在离线和涉密环境中本地部署和运行。Wings与OSPilot构成算力使能层与智能交互层的双向协同：Wings为OSPilot提供低功耗、低延迟的推理支撑，OSPilot通过任务执行反馈持续优化推理调度。

- xTuning性能加速框架

  xTuning面向国产NPU/GPU进行垂直调优，以插件化方式对接推理引擎，不侵入基础引擎源码。当前版本重点解决国产算力平台上的算子执行效率问题，通过算子加速库减少Kernel Launch开销，优化算子调度和执行路径，提升国产算力平台上的推理吞吐。

  后续版本中，xTuning将围绕长输入短输出、上下文渐增、多轮对话等典型推理场景，进一步构建推理运行时增强能力，包括KV Cache分层卸载与量化、KV稀疏、异构PD分离、动态调度和投机推理等机制，以可配置、可回退的方式实现端到端推理加速。

- KV cache部署与缓存优化（后续版本规划）

  大模型推理中，KV cache占用大量显存且换入换出频繁，是影响推理吞吐和Token生成效率的关键瓶颈。xAI规划通过细粒度的显存管理和跨请求缓存复用，降低显存浪费，提升Token生成效率。

- GPUDirect文件系统（后续版本规划）

  GPUDirect文件系统规划打通GPU内存与存储之间的DMA快速通道，绕过CPU bounce buffer，缩短数据加载时延和checkpoint写入耗时。该能力面向配备高性能GPU和NVMe存储的特定硬件环境，为数据密集型AI负载提供存储通路加速。

 版权所有 © 超聚变数字技术股份有限公司

典型应用场景

xAI主要面向AI推理与智能计算场景。在大模型在线推理场景中，Wings推理引擎的多后端适配与xTuning的算子级调优协同工作，为高并发推理请求提供低延迟、高吞吐的运行环境。在边缘本地推理场景中，Wings的轻量部署特性使其可以在资源受限的边缘设备上运行推理任务。Wings同时为OSPilot提供CPU端本地推理支撑，使智能运维能力在离线和涉密环境中可用。随着KV cache优化和GPUDirect文件系统在后续版本中落地，xAI将进一步覆盖显存管理和存储通路加速，形成从算子到数据通路的全栈AI加速能力。

5.2.1 xAI 加速引擎特性介绍

xAI在FusionOS 26版本已实现Wings自研推理引擎（多后端适配、轻量部署、OSPilot本地推理支撑）和xTuning算子加速库（国产NPU/GPU垂直调优、Kernel Launch优化）两个核心组件，KV cache部署与缓存优化、GPUDirect文件系统作为架构规划能力在后续版本中落地，同时完成了已有AI支撑特性在6.6 LTS内核上的适配增强。以下聚焦版本新增特性。

- Wings高性能推理引擎

  OS原生轻量推理运行时，三层解耦架构（wings-infer控制层/engine执行层/wings-accel加速层），Adapter框架统一MindIE/sglang/vllm多引擎接口，支持K8s分布式部署与健康检查门禁。

- xTuning-ops特定芯片定向优化算子库

  面向鲲鹏/昇腾的算子级垂直调优，释放国产芯片算力上限。

- CXL共享内存统一管理

  单节点DDR容量上限已难以满足大模型推理的KV cache与权重常驻需求，跨节点通信又受限于网络带宽与延迟。该特性基于CXL 2.0 Type 3设备，构建FM Server（256MB粒度全局Buddy分配）+ Local Server（细粒度本地缓存）+ Client库的分层架构，最大支持64个主机、1024个客户端规模。分配时采用快速路径（本地缓存命中直接返回）与慢路径（向FM Server申请新区块）两级策略，以clflush指令保证跨节点缓存一致性，多级锁机制保障并发安全。CXL共享内存对上层应用提供标准编程接口，透明突破单节点内存容量限制。

- TCMU性能增强

  用户态存储后端（如分布式块服务、iSCSI Target）通过TCMU与内核块层对接，传统IO路径在128KB以上大块数据上存在双重内存拷贝（内核→共享内存→用户缓冲区），并且UIO子系统的info_lock互斥锁在高并发时成为瓶颈。该特性引入Zero-copy模式——将内核scatterlist pages直接映射到用户空间VMA（vm_map_pages_special批量映射32页），消除第一次拷贝；同时提供Bypass Data Area模式绕过UIO数据区直接完成数据搬运；将UIO访问锁替换为percpu_ref实现无锁化。大块IO吞吐性能显著提升，高并发IO延迟改善，降低存储抽象层的CPU开销。

- 智能调度器（含分组智能调度器）

  AI推理服务要求延迟确定性（需独占核心），训练任务追求吞吐（需充分利用剩余算力），两者混部时现有CFS/cpuset/cgroup配额无法兼顾。智能调度器以分组智能调度器（GSS）为核心，在CFS之上构建增强调度层，感知NUMA/Socket/LLC多层拓扑；引入软CPU绑定机制在"性能确定性"与"资源灵活性"间取得平衡；任务分类感知模块（TC）运行时检测任务特征（五类分类），动态修正vruntime优先级。推理服务响应性与训练吞吐的同时保障，缓存命中率提升，自适应动态调度避免人工频繁调参。

- 跨NUMA场景下代码页副本

 版权所有 © 超聚变数字技术股份有限公司

多Socket服务器上AI算子频繁访问远端NUMA节点代码段，跨节点内存延迟显著高于本地访问，导致指令流水线空转。TextMirror机制为远端代码页在本地节点创建只读副本，通过xarray结构管理副本页映射关系，支持THP透明大页并以memcg为粒度进行策略隔离，应用无感知、无需修改即生效。跨NUMA代码页访问延迟降至本地访问水平,AI推理和训练中频繁调用的公共算子库执行局部性显著改善。

- 面向AI场景的内存管理优化

  大模型训练/推理消耗海量内存，OOT加速器驱动可能引发内核内存损坏，多核RSS统计在大规模系统上存在精度偏差，CXL扩展内存故障缺乏恢复通路。该特性从四个维度优化：(1) CXL共享内存管理（与前述CXL特性协同，256MB粒度、64×1024规模并发）；(2) 内核模块拦截CXL内存故障并执行页表重映射自动恢复；(3) RSS采用percpu_counter_tree三级分层计数架构（Level 0-N），改善大规模系统统计精度；(4) OOT驱动预分配多套kmalloc缓存集合+符号重定向+两级隔离，防止加速器驱动内存损坏波及内核。以上机制组合为AI大场景提供高可靠、高精度、强隔离的内存基础设施。

- AIOS软件生态扩展能力

  AI生态高度碎片化——不同框架对glibc/Python/CUDA/CANN版本要求各异，"依赖地狱"导致应用跨系统部署困难、交付周期长。AIOS生态扩展基于FARE分层模块化架构，定义统一FPK软件包格式并通过Builder支持DEB/RPM/目录等多源转换；运行时以Mount Namespace + OverlayFS双层隔离为应用提供独立文件系统视图，配合Cgroups资源限制与Seccomp系统调用过滤实现"安全沙箱"效果；CLI统一命令行入口覆盖构建-安装-运行-卸载全生命周期。实现"一次构建、到处运行"，跨发行版兼容，国产AI应用快速交付。

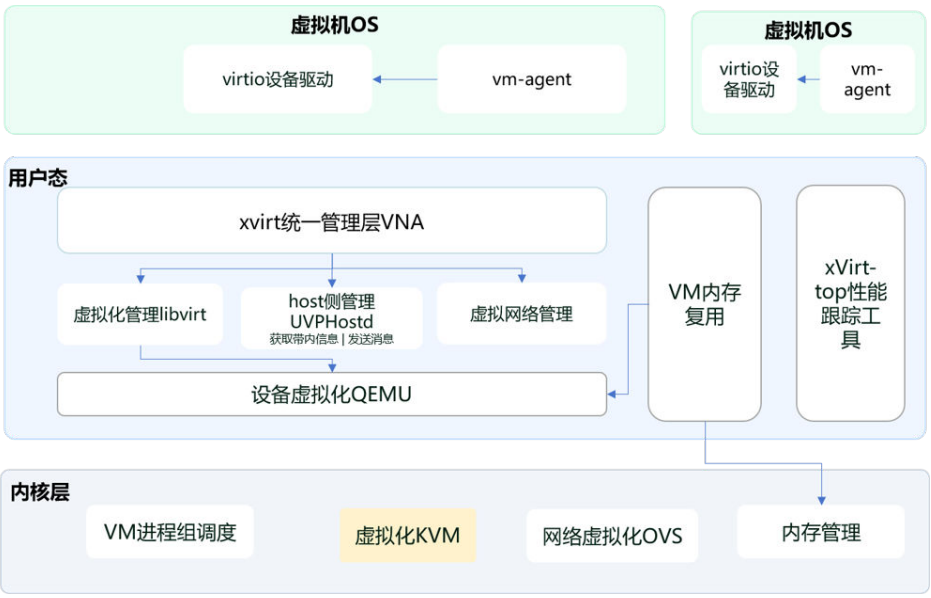
FusionOS 26在AI Native OS底座上还继承并向6.6 LTS内核完成适配增强了多项能力：xTuning-bench算力硬件性能评估工具（提供CPU/GPU/NPU/内存/存储端到端基准测试，输出硬件利用率瓶颈定位报告）、xTuning-devtools算子开发效率提升库（算子性能profiling与kernel优化建议，加速国产芯片算子开发迭代）。

5.3 虚拟化引擎（xVirt）

虚拟化是数据中心的基础能力，但传统KVM虚拟化方案存在几个现实痛点：虚拟化层与物理加速器之间存在性能损耗，GPU/NPU直通和共享的管理分散在多个工具中；虚拟机内部运行状态对宿主机不透明，故障定位和性能调优缺乏跨层信息；计算、存储、网络的虚拟化管理各自为政，难以统一编排。

xVirt是FusionOS 26的虚拟化引擎，在KVM基础虚拟化之上做了三个方向的增强：统一观测与管控、宿主机-虚拟机协同、平台一体化集成。

 版权所有 © 超聚变数字技术股份有限公司



- 统一观测与管控。

  传统虚拟化管理通常只能看到VM粒度的资源占用，xVirt将观测粒度下沉到VM、vCPU、线程级别，同时覆盖计算、网络、存储的实时状态。管理员可以在统一界面中查看虚拟化节点的全维度运行状况，而不需要在多个工具之间切换。这使虚拟化管理从单纯的"创建-启动-停止"升级为"可观测、可调度、可管控"的完整能力。

- 宿主机-虚拟机协同。

  xVirt在宿主机和虚拟机之间建立了CPU亲和拓扑感知和状态同步通道。宿主机可以感知虚拟机内部的vCPU运行模式（用户态/内核态/空闲），据此动态调整物理CPU的调度策略，减少不必要的上下文切换和调度冲突。虚拟机侧的关键事件（异常、性能瓶颈）也可以通过该通道传递给宿主机的日志和诊断体系，打通虚拟化栈与物理基础设施栈之间的信息壁垒。

- 平台一体化集成。

  在虚拟化与云基础设施场景中，xVirt提供统一管理框架，将计算虚拟化、存储虚拟化和网络虚拟化的管控能力整合到同一套管理面中。结合组级负载均衡调度能力，xVirt支持CPU与GPU/NPU的协同调度，配合CXL内存池化技术打破单节点内存容量限制，实现跨资源类型的全局最优编排。

典型应用场景

xVirt面向虚拟化与云基础设施场景。在私有云和超融合部署中，xVirt的统一管理框架将计算、存储、网络虚拟化的管控能力整合到同一套管理面，为上层云管平台提供完整的底层API支撑。在AI与虚拟化混合部署场景中，xVirt的加速器直通/共享能力和组级负载均衡调度支持GPU/NPU资源在多个虚拟机之间的灵活分配。在多租户场景中，Guest-Host状态同步通道使宿主机能够感知虚拟机内部运行状态，提升跨层故障定位和性能调优效率。

5.3.1 虚拟化引擎特性介绍

xVirt在FusionOS 26版本重点强化了宿主机-虚拟机跨层协同（CPU亲和拓扑感知、Guest运行状态同步通道）和加速器资源统一编排（GPU/NPU直通与共享）等能力，同时完成了虚拟化特性在6.6 LTS内核上的适配增强。

版权所有 © 超聚变数字技术股份有限公司

- xVirt-top虚拟化性能统计工具

  开源perf kvm工具仅能观测宿主机整体KVM事件热点，缺少按VM/vCPU/线程粒度的性能归因视图，线上CPU抖动或exit异常时无法快速定位责任VM。xVirt-top基于procps-ng top工具扩展，通过libvirt获取VM PID、procfs获取线程信息、kvm debugfs获取vCPU统计数据，以双缓冲帧差方式计算增量，渲染为top-like实时界面。在10 VM场景下刷新延迟<50ms、CPU占用<2%、内存<100MB；50 VM场景刷新延迟<100ms、CPU<5%；100 VM场景刷新延迟<200ms、CPU<10%。管理员无需额外部署APM即可在终端完成VM/vCPU/线程级性能快速归因与瓶颈定位。

- xVirt-vna虚拟化节点代理

  大规模虚拟化集群的计算、网络、存储资源分散在各节点独立管理，上层云管平台缺乏统一的节点级接入接口，资源编排效率低且网络配置复杂。xVirt-vna采用三层架构（资源抽象层/业务逻辑层/接口适配层），底层通过libvirt管理计算资源、OVS管理网络、对接多种存储后端，以多线程+分布式锁保障并发一致性。API响应时间P95<100ms，虚拟机启动<30s，并发处理>1000 QPS，系统内存<2GB、CPU<150%。xVirt-vna为云管平台提供统一节点接入面，支持水平/垂直弹性扩展，满足千节点级集群动态管理需求。

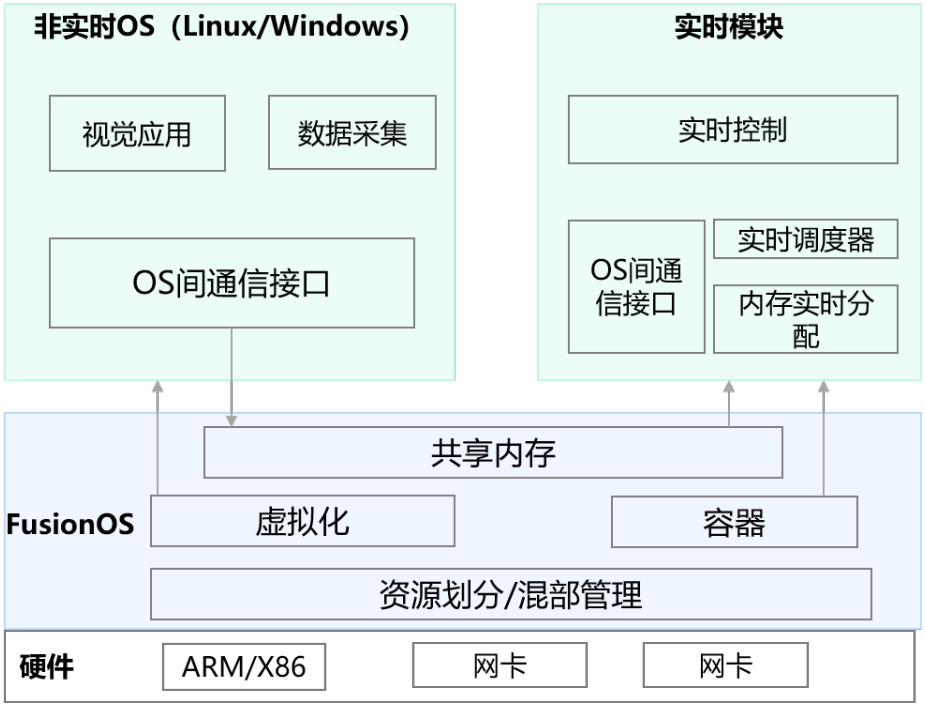
FusionOS 26在虚拟化引擎上还继承并向6.6 LTS内核完成适配增强了多项能力：Hostd虚拟机带内管理服务（VM内部带内信息采集与管理，可获取Guest网络/磁盘/OS等状态）、memoc内存复用（KSM与Balloon协同实现多VM内存超分与页面共享）、vmtools虚拟化管理工具（Guest端驱动与工具集，支持时钟同步与心跳）、xVirt虚拟化引擎统一管理框架（计算/存储/网络虚拟化资源的统一编排与生命周期管理）以及xVirt虚拟化引擎统一系统配置管理（集中式配置变更与版本化管控）。

5.4 实时计算引擎（xRT）

工业控制、边缘网关、电信协议处理等场景对操作系统有一个共同要求：确定性低延迟。传统Linux内核采用公平调度策略，面向吞吐量优化，在实时性要求高的场景中调度抖动难以消除。行业常见的做法是部署一套独立的RTOS，但这又带来两套系统的开发、运维和通信成本。

xRT是FusionOS 26的实时计算引擎，目标是在一台物理设备上同时满足通用计算和实时控制两类需求，让FusionOS 26与边缘实时OS能够共存协作、各司其职。xRT从三个层面构建这种能力：混合部署架构、实时容器、跨OS高效通信。

 版权所有 © 超聚变数字技术股份有限公司



- 混合部署架构

  xRT在一台物理设备上为FusionOS 26和边缘实时OS划分独立的资源域——CPU核、内存区域、设备通道各自预分配，互不干扰。FusionOS 26负责通用计算、管理和网络通信，实时OS负责确定性低延迟的控制任务。两个系统共享同一硬件平台，但在资源层面彼此隔离，避免通用负载的调度波动影响实时任务的时序确定性。
- 实时容器

  传统实时应用通常直接部署在裸金属RTOS上，缺少统一的生命周期管理手段。xRT通过提供实时容器能力，将实时OS及其应用封装为容器，纳入与通用容器一致的管理体系。实时容器支持设备直通、时钟同步、资源配额管理和网络通信，使实时应用具备与通用应用相同的部署、升级和监控体验，同时保持实时性能。
- 跨OS高效通信

  混合部署场景中，通用域和实时域之间需要频繁交换数据和控制指令。xRT基于openAMP构建跨OS通信通道，通过RPMsg协议实现两个系统之间的高效核间通信，支持实时数据上报、控制指令下发和状态同步。通信路径独立于网络协议栈，延迟可控、开销低，满足工业协议处理和低时钟抖动场景的要求。

典型应用场景

xRT面向需要确定性低延迟的边缘实时控制场景。在工业网关场景中，xRT的混合部署架构支持FusionOS 26与实时OS在同一设备上共存——FusionOS 26负责数据采集、协议转换和远程管理，实时OS负责PLC控制和工业协议处理，两者通过openAMP跨OS通信通道高效交换数据。xRT的实时容器能力将实时应用纳入与通用容器一致的生命周期管理体系，简化边缘节点的部署和运维。xRT还提供实时应用性能调优工具链，覆盖CPU绑定、中断亲和、tracepoint追踪和调度延迟分析，帮助开发者定位实时路径上的抖动源。

5.4.1 实时计算引擎特性介绍

xRT在FusionOS 26版本重点构建了Linux与实时OS混合部署架构（CPU/内存/设备资源预分配隔离）、实时容器（containerd shim/nerdctl、设备直通、时钟同步）和跨OS

 版权所有 © 超聚变数字技术股份有限公司

高效通信（openAMP/RPMsg核间通信）等能力，同时完成了实时相关特性在6.6 LTS内核上的适配增强。

- 实时应用性能调优工具集

  电力、车载、智慧交通、通信算网等关键场景对实时任务的时序确定性有极致要求，但实时应用在生产部署中仍受内核调度冲突、网络中断干扰、任务优先级管控粗放等因素影响。FusionOS 26在xRT引擎中内置实时应用性能调优工具集，以monitor与trace两个内核模块协同工作，提供任务调度精细化绑定、网络中断隔离、任务执行轨迹追踪与抖动分级报警四类手段，帮助xRT在标准硬件平台上将端到端调度抖动收敛至300μs以内，使工业控制、车载与电信协议处理类应用具备可被严格保障的确定性运行环境。

- 实时引擎2.0 —— 混合虚拟化

  边缘控制节点除运行RTOS实时控制任务外，常需承载Windows业务VM、私有协议网关等异构操作系统，但传统方案仅支持"Linux + RTOS"两层共存，无法满足多OS混部需求。FusionOS 26在xRT引擎中引入混合虚拟化能力——基于KVM/QEMU构建企业级虚拟机管理层，通过VFIO直通将I210网卡、USB、GPU等关键硬件分配给客户机，统一以vmdeploy CLI完成全流程管理，并通过vsock低延迟通道、电源/时间同步服务实现宿主机与Windows客户机协同。Windows应用与容器应用、容器间应用在100K数据规模下通信时延稳定低于1ms，把xRT节点扩展为"通用OS + RTOS + 异构虚拟机三层共存"。

- 实时引擎2.0 —— 容器化实时管控体系

  行业普遍以裸金属方式部署RTOS，缺乏统一的生命周期管理手段，运维、升级与监控难以纳入云原生体系。FusionOS 26在xRT引擎中提供MicRun容器运行时，基于containerd shim v2协议实现——通过OCI注解识别RTOS容器，将nerdctl等标准容器命令透明映射到底层Mica工具链，完成Uniproton等RTOS实例的创建、启动、停止、删除全流程管理。容器创建启动延时低于2s、停止/重启延时低于5s、删除连同RTOS实例回收延时低于2s。该机制让RTOS首次以"标准容器"形态融入云原生工具链，为后续与K8s调度面对接预留扩展空间。

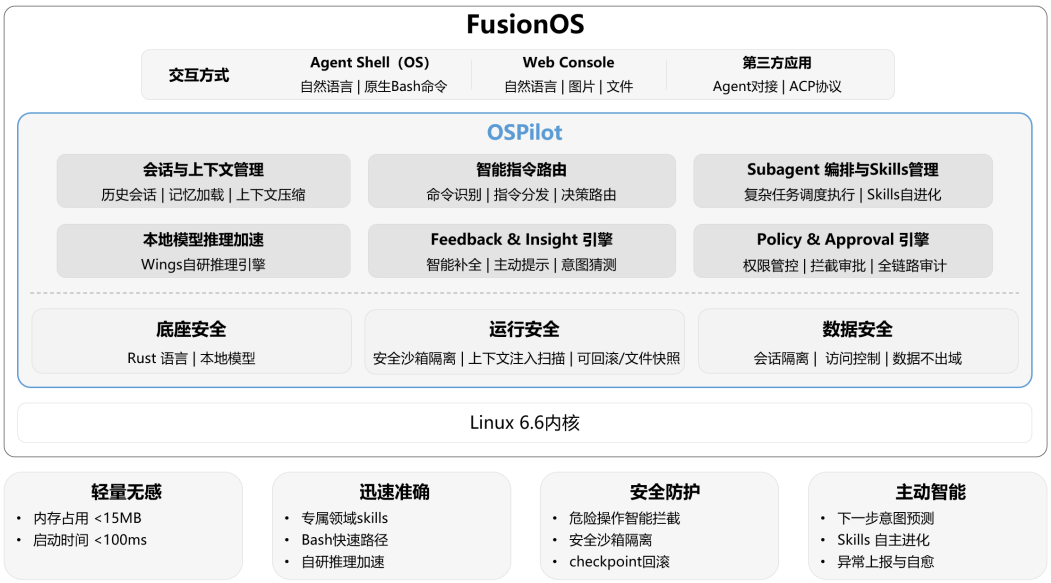
FusionOS 26在实时计算引擎上还继承并向6.6 LTS内核完成适配增强了多项能力：OS间高效通信（基于openAMP与2MB核间共享内存，合并多次拷贝与中断通知，显著降低非实时域与实时域用户进程间的核间通信时延）、多实例边缘实时系统管理（基于MCS混合关键性系统在同一工控机拉起多个Uniproton实例，单终端管理多条产线主站，提升硬件利用率）。

5.5 智能交互入口（OSPilot）

服务器操作系统的运维长期依赖命令行，操作过程缺乏预校验和可撤销机制——一次网络策略误配可能导致集群隔离，一组内核参数调整不当可能引发全局性能劣化。随着数据中心规模持续扩大，人工逐机操作的运维模式已难以应对日益增长的系统复杂度。与此同时，随着大模型和智能体技术的成熟，操作系统的使用主体正从"人"扩展为"人+AI Agent"，系统需要为智能体提供安全可控的执行环境。

OSPilot是FusionOS 26原生的系统级智能体，将自然语言、命令行和标准API统一为一个受控的系统任务入口，让"会表达意图的人"也能安全地管理系统。

 版权所有 © 超聚变数字技术股份有限公司



- 轻量原生，无感嵌入生产环境

  OSPilot采用全栈Rust构建，常驻内存小于15MB，启动即就绪，无需额外安装Python运行时或AI框架依赖。作为操作系统原生组件随系统镜像发布，可直接运行在生产环境中，对系统资源几乎无感知负担。

- 双路径执行，按需启用推理

  OSPilot内部区分两条执行路径：对于简单确定性操作（如查看磁盘用量、重启某个服务），通过Bash快捷路径直接执行，零推理开销，响应速度与手动敲命令一致；仅当意图复杂或需要多步编排时（如"检查近一周内存持续增长的进程并生成报告"），才启用本地轻量模型进行推理。这种设计避免了所有操作都过模型带来的延迟和资源消耗。

- 四层安全边界，受控执行

  智能体自主执行系统操作，最大的风险是"智能失控"——越权操作、误删数据、注入攻击等。OSPilot与xSec安全引擎联动，建立四层执行边界：

安全层	机制	防护目标
执行层	沙箱隔离，限制文件系统和网络访问范围	防止操作逃逸到非授权区域
权限层	高危指令二次审批，敏感操作需人工确认	防止误操作和越权执行
输入层	上下文防注入，过滤恶意prompt构造	防止通过自然语言注入绕过安全策略
恢复层	操作前自动快照，执行异常时一键回滚	保障操作可撤销、状态可恢复

- 本地推理，离线可用

  OSPilot所依赖的本地轻量模型基于Wings推理引擎在CPU端运行，无需GPU，推理延迟低。这意味着OSPilot可以在离线、断网、涉密等不允许连接外部AI服务的生产环境中正常工作，是目前少数能在纯本地环境中运行的操作系统级智能体。

 版权所有 © 超聚变数字技术股份有限公司

典型应用场景

OSPilot作为统一智能交互适用于所有部署场景。在大规模数据中心场景中，OSPilot的意图驱动运维能力将复杂的多步运维操作（如"检查近一周内存持续增长的进程并生成报告"）转化为受控的自动化任务，减少人工逐机操作的重复劳动。在边缘场景中，运维人员难以现场触达设备，OSPilot支持远程意图驱动运维，降低对现场人员的依赖。在涉密和离线环境中，OSPilot基于Wings的CPU端本地推理能力运行，无需连接外部AI服务也可使用。

5.6 可靠性与维测增强

金融、电信等行业要求操作系统支撑7×24小时连续运行，任何计划外停机都意味着业务损失。但现实中故障无法完全避免——硬件老化、内核Bug、存储链路异常、补丁升级引入兼容性问题，这些都是生产环境中的常态。关键问题是：故障发生后，系统能多快发现、把影响控制在多小的范围、多快恢复业务、事后能否追溯根因。

FusionOS 26的可靠性设计围绕：感知、收敛、持续、保全、恢复、追溯——故障可感知、影响可收敛、业务可持续、状态可保全、数据可恢复、问题可追溯。维测增强（DFX）则为可靠性主线提供贯穿全栈的观测、诊断和维护工具支撑。

- 故障感知

  系统通过内核检查点、状态追踪和维测增强机制，建立对异常事件、关键路径状态、设备故障和资源异常的实时可见性。针对长期处于D状态（不可中断睡眠）的进程，系统通过hungtask-monitor增强监控，识别I/O阻塞、调度等待、底层设备异常等根因，为后续故障隔离和恢复提供前置判据。

- 故障收敛

  传统Linux在存储链路故障时倾向于全局重置——一块磁盘出问题，整条SCSI Host路径上的设备都受影响。FusionOS 26在SCSI子系统中引入细粒度故障处理，围绕LUN、Target、Host三个层级实现分层隔离式恢复。单一设备或单一路径出现异常时，系统在最小范围内执行错误注入、临时隔离和恢复操作，避免波及无关业务和设备。

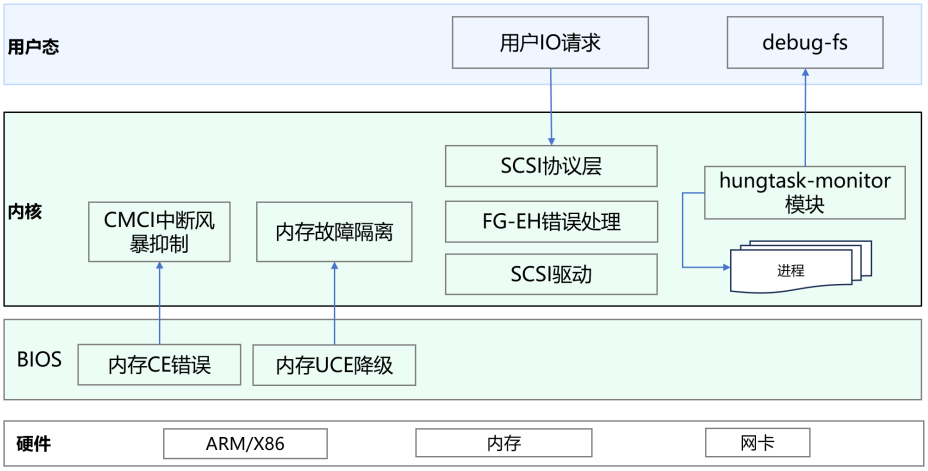
- 业务持续

  内核热补丁支持在不重启系统的情况下修复内核漏洞和缺陷，消除传统"打补丁必须停机"的矛盾。对于需要内核版本切换的场景，FusionOS 26通过kexec机制支持关键会话和内存状态的保留与恢复，在最小化业务中断的前提下完成版本切换。用户态服务热升级进一步将在线维护能力从内核层扩展到应用层。

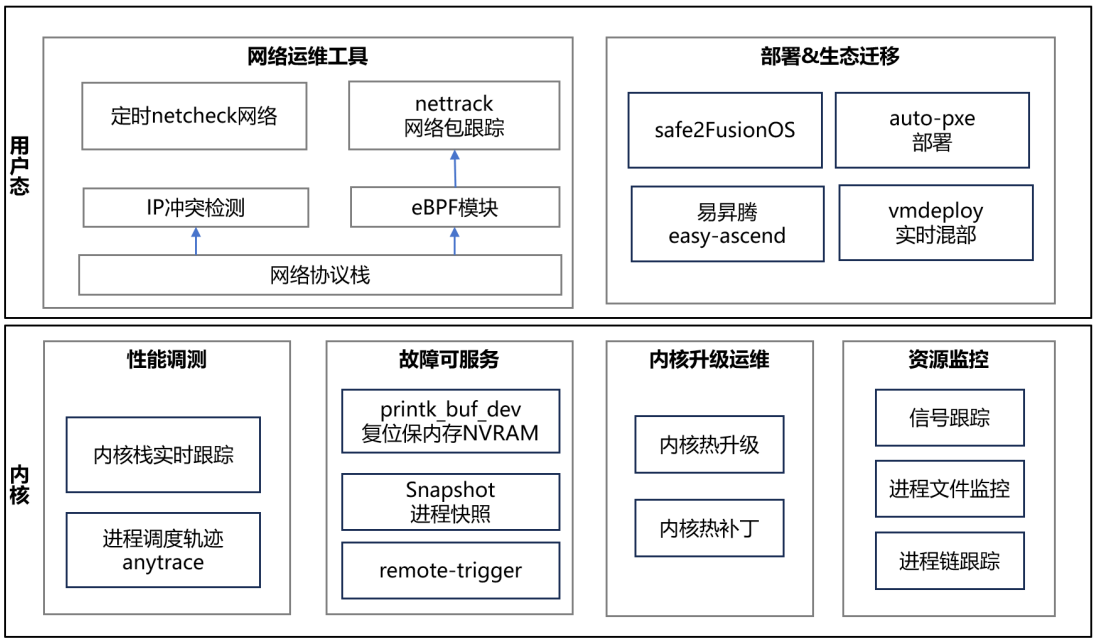
- 现场保全与数据恢复

  系统在异常发生时自动采集内存、日志、寄存器、消息队列等关键现场信息并持久化保存，确保故障发生后的证据完整可用，降低问题复现难度和证据丢失风险。块设备实时数据保护作为可靠性基线能力之一，在块设备层提供时间点快照、数据追踪、模式切换和状态查询，使关键业务在持续写入的同时具备数据保护和定点恢复能力。

版权所有 © 超聚变数字技术股份有限公司



维测增强（DFX）。 可靠性机制解决的是"出了问题怎么办"，维测增强解决的是"怎么更快地发现问题、定位问题、修好系统"。FusionOS 26的DFX体系覆盖五类场景：



能力类别	覆盖内容
运行态观测	进程状态追踪、内存使用分析、网络连接监控、IP冲突检测、内核栈异常捕获等，支持常态巡检和按需诊断
现场保全	异常定位、内核crash、极端故障场景下的关键证据自动采集和持久化
在线维护	内核热补丁、用户态热升级、kexec内核切换，支撑不停机或最小中断的补丁修复和版本升级
迁移辅助	系统替换和环境构建场景下的迁移准备、执行和校验支持
软硬协同维护	通过系统内部通道获取硬件状态、温度、功耗信息，为硬件监控、设备管理和故障处理提供统一硬件视图

 版权所有 © 超聚变数字技术股份有限公司

典型应用场景

可靠性与维测体系横贯各层，在高可靠关键业务场景中价值最为突出。金融、电信等场景要求系统可用性达到五个九以上——内核热补丁和用户态热升级支持不停机修复漏洞和缺陷，SCSI细粒度故障处理将存储链路故障隔离在最小影响域内，块设备实时数据保护为持续写入的关键业务提供定点恢复能力。在大规模集群场景中，DFX维测增强的运行态观测和软硬协同维护能力为集群级故障定位和容量规划提供数据基础。

5.6.1 可靠性与维测特性介绍

可靠性与维测增强在FusionOS 26版本新增自研免卸载实时增量快照（块设备实时数据保护：时间点快照、定点恢复等）、带内硬件管理服务（软硬协同维护：硬件状态、温度、功耗统一视图）、存储链路细粒度故障隔离（SCSI LUN/Target/Host分层恢复）等能力，同时完成了全量可靠性与维测特性在6.6 LTS内核上的适配增强。

- 免卸载实时增量快照

  块设备数据保护的传统方案要么依赖文件系统快照（受FS类型限制）、要么需快照前停止业务IO（导致中断），无法满足金融、电信"业务零中断"的要求。该特性在块设备层通过修改bd_disk->fops拦截IO，采用写时拷贝（COW）将原始数据写入独立COW文件，由4KB Header、按16GB分节的映射索引区与数据区组成，支持自动扩容与LRU节区缓存。提供"快照模式"与"增量模式"灵活切换，通过序列号链接形成连续增量链，配合update-img工具完成增量合并。整个过程业务无感、无需卸载文件系统，将数据保护从"周期性窗口备份"升级为"实时持续保护"。

- 带内硬件管理服务

  传统BMC带外管理在部分配置中缺失或功能受限，运维人员无法通过OS自身获取全面的硬件健康状态。inband-sysinfo基于Redfish协议，采用分层架构（服务层Manager/Monitor/Redfish Server + 业务逻辑层资源/事件/配置/存储/网络/日志六大模块 + 驱动层1710虚拟网卡与BMC对接），通过OS带内通道实现CPU/内存/磁盘/网络全维度硬件信息采集与监控。无需外接BMC即可完成关键硬件健康检查与告警，降低运维成本，扩展对多厂商异构服务器的管理兼容性。

- SCSI细粒度错误处理框架

  传统Linux SCSI错误处理在单块磁盘命令超时或错误时重置整条Host路径，使局部小概率故障放大为全局IO阻塞，严重影响业务连续性。该特性实现LUN级、Target级、Host级三层分级细粒度隔离式恢复，通过Sense Data快速识别可直接恢复的错误类型（CHECK CONDITION状态码匹配），采用阶梯式策略逐层升级恢复力度。将故障影响范围严格限制在单一设备/路径，其他设备保持正常IO，存储子系统可用性显著提升。

- 远程主机故障诊断信息收集

  系统死锁、卡死、SSH无法登录等严重故障场景下，常规远程诊断手段完全失效，问题根因分析依赖人工到场。remoteTrig通过Linux input子系统监听物理键盘事件，识别特定组合键序列（有限状态机跟踪按键状态），支持RT_ENABLED（触发panic收集完整dump）、RT_DEBUG（记录诊断日志但不重启）、RT_DISABLED（关闭）三种模式，并提供异常输入防护防止误触发。在系统完全无响应时仍可远程触发故障现场信息采集，大幅加快严重故障的根因定位，减少系统停机时间。

- snapshot进程快照

  watchdog复位或内核panic后，进程运行现场信息随复位丢失，问题难以复现，根因分析效率极低。snapshot特性在watchdog复位或崩溃触发时自动收集所有线程的进程快照——包括线程名、PID/TGID、状态、优先级、运行核号、寄存器上下

 版权所有 © 超聚变数字技术股份有限公司

文、调用栈等，通过procfs接口持久化到存储介质（重设printk优先级为4确保输出完整）。系统复位后运维人员可直接读取快照定位崩溃时刻的进程状态，无需复现即可回溯根因，显著缩短平均修复时间（MTTR）。

- 内核热升级

  传统内核升级需要完整重启，导致VM中断和业务暂停，无法满足金融/电信五个九的高可用要求。该特性基于kexec机制实现无缝内核版本切换——KMT（Kexec Memory Transfer）模块负责跨新旧内核传递关键内存区域与元数据，LFM（Live File Manager）模块负责会话、文件描述符、共享资源的序列化保留与恢复（memfd传递+FDT序列化）。内核升级过程中关键会话与内存状态完整保留，业务零中断，VM内应用持续运行，满足高可用场景"不停机内核换版"需求。

- 内核栈实时监控工具

  内核栈越界写导致的静默损坏难以定位——最终崩溃位置往往与真正的越界写入点相隔甚远，调用链被破坏使日志无效，根因分析困难。该工具采用硬件断点（HWBP）与内核探针（Kprobe/Fprobe）双机制，在目标函数入口触发trace并激活硬件断点监控栈地址，配合栈金丝雀（Canary）检测，在栈损坏发生的第一时刻捕获完整现场（通过debugfs配置参数）。将栈损坏的定位时间从"事后回溯"压缩到"破坏瞬间捕获"，大幅缩短内核级问题的诊断周期。

FusionOS 26在可靠性与维测体系上还继承并向6.6 LTS内核完成适配增强了以下能力：

- auto-pxe批量部署增强（PXE无人值守批量装机流程优化，支持大规模集群快速扩容）
- easy-ascend易昇腾工具（一键配置昇腾AI环境，降低国产AI基础设施部署门槛）
- FusionOS-verify鉴权ESN信息获取（设备序列号自动采集与鉴权，支撑License管理）
- hungtask-monitor D状态监控增强（识别IO阻塞、调度等待、设备异常等D状态根因并告警）
- ip-conflict-check IP冲突检测（ARP探测+通知联动，上线前自动发现IP冲突）
- kpgenm-tools内核故障场景模拟套件（注入内存/IO/调度异常验证可靠性机制有效性）
- netcheck网络配置检查（网卡/路由/DNS/防火墙规则一键合规扫描）
- nettrack网络包追踪工具（端到端网络路径tracing与丢包定位）
- safe2FusionOS迁移工具（从CentOS/RHEL等系统原地迁移至FusionOS，最小化业务改造）
- 内核定时器中断聚合（合并高频定时器中断降低功耗与调度开销）
- anytrace调度轨迹记录（调度路径回溯诊断）、kmem-analyzer内存分析工具（内核内存使用诊断）、sysguard系统监控工具（关键资源/进程异常告警）、内核CMCI风暴抑制（抑制硬件错误风暴淹没日志）、内核内存故障降级（ECC不可纠正错误降级识别与故障隔离）以及printk-buf-dev复位保内存NVRAM（系统复位后保留内核日志辅助排障）。

 版权所有 © 超聚变数字技术股份有限公司

6 技术规格

6.1 平台与组件规格
6.2 技术能力规格
6.3 生态兼容与适配

6.1 平台与组件规格

类别	规格项	规格
硬件要求	CPU架构	CPU架构 x86_64（海光、兆芯、Intel、AMD）、AArch64（鲲鹏、飞腾）
	最低内存	4GB（建议不低于8GB）
	最低磁盘	32GB（建议不低于120GB）
	板卡支持	SATA、SCSI、RAID、NVMe存储设备；HBA、InfiniBand高速卡；LAN、USB等标准接口
	安装方式	光盘、USB、网络存储、PXE网络安装
内核与基础组件	内核	Linux 6.6 LTS
	Glibc	2.38
	GCC	12.3.1
	Python	3.11.6
	OpenSSL	3.0.12
	systemd	255-59
	java	1.8.0
	包管理	RPM / DNF
	标准符合度	POSIX、LSB

版权所有 © 超聚变数字技术股份有限公司

6.2 技术能力规格

类别	技术参数	FusionOS 26
文件系统与存储	支持的文件系统	全面支持本地文件系统(EXT4、XFS、exFAT、FAT、ISO9660等)、网络文件系统(NFS客户端/服务端、SMB等)、容器与只读镜像文件系统(OverlayFS、SquashFS等)及FUSE用户态文件系统框架
	最大文件大小	XFS：最大文件8EB/文件系统1PB；EXT4：最大文件16TB/文件系统50TB
	存储管理工具	磁盘分区管理的机制LVM2
网络技术	网络协议支持	TCP/IP、IPv4/IPv6、DHCP等
	安全与管理工具	iptables/nftables/eFilter防火墙、firewalld动态防火墙管理、NetworkManager网络配置管理
	安全通信	IPsec、SSL/TLS可信信道、OpenSSH等
虚拟化技术	Hypervisor支持	xVirt虚拟化引擎（基于KVM增强）、QEMU
	虚拟化管理	libvirt、统一虚拟化管理框架
	宿主机-虚拟机协同	CPU亲和拓扑感知、Guest运行状态同步通道
	加速器虚拟化	GPU/NPU直通与共享、组级负载均衡调度
云原生技术	容器引擎	Docker Engine、containerd
	容器运行时	标准容器：containerd + runc（OCI标准低级运行时）；安全容器：containerd + Kata Containers（基于轻量级虚拟机的容器隔离，每个Pod独立内核，提供虚拟机级别的安全隔离）
	容器编排	Kubernetes（containerd作为默认CRI运行时，支持RuntimeClass多运行时选择，标准容器与安全容器可在同一集群内按需混用）
安全技术	安全框架	xSec安全可信引擎，三支柱架构（安全中心+主动免疫+安全使能服务），10维度安全功能体系

版权所有 © 超聚变数字技术股份有限公司

类别	技术参数	FusionOS 26
	访问控制	SELinux（BLP模型）强制访问控制、IAC（BIBA模型）完整性控制、DAC+ACL自主访问控制、应用白名单
	身份与认证	PAM模块化认证框架（口令鉴别、多因素认证、失败锁定、超时断连）、统一身份认证
	可信保护	安全启动、可信启动（TPCM/TPM/TCM PCR度量）、IMA完整性度量、可信计算3.0
	国密算法集成	SM2/SM3/SM4全算法，覆盖数据加密、IPsec、OpenSSL等场景
	内核内存安全	KPTI页表隔离、SMAP/SMEP硬件隔离、KASLR地址空间随机化、SLAB空闲链保护、内核模块签名、mcage内存安全检测
	数据保护	文件系统/块设备加密（ecryptfs/dm-crypt+LUKS）、EVM文件扩展属性保护、客体重用清零
	安全隔离	命名空间、cgroups v2、seccomp-bpf沙箱、容器隔离（Docker/containerd）、KVM虚拟化隔离、安全SHELL资源隔离
	威胁检测与防护	内核审计（kauditd+auditd）、高特权防诱骗、进程防杀、AIDE入侵检测
	安全部署	安全安装与最小化安装、安全加固工具、签名校验升级、可信恢复
	权限管理	三权分立（系统管理员/安全管理员/审计管理员）、Linux Capabilities最小授权
	安全认证目标	网络安全专用产品认证四级（申请中）、商用密码产品认证二级（申请中）、中文编码认证符合GB18030-2022标准（申请中）
AI支持	推理引擎	Wings自研轻量级深度学习推理引擎，多后端适配（昇腾NPU/NVIDIA GPU/Intel CPU），KV cache优化
	算子加速	xTuning算子加速库，面向国产NPU/GPU垂直调优，减少Kernel Launch开销
	系统级AI调优	xTuning性能加速框架，GPUDirect存储通路、内核调度优化、内存层级管理（HBM/DDR/CXL）

 版权所有 © 超聚变数字技术股份有限公司

类别	技术参数	FusionOS 26
	系统级智能体	OSPilot原生系统级智能体，全栈Rust构建，常驻内存<15MB，支持CPU端本地推理
	算力平台兼容	昇腾NPU软件栈、NVIDIA CUDA软件栈
	内存扩展	CXL内存池化
实时技术	实时引擎	xRT实时计算引擎
	混合部署	FusionOS 26与实时OS共存，CPU/内存/设备资源预分配隔离
	实时容器	基于containerd shim/nerdctl的实时容器，支持设备直通、时钟同步
	跨OS通信	基于openAMP的核间通信（RPMsg协议）
	调优工具	实时任务CPU绑定、中断亲和绑定、tracepoint追踪、调度延迟分析
管理与维护	智能运维	OSPilot智能交互入口（自然语言+CLI+API三位一体），双路径执行（Bash快捷路径+模型推理路径），四层安全边界
	内核热补丁	支持livepatch，不停机修复内核漏洞和缺陷
	内核热切换	基于kexec机制，支持关键会话和内存状态保留
	故障感知	hungtask-monitor增强监控、运行态观测、异常事件实时采集
	故障隔离	SCSI细粒度故障处理（LUN/Target/Host分层隔离恢复）
	现场保全	异常时自动采集内存/日志/寄存器等关键证据并持久化
	数据保护	块设备实时数据保护（时间点快照、数据追踪、定点恢复）
	软硬协同维护	通过系统内部通道获取硬件状态、温度、功耗信息
	系统安装	提供全中文化的图形操作界面及帮助

 版权所有 © 超聚变数字技术股份有限公司

6.3 生态兼容与适配

FusionOS 26采用13年全生命周期维护策略，为企业级关键业务系统提供覆盖完整硬件生命周期的持续技术支持。

类别	适配对象	适配详情
芯片适配	CPU	鲲鹏、飞腾、海光、兆芯、Intel、AMD
	AI加速卡	昇腾Atlas 300I Pro、瀚博VA10/VA16/VA1系列、摩尔线程S2000/S3000/S4000、燧原S60、昆仑芯等
板卡适配	国产网卡	中科驭数SWIFT-2200N Pro、网讯FF5025/RP1000P2SFP/WX1860A4、光润通FF-902E-V3.0/FF-902T-V3.0/FF-904E-V3.0/FF-904T-V3.0、北中网芯N5E010P2/N5E025P2/N6S100P2 东大金智
	RAID卡	9560-8i 、SP686C-M-16i、9560-16i、南京飞鱼
数据库适配	国产数据库	崖山数据库V23、海盒通用数据库管理系统V11.5、瀚高数据库管理系统V9.0、神通数据库V7.0、海量数据库、万里数据库、南大通用数据库、人大金仓数据库、虚谷数据库、达梦数据库、磐维数据库、OceanBase数据库软件、工业时序数据库、优炫数据库、平凯星辰数据库
中间件	中间件	普元信息、中创科技、东方通、金蝶软件、宝蓝德
云平台适配	国产云平台	天翼云虚拟化云平台、云宏信息、志凌海纳（smartX）
安全软件适配	终端安全	火绒、软按科技、飞致云、聚铭网络、北京江民、猎鹰安全、远江盛邦安全、奇安信、绿盟软件、瑞星杀毒
应用软件适配	行业应用	爱数、骞云、海泰方圆、赛通港联、万全科技、联通智网、华胜天成、合明软件、创业慧康、骞云信息、沄熹科技、极限数据、汇智灵曦、蓝凌软件、航天壹进制、沃趣科技、智游网安等
开源生态	开源软件	已上线eco官网，兼容开源软件300,000+（持续更新中）

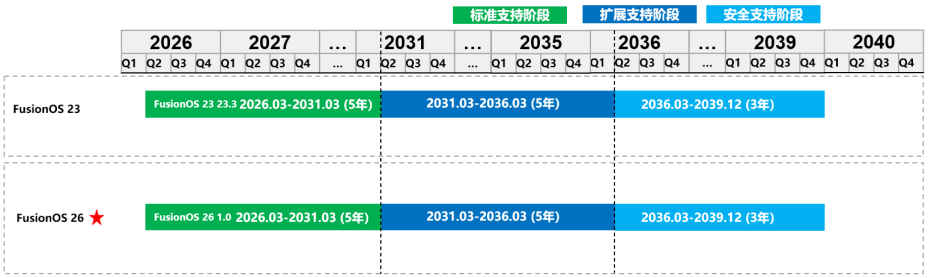
版权所有 © 超聚变数字技术股份有限公司

7 持续服务与支持

7.1 版本生命周期
7.2 技术服务

7.1 版本生命周期

FusionOS 26采用13年全生命周期维护策略，为企业级关键业务系统提供覆盖完整硬件生命周期的持续技术支持。



阶段	周期	维护范围
全量维护期	5年	全功能更新，包括新特性、安全补丁、缺陷修复、硬件驱动适配
扩展维护期	5年	安全补丁与关键缺陷修复，不再引入新特性
长尾维护期	3年	关键安全漏洞修复，保障存量系统的基本安全运行

7.2 技术服务

技术服务方面，FusionOS 26依托超聚变完善的组织运作机制、专业的技术服务体系和覆盖全国的服务能力，面向客户提供标准化、规范化、专业化的技术服务支持。围绕客户业务需求，超聚变可提供软件订阅、系统安装、迁移、培训及现场服务，确保系统高效部署、平稳上线、稳定运行，满足不同业务场景下的应用需求。详细服务参见：https://www.xfusion.com/cn/service

 版权所有 © 超聚变数字技术股份有限公司

序号	类型	服务描述	备注
1	操作系统安装服务	服务内容包含操作系统安装、基本配置和测试验收	无
2	软件订阅服务	24×7 覆盖，P1 问题：30 分钟内响应；P2 问题：60 分钟内响应； P3 问题：2 小时内响应；P4 问题：NBD响应（NBD下一个工作日）	远程问题处理服务响应时间定义：自技术支持中心响应工程师受理客户故障之时算起，直到技术服务工程师首次联系用户开始远程技术支持服务为止
3	现场服务	重大事件保障、专家派驻服务、健康检查服务、驻场服务等	无
4	迁移服务	通过借助迁移工具，将原CentOS平滑迁移到FusionOS，服务内容包括评估调研、规划设计、适配验证、迁移实施、验收上线六个关键步骤。	无
5	培训服务	提供技术培训：涵盖系统部署、管理、开发、安全加固和迁移等内容。 认证服务培训：助力客户掌握FusionOS产品特点及基础知识，具备FusionOS的安装、实施规范、基础调测、迁移与故障处理的能力	无
6	定制化服务	系统定制服务：根据用户需求对操作系统进行定制	无

 版权所有 © 超聚变数字技术股份有限公司

8 附录

8.1 术语表

8.1 术语表

术语	全称/说明
xSec	FusionOS 26安全可信引擎
xAI	FusionOS 26 AI加速引擎
Wings	FusionOS 26自研轻量级深度学习推理引擎
xTuning	FusionOS 26系统级AI性能加速框架
xVirt	FusionOS 26虚拟化引擎
xRT	FusionOS 26实时计算引擎
OSPilot	FusionOS 26原生系统级智能体，统一智能交互入口
SBOM	Software Bill of Materials，软件物料清单
IMA	Integrity Measurement Architecture，完整性度量架构
TPM	Trusted Platform Module，可信平台模块
TPCM	Trusted Platform Control Module，可信平台控制模块
BLP	Bell-LaPadula模型，机密性访问控制模型
BIBA	Biba模型，完整性访问控制模型
KV cache	大模型推理中Key-Value缓存，用于存储注意力机制的中间状态
GPUDirect	GPU内存与存储/网络之间的直接DMA数据路径技术
CXL	Compute Express Link，高速互联协议，用于CPU与加速器/内存间的一致性互联
openAMP	开源异构多处理框架，用于跨OS核间通信

版权所有 © 超聚变数字技术股份有限公司

术语	全称/说明
RPMsg	Remote Processor Messaging，基于openAMP的核间消息传输协议
DFX	Design for X，面向可测试性/可维护性/可靠性的设计
LSB	Linux Standard Base，Linux标准规范

 版权所有 © 超聚变数字技术股份有限公司