邦彦技术股份有限公司
BANGYAN TECHNOLOGY CORP., LTD.

www.bangyan.com.cn
4008-688-132
深圳市龙岗区园山街道志鹤路100号邦彦绿谷工业园区

BANGYAN邦彦

股票代码:688132

BANGYAN邦彦

下一代商用计算机(NGCC)
技术架构白皮书

扫码关注官方公众号

[version 1]

NGCC | 下一代商用计算机

NGCC | 下一代商用计算机

NEXT-GEN COMMERCIAL COMPUTER

BANGYAN 邦彦

邦彦技术股份有限公司

BANGYAN TECHNOLOGY CORP., LTD.

CONTENTS

目 录

BANGYAN

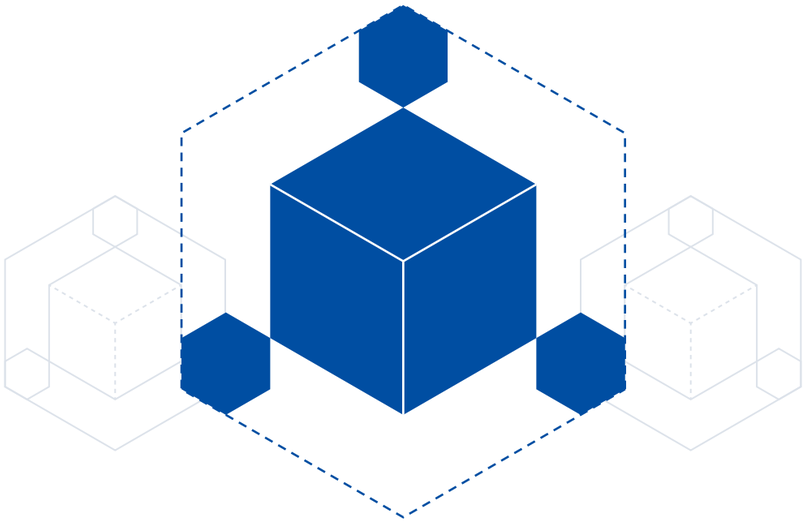
NGCC

下一代商用计算机

NEXT-GEN COMMERCIAL COMPUTER

前言

当今组织的数字化办公环境正经历深刻变革，传统以个人计算机（PC）为中心的架构正面临前所未有的工程挑战。安全合规要求日益严苛、多网络并行接入成为常态、终端设备数量爆炸式增长，以及数据日益成为核心资产，都在逐步削弱传统PC架构的有效性。组织迫切需要一种在保证现有计算能力和用户体验的前提下，从架构上重塑计算、安全与管理模式的新型计算机体系。本白皮书正式提出 "下一代商用计算机（NGCC） "的概念 ，系统阐述其背景动因、核心原则、体系架构、产品形态、工程要求、典型部署场景和未来展望，旨在为企业级计算架构的演进提供专业指引。



摘 要

本白皮书介绍了下一代商用计算机（NGCC）的概念、架构、核心原则以及实际应用场景等。首先，白皮书分析了传统个人计算机（PC）和虚拟化云桌面（VDI）在现代计算环境下的局限性，阐明了在面对多网络、多安全域并行、数据安全和合规要求等新挑战时，传统 PC 架构的不足。接着，本文提出NGCC作为下一代计算架构的定义，详细介绍了 NGCC 的七大核心原则，并通过系统架构设计展示了NGCC 如何在性能、安全性和管理上提供全面的创新。

白皮书还深入探讨了 NGCC 的系统组成，包括终端设备、计算节点和管理平台，并提供了多种部署模式的方案，适用于不同规模和需求的企业。最后，本文总结了NGCC 的适用场景，指出其在高安全、灵活办公和大规模运维环境下的优势，同时也明确了 NGCC 在某些场景下的应用边界。总体而言，本白皮书为企业和技术专家提供了关于 NGCC 系统架构、产品能力以及部署实施的全景视图，是理解和评估这一新兴计算架构的全面指南。

CHAPTER

01

第一章

背景与挑战

第一章 背景与挑战

1.1 传统PC的工程假设

传统PC架构建立在几个隐含的工程假设之上：

- **计算发生在终端本地。**用户的所有计算任务都在PC终端设备上执行。
- **数据存储在终端本地。**用户的数据文件主要保存在PC本地磁盘上。
- **安全主要依赖管理制度与人工约束。**系统安全更多通过人为制定规章、安装防护软件、人工操作来维持。

在早期单一网络、低安全威胁的办公环境下，上述假设在工程上长期成立，传统PC作为独立、自足的计算单元运行良好。然而，环境已经发生巨变。

1.2 组织级计算环境的主要变化

当代组织级计算环境相比过去出现了显著的变化和新要求：

- **多网络并行成为常态。**企业内部网、外部互联网、专用涉密网等多种网络长期并存，许多员工需要同时访问不同网络资源。传统"一台PC只连一张网"的模式已经失效，用户不能再用单一终端满足多网络并行办公需求。
- **数据演变为核心资产。**数据已从业务支撑资源上升为企业的核心资产，数据安全的重要性空前提高。大量敏感数据散落存储在终端本地，成为主要的数据泄露源。一台笔记本的遗失或入侵，都可能导致重要数据外泄，给组织造成难以弥补的损失。
- **终端管理复杂度上升。** 企业员工使用的计算终端数量急剧增长，包括PC、笔记本、移动设备等各类终端大规模铺开。终端规模化带来运维、安全与合规管理的复杂度呈非线性上升。逐台人工维护、逐端加固在大规模场景下几乎不可持续，终端管理正变得失控。
- **安全与合规要求前置化。**如今许多行业的监管要求将安全与合规视为先决条件，不能满足合规就无法开展业务。计算环境在设计之初就必须满足数据不落地、行为可审计等要求，不能再将安全当作事后补救。这种安全观念的转变对传统PC架构提出了超出其能力范围的新要求。

1.3 传统PC的四大局限

传统PC架构在当前环境下面临以下四大局限：

局限一：安全靠运气，终端成为短板。传统PC将计算和数据都放置在终端上，安全很大程度上依赖于人为管理和事后补救措施。例如要求安装杀毒软件、设置复杂密码、依赖用户遵守操作规范等。换言之，PC的安全性高度依赖"人"和"运气"。只要任一环节疏漏，就可能导致数据泄露或系统沦陷——典型案例如员工笔记本未加密遗失、U盘中病毒、违规接入外网导致内网感染等。这种将安全寄托于人的方式在面对职业黑客攻击和严监管要求时显然已不再可靠。

局限二：终端数据分散，隐患重重。在PC时代，每台终端都存放着用户的业务数据（文档、邮件、缓存等）。尽管可以采用网络共享盘等方式集中部分数据，但大量操作数据仍不可避免地"落地"在终端本地。本地数据意味着"一处失守，处处失守"：攻击者只要攻破任意一台PC便可窃取敏感信息。对于政府、金融等严格禁止数据外泄的行业来说，这种架构隐患使传统PC难以满足合规要求。

局限三：多网络隔离粗放，设备堆叠低效。 在传统PC架构下，实现多网络或多安全域隔离往往采取笨重的方式。"双机办公"是常见做法：一台PC连接内网，另一台连接外网。这种方式成本高、使用不便，用户需要在两台设备间频繁切换，而且仍可能通过U盘拷贝、拍照等方式在两张网之间私自传输数据，造成泄密。可见在PC架构下，很难优雅地解决多网络并行使用和物理隔离的问题，往往诉诸于增加终端设备数量的笨办法，既不经济也不安全。

局限四：运维失控，规模效应负面。 当终端数量很少时，逐台人工维护尚可应付。但如今动辄成百上千的终端需要统一打补丁、安装软件、排除故障，传统PC架构下缺乏集中管理手段，只能靠人力或借助第三方工具逐点维护，规模一大就几乎不可控。有人也许认为给每台PC装上严格的管理软件即可解决，但这些代理软件本身跑在终端上，一旦终端被攻陷或离线，管理软件就失效，其可靠性仍然取决于终端自身的安全性。因此，终端规模扩张带来的运维难题在传统架构下难以根本解决。

1.4 虚拟化云桌面的不足

虚拟化云桌面（VDI）架构将终端的计算集中到数据中心的服务器上，通过在服务器上运行多个虚拟机，将每个用户的桌面环境以远程显示的方式呈现到瘦客户机终端上。VDI由于终端数据不落地，在一定程度上缓解了传统PC的部分局限，但它先天存在以下明显不足：

- **性能与用户体验折扣：** 在VDI模式下，多位用户共享同一台物理服务器的资源（通过多个虚拟机）。随着用户数量增加或有用户运行重载应用，资源争用会导致整体性能下降。某些高算力需求的工作（如图形设计、视频剪辑、CAD仿真）在VDI环境下往往出现图形性能不佳、操作延迟高的问题，难以提供媲美本地PC的流畅体验。即使引入GPU虚拟化等改进措施，传统VDI总体上仍难以达到本地PC的极致性能水准，用户体验或

- **隔离依赖软策略，难满足多网并行：** VDI环境中，不同用户间的隔离主要通过软件逻辑和虚拟化手段实现。在需要多安全域并行的场景下，大多依赖虚拟网络（如VLAN）、防火墙策略等逻辑隔离方式来模拟物理隔离，其隔离强度取决于配置正确性和软件漏洞情况，隔离边界并非高强度的"硬隔离"，存在因配置不当被突破的风险。此外，当需要同时访问内外网时，传统VDI通常无法让一个虚拟桌面同时连接两张物理隔离的网络，不得不采用复杂的跳板机制或为每个网络各分配一个虚拟机，使用上非常不便。这使得VDI在多网络并行场景下并不能提供比"双机办公"更好的体验。

- **系统复杂度高，长期可控性一般：** VDI虽然实现了集中管理，但系统复杂度也同时升高。其架构涉及虚拟化平台、集中存储网络、远程显示协议等多个层面，运维人员需掌握跨越计算、网络、存储的多层次技术。一些VDI方案在大规模部署后出现性能瓶颈和故障排查困难，导致系统长期运行的稳定性和可维护性不尽理想。

有专业评估指出，无论传统PC还是云桌面，其长期可控性都只能算"一般"。当VDI无法持续在体验和可靠性上明显优于PC时，用户的新鲜感过去就可能倾向于回归传统模式。这也是许多VDI项目难以大规模复制推广、已部署用户抱怨较多的原因。

1.5 结论：计算机需要被重新设计

综上，当安全与合规成为前置条件时，以终端为中心的传统计算机架构在工程上已不再成立，计算机必须从结构上被重新设计。组织需要一种全新的架构来解决上述挑战，即在确保用户体验与业务连续性的同时，实现数据不落地、多网络隔离并行、统一管理与安全内生的计算模型。这正是"下一代商用计算机（NGCC）"所要实现的目标。

CHAPTER

02

第二章
NGCC是什么

第二章 NGCC是什么

2.1 定义

下一代商用计算机（NGCC，Next-Generation Commercial Computer）是一种面向商用的新形态计算机。它旨在解决传统PC在应对当前组织级计算环境发生翻天覆地的变化时存在的各种不足。

NGCC采用**三域分离架构**，将计算责任、数据存储和显示交互等功能进行结构化重构，遵循**七大核心原则**，通过集中计算、终端零数据、结构级物理隔离、专属算力和统一管理等设计，向企业用户提供高安全、高性能以及灵活可扩展的个人计算环境，为企业提供一整套商用计算解决方案。

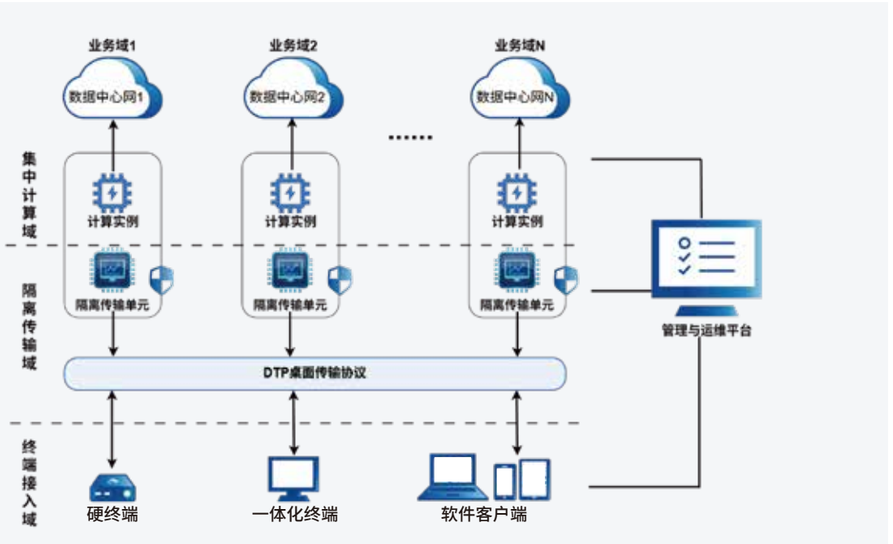
2.2 系统架构

在传统PC架构中，交互入口、计算主体（含存储）和网络三者紧密耦合，缺乏有效的隔离，导致安全性和灵活性方面的局限。尤其是随着组织级计算环境的变化，PC架构已经无法应对当今多网络并行、数据安全和高效管理等需求。在这种情况下，VDI（虚拟桌面基础架构）虽提供了集中计算和简化管理，但它仅仅依赖于两个域——终端域和集中计算域，缺乏真正的物理隔离，导致安全性不够高，尤其是在面对多安全域和跨网络访问时。为了解决这些问题，NGCC采用了三域分离架构，将整个计算环境划分为终端接入域、隔离传输域和集中计算域。这一架构设计不仅实现了网络物理隔离，有效保护了集中计算域内的网络、设备和数据，还能针对不同域实施不同的安全策略，提升系统的安全性与灵活性。通过三域分离，NGCC能够在确保高效计算和便捷管理的同时，充分应对复杂的多安全域、跨网络并行办公等需求。这种架构模式的优势在于，它不仅提供了对计算和数据的集中管控，还通过硬件级别的隔离，确保了系统的高安全性和稳定性。这为NGCC的七大核心原则提供了坚实的基础，确保其在复杂计算环境中的稳定运行和高效管理。

2.2.1 三域分离总体架构

NGCC采用终端接入域、隔离传输域、集中计算域三部分**分离又协同**的总体架构设计。各域之间边界清晰、职责独立：终端接入域负责为用户提供灵活的接入，但不直接接触核心数据；隔离传输域承担通信隔离和信号转发的功能，保证各网络间不发生直接数据交换；集中计算域集中提供算力并守护业务数据安全。通过上述三域的分离与配合，系统在实现高安全性的同时不失对终端用户的友好体验。

▼ NGCC三域分离架构图



▲ NGCC三域分离概念图

各域的描述如下：

- **终端接入域：**包含用户终端及其所连接的接入网络。终端接入网络用于将终端设备连入NGCC系统，并提供通往隔离传输域的通道。终端接入域本身不处理敏感数据，也不承担安全防护职责，因此对网络安全性要求相对较低，可以是企业内部网、互联网等任何现有网络。这一域的作用是方便用户随时随地接入NGCC，而终端设备本身不接收和保存任何业务数据。

- **隔离传输域：** 位于终端接入域与集中计算域之间，包含传输网络和必要的隔离部件。隔离传输域的主要职责是将终端的输入（键盘、鼠标、音频、USB外设）安全、高效地传送到集中计算域，将集中计算域的输出（音、视频和USB外设）同样安全高效的传送到终端接入域，同时确保两个域在物理上网络隔离。为达成这一点，隔离传输域通常采用专门的硬件隔离手段：例如通过非网络方式连接集中计算资源，只传递视频、音频和USB等外设信号，没有网络各层的通路。隔离部件一侧连接传输网络，另一侧以视频/音频信号和外围设备接口连接计算实例，从物理层面阻断直接的网络数据包交换。传输网络可以是覆盖企业内网及互联网的混合网络，需要具备基本的安全防护（如加密传输、抗DoS攻击等）以防止通信受阻，但它不承担对集中计算域内部设备和数据的深度安全防护责任——后者由集中计算域自身的物理隔离来保障。通过这种设计，隔离传输域实现了终端与计算实例之间的信号连接，同时保持两端网络环境的物理隔绝。

- **集中计算域**：集中部署位于数据中心内的所有计算和网络资源，是NGCC体系的计算核心所在。该域包括用于运行用户计算实例的服务器硬件及其所在的内部业务网络。集中计算域的特点是高度隔离：其业务网络与任何其它网络在物理上严格隔离，绝不连接终端接入网或互联网等不可信网络。通常，每台物理服务器仅连接到一个内部业务网络，但是不同服务器可以连接到不同的内部业务网络，也就是说，集中计算域可能是由多个子域组成的复合域，每个子域都有一套自己服务器集群和网络。上图的例子中，集中计算域就分为两个子域，一个内网域，一个外网域。内网域的计算实例用于内部办公，外网域的计算实例用于互联网查询资料。这些网络除非用户通过网络设备将其相互连接或与另两个域的网络连接，否则它们是不会因为NGCC的集中计算服务器而产生网络连接关系。这样即使传输域和终端接入域的网络遭受攻击，也不会波及集中计算域内部的业务网络和数据安全。集中计算域负责提供每个用户的计算实例运行环境，包括操作系统、应用软件和数据存储，由于具备专属算力和存储，用户的计算体验在该域内得到充分保障。

2.2.2 多安全域并行机制

多安全域（Multi-Domain）并行支持是NGCC架构的一大亮点。传统PC时代同时访问多个隔离网络往往需要多台终端，而NGCC通过架构设计使**单一终端即可安全地并行访问多个安全域（集中计算域下的多个子域）。**

在NGCC中，如果用户需要同时使用不同安全级别的网络（例如既要访问内部内网又要访问外部互联网），平台可以为该用户分配分别位于不同安全域的两个计算实例，比如一个实例连接内部专网、另一个实例连接互联网。两个实例被严格隔离运行在不同的物理服务器和网络中。用户端的云终端则可以同时连接这两个实例，通过隔离传输域分别获取它们的桌面画面和交互控制。用户可以在一个屏幕上打开内网计算机桌面，在另一个屏幕上打开外网计算机桌面，实现在一套终端上的"双机"体验。终端设备本身仍不存储任何数据，不同网络间也没有直接的数据通路：用户虽然可以同时查看多个安全域的内容，但如果需要在它们之间传递数据，必须经过受控的渠道（例如预先设置的单向数据导入机制等），不会出现任意拷贝粘贴的不受控数据流动。这种多安全域并行机制从结构上解决了一人多网的办公需求，替代了传统的"双机双网"模式，既减少了终端设备，又杜绝了人为"飞线"跨网的安全隐患。

值得一提的是，为了在管理上支持多安全域并存，NGCC的管理平台可对不同网络域的计算资源进行统一编排管理，但不会因为集中管理而破坏物理隔离原则。通常的做法是在每个安全域内部署受控的管理节点，由主管理平台统一调度，通过安全网关或节点同步策略和状态，从而实现"集中管理、域内执行"，既保证了各域隔离又达到了统一管控的目的（详见后文管理平台部分）。通过以上架构，NGCC能够让多个安全域环境在同一套系统中并行运行，为用户提供无缝的多域使用体验，同时满足严苛的保密隔离要求。

2.3 七大核心原则

原则一：终端零数据

原则二：结构级别物理隔离

原则三：专属无损算力

原则四：一个用户访问多个计算实例

原则五：一个计算实例绑定一个网络域

原则六：原生支持移动办公

原则七：集中统一运维

根据前述现实变化、传统PC架构局限以及VDI云桌面不足之处，NGCC提炼出了七大核心工程原则，用于指导其体系设计。这七项核心原则既是NGCC所应具备的原生能力定义，也可作为判断一个系统是否符合NGCC架构的工程依据——任意一条原则不满足，该系统就称不上真正的NGCC。

原则一：终端零数据

1. 定义：在NGCC体系中，终端设备不得持久化存储任何业务数据，不形成可还原的业务数据落地路径。终端仅承担显示输出与输入采集的职责。

2. 工程说明：NGCC通过如下措施确保终端"零数据"要求：

- 所有业务数据、操作系统运行状态和应用处理结果，均存放在集中计算域的受控环境中，终端本地不保存。
- 终端不具备离线访问任何历史业务数据的能力。
- 即使终端设备丢失、被盗或损坏，业务数据也不会因此泄露。
- 终端上的各种数据通道（如USB接口、剪贴板、打印、截屏/录屏等）都受到平台策略控制或审计，防止数据经由终端落地。

3. 工程意义：

- 将终端从系统安全边界中剥离出去，大幅缩小了需防护的边界范围。
- 数据安全不再依赖终端可信，终端即使不可靠也不会导致数据泄漏。
- 为移动办公、换机办公、多终端接入提供了安全前提，终端成为可随时更换的工具，不再承载敏感数据。

4. 判定边界：若出现以下任一情况，则终端零数据原则不成立：

- 终端本地存在可还原的业务文件或缓存数据。
- 终端在离线状态下仍能访问历史业务内容。
- 可以通过提取缓存、取证或调试等手段从终端恢复出业务明文数据。

原则二：结构级物理隔离

1. 定义：NGCC的安全防护能力主要应来源于系统架构本身，通过硬件物理手段或等效的结构方式实现不同环境隔离，而不依赖易出错的纯软件策略或人工配置来隔离。

2. 工程说明：

- 网络隔离、域隔离、实例隔离等安全隔离在NGCC架构中都有明确的物理或硬件结构体现。
- 安全边界的实现可通过拓扑、专用设备、物理链路等手段加以验证，而不仅是配置上的概念。
- 隔离强度不依赖"配置是否长期正确"，即使管理上偶有配置纰漏也不致破坏整体隔离。
- 系统应具备先天的防错能力：单点配置错误不应破坏整个系统的安全结论。

3. 工程意义：

- 将安全防护从"运行正确性问题"升级为"结构成立性问题"，避免纯软件隔离因漏洞或配置错误失效。
- 系统具有先天防错特性，降低对持续正确配置和人为操作的依赖。
- 为等级保护、涉密防护、金融合规等场景提供架构层面的安全基础，更容易通过严格合规审计。

4. 判定边界：如果系统的隔离主要依赖以下任一种方式实现，则不符合结构级隔离原则：

- 完全依赖VLAN划分或防火墙规则实现逻辑隔离。
- 主要通过ACL访问控制列表等软件策略实现隔离。
- 依赖人工流程（例如人工切换网络、电源）来保证隔离。

原则三：专属无损算力

1. 定义：NGCC为每个用户提供的计算实例必须拥有专属或准专属的计算资源。每个实例在运行期间的CPU、内存、GPU等资源份额应当具有确定性，不受其他用户负载波动的影响。

2. 工程说明：

- 资源独享，不可超分：平台不允许不可控的资源超额分配（Overcommit），杜绝过度透支硬件算力。
- 负载隔离：任一用户的高负载运行不会影响其它用户的性能体验。
- GPU专属/定额：GPU资源要么直通独占，要么通过硬件机制静态划分，不采用高密度的时间片共享模式。
- 性能可测可证：系统性能表现应当可重复、可测量，并可通过测试验证满足要求。

3. 工程意义：

- 确保每个NGCC计算实例都相当于一台"完整的计算机"，不会因为共享资源而性能退化。
- 支持CAD/CAE、视频剪辑、AI训练等专业高负载应用，将云桌面常见的"高峰期卡顿"问题降至最低。
- 提升用户对系统性能的信任度，可将性能瓶颈预测和优化成为可能。

4. 判定边界：若出现以下任何情况，则视为不满足专属无损算力原则：

- 系统整体性能随着并发用户数量明显波动、不稳定。
- 某用户的高强度计算使其他用户的体验明显下降。
- GPU等关键资源无法预测、争用严重，用户感知性能不确定。

原则四：一个用户访问多个计算实例

1. 定义： 在NGCC中，用户是业务操作的主体，每个计算实例只是其工具。架构应允许一个用户同时并行访问多个计算实例以满足业务需要。

2. 工程说明：

- 用户身份与实例解耦：平台设计将用户账户与具体计算实例解绑，用户不是固定对应一台机器。
- 多实例灵活分配：一个用户可以按需同时拥有多个不同类型的计算实例（例如连接内网的安全实例、连接互联网的外网实例、高性能算力实例等）。
- 并行使用而非混用： 多个实例可并行运行，用户可在多个实例间自由切换或同时查看，而不是将多种需求强行混装在单个实例上。

3. 工程意义：

- 从架构上优雅解决一人多安全域办公的需求，无需"多机多终端"堆叠设备。
-摆脱以往"双机办公""多PC叠罗汉"的局面，一个NGCC终端即可满足多网络多任务，提高了用户工作效率和体验便利性。
- 用户可针对不同任务使用最合适的实例环境，整体生产力提升。

4. 判定边界：若系统有以下任一情况，则不符合该原则：

- 单实例绑定用户：平台限制每个用户只能使用一个固定实例，无法同时获取多个环境。
- 多任务串行低效：用户必须频繁注销/登录或切换单一实例来完成不同网络或不同任务的工作。
- 通过单实例多网卡硬拼：多网络需求被迫通过在一个实例中配置多网卡/多网络接入来实现（这是传统PC思路，并未真正隔离）。

原则五：一个计算实例绑定一个网络域

1. 定义：每一个计算实例在其生命周期内必须且只能隶属于一个网络安全域，其网络归属在创建时确定后不可变更。

2. 工程说明：

- 单实例单域：任一计算实例不得同时接入多个不同安全级别的网络域。
- 禁止逻辑分域：不允许通过在一个实例的操作系统内部用逻辑方法（如VPN、虚拟网卡）混合访问不同安全域网络。
- 跨域需求用多实例满足：如果用户有跨安全域办公需求，必须通过为其提供多个不同网络归属的计算实例来实现，绝不在单实例内"开口子"连通两域。

3. 工程意义：

- 将安全域属性固化为实例的先天属性，而不是运行期可变的配置，使安全边界清晰明确定义在实例边界上。
- 从架构上杜绝利用单台计算实例同时连接多网充当"跨网跳板"的可能，消除内外网被意外串通的隐患。
- 简化安全合规审计模型，每个实例只需针对其所属单一域进行审计评估，不必考虑多域混杂的复杂情况。

4. 判定边界：出现以下任一情况，则视为违反单实例单域原则：

- 单一计算实例同时拥有多张网络网口并行连接不同网络。
- 运行过程中通过配置切换实例的网络归属（动态跨域）。
- 在实例内部通过软件逻辑手段连接两个原本物理隔离的网络域。

原则六：原生支持移动办公

1. 定义： NGCC应在不削弱任何安全结构的前提下，原生支持用户在不同地点、使用不同终端访问其计算环境。换言之，移动办公能力需成为系统与生俱来的特性，而非事后附加的例外。

2. 工程说明：

- 权限与用户绑定，而非设备绑定：用户的使用权限仅与其身份相关，不局限于特定终端设备。用户可使用授权的任意终端登录访问其云端计算实例。
- 终端可更换、可失效、可不可信：终端被视作临时I/O工具，可以自由更换。终端即使遗失或不被信任（如公共设备）也不影响用户访问，只需身份可信。
- 移动接入不引入安全例外：用户通过外网或移动网络访问时，应走与内部终端相同的传输连接路径，不因为适配远程而放宽安全策略或引入额外未经严格控制的通道。

3. 工程意义：

- 移动办公不再是安全妥协：用户无需在安全与远程办公间二选一，NGCC架构保证了在任何地点访问都与在办公室使用相同的安全级别。
- 一致的使用体验：出差、居家办公与本地办公拥有同等的性能和安全体验，工作延续性和灵活性大幅提升。
- 终端不再是"例外设备"：组织不需要为出差笔记本等特殊终端放宽安全策略，终端类型的变化对安全体系零影响。

4. 判定边界：如果为了实现远程移动办公而需要：

- 放宽终端设备权限（例如给予远程笔记本更高信任级别），
- 允许敏感数据落地到远程终端，
- 或引入任何未经过严格控制的特殊传输途径或例外策略，

则不能算作NGCC原生具备的安全移动办公能力（说明架构仍需妥协安全来换取移动性）。

原则七：集中统一运维

1. 定义：NGCC必须具备统一的管理和控制平台，作为系统唯一的控制平面，对计算实例、终端、用户策略与审计日志实行集中管理。整个系统的资源调度、安全策略下发和运维操作应通过这一平台完成，实现集中统一运维。

2. 工程说明：

- 实例全生命周期管控：计算实例的创建、回收、迁移等操作必须经由管理控制平面授权执行。用户无法绕开平台私自创建或使用计算资源。
- 无隐形访问路径：不得存在绕过平台的访问通道，例如直接通过IP连接实例而不经过认证控制。所有用户访问都应在平台监管之下。
- 运维行为可审计可追溯：所有运维和管理操作都有审计日志记录，并可追溯责任人。必要时应支持快速回滚更改或回收权限，实现闭环控制。

3. 工程意义：

- 系统具备长期可控性：随着部署规模扩大，统一的平台管理确保运维复杂度不会与终端数量线性上升，而是保持相对平稳。
- 权限即时可控：通过集中平台可以即时授予或回收用户和终端的访问权限，一旦发现安全风险可立刻止损，避免失控。
- 合规审计便利：集中日志和审计功能使安全合规检查变得简洁高效，满足监管要求的成本大大降低。

4. 判定边界：若存在以下任一情况，则不符合集中统一运维原则：

- 平台无法管理到某些计算实例（存在游离于平台之外的"裸奔"实例）。
- 存在未纳入集中管控的私自计算资源（例如用户私接的服务器运行计算任务）。
- 关键管理操作无法审计追踪（运维行为留不下记录或无法溯源）。

本章总结：七大核心原则并非孤立的功能点，而是一套相互支撑、相互约束的工程成立条件。NGCC只有在上述原则全部满足的情况下，架构才能闭环运作、达到预期目标；缺失任一原则，NGCC的结构完整性都将遭到破坏，其安全或性能优势将不复存在。

2.4 与传统PC、VDI云桌面对比分析

与传统PC及虚拟化云桌面（VDI）架构相比，
NGCC在计算模式上存在根本性的区别，主要体现在以下几个关键维度：

维度 / 架构	传统 PC	云桌面（VDI）	NGCC
计算责任	终端本地	共享资源池	专属实例
数据位置	终端本地	集中存储	集中存储
性能确定性	高：本地算力独享	不确定：资源争用	确定：专属算力
安全保障来源	人的管理与制度	策略配置	物理级架构隔离
终端角色	计算执行主体	交互入口	交互入口

▲ 与传统PC、VDI云桌面对比分析

通过对传统PC与VDI架构的分析可以看出，无论是本地计算模型的局限，还是虚拟化以及逻辑隔离方案的不足，都已难以满足当前政企客户对数据安全、性能体验、多域并行、集中可控的综合要求。
NGCC并不是在传统PC或VDI架构基础上的局部增强，而是以“三域分离架构”为基础，结合“七大核心原则”从根本上重构计算机的结构边界与能力模型。

从工程角度看，NGCC实现了**“终端职责最小化、计算职责集中化、网络职责结构化”的再划分，其本质是将计算机从设备形态升级为系统形态**，具备可控、安全、可持续演进的系统能力。它不再以“提升性能”“节省成本”为主要诉求，而是从底层设计解决传统架构的信任崩塌问题，构建起一种新范式的组织级个人计算环境。

CHAPTER

03

第三章
系统组成

第三章 系统组成

NGCC是一套完全依托网络为组织中的成员提供个人计算环境的系统，简单分析可以得出它应该至少包含三类设备：终端设备、集中计算服务器和管理平台。三者协同工作，共同构成完整的NGCC解决方案。本章分别介绍各组成部分及其在工程上的设计要求。

▼ NGCC 系统组成

▲ 终端设备 · 集中计算服务器 · 管理平台 三类组件协同构成 NGCC 系统

3.1 终端设备

NGCC终端设备作为用户的交互入口，主要承担显示输出、输入采集和外设中转职责。终端本身不承载业务计算与数据存储，具备轻量化、低功耗、部署灵活等特点。系统支持专用硬终端、软终端与一体化形态，适应多种使用场景，但所有终端都须服从“零数据、不可信”的体系原则。

3.2 集中计算服务器

集中计算服务器位于数据中心，是NGCC提供算力和运行环境的核心组件，相当于"云端的电脑主机"。对于用户而言，他们的计算实例实际运行在这些服务器上。可以说，**集中计算环境**才是NGCC的计算机本体。

NGCC强调**专属算力**，因此推荐的实例形态是**物理计算实例**：即每个用户实例直接运行在单独的一块物理计算板卡（刀片）上，独享该板卡的CPU、内存和GPU等资源。这种方式下，一个刀片就是一台用户的云端电脑，性能确定、互不干扰。根据成本和性能需求，也允许受控的准物理虚拟实例（vPC）形态：即在保证资源不超配的前提下，在一块物理板卡上虚拟出少量多个隔离的虚拟机供多个用户使用。但vPC的资源配额是静态固化的，绝不允许动态争抢，从而保持类似物理机的性能确定性。一般而言，针对高性能要求场景一块刀片只运行一个物理实例；在性能要求不是很高的场景，可以在单刀片上运行不超过4~8个vPC，以平衡成本。

集中计算服务器根据安全域划分进行网络部署：为了隔离不同安全域，每组服务器只接入其所属的一个业务网络，例如一组服务器接入内部生产网，另一组服务器接入外网等。不同组别之间通过物理隔离和隔离传输域的隔离模块来避免跨域数据流动（正如原则五所述，一个服务器/实例只连接一个域）。这样设计使即便外网环境遭到攻击，内部网的服务器也不会受波及。对于需要跨网的需求，则通过给用户分配对应不同组服务器上的多个实例来实现，并借助隔离的传输通道传递信息。

3.3 管理平台

管理平台是NGCC的大脑和中枢神经，承担整个系统统一管理与控制的职能。它通常以软件平台形式存在，部署在受信任的环境中，用于协调终端、网络和云端计算资源的运行。

NGCC的管理平台提供一个统一的控制平面，管理员通过它可以完成用户与计算实例的全生命周期管理、策略下发和系统监控等操作，主要包括：

▲ NGCC的管理平台提供统一的控制平面

通过管理平台，NGCC实现了过去PC时代难以想象的统一运维模式：数百上千台"云端PC"的运行状态尽在掌握，新用户从申请到拥有专属云计算机只需几分钟，出了问题随时可以追责回溯甚至快速重建环境。一句话，管理平台赋予了NGCC"以系统对抗规模复杂度"的能力，使大规模计算环境的运维复杂度不再随设备数量线性增长，而是被平滑控制在可管理范围内。

CHAPTER

04

第四章
能力和工程要求

第四章 能力和工程要求

NGCC作为对传统PC的全面升级方案，需要在各方面能力上满足甚至超越传统PC，同时满足更严格的安全和管理要求。本章从系统整体、终端、集中计算、管理平台等角度，分别梳理NGCC应具备的关键能力和相应的工程要求。

4.1 系统功能、安全和体验要求

功能完整性要求	支持标准的操作系统与应用生态	提供与PC一致的人机交互界面	集中运维功能
安全性要求	业务数据集中保护	结构级隔离	满足各项合规要求
用户体验要求	性能体验	使用便利性	连续性和可靠性

▲ 系统功能、安全和体验要求

- **功能完整性要求：**NGCC系统必须提供不亚于传统PC的完整计算功能。包括支持标准的操作系统与应用生态（能够运行现有的各类桌面应用程序，而不是局限于Web App或虚拟化的简化应用），支持各种外围设备的接入，以及提供与PC一致的人机交互界面（桌面GUI）。换言之，用户应感觉NGCC提供的依然是一台"完整的电脑"，而非功能阉割的终端。另外，在功能范畴内还需考虑集中管理能力：系统应该内建统一的管理和控制机制，具备PC所不具备的集中运维功能，这也是NGCC方案区别于传统PC的附加价值。

▲ 功能完整性要求

- **安全性要求：**安全是NGCC设计的出发点之一。系统必须确保数据不落地终端，所有业务数据都得到集中保护，杜绝因终端丢失或被攻破导致的数据泄漏风险。系统架构要实现结构级隔离，保证不同安全域、不同用户之间在硬件和网络上隔离到位，消除"隔离依赖人为"的不确定性。

  整个环境应内生安全，满足各项合规要求（如等级保护、GDPR等）而不需要大量额外的补丁式加固措施。此外，安全措施的实施不能依赖用户的觉悟或繁琐的人工操作，应通过系统机制自动实现，降低人为因素导致的安全隐患。

- **用户体验要求：**NGCC必须提供与本地PC近乎一致的用户体验，这是其能否被用户接受的关键。首先是性能体验，包括交互延迟、图形处理速度、文件读写速度等，都应接近本地使用体验，不能因为转到云端就明显变卡或变慢。网络传输协议需要高度优化（如利用无损压缩编解码、智能帧率调整等）以做到"云上桌面与本地同屏同质"。其次是使用便利性，NGCC系统应该支持用户像使用笔记本一样方便地移动办公、远程访问，而且跨设备切换应尽可能顺畅。最后，连续性和可靠性也属于体验范畴：系统应保障较高的可用性，出现局部故障时对用户工作的中断时间要尽量短（例如断线后能快速重连到原有会话）。只有做到性能、便利、可靠三者兼顾，NGCC才能真正实现"体验不牺牲"的目标。

4.2 终端能力和工程要求

NGCC终端在能力上需要完整继承传统PC终端的一切优点，同时通过架构增强可靠性和安全性。具体要求如下：

- **高清显示与多媒体：**终端须支持高质量的显示输出，满足办公对高清、多屏的需求。典型要求包括支持双屏甚至多屏显示，分辨率达到1080p以上（常见到2K、4K），刷新率60Hz或更高以保证画面流畅，颜色无损还原（采用无损或低压缩比编码，如YUV444色彩空间）等。同时，对于视频、音频等多媒体内容，终端应通过硬件编解码等手段流畅播放，确保视频会议、高清视频等场景下用户体验良好。简而言之，用户在NGCC终端上看到的画质和流畅度应与直接在PC本地观看无异。

- **实时输入与低延迟交互：**键盘、鼠标、触控板、手写笔等各种输入操作通过终端传输到云端计算实例，要做到近乎实时响应。NGCC的远程传输协议需高度优化网络延迟，在典型的局域网环境下，用户从输入操作到在屏幕看到响应的端到端时延应控制在50毫秒以内，这样主观上感觉不到明显滞后。对于一般办公操作（打字、点鼠标），这种延迟基本等同本地；即便在稍高延迟的广域网环境，协议也应有自适应机制保持操作顺畅。工程指标上，NGCC需将交互延迟作为硬性性能指标加以验证，而非仅凭用户主观感受。

- **外设全面支持且可控：**终端必须能够支持用户在PC时代使用的各种外设，并在此基础上实现集中管控。外设种类包括但不限于：USB接口的身份认证钥匙（如U盾）、加密狗、工业控制设备，打印机、扫描仪，绘图板、3D鼠标等专业输入设备等。NGCC通过类似于USB over IP+PCIE/USB（多传输链路组合）等技术，将终端接入的本地USB设备映射到云端对应用户的计算实例上，使用户仿佛直接在本地使用设备一样。升级之处在于，平台可对外设接入进行统一策略管理和审计记录。管理员能够规定哪些类别的USB设备允许连接（白名单）、哪些必须禁止（黑名单），以及对接入行为进行日志记录和水印防护。这样既保证了用户必要的外设使用自由，又堵住了通过USB存储擅自拷贝数据等安全漏洞。这一能力是传统PC难以实现的，因为传统PC很难防范用户本地接入设备的行为。而NGCC使外设使用变得"既开放又可控"。

- **终端故障零数据风险：** NGCC终端如发生丢失、被盗或损坏，原则上不应给业务数据和安全造成任何影响。这要求终端本地不存储业务数据，包括临时和永久，或者说，数据根本不到终端，而不是存不存（对应原则一），并且终端认证机制能够在设备丢失时快速失效该终端的访问权限。比如当员工笔记本（作为软终端）遗失时，管理员可在管理平台上立即吊销其访问令牌，该终端即使联网也无法再连接云端实例。专用硬件终端若被盗，由于无有用数据且需要联网认证才可使用，拿到也无意义。因此相较传统PC遗失可能导致的数据泄密，NGCC终端的故障或遗失不会造成数据安全事件，顶多是更换设备的问题。这极大降低了终端层面的安全风险。

- **终端易管理、可远程运维：**对于部署在现场的大量硬件终端，NGCC要求能够实现比PC更高效的管理。终端应支持即插即用和集中配置：首次连接时自动从管理平台获取配置并注册，后续固件升级、配置变更可由平台批量下发，而不需人工逐台操作。终端状态（在线/离线、硬件健康度等）也应能被平台监控。一旦发现某终端异常（如温度过高、网络异常），运维人员可以提前干预处理，避免用户报障。总之，NGCC终端设计秉承"零维护"理念，其运维工作主要在中心平台上完成，而不需要技服工程师频繁跑现场。

4.3 集中计算服务器能力和工程要求

集中计算服务器承担提供算力和运行计算实例的功能，相当于云端的"PC主机集群"。相比每台PC分散提供算力，集中计算模式反而提出了更多能力要求：

- **完整的PC级计算环境：**每个用户的计算实例都应是完整的PC操作系统环境，具备独立的OS内核、完整的桌面和应用运行时，支持安装用户所需的各类软件。NGCC不应强制要求应用必须改造为Web或SaaS形态才能运行，而是直接兼容现有丰富的软件生态。这是NGCC区别于简单DaaS（桌面即服务）或Web应用云的关键点：用户获得的依然是一台功能完备的Windows或Linux电脑，只不过这台电脑是在云端运行。

- **可弹性伸缩的算力供给：**相较固定配置的PC，NGCC的集中算力池应体现出弹性优势。系统应允许根据不同用户或任务需要，按需分配相应规格的计算实例。例如普通办公用户分配2核CPU+8GB内存的实例即可，而研发人员可能需要8核+32GB甚至配GPU的实例。NGCC能够提供多种规格的实例供选择，便于精细匹配用户需求。同时，当用户的算力需求增长时，可以通过平台快速迁移到更高规格的实例，而不必像PC那样只能更换整台硬件设备。这一能力使计算资源利用更加灵活高效，打破传统PC硬件固定带来的瓶颈。

- **专属算力与性能确定性：**针对每个计算实例，必须保证其获得的CPU、内存、GPU资源不被其他实例抢占，满足原则三的要求。工程上要求服务器不超售关键资源，比如一块物理GPU最多分给一个或少数固定的实例，不使用动态按需竞争的方式。CPU调度也倾向于给每实例预留确定的核数/频率上限，避免高负载实例造成其它实例的上下文切换开销剧增。存储和网络I/O亦应做隔离限流等处理。通过上述措施，NGCC集中计算服务器应实现每个实例的性能可预测、可复现：无论何时测试，给定实例在满负荷下的性能指标都近似一致，不会因为别的用户上线或下线而大幅波动。这对于需要精确评估性能的场景（如CAD 、仿真）尤为重要，也让运维人员可以更容易定位性能瓶颈（因为排除了资源争用的不确定因素）。

- **高性能计算与图形能力：**NGCC应至少达到传统PC单机硬件上限，为用户提供强大的计算和图形处理能力。由于集中部署，服务器可以堆叠强劲的资源，如高端CPU、海量内存、企业级NVMe存储，以及专业图形GPU。每个用户实例根据需要可独享一块GPU或至少独享一定比例的GPU显存和核心。这使得NGCC能满足如三维设计、视频渲染、深度学习训练等高算力场景的需求，而无须为每个用户购置高配工作站。例如，在NGCC中可以集中部署数块顶级GPU供几十名需要它的设计师轮流或并行使用，提高设备利用率的同时，也让一般用户不必承担闲置高端硬件的成本。通过合理调度，NGCC把"高配PC"升级为一种系统能力，按需提供给相应用户。同时，服务器之间还能通过高速网络互连，未来有潜力支持分布式计算任务，这是单台PC无法企及的。

- **可靠性和业务连续性提升：**相较单台PC故障即用户停摆，NGCC通过架构提供更高级别的可靠性。要求集中计算服务器可以和高性能、大容量及高可用网络存储设备配套适用，整体提升可靠性和业务连续性，例如服务器集群间自动接管故障计算实例、存储采用分布式多副本等。NGCC平台应实现实例的快速迁移和恢复：当某个物理节点发生故障，受影响的实例可在几分钟内自动重新调度到备用节点运行，用户数据和环境通过集中存储迅速重建。这样一来，单点硬件故障的影响被降到最低，用户只需重新登录即可继续工作，不像PC坏了可能要等待维修更换硬件。对于计划内的升级维护，平台也可通过动态迁移技术在不中断用户业务的情况下将其实例转移到其他节点，然后释放原节点维护，再迁移回来。总之，NGCC提供的是一种连续计算服务，让用户摆脱单机硬件故障的羁绊，显著提升整体可用性。

- **规模运维效率与智能调度：**在大规模用户和实例的情况下，NGCC的集中计算资源应该配合管理平台实现智能调度和效率优化。例如平台可以根据实时负载调整实例部署，尽量将资源利用率控制在最佳范围（避免有的服务器过载有的空闲）。对于长时间无人使用的实例，可配置策略让其休眠或合并以节省能源，实现绿色节能目的。这些都是集中计算环境独有的优势，也是工程要求的一部分：即需要软硬件配合，提供比传统PC更"聪明"的资源管理能力。

4.4 管理平台能力和工程要求

管理平台作为NGCC系统的大脑，其能力直接关系到系统的可管可控性。以下是管理平台需要满足的核心要求：

- **统一的控制平面：**管理平台应实现对所有关键资源的一站式管理，包括用户账户、终端设备、计算实例、网络配置、存储分配等，避免出现"管理真空"地带。具体来说，任何计算实例的创建与销毁、终端的注册与注销、用户权限的赋予与收回，都必须通过管理平台执行。不得允许存在绕过平台的途径，这确保了平台始终拥有全局视图和控制权。对于管理员而言，一个统一的控制台就能完成绝大部分日常运维管理任务，无需频繁登录不同系统界面，大幅提高效率。

- **安全策略集中配置：**平台需要提供丰富的安全策略配置项，涵盖终端、网络、数据等各层面，并能集中下发使全局生效。例如，USB外设的使用策略、剪贴板和打印策略、水印策略等可在平台统一设定，然后施加到所有终端和实例上。又如，不同安全域内部的网络访问白名单策略也应能在平台集中管理，分别下发到各域的实例。这种集中策略管理减少了人为配置失误，同时因为策略是结构化的数据，可以被版本控制和审计，符合合规要求。

- **完善的审计与日志：**NGCC平台必须提供全量的操作审计日志，记录谁在什么时间对系统进行了什么更改或操作。包括管理员的操作日志（新增/删除用户、分配资源、调整策略等），用户的关键操作日志（登录、上传/下载文件等），以及系统事件日志（实例启动/关机、异常告警等）。这些日志应安全保存并提供方便的检索分析接口，以支持安全审计和问题追查。一旦发生安全事件，可以通过审计日志追溯到相关的操作记录，做到可查可究责。同时日志数据也可用于运营分析和规划，比如统计每天有多少活跃用户、资源利用率如何等，为系统扩容提供依据。

- **高可用和扩展性：**管理平台本身应采用分布式或高可用架构设计，避免成为系统单点瓶颈。对于大规模部署，平台需要能够横向扩展承载更多的终端和实例管理。比如，当管理一万台以上终端时，需要有模块化的设计，通过增加管理节点来分担负载。另外，平台应设计有自动故障转移机制，确保即使个别管理节点故障，整体管理功能仍可用，不会中断用户工作。毕竟管理平台承载着整个系统的调度指挥，一旦不可用影响面很大，因此其可靠性必须经过严格验证（如主从热备、心跳检测、数据库高可用等方案加持）。

- **丰富的运维工具集成：**一个成熟的NGCC管理平台不仅是配置和监控界面，还应整合各种自动化运维工具，帮助运维人员更高效地管理系统。例如，一键式的批量操作功能：一键安装新计算节点的系统镜像并加入集群，一键分配新用户的办公环境，一键还原用户的云端电脑到初始干净状态，一键清除回收用户数据并注销其实例以确保不留痕迹，一键置换出现故障的硬件并自动接管原有环境等。这些所谓"五个一键"功能可大幅降低维护难度，提高维护速度。此外，平台还应支持与现有IT服务管理流程集成，例如通过API与工单系统对接，实现从用户申请到自动开通实例的无缝流程。

- **支持边缘和多站点协同：**对于采用中心+边缘协同部署的场景（详见第六章），管理平台需要具备将边缘节点纳管的能力。边缘节点作为中心的延伸，应该由中心管理平台统一控制，其上的用户实例、策略等均由中心下发。平台要能识别网络状态，当边缘与中心暂时断网时，边缘节点可短时独立维持既定策略运行，但一旦连接恢复应立即同步与校验，确保中心策略一致性不被破坏。这种中心-边缘的层级管理关系需要体现

CHAPTER

05

第五章

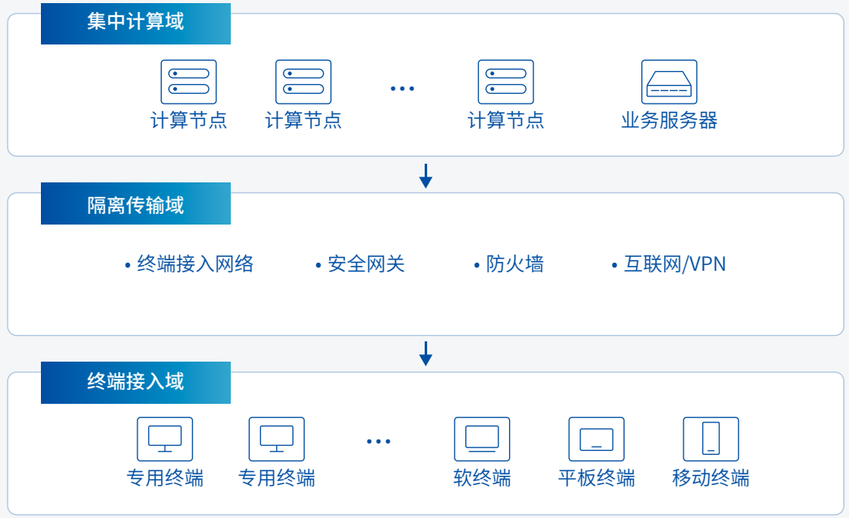
典 型 部 署

第五章 典型部署

NGCC方案具有灵活的部署模式，可根据组织规模和网络架构选择适合的拓扑。

以下介绍三种具有代表性的部署方式。

5.1 单数据中心部署



▲ 系单数据中心部署图

单数据中心模式（如上图所示）是NGCC最基础和直接的部署方式，适用于组织内部网络环境相对集中统一的情况。在这种模式中，所有NGCC服务器（集中计算域）和管理平台都部署在同一个数据中心内，用户无论身处总部还是通过远程网络接入，均连接到该中心的数据中心获取计算服务。终端通常经过网络交换设备直接接入传输网，或者如果在互联网上，则通过VPN接入传输网。

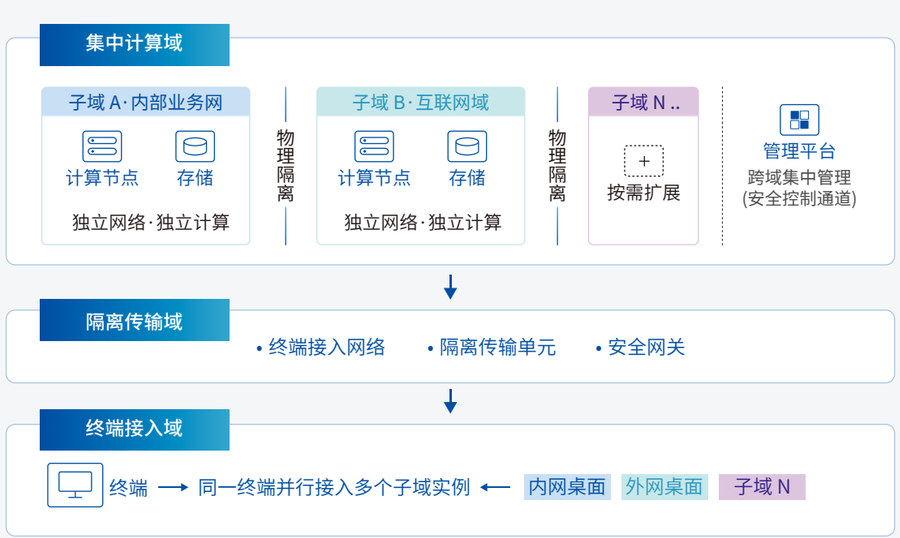
单数据中心部署具有架构简单、集中度高的特点：计算和存储资源集中，易于维护和扩展；安全边界明确，数据不出中心机房，符合很多合规要求；管理统筹，所有实例和终端由一个平台调度。对于地域上高度集中的组织（如在一个城市内办公）或已有大型数据中心资源的企业，这是首选方案。其网络拓扑往往在总部/机房部署NGCC服务器集群，员工通过千兆/万兆局域网连接终端到数据中心，这样延迟低且带宽充裕，用户体验最佳。

如果有少数远程用户，可以通过安全的远程接入VPN/专线连接至数据中心访问。同样，数据备份和容灾也在中心层面完成（如建设双活数据中心提高可靠性）。总体来说，单数据中心部署类似"云在本地"的模式，将所有算力汇聚，提供给所有用户，运维和安全控制都在同一套系统内完成。

需要注意的是，单数据中心部署时，应确保数据中心本身的高可用和灾备能力。因为计算集中于此，一旦数据中心整体不可用（如重大灾害或网络中断），所有用户都会受影响。因此大型组织通常会在单数据中心基础上配套异地灾备中心或租用云上资源作为紧急备用。不过在日常，这种模式无疑是效率最高、性能最好的，故障点少易于管理。

5.2 多安全域并行部署

多安全域并行部署（如下图所示）适用于需要同时支持多个隔离网络环境的组织，例如涉密单位需要内网和外网并存，金融机构需要业务网与办公网分隔等。在这种模式下，NGCC在的集中计算域逻辑上被划分为多个独立子计算域，每个域有自己的业务数据网络，各域网络物理隔离或通过单向网闸等手段单向隔绝。但在管理上，这些计算域仍由同一个NGCC管理平台进行集中管控（通过安全控制通道实现，不直接连通业务数据网络）。



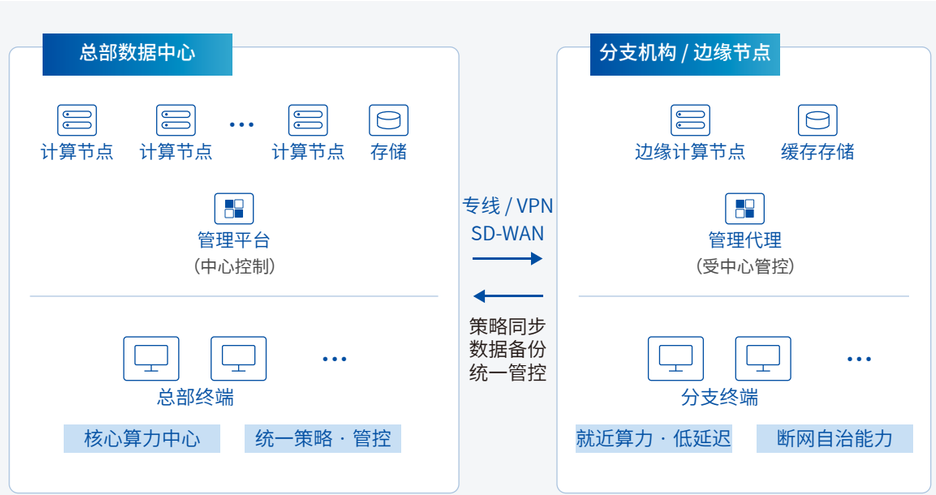
▲ 多安全域并行部署图

具体实现上，通常会在每个子计算域内部署一组独立的集中计算服务器。例如在内网部署一套NGCC服务器集群供内网应用使用，在外网部署另一套NGCC服务器供上互联网的需求使用。两套环境各有各的网络和存储，物理上互不相通。用户如果需要同时访问内网和外网，则按原则四/五拥有两个计算实例，分别跑在内网集群和外网集群上。用户的终端可以同时连接这两个实例，通过终端菜单切换或使用双屏幕来并行操作不同安全域的桌面。这样用户体验上相当于两台隔离PC同时使用，但实际只用一个终端就实现了，而且数据仍然各自在其域内保存，没有跨网传输。

为了解决多域管理的问题，中心管理平台通过数据安全网关等隔离装置与各域计算服务器通信，经过单向隔离或严格过滤，保证不会通过管理链路把各域业务数据串通。当然，也可以采用5.3所示方案，在不同域分别部署各自的管理平台，设置其中一个为中心管理平台，可以纳管其它管理平台。这实现了"一中心管多域"，却又"不让多域直接联网"。对于用户而言，他们只需登录一次管理平台，就能获得其对应的多域计算实例列表，一键启动需要的实例，无需分别登录不同系统，使用非常方便。

多安全域并行部署使NGCC成为一种理想的内外网一体化办公解决方案：既满足了等保等规定的内外网物理隔离要求，又让用户摆脱了以往双机切换的低效。不同行业可以按需扩展更多域，例如研发网、生产网、互联网三域并行，在NGCC中都可以通过多实例方式得到支持。同时，每个域的扩展互不影响，例如外网用户增多只需在外网域增添服务器，不会涉及内网域的调整，架构扩展性良好。

5.3 中心+边缘协同部署



▲ 中心+边缘协同部署图

对于组织机构庞大、分支机构众多或者对网络时延特别敏感的场景，可以考虑中心+**边缘协同部署**（如上图）模式。其思路是在总部数据中心部署中央的NGCC集群，在异地分部或网络条件一般的园区部署若干较小规模的边缘NGCC节点，两者协同为用户提供服务。

在中心+边缘模式下，**中心节点**承担主要的计算和管理职能，运行管理平台并存储核心数据；**边缘节点**则作为中心的延伸部署在靠近用户的地点，为当地用户提供就近算力，以降低广域网延迟带来的影响。边缘节点一般规模较小，可能只部署少量服务器，缓存部分用户实例或承担特定部门的计算任务。关键是，边缘节点在逻辑上并不独立成一个完整NGCC系统，而是在中心的控制之下统一管理。边缘环境的策略、用户权限、数据同步等均由中心管理平台掌控，边缘自身不存储长期数据，不能脱离中心独立运行。

典型的协同机制是：当总部和分部之间网络畅通时，边缘节点定期与中心同步用户的数据变化和策略变更，保证边缘上运行的实例与中心备份一致。同时用户身份认证、权限审计等仍通过中心完成；当网络临时中断时，边缘节点可以短时自治维持现有已登录用户继续使用（因为所需的数据和认证已在本地缓存），但无法接受新用户登录或更改策略。待网络恢复后，边缘会立即将期间的操作日志和数据变化同步回中心，保证中心数据完整。这样设计的目的，是在不牺牲集中管控的前提下，提高系统对网络不稳定的鲁棒性以及远程用户体验。

中心+边缘部署的优势在于两点：首先，对于地理上距离中心较远的用户，边缘节点提供**低延迟、高带宽**的本地接入体验，减少每次操作都跨WAN调用的迟滞。例如跨国公司的海外办公室可以部署边缘节点服务当地员工，以避免长距离网络延迟对桌面流畅度的影响。其次，在网络抖动或中断场景下，边缘节点的**临时自主能力**可以保障业务的连续性——哪怕总部分中心断网，分部员工也可在短时间内继续使用最近的缓存环境，不会立刻工作中断。在恢复后，数据再与中心一致化，不影响全局数据完整和管理。

需要权衡的是，边缘节点往往会增加系统复杂度和成本。只有在确有必要时才引入该模式，例如分支机构网络质量无法保障实时连接中心，或边远地区大量用户通过公网访问中心导致体验不佳等情况。对于多数中小规模组织，单中心模式已经足够。但对于大型组织，中心+边缘模式提供了**规模化部署**的新思路：既保持了中心集权管理，又在物理上实现了算力分布式，就近服务用户。这种模式在5G时代和未来算力网络架构下可能会更加普遍应用。

CHAPTER

06

第六章

适 用 场 景

第六章 适用场景

6.1 适用场景

NGCC的特点使其特别适用于以下场景和行业：

- **高安全与强合规要求的行业：**政府、军工、金融、能源等行业对数据安全和合规性要求极高，通常禁止敏感数据存留在终端上。NGCC通过终端零数据和集中管控完全满足这类要求，避免笔记本遗失泄密等风险。例如政府机关内网采用NGCC，可确保所有公文档案都留存在机房服务器中，终端即使丢失也不泄密。同时集中运维也方便了严格的安全审计。

- **多网隔离并行办公：**诸如涉密研究所、金融交易部门等需要在不同安全网络间切换工作的场景，非常适合NGCC。传统做法是多台PC物理隔离，使用繁琐且存在人为跨网隐患。NGCC允许一个用户一套终端同时安全使用多套隔离环境（如一套连内部业务网、一套连外部互联网），极大提高工作效率且消除了随意跨网的可能性。凡是存在内外网并行或多业务网隔离需求的场景（如科研既要上互联网查资料又要在涉密内网编程），NGCC都是理想选择。

- **大型企业统一运维：**拥有上千台计算终端的大型企业，如跨国公司、连锁企业总部等，传统PC逐一维护成本极高且难以实时管控。引入NGCC后，可在数据中心集中部署计算资源，所有员工使用云端实例办公，由IT部门通过管理平台统一维护系统和应用版本、下发安全策略，减少现场支持工作量。特别是软件分发和补丁管理在NGCC模式下只需在集中镜像上操作一次，所有实例同步更新，不再需要逐台电脑打补丁，大幅提升运维效率和一致性。

- **需要远程办公和弹性用工的场景：**随着远程办公成为常态，很多企业允许员工在家或异地工作。NGCC的架构非常适合这种场景——员工可使用家中的普通PC通过受控软终端访问公司云端实例，享受与在办公室相同的桌面环境和权限，无需携带敏感资料在路上奔波，安全性更高。对于临时外包、合作伙伴访问等，也可通过NGCC临时开通云端工作环境给对方，终止合作后立即收回，不担心数据泄露。在保证安全的前提下实现了灵活用工和移动办公。

- **需要高性能算力集中共享的场景：**一些行业存在少数用户需要超高算力、大内存或专业GPU支持（如动画渲染、科学计算），传统办法是为他们配备昂贵的高配工作站。但这些设备闲置时无法被他人利用。NGCC通过集中算力池可以实现资源按需供给：为重度用户分配强大云实例，为普通用户分配标准实例，统一在服务器集群上运行。这样昂贵资源得以池化共享，提高利用率，降低总体IT投入。典型如设计院、影视制作公司、研究机构等，高性能工作站可在云端集中配置，由多人轮流或并行使用，各自隔离且性能有保障。

6.2 不适用场景

尽管NGCC具有诸多优势，但在以下场景下可能并非最佳选择：

- **单一网络且安全要求低的环境：**如果一个组织的IT环境非常简单，所有人都在同一个局域网工作，且对数据安全没有特殊要求（比如小型初创企业），传统PC可能已能满足需求。引入NGCC会增加不必要的成本和复杂性。这类环境下，PC的灵活性和低成本反而是优点。因此NGCC主要面向有复杂管理或高安全需求的场景，对于单一网络、普通安全办公的小规模场景，不是迫切需要。

- **完全离线工作的场景：**NGCC依赖网络连接将终端与云端实例连接，因此在长期无法联网或网络极其不稳定的情况下并不适用。例如野外勘探、海上船舶、偏远地区施工等强离线环境，仍需要依靠传统PC或笔记本在本地完成计算。NGCC可以设计本地缓存和短暂脱网运行，但不适合持续数天完全无网络的情况。在这种场合下，传统PC因独立运行能力反而有优势。

- **极端成本敏感且IT管理能力弱的组织：**虽然NGCC在总体成本上可能通过集中管理等降低长期TCO，但前期投入（服务器、存储、网络设备、软件授权等）相比采购若干PC要高。同时需要专门的IT运维人员来管理系统。对于只追求最低初期成本的小企业或没有专业IT人员的组织，部署和维护NGCC可能超出其承受范围。这种情况下，与其勉强上NGCC却管理不善，不如继续使用简单的PC方案更实际。因此，NGCC更适合有一定规模并愿意投资IT基础设施以换取长期收益的组织。

- **对实时性要求极端苛刻的特殊应用：**尽管NGCC已经可以做到毫秒级延迟，但对于某些极端实时要求的应用（例如金融高频交易中的毫秒争夺、专业电竞竞技等），任何额外的网络跳跃都有可能不满足要求。这类特殊场景对延迟容忍几乎为零，往往需要在本地裸机上运行。NGCC在大多数办公/生产环境的实时性都足够了，但在这些极端领域仍需要慎重评估。当然，随着网络技术进步和NGCC架构优化，将来这种差距可能进一步缩小。

CHAPTER

07

第七章

未 来 展 望

第七章 未来展望

NGCC作为新一代计算架构的探索方向，已经展现出巨大潜力。展望未来，随着技术和应用环境的发展，NGCC有望在以下几方面取得进一步的突破和演进：

1.更广泛的行业普及：目前NGCC率先在安全敏感和IT架构相对成熟的行业落地，但未来它可能逐步走向普惠。随着企业对数据价值和安全重视程度提高，即使是中小企业、教育、医疗等领域也可能部署NGCC或其云服务形态（如由服务商提供的云端安全桌面）。特别是在数字化转型大背景下，传统PC模式的种种弊端会更明显地暴露出来，从而驱动各行各业考虑采用NGCC架构改善管理和安全。可以预见，NGCC的理念会逐步融入主流IT建设规范中，成为企业IT架构选型的常见选项。

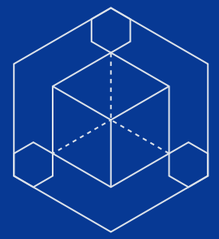
2.云边协同与算力网络：随着5G、大带宽光纤的普及和边缘计算的兴起，NGCC有望与更宏观的算力网络融合。在国家"东数西算"等工程推动下，算力将像水电一样通过网络调度。NGCC的中心+边缘部署实际上契合了这一趋势——它可以视作企业内部的算力网络实践。未来NGCC可能通过标准化接口接入社会化算力调度平台，实现企业计算资源在云、边、端的智能调配。例如，工作日白天用本地边缘算力保证低延迟，夜间将批处理任务切换到云上大规模集群。云边端协同将使NGCC更加高效和弹性，也能进一步降低企业自建成本。

3.人工智能辅助运维与安全：下一步演进中，NGCC的管理平台可能深度结合AI技术，实现更加智能的运维和安全防护。比如引入智能运维助手，通过机器学习分析海量日志，提前预测硬件故障、性能瓶颈，自动调整资源

调度；在安全上，AI可以实时监测用户行为异常，检测潜在入侵迹象，比传统策略更灵活有效。AI还可用于智能助手，辅助用户在不同终端无缝切换工作环境，提供个性化优化。总之，AI技术将让NGCC的管理和安全水平再上台阶，向自治系统迈进。

4.更丰富的终端形态融合： 未来的终端形态可能发生革命性变化，如AR/VR设备、脑机接口等投入商业应用。NGCC架构在这方面有天然优势：它能很容易地在云端适配支持新型终端，而终端只需负责呈现与采集。可以想见，将来员工也许戴着AR眼镜就能调用NGCC的算力处理复杂任务，而体验如同使用高性能PC。NGCC终端范畴会扩展到各种IoT设备、移动智能终端，实现真正无处不在的计算。这进一步验证了NGCC"终端降权"的前瞻性：当终端形态不断演进时，有一个恒定可靠的云计算后端，才能保证应用的连续性。

5.标准化和生态完善：如同虚拟化、容器技术的发展一样，NGCC相关技术也需要标准化和生态系统支持。未来我们可能看到NGCC接口标准的制定，使不同厂商的终端、服务器和管理软件互通兼容。业界也可能形成围绕NGCC的生态联盟，包括硬件供应商（专用终端、加速卡）、软件厂商（远程协议、中间件）、集成商和云服务商共同丰富NGCC解决方案。随着生态的成熟，NGCC部署成本会降低，功能特性会更加多样化，从而吸引更多用户加入。这种正向循环将推动NGCC不断演进并成为数字化基础设施的重要组成部分。



下一代商用计算机（NGCC）
NEXT-GEN COMMERCIAL COMPUTER

结 语

NGCC不是"远程桌面"的代名词，也不是"云桌面升级版"。它是在安全成为前置硬性条件的时代背景下，依然完整覆盖并全面升级传统PC的一种商用计算机形态。通过架构上的系统性重构，NGCC成功化解了传统PC难以应对的安全与管理挑战，同时保持了用户习以为常的性能和体验。对于致力于数字化转型并追求高安全、高效率的组织来说，NGCC提供了一条可行的道路，将计算机从单点设备升级为云端一体的敏捷体系。展望未来，NGCC有望引领新一轮的计算架构革新，成为企业IT基础架构的新基石。

附 录

附录A 术语表

- **NGCC（Next-Generation Commercial Computer）：**下一代商用计算机。指通过集中计算、终端降权、结构隔离和统一管理等架构实现的新型计算机体系，详见正文2.1节定义。
- **计算实例：**在NGCC系统中运行的逻辑计算单元，类似于一台用户的云端电脑。每个用户的操作系统、应用程序和数据都运行在其计算实例内。计算实例可以是物理的（独占一块服务器板卡）或受控虚拟的（独占固定份额资源的VM）。
- **终端：**用户接入NGCC系统的设备或客户端应用。终端负责将云端计算实例的画面显示给用户，并将用户输入上传。终端本身不处理业务计算、不保存业务数据。如瘦客户机、软终端客户端等均属于终端。
- **安全域：**指具有不同安全等级或网络隔离要求的网络环境边界。例如内网和外网是两个安全域。不同安全域通常物理隔离或通过特殊网闸单向连接。在NGCC中，每个计算实例固定隶属单一安全域。
- **VDI（Virtual Desktop Infrastructure）：**虚拟桌面基础架构。业界常见的云桌面方案，通过在服务器上虚拟出多个桌面操作系统供用户远程使用。与NGCC的区别在于VDI资源共享程度高且隔离主要依赖软件，对性能和安全有一定影响（详见1.4节）。
- **vPC（Virtual PC）：**虚拟计算实例的一种说法。在本白皮书中特指NGCC中受控的准物理虚拟机实例。vPC拥有独立操作系统和应用环境，但和物理实例运行在同一硬件上，资源分配固定且不过度超售。
- **数据安全网关：**部署于管理平台与多安全域服务器之间的安全装置。它使管理平台能够同时管理不同网络下的NGCC服务器，又确保不会因为管理通信导致网络串通。通常具有单向隔离或严格协议过滤功能。本方案中未直接使用该术语，但在多域协同管理中有所涉及。
- **单向隔离网闸：**一种硬件安全设备，只允许数据流单方向通过，从高安全侧到低安全侧或反之。用于在保持物理隔离的同时，实现有限的数据导入/导出需求。例如允许从低密级网络将文件单向传输到高密级网络。NGCC在多网数据交换场景下可选用该设备保证不同安全域间无双向链路。

附录B 文档版本信息

版本	发布日期	说明
版本 1.0	2026年1月28日	本白皮书第一版，完整阐述NGCC的背景、原则、架构和实现细节，由邦彦技术股份有限公司NGCC项目组编撰，经内部审核发布。

邦彦技术股份有限公司
BANGYAN TECHNOLOGY CORP., LTD.