

微软桌面云解决方案建议书

目录

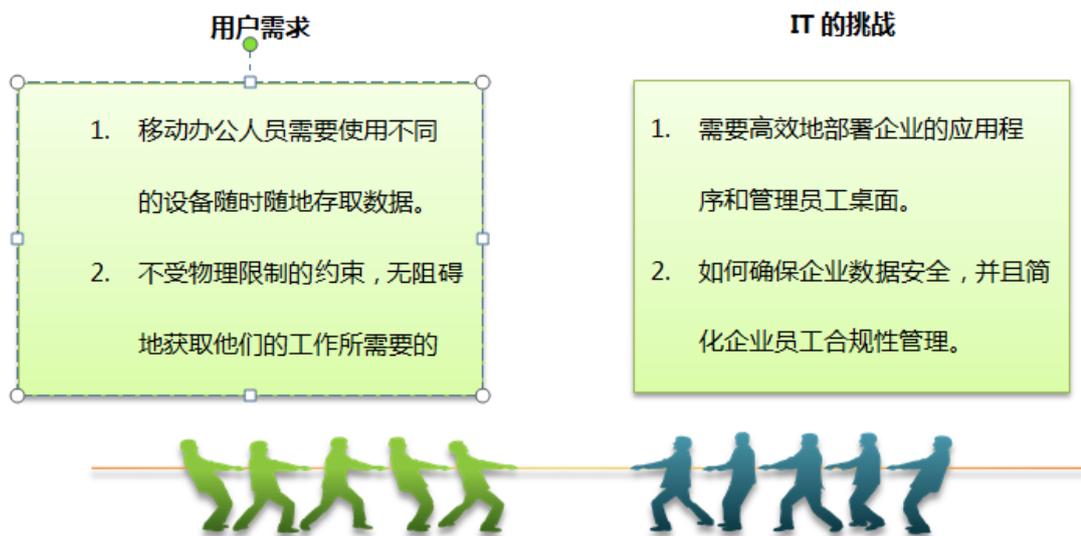
1	概述	1
1.1	桌面云发展趋势、演变过程	1
1.2	国际桌面云应用状况及成功案例	2
1.2.1	国外桌面云应用状况	2
1.2.2	国外桌面云应用状况	3
2	需求分析	5
2.1	企业桌面环境面临的挑战	5
2.1.1	办公桌面管理琐碎、困难	5
2.1.2	用户办公桌面恢复缓慢	6
2.1.3	兼容性问题	6
2.1.4	安全管理	6
2.1.5	移动办公	6
2.1.6	办公资源浪费	7
2.2	企业桌面环境的需求	7
2.2.1	桌面环境标准化管理	7
2.2.2	降低桌面环境宕机时间	8
2.2.3	解决应用兼容性问题	8
2.2.4	确保企业信息安全	8
2.2.5	随时随地安全访问桌面环境	8
2.2.6	计算资源利用率最大化	9
3	建设方案	9
3.1	总体架构	9
3.1.1	总体设计目标	9
3.1.2	总体设计原则	9
3.1.3	总体结构设计	9
3.2	技术构架	13
3.2.1	设计原则/核心设计理念	13
3.2.2	桌面环境分类	13
3.2.3	总体逻辑架构	14

3.2.4	系统功能	19
3.2.5	物理拓扑架构	41
3.2.6	拓扑结构组成	41
3.2.7	平台用户接入	51
3.2.8	虚拟桌面管理	52
3.2.9	安全管理	52
3.2.10	系统运维	55
3.2.11	方案特性	69

1 概述

1.1 桌面云发展趋势、演变过程

企业越来越多的员工需要随时随地工作，不管是在出差，还是在家，并随时访问自己所需要的数据和信息。这为企业的 IT 部门带来了额外的管理开销和安全负担。提供灵活的配置，脱机访问应用程序和数据，以及让员工自定义自己的 PC 环境，固然都很重要，但 IT 部门还需要管理这些环境，这包括允许用户访问哪些应用程序，确保数据被正确备份，以及提供一个选项，以便集中执行那些要使用敏感数据或需要高数据传输带宽的应用程序。



传统桌面计算模式是这样的，将操作系统、应用程序、用户数据和设置都包含在一台计算机中进行处理，用户一旦需要进行升级，或者笔记本电脑丢失、失窃，很难立刻从一台计算机迁移到另一台。由于使用环境以及业务需求，在用户的灵活性和集中控制之间，很难确立准确的平衡级别，尤其是在需要跨越不同的组织，甚至跨越每个组织的多个用户组的情况下。如今，灵活的 Windows 桌面场景让组织可以选择客户端计算环境，从而最能满足组织特定的业务需求。特别是随着云技术的发展，通过桌面云的管理使得桌面管理可以更有效，并且更易于进行变更和用户迁移。

桌面云是可以通过瘦客户端或者其他任何与网络相连的设备来访问跨平台的应用程序。桌面云改变了过去分散、独立的桌面系统环境，通过集中部署/管控，IT 人员在数据中心就可以完成所有的管理维护工作。桌面云的用户桌面环境都是托管在企业的数据中心或在 IT 的严格监管之下。本地终端将会与桌面云中的桌面环境相互隔离。甚至只是一个显示设备而已。同时，桌面云采用集中部署所有托管桌面的方式，所有的桌面数据都是集中存储在企业数据中心。在桌面云的环境下，当灾难发生的时候，可以迅速恢复所有托管桌面，保证完全恢复业务的处理能力。

1.2 国际桌面云应用状况及成功案例

1.2.1 国外桌面云应用状况

1.2.1.1 国外桌面云市场分析

基于当前市场的调研，远离办公室的作业基地、呼叫中心是虚拟桌面解决方案最佳应用的业务场景。由于虚拟化桌面项目的初期投入成本较大，很多企业把虚拟桌面的项目推到了 2011 年之后。根据 Gartner 的报告显示，到 2014 年，传统的专业 PC 工作站会有 15% 左右迁移到虚拟桌面。根据企业调研结果，从用户体验的角度，越来越多的企业在虚拟桌面中部署 Win 7 或将要发布的 Win 8，以提供员工的工作效率。

1.2.1.2 国外成功案例

(1) 意大利电信案例

在意大利电信，呼叫中心和网络管理中心有 20,000 多台桌面电脑已经超过 6 年的服务年限，性能比较差。

为了在电脑更换过程中加快桌面应用的部署，意大利电信决定用虚拟桌面方案来替代硬件 PC，同时借助于桌面云方案中的镜像模板管理，在一夜之间完成了虚拟办公桌面中操作系统和应用系统的部署。

由于实现了集中管控，意大利电信节省了原来对桌面 PC 的现场支持费用，每年每台电脑节省了美金 221 元。

(2) RehabCare 集团案例

RehabCare 集团是美国一家大型医疗机构，在全美 43 个州有超过 1200 多家医院。对于总部 IT 部门来说，应用程序要在这么多个站点进行部署，是一件很头疼的事情，而且应用程序的版本太多，容易造成冲突，影响客户端的使用。

因而，RehabCare 集团微软提供的应用虚拟化和虚拟桌面的方案实现了应用程序的自动化部署和应用标准化。

这一方案的采用，使得原本数周的应用程序部署工作量减少了一半以上，而更新部署速度提高了 80%。

1.2.2 国外桌面云应用状况

1.2.2.1 国内桌面云发展现状及发展趋势

目前在国内的信息化市场中，虚拟桌面还处于起步阶段，大概有 17%左右的国内企业在尝试进行虚拟桌面的应用。

易于部署、数据集中和安全防护这两点，是国内企业考虑虚拟桌面的主要动因，而企业内部广域网的网络带宽、软件许可、解决方案的市场价格是影响虚拟桌面技术推广的最大障碍。

1.2.2.2 国内成功案例

(1) 中国银联案例概述

用户需求

随着业务的发展，上海银联电子支付研究院（以下简称上海银联）涉及应用开发的合作公司人员日益增多，目前已经达到 400 人左右的规模，且有日益增长的趋势，对这个区域的管理日渐复杂。

由于涉及核心业务系统开发，上海银联对于开发区域有严格的安全要求，特别是业务系统代码部分，提出了以下需求：

- ✧ 严格限制开发所用数据（含源代码）被移出开发场所；
- ✧ 所有用户开发行为必须经过严格的授权管理且易于被审计；
- ✧ 加强合规检查，对外部公司开发人员不恰当的上网访问进行监督与处理。

解决方案架构

中国银联电子支付研究院采用纯微软 VDI 解决方案，部署 10 台刀片服务器满足 400 名开发人员的日常使用。

使用 VDI 解决方案时，由于用户数据全部在虚拟桌面中保存，数据不落地，最大程度地实现了数据安全。同时，默认情况下，只有管理员和操作系统对虚拟机的 VHD 文件有读写权限，普通用户无法将 VHD 文件拷贝带出，保证了 VHD 文件的自身安全。

◇ 用户收益

- 提供一个安全、稳定并且易于监管的开发环境
- 杜绝数据外流情况，对用户后端代码及文档访问进行授权控制及审计
- 基于项目组的开发环境生命周期管理，包括自服务，批量创建，监控、备份、归档及回收等
- 良好的用户使用体验，性能完全满足日常开发要求
- 提升服务器的利用率

(2) 上海浦东发展银行案例概述

用户需求

随着浦发银行业务的发展，浦发银行合作公司的人员日益增多，目前已经达到 700 人左右的规模，且有日益增长的趋势，对这个区域的管理日渐复杂。同时审计部在对开发中心进行业务运行稳定性及开发外包专项审计时，提出以下问题：

- ◇ 开发人员使用自带便携式计算机开发会导致开发所用数据（含源代码）易于被移出开发场所
- ◇ 开发人员未遵守我行规定使用我行内部账号上网，可向外发送数据，并存在将开发环境与因特网连通的风险
- ◇ 建议加强检查，对外部公司开发人员不恰当的上网访问进行监督与处理

解决方案

浦发银行采用桌面云方案，将 20 台刀片服务器组成开发平台核心，用来承载 750 台客户端及 11 台服务器虚拟机（包括：微软的 System Center、统一沟通及安全产品），使最终用户安全的连接到开发平台的 750 台虚拟桌面进行日常工作。

◇ 用户收益

- 杜绝数据外流情况
- 提高对客户端上网行为的限制、监控
- 保证平台的整体安全性
- 基于项目组的开发环境生命周期管理，包括自服务，批量创建，监控、备份、归档及回收等
- 保证平台的可恢复性
- 简化平台的管理、监控的工作
- 保证平台的灵活性和高可用性
- 提升服务器的利用率
- 降低总体成本
- 方便客户端与浦发银行人员通讯

2 需求分析

2.1 企业桌面环境面临的挑战

企业办公桌面环境是让员工提高工作效率的技术手段，其上运行的各种公司办公软件、应用系统是让员工协同工作的好工具。但由于企业 IT 的不断普及，几乎大多数员工都拥有使用的电脑，这也带来了相应的管理维护上的挑战。

2.1.1 办公桌面管理琐碎、困难

办公桌面分布在每个员工的面前，公司规模越大，办公桌面的物理分布就越广。一旦用户使用过程中办公桌面出现问题，维护起来就会很困难。首先由于办公桌面和不同的用户进行互动，而每个用户的使用习惯、了解 IT 的知识水平都不同，所以出现的问题就会千奇百怪，并且办公桌面上的应用众多，使得维护人员难以定位问题所在，维护工作非常困难。而且办公桌面数量众多、分布有广，维护周期就会更长。每个企业中管理维护数据中心的难度都不会比维护办公环境的大。这一点让很多公司的 IT 部门头疼。

2.1.2 用户办公桌面恢复缓慢

当用户使用办公环境过程中经常会因为各种原因使得办公桌面不能够正常工作。如：病毒、误删除应用系统文件、误操作等。而由于办公桌面环境包含大量的应用程序和参杂着用户自身的个性化信息，使得环境构成各不相同，这都为 IT 维护人员及时定位问题的原因，带来了艰巨的困难。更何况使用者大多数对 IT 知识比较缺乏，甚至连问题都有可能无法描述清楚，这种情况下办公环境也许只有重装是解决问题的唯一手段。但对于用户来说，他们可能只是认为出的问题解决起来非常简单，维修结果的冗长必然超过了他们的期望值，同时也严重阻碍了用户的办公效率。因此用户的在办公桌面环境维护过程中的体验是非常差的。这种负面的反馈同样又给 IT 维护人员带来了巨大的压力，甚至很多维护人员听到办公桌面环境的维护就会紧张、恐惧。经过调查 IT 部分用于维护桌面环境的工作量和花费的时间占整个工作时间的 50%以上。

2.1.3 兼容性问题

IT 技术不断发展，面临的 IT 威胁也不断增加，且破坏力也增大。企业为了自身需求不断提升、改善自身企业的 IT 水平，但越来越先进的技术手段和已存在的原有系统之间并存问题，将会越来越突出。原有系统成为了阻碍 IT 快速发展的绊脚石，让企业的 IT 部门非常头疼。如何解决这个问题是加快企业 IT 发展的关键所在。

2.1.4 安全管理

每个企业都有自己的特有的商业机密，而随着 IT 假设的不断发展，很多机密/敏感信息都会以某种形式存在于企业的 IT 系统中。而有些时候这种纯电子数据的保存方式比传统保密方式更容易泄露。很多时候企业会选择模拟传统手段的方式去保护电子信息。比如编写机密信息访问安全守则，贴到墙上随时提醒员工；堵住桌面电脑的 USB 口，禁止使用者复制机密信息；只有特定的桌面计算机能够访问机密/敏感信息，而这些计算机摆放在一个封闭的房间内，有摄像头随时录像等等。而这些手段其实都是被动防护手段，只能做到时候审计，找到泄露信息的人，却不能及时预防。

2.1.5 移动办公

随时随地处理业务的需求越来越突出，因此我们能够看到很多人都随身背着自己的办公电脑行走在路上。但是随身携带办公电脑一来让人感到行动不便，而来如果电脑丢失或损坏可能会给企业带来不可预知的风险。如：机密信息泄露、办公数据彻底丢

失/损坏等。即使企业允许员工随时携带办公电脑出行时，也无法避免一些突发事件的出现。如：突发事件出现需要员工快速处理，而此时员工并未随身携带办公电脑；出差在外电脑丢失/损坏，急需事物无法处理等。在此种突发情况下，企业还是无法提供更好的技术手段加以解决。

2.1.6 办公资源浪费

企业为了提高办公效率尽可能的为每个需要电脑的员工配备计算机，甚至有些员工同时拥有 2 台以上的个人电脑。虽然这样某些员工的办公效率随之提升，但同时也出现了电脑资源浪费的情况。大多数拥有多台电脑的员工，在不同时间段中只能使用一台电脑，而其它电脑资源必然处于闲置状态无人使用，从而造成了电脑资源的浪费。有些企业想采取手段将那些短期内闲置的电脑调配给其他急需的员工，但多数情况下由于闲置电脑中存有原有员工的个人/办公信息，而无法实现调配的愿望，只能让这些电脑资源继续闲置。最终只是企业中办公电脑资源的重复/浪费，同时也让 IT 部门管理难度不断增加，成为企业 IT 管理的一块心病。

2.2 企业桌面环境的需求

2.2.1 桌面环境标准化管理

企业需要 IT 部门采取一切手段降低办公桌面环境出现问题的次数，这样既能够降低维护成本，同时也能够提高用户的使用体验。办公桌面的标准化管理是降低出现问题次数、降低维护难度、提高恢复速度的最佳选择。但是由于企业向员工提供的办公桌面环境，随着员工的使用，会形成个人信息与办公信息混合，换句话说，是个人桌面环境与办公桌面环境的混合体。这样的混合体致使企业 IT 部门经过大量的投入建立的办公环境标准化体系最终不能获得最初的设定效果。这种现象在企业的 OA 环境下要比在生产环境下要突出很多。很多企业生产环境的标准化会获得成功，为企业带来显著的效益。而当企业将标准化工作推广到 OA 环境下时，首先会获得员工的极力反对，因为标准化使得员工感到被束缚，失去创造力的体验。其次如何在标准化过程中确保员工在桌面环境中存储的数据不丢失以及员工长久以来形成的操作使用习惯得以保存是项目实施过程中的难点所在。最重要的是即使标准化实施成功后很多企业 IT 部门发现，一段时间后标准化的办公桌面环境已经严重走样与最初的设定大相径庭。造成这种结果的原因之一就是个人桌面环境和办公桌面环境很难分开造成的。

2.2.2 降低桌面环境宕机时间

办公桌面环境在维护过程中使用者将会停止办公/降低办公效率,直到自己熟悉的办公桌面环境恢复正常。由于办公桌面环境直接和人发生互动,产生问题的原因多种多样,因此维护起来难度很大,问题定位非常困难。换句话说,办公桌面环境维护周期普遍情况下会很长。企业需要找到一种手段在为员工进行办公桌面环境维护过程中,能够给员工一个提供临时办公环境,且这个办公环境和正在维护的环境相同或相近,从而避免员工因为找重新熟悉一个新的办公桌面环境而降低其办公效率。同时通过快速提供临时办公环境,从而降低了维护人员的现场维护压力,争取更多的维护时间找到问题所在并将其恰当解决。

2.2.3 解决应用兼容性问题

IT 技术不断发展,面临的各种挑战也随之增加。企业的 IT 环境只有不断的发展、提高、完善才能应对各种新出现的威胁。而且只有不断应用先进技术,才能提高企业综合管理水平。但是随着企业 IT 建设的不断投入,新的应用系统的投入使用,相对的就会有一些应用系统技术过时、难以适应当前的 IT 技术水平,维护他们越来越困难、维护成本越来越高。更重要的是,这些旧的应用系统会阻碍企业 IT 建设的发展,因为 IT 部门必须考虑旧应用系统与新技术的兼容性问题。企业需要一种技术能够很好的解决两者之间的矛盾,既能够确保原有系统的持续正常运转,又能够不断的提升整体的 IT 水平,防御不断出现的外界挑战。

2.2.4 确保企业信息安全

企业在业务活动过程中会产生大量的商业信息。而随着企业不断的利用 IT 技术提高自身在市场上的业务竞争能力、加快办公效率,大量的商业信息转化成电子数据的方式留存在企业的 IT 系统环境中。以电子方式存储的企业信息从技术手段上来看更容易泄露,企业防护起来更加困难。企业需要一种技术手段能够确保企业机密信息安全的运转在公司网络内部或被预想的控制范围之内。让办公应用的使用控制在一个安全的、合法的环境中,即不影响企业业务活动,又能够让企业信息控制在合理的范围内流转。

2.2.5 随时随地安全访问桌面环境

员工在工作当中经常会遇到一些紧急状况,需要立即处理信息和数据,但办公电脑又没在手边。企业为了解决这种问题,会给那些会出现突发现象的员工配备移动电

脑，结果还是无法杜绝现象的发生。企业需要一种技术手段，能够让员工随时随地的安全访问到自己的办公桌面环境。甚至是在外面的网吧里，员工都能够很安全的使用企业的办公桌面环境。而且不管员工从哪里访问自己的办公桌面环境，熟悉的用户界面、使用习惯、个人文档资料都会原封不动的保持一致，让员工感觉不到使用体验的任何差异。

2.2.6 计算资源利用率最大化

企业的桌面计算机资源随着 T 建设的不断推广，应用越来越广泛，数量越来越多。企业为了进一步提高员工的工作效率，甚至会为某些人配备多台电脑。但由于每个员工同一时间只能使用一个办公电脑进行办公，因此企业中很多桌面计算机会出现闲置现象，造成一定程度的资源浪费，而企业中的有些员工却因为某种原因急需一台计算机应急。企业需要有种技术能够充分发挥闲置的计算机资源，能够准确了解闲置资源的状态，在调配给他人使用和归还给原所有者时，双方都不会感觉到使用的计算机曾经被别人使用过。

3 建设方案

3.1 总体架构

3.1.1 总体设计目标

在企业制定的企业桌面环境管理规范下，通过桌面云的建设实现企业桌面环境的使用方便快捷、稳定高效运行、信息安全合规、集中管控、维护便捷。

3.1.2 总体设计原则

- 结合企业 IT 现状和建设规律设计合理的建设方案。
- 既要保持企业整体的管理规范，又要以各子公司/部门的需求不同有所差异。
- 根据实际应用需求提供合理的桌面虚拟化技术方案。
- 集中管控是实现企业桌面环境标准化和确保桌面云日后按照设计规范稳定运行的必要手段。

3.1.3 总体结构设计

根据对企业 IT 现状和以往建设规律的理解，企业桌面云将由企业总部统一制定规范和框架，统一服务流程，统一配置和调度流程，统一监控维护流程，各子公司/部门根

据实际需求进行建设实施，并在企业总部的总体框架下进行实例化。换句话说，子公司/部门的整个桌面云的系统总体架构和各桌面虚拟化技术构建架构，以及制定运维管理流程、配置调度流程的流程保持完全一致。各子公司/部门根据自身的需求挑选适用的桌面分类并以相关的规定和框架为基础，进行实例化，并最终加以实施。子公司/部门的实例化不能破坏企业总部对桌面云的整体规划，以便企业总部对桌面云进行不断的完善和扩展。

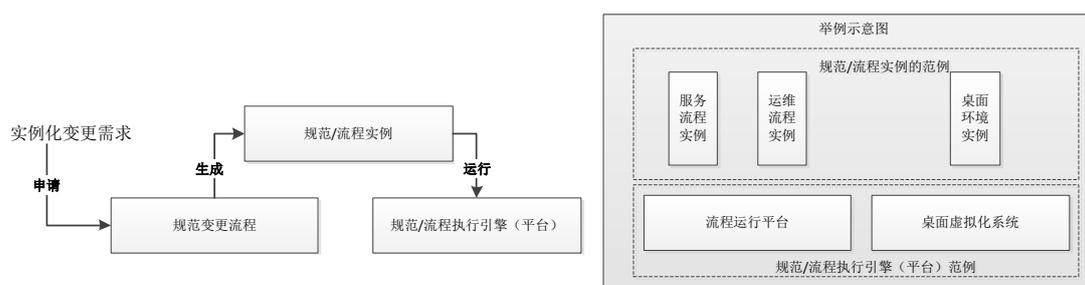
- 规范制定



桌面环境标准化和规范化层级

企业的桌面云要实现上述的四个统一，企业总部首先要对整个企业中的企业桌面环境进行统一的分类汇总，然后对各类桌面环境的组成特征、操作/运行行为进行归纳，并对相关的管理、运维、安全等进行标准化和规范化。为了便于日后的升级、管理、维护，桌面环境的标准化和规范化将会被分成 4 级：集团级、企业级、部门级、个人级。集团级具有最广泛和普遍性的标准化指标，所有整个企业/集团内的桌面环境必须符合集团级的规定。如所有集团的桌面必须安装杀毒软件、防火墙软件等。而企业级是具体的子公司根据自身的实际要求提出的标准化指标和规范，是对集团级指标的一种补充。以此类推，部门级是企业级的补充，个人级是对部门级的补充。这种分级标准化/规范化的好处在于更加贴近未来实施/使用时的实际情况。每个子公司、每个部门，甚至每个员工因为自身所处环境的不同，需求的不同，对于标准化的要求不尽相同。虽然所有人都希望通过桌面环境标准化，使得自己的桌面环境少出错，从而提高工作效率。而不恰当的标准化反而会约束他们的行为，降低其使用体验和办公效率。而涵盖范围过大的标准化就是一种不恰当的标准化。因为要从越多的桌面环境实例中找出共性，其共性就

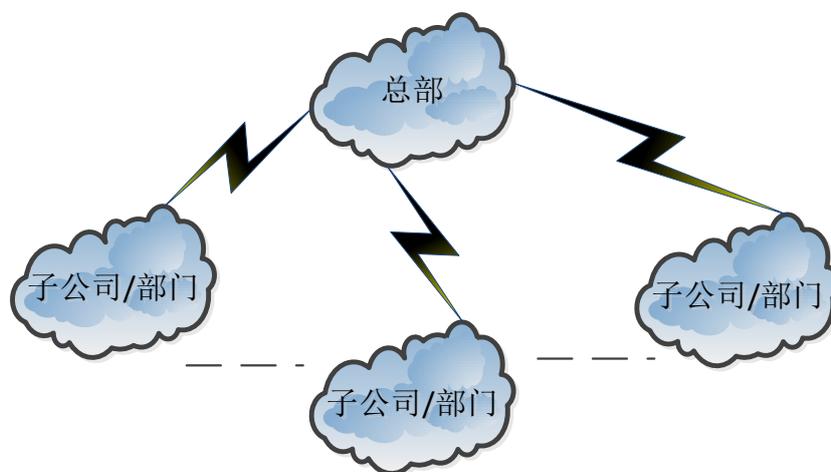
越少。如果按照此种标准化实施的桌面环境，大部分使用者的使用习惯都不会包含在标准化规范中，也就是说，大多数人的正常的操作行为会被限制住，从而极大的降低了工作效率。因此将标准化分成恰当的层级，逐级进行归纳汇总，制定标准化指标是最佳解决手段。这种通过多级累积标准化指标集合将会最大限度的表述某个桌面环境使用者的行为规律，同时又对其进行了有效的规范，使其行为在企业的约束下。



在桌面环境进行了良好的标准化和规范化后，更重要的统一就是对企业整个桌面云系统环境的架构标准化，对实施建设、运维和升级完善的过程规范化，从而确保子公司/部门中分别建设的桌面云系统实例保持高度的一致性。实现从企业总部制定的桌面云系统模板上复制出各子公司/部门的桌面云系统运行实例的效果。换句话说，就是企业总部负责对规范的流程进行规范。虽然每个桌面云系统实例在各自的子公司/部门中运行，但是其整体组成结构和逻辑框架完全相同。这样便于企业总部对子公司/部门的桌面云进行宏观把控、优化完善。企业总部为整个桌面云系统结构和实施提供标准/推荐方案。依据企业总部推荐的实施建设方案能够快速、准确无误的搭建出一个完整的桌面云系统实例。企业总部同时对实施建设扩展、运维流程变更和系统升级完善的流程进行规范。换句话说，实施子公司/部门在建设自己的桌面云实例时不可能与企业总部提供的推荐方案 100%一致。有可能是桌面系统细节要求、有可能是维护管理流程各不相同。如同是服务器扩容采购流程，但有些子公司/部门需要经过 3 层领导审批，而有些子公司/部门则只需经过 1 层领导审批。又如同样都是开发团队专用虚拟机环境，有些子公司/部门使用的是 J2EE 的开发环境，而有些使用的是微软的.NET 开发环境。或者是有些服务流程在某子公司/部门中根本不需要，从而要去除掉，而另一些子公司/部门因为自身的特殊需求，需要额外添加新的服务流程。随着各子公司/部门实例化桌面云，以及日后的不断维护、完善过程中，各种变更和调整将会层出不穷。而子公司/部门的这

些变更需求是合理的，但随着时间的推移结果也是可以预见的：未来的桌面云系统实例差异越来越大。而规范这些变化的流程，让变化按照集团规定的方式，创立、生效、废止，并对这些变化进行准确的跟踪和记录，这个流程是可以规范化的。换句话说，子公司/部门的桌面云实例的变化将不是随心所欲的任意变化，而是遵循集团的规范，沿着指定途径进行着。这样即使桌面云系统实例再如何变化，系统的框架还是集团规划好的，稳定可靠的，健康的。日后企业总部还可以不断的对整个企业的桌面云进行完善升级，而这些新的建设实施规范能够很顺畅的推动企业所有桌面云系统实例的提升。

- 系统分布/实施



每个子公司/部门建设的桌面云系统实例在主体结构上基本相同，不同的是子公司/部门选择的桌面环境种类和数量不同。各桌面云系统实例相对独立，由子公司/部门各自进行建设、管理和运维。这样可以确保各子公司/部门范围内获得性能和使用体验最佳的效果。企业总部为各子公司/部门提供如何构建标准桌面云环境的实施方案和方法。子公司/部门如果没有特殊需求，可以直接使用企业总部的实施手册快速在子公司/部门内复制出所需的桌面云系统实例。而那些有能力且有需求进行功能扩展的子公司/部门，则必须将企业总部推荐的实施系统框架、运维流程框架予以实施，然后依据企业规范中的扩展规范流程对运维和管理流程实例进行增删改或对桌面环境的组成结构可以进行调整/扩展。这样可以确保整个桌面云系统实例的管理、运维流程建设、维护保持一致。具体流程内容可以不一样。

- 容灾

总部将会为所有子公司/部门提供容灾环境。总部为提供最为全面的桌面环境种类的实现环境。同时为各子公司/部门桌面云系统实例中的数据提供加密备份空间，从而确保数据的安全性和完整性。总部数据中心中还保存子公司/部门桌面云系统实例中桌面环境的定制实例模板。当某子公司/部门桌面云系统实例出现事故，需要远程恢复时，总部数据中心可以将使用保留的最新桌面环境实例模板创建出桌面环境实例，并且将备份的数据与桌面进行动态拼接，从而快速恢复出现事故的桌面环境，供使用者远程使用。

3.2 技术构架

3.2.1 设计原则/核心理念

- 充分采用全球最佳技术，并兼顾未来技术发展趋势。
- 桌面云是一种 IT 部门提供的服务输出。
- 标准化、虚拟化、自动化、自助式服务、SLA 式的交互方式等私有云核心特征必须要在设计中充分得以体现。
- 信息安全管理确保信息在合规的环境中流动。

3.2.2 桌面环境分类

分类原则：

- 以信息安全范围进行分类规划
- 以生产环境和办公环境进行分类规划
- 以建设、管理维护进行分类规划

工作环境分类	使用虚拟桌面种类
固定式办公环境	托管专属虚拟机环境，客户端专属虚拟机环境
移动式办公环境	托管专属虚拟机环境，托管共享虚拟机环境
生产环境	托管共享桌面环境，托管专属虚拟机环境

3.2.3 总体逻辑架构



企业桌面云是由企业总部统一设计，各子公司/部门分别建设，因此每个桌面云系统实例的结构基本相同。此处描述的是企业总部统一设计的桌面云的标准系统架构。总体来说整个桌面云系统采用云计算的架构，主要由基础计算资源服务层和通用虚拟桌面服务层，专属应用桌面环境服务层构成，用户通过用户自服务门户使用相应的虚拟桌面环境，而管理员通过运维管理门户对基础计算资源服务层和通用虚拟桌面服务层，专属应用桌面环境服务层进行维护管理工作。

基础计算资源服务层实际上就是私有云中的 IaaS。其主要负责将物理计算资源，如服务器、网络、存储等相关计算资源，进行抽象/虚拟化，转变成逻辑计算资源，以满足上层虚拟桌面服务层对计算资源的需求。而虚拟桌面服务层不用去关心所需计算资源的相关维护、扩容、稳定性、高可用的相关问题。这些相关维护管理工作全部由基础计算资源服务层全权负责。

在基础计算资源服务层中需要负责确保：

- **硬件设备：**健康运行、问题要及时解决、容量要稍有富余。
- **资源池：**资源要稳定输出（最大限度不出问题，问题要及时预测避免）、出问题要及时解决、容量稍有富余（如果不足要及时补充）、物理资源利用率最高
- **服务：**计费信息要准确、收费要及时、服务不能出问题、资源分配要最佳。

通用虚拟桌面服务层中包含各种虚拟桌面服务。每种虚拟化桌面服务相对独立运行对外提供相关的虚拟桌面技术输出。每种虚拟桌面服务都是私有云中的 PaaS 服务。子公司/部门可以根据自身的实际需求挑选所需的虚拟桌面服务类型加以部署。

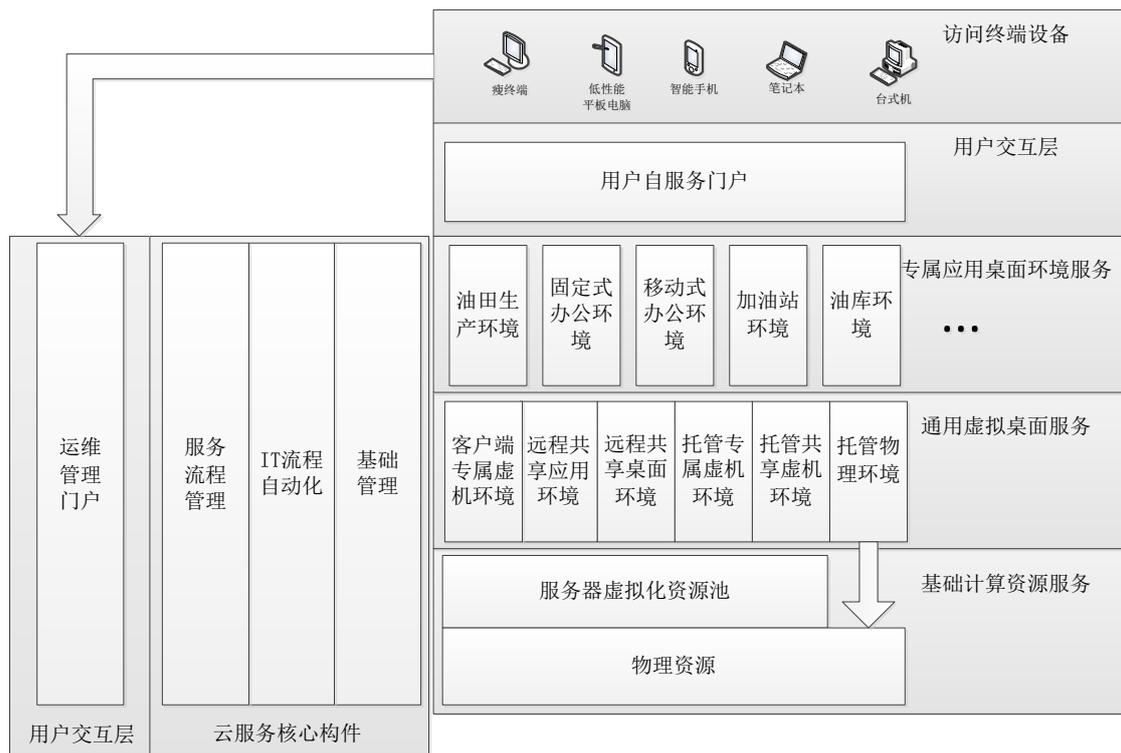
在虚拟桌面服务层中需要负责确保：

- **服务：**计费信息要准确、收费要及时、指定虚拟桌面环境要精准配发、虚拟桌面所配置的虚拟计算能力要稳定输出、虚拟桌面环境要稳定运行不出现问题（不能出现非消费者致使的错误）
- **服务相关容量变更：**镜像、虚拟机 VHD 等容量控制。不够要扩展，富余了要压缩优化。

专属应用桌面环境服务层是各企业根据自身实际应用环境需求，定制的专有应用桌面环境。从云计算的分类上其属于私有云中的 SaaS 服务。每个专属云中的服务都是提供给企业特定应用环境使用的桌面环境。每个服务可能是将多个通用虚拟桌面技术进行组合，并结合企业对特定应用环境的具体要求、规范进行定制的综合体。

用户自服务门户中采用全新的自服务方式进行功能提供。门户中包含服务目录，将用户所需的各种 IT 服务分层列举出来，以使用户快速定位自助使用。同时每种桌面云提供的服务项目都会通过 SLA 条款准确描述用户将会获得的用户体验（服务承诺），以便用户对将要使用的服务效果有恰当的预期，从而保证良好的用户满意度。

运维管理门户中充分融合了 ITIL 的管理理念，并确保服务正常输出为核心管理目标来组织整个门户网站的功能。在门户中将会形成统一的管理、监控、运维平台，不管是基础计算资源服务层还是虚拟桌面服务层上的所有管理、监控、运维工作都在此统一平台上进行。这样可以极大的降低维护人员的工作量，同时也对基础计算资源服务层还是虚拟桌面服务层进行了有效的标准化。从此统一的管理、监控、运维平台角度看，平台自身就像是主板，各种服务就像是显卡、网卡等设备，一旦插入主板，一切皆快速、良好的对接完毕。



上图是更进一步的展示桌面云系统的逻辑架构。

- **计算资源服务层：**此模块中主要负责将物理计算机、网络、存储等物理资源虚拟化并进行池化，然后加以有效管理。由于各种技术限制和未来实施过程中的各种因素的要求，服务器虚拟化资源池中实际上不是一个资源池，而是一组资源池。有些资源池可能所在地理位置不同，有些可能硬件配置性能不同，甚至有些资源池的实现厂商和技术也不尽相同。此模块负责将这些资源池有效管理，能够根据业务需要，快速精准的从符合服务申请者要求的资源池中切分出相应的资源供服务消费者使用。这种资源切分逻辑复杂且多样，如为了确保性能，从离消费者最近的、有充足容量的资源池中切取资源。当然此模块也负责将物理资源直接且分给服务消费者。这需要对物理资源的使用情况有精准的掌握。
- **通用虚拟桌面服务层：**此模块中包含各种相对独立的 PaaS 服务。每种虚拟化桌面实现技术，就是一种独立的 PaaS 服务。企业在实施过程中可以根据自身的实际需求，挑选所需的 PaaS 服务加以部署。每种虚拟化桌面服务通过一组业务流程和 IT 自动化流程，确保相应虚拟机桌面能力的稳定输出。

-
- **专属应用桌面环境服务层：**是企业总部将企业典型的业务应用环境，或子公司/部门根据自身的实际需求进行抽象汇总，然后挑选一个或一组通用虚拟桌面技术，并根据业务应用桌面环境的安全、管理、性能等具体特征/需求，定制的一个行业/业务专用桌面环境。此模块中的每一种桌面环境可能只使用一种虚拟桌面实现技术，更有可能是多种虚拟桌面技术的综合体，每一种完成部分业务应用场景。同时可以很清晰的预见到，此模块中的专用桌面环境具有显著的子公司/部门，甚至地域的差异性。换句话说，即使都是同一个业务桌面环境，每个子公司/部门的都会有不同的业务逻辑、IT 流程甚至技术组合上的差异。

图中将基础计算资源服务层和通用虚拟桌面服务层，专属应用桌面环境服务层中的共通的云服务核心模块抽取出来合并成图中的云服务核心构件。云服务核心构件组合中包含：

- **基础管理：**此模块包含用于确保计算资源服务、通用虚拟桌面服务、专属应用桌面环境服务稳定运转，问题监控、系统维护具体执行等必备的基础维护功能。如监控、备份、修复、软件分发、病毒管理等。此模块是维护管理最具体的执行者，对各种硬件、软件、应用进行维护指令的具体执行。同时也是最详细的运维管理信息收集者。收集上来的数据为更上层的云服务模块提供精准的参考信息。
- **IT 流程自动化：**此模块是综合运维调度的枢纽，是云平台的核心引擎。此模块包含一个通用的 IT 自动化流程执行引擎。云服务中的各种复杂运维管理逻辑最终都会转化成一系列自动化流程描述，而 IT 自动化流程执行引擎负责将这些流程描述加以正确解释并精准执行的平台。此模块还会以自动或被触发的方式，选择性的收集基础管理模块中的运维管理信息，然后根据预先设定好的判断逻辑进行全自动化运维管理工作。这种全自动的运维管理流程将会极大的降低维护人员的维护工作量。同时通过不断的完善和生成全自动的运维管理流程，可以有效的把维护人员积累下来的维护管理经验固化在云平台之中，从而形成维护经验的积累效果。计算资源服务、通用虚拟桌面服务、专属应用桌面环境服务三层中的 IT 自动化流程最终都会运行在此模块中。

-
- **服务流程管理：**此模块是实现各服务层业务逻辑的平台。如计算资源服务层如何向通用虚拟桌面服务层提供虚拟计算资源服务的行为，此处称为业务逻辑。更详细的例子如如何确保所需的虚拟机稳定运行，相应的虚拟计算能力稳定输出；如何确保物理资源的利用率最大化；如何进行开通服务；如何关闭服务等。此模块包含一个业务流程执行引擎。云服务中的各种业务逻辑最终都会转变成一个/一组业务流程描述的形式予以实现，而业务流程执行引擎负责将这些流程描述加以正确解释并精准执行的平台。计算资源服务、通用虚拟桌面服务、专属应用桌面环境服务三层中的业务流程最终都会运行在此模块中。

图中的用户交互层主要包含用户自服务门户和运维管理门户两大门户网站。

- **用户自服务门户：**用户通过此门户完成所有与专属应用桌面环境服务互动的操作。如操作权限申请、使用问题申报、业务数据权限变更等。同时用户也能够从门户中找到相应虚拟桌面环境的入口，从而进入桌面环境中完成相关的业务活动。在门户中最重要的组成部分是服务目录，相当于服务能力集合的分类展示列表。服务目录能够帮助用户快速找到自己想要做的事情。
- **运维管理门户：**维护人员运维管理工作的总入口。各种日常维护管理工作均会从此门户网站中找到入口点，从而降低维护人员的维护操作难度。

3.2.4 系统功能

3.2.4.1 云服务核心构件及用户交互层

用户交互	用户自服务门户		运维管理门户			
	门户网站					
服务流程管理 / IT流程自动化	服务目录					
	服务管理	计费管理	资源调度	事件处理	统计分析	用户管理
	业务流程引擎					
	IT流程自动化引擎					
	配置管理数据库(CMDB)					
基础管理	信息安全 管理	监控	备份	软件/ 补丁 分发	身份 和 权限 管理	

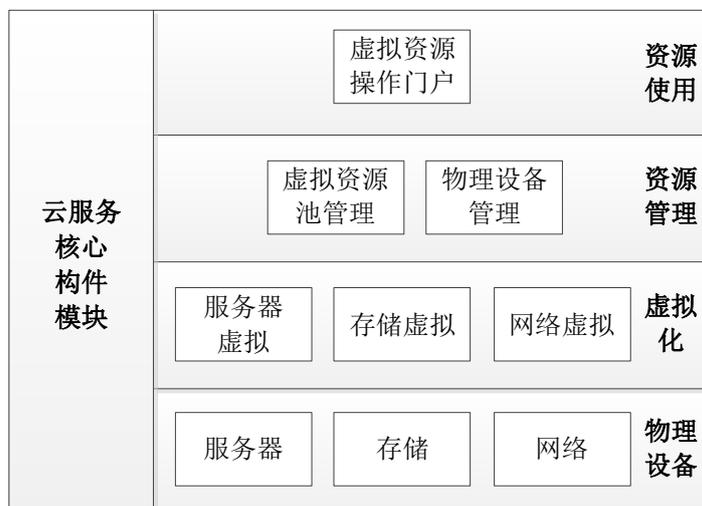
图中对云服务核心构件及用户交互层技术架构进行了展开阐述。这两个模块是基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层均包含的功能组成。此处做统一功能阐述。所有服务层中的不同服务项目虽然均包含图中的功能模块，但每个服务项目的具体规范、指标、业务逻辑却各不相同。不过所有服务项目中相同功能模块的组成结构、实现方法和运维模式是相同的。换句话说，云服务核心构件及用户交互层的构建方式更像是模板和实例的关系。整个桌面云系统在设计 and 构建上会形成一个统一的运行基础平台，这个基础平台会为每个功能模块构建好统一的系统实现结构，运行管理形式。每个服务项目会依据此基础平台的框架制作具体的业务流程、监控指标、运维逻辑，然后部署到此基础平台上进行运行。如监控模块，桌面云系统会构建统一的监控平台，此平台具有良好的扩展性。基础计算资源服务层中的服务器虚拟化资源池和通用虚拟桌面服务层中的远程共享应用环境会分别设定自己要监控的技术指标，以及时查看各自服务的运行状态。而各自设定的技术指标会部署到监控基础平台上，由平台负责执行实现。

-
- **信息安全管理：**负责对整个基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层环境中的信息安全的管控工作。如确保虚拟机文件的安全、防止被窃取，被租用的（划拨出来的）资源间的信息相互隔离，病毒防范，网络通道数据监控和通阻管理等。
 - **监控：**负责监控基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目运行环境的运行状态。此模块中应该包含最为全面的监控指标和最精准的监控数据和方便的扩展能力，以便能够充分全面的反应各服务项目的运行现状。同时提供良好的历史记录保存、快速检索、趋势预测的能力。
 - **备份：**负责对基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目的自身运行数据、系统环境进行备份，以便出现异常情况时能够快速恢复。为了提高备份和恢复效率，备份应该需要提供差异性备份能力。并且应该采用效率最高的磁盘级备份方式。
 - **软件/补丁分发：**负责对基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目的自身进行升级、完善所需的软件/系统部署操作。
 - **身份和权限管理：**负责基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目的内部各模块之间和本服务层与外界使用者的身份认证和授权的相关工作。确保功能被合法调用，数据合规的范畴下创建、读取、传输、保存。
 - **配置管理数据库(CMDB)：**整个桌面云系统的核心信息库。负责将所有软硬件和系统变更，系统运行变化，服务运维情况，用户变更等系统产生的所有变化信息记录在案，以便日后进行审计、运维状况分析、服务趋势分析等工作。换句话说，桌面云系统所有历史演变过程应有条不紊的记录在此。
 - **IT 流程自动化引擎：**负责解释和执行预先定制好的 IT 流程描述。此模块不仅提供解释和执行能力，同时应该具备编制流程描述的开发、定制框架和手段。
 - **业务流程引擎：**负责解释和执行预先定制好的业务流程描述。此模块不仅提供解释和执行能力，同时应该具备编制流程描述的开发、定制框架和手段。
 - **服务管理：**负责制作和管理基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目中的所有服务类型和业务流程。

-
- **计费管理：**负责基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目的服务输出的相关租赁费用计算工作。并且负责根据计费情况进行服务开通/关闭管理工作。计费报告和相关消费通知等功能也数据此模块实现范畴。
 - **资源调度：**负责对基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目的资源、资源池进行性能优化，虚拟资源智能划分等工作。如根据申请的需求，寻找最佳的资源池，然后切分出所需的虚拟资源；判断虚拟资源/资源池的利用率情况，并且进行容量趋势预判，如果即将到达容量极限，自动触发容量扩充处理。
 - **事件处理：**负责处理基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目产生的异常，用户提出的事件申请，以及例行运维工作。
 - **统计分析：**负责对基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目的运维、管理、服务输出、资产使用等各个方面进行统计分析，趋势预判。此模块可以根据需求进行统计分析报告的模板定制、以及按照模板生成指定报告。
 - **用户管理：**负责用户账号相关管理工作。如用户的账号基本信息；开通了哪些基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中的服务项目；能够使用服务项目中的哪些服务内容；服务费用的使用情况；用户操作权限委派等。
 - **服务目录：**负责将基础计算资源服务层、通用虚拟桌面服务层和专属应用桌面环境服务层中各服务项目提供的服务，或需要与用户进行互动的项目按照一定的逻辑，编排成一个目录列表。此模块将会内嵌在门户网站中，在用户自服务门户或运维管理门户上供使用者使用。此模块必须提供良好的编辑扩展工具/手段对不断变化/增加的服务项目进行维护组织工作。
 - **门户网站：**负责用于实现用户自服务门户或运维管理门户的基础技术平台。此模块可以进行快速的构建、编辑用户自服务门户或运维管理门户的内容和展现形式。同时提供良好的性能、安全、扩展能力。
 - **用户自服务门户：**负责为用户提供申请、消费、废除基础计算资源服务层提供的服务。用户可以通过门户中的服务目录快速找到自己所需的服务项目，并且自行操作使用。同时此门户也是用户向维护人员提供反馈意见的主要通道。

- **运维管理门户：**负责为维护人员提供运维、管理基础计算资源服务层的主要通道。维护人员通过此门户处理用户提出的事件处理请求，监控、维护系统的健康运转。

3.2.4.2 基础计算资源服务层

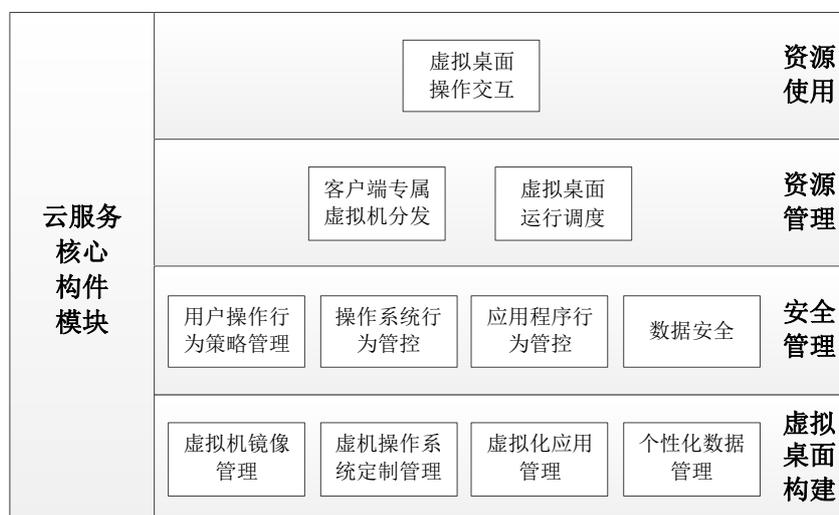


- **物理设备：**此层中包含所有物理设备，是整个桌面云的根本。所有桌面云中的虚拟桌面服务最终都会转化成物理设备上的运算加以最终实现。此模块中包含核心物理计算资源是服务器、存储和网络设备，而服务器又是整个桌面云物理资源中的核心。
- **服务器虚拟化：**用于将物理服务器转变成虚拟资源，从而实现比整个服务器为单位进行能力输出的更小粒度的资源划分，从而提供物理服务器的资源利用率/使用密度，同时实现资源归属的快速切换。此模块包含物理服务器虚拟化，虚拟机控制（创建、删除、克隆、快照等），虚拟机状态管理（开机、关机、暂停等）等虚拟化基础功能。
- **存储虚拟化：**用于将各类存储转变成虚拟资源，从而存储容量的更小粒度的切分。此模块包含存储虚拟化的基础功能。如划分容量空间、扩展/缩小容量空间等。
- **网络虚拟化：**用于将网络设备转变成虚拟化资源，以便能够实现资源归属的快速划拨和切换。此模块包含网络虚拟化的基础功能。
- **虚拟资源池管理：**用于对所有的资源池进行统一管理。某种意义上是将下面的若干资源池实例抽象成一个逻辑虚拟资源池。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，进行虚拟资源/物理资源的切分、归还，

同时负责虚拟资源池和物理设备的优化，对资源的各种变化和运行状态管控的具体操作工作。

- **物理设备管理：**负责对基础计算资源服务层中的物理设备，如服务器、网络、存储进行管理。负责物理设备的优化，对设备的各种变化和运行状态管控的具体操作工作。
- **虚拟资源操作门户：**划分的虚拟资源最终需要被用户使用，虚拟资源操作门户提供一个统一的入口界面，用户可以在其上管理自己拥有权限的虚拟机，并对其进行直接操作。如安装操作系统、开关虚拟机、在虚拟机中的系统环境中进行业务操作等。

3.2.4.3 客户端专属虚拟机环境



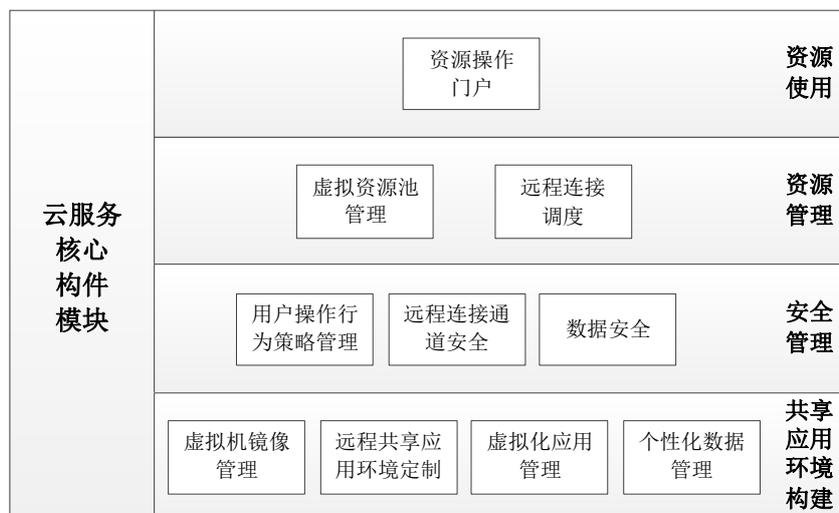
客户端专属虚拟机环境是通用虚拟桌面服务层中的一个服务项目，主要在用户的本地计算机中分离出一部分物理计算资源，供本地虚拟机使用，从而形成一个隔离的虚拟系统空间。虚拟机可以在离线状态下进行使用，同时可以将信息固封在一个独立的环境中，防止非法泄露。虚拟机中的应用在用户使用体验上会和本机安装的应用程序基本相同，同时又能将同一台物理计算机的资源划分成 2 个相互隔离的桌面环境。

- **虚拟机镜像管理：**负责对客户端专属虚拟机镜像安装包进行管理。包括分类保存、版本更新、补丁升级等工作。
- **虚拟机操作系统定制管理：**负责对虚拟机的模板中的标准操作系统进行定制化。通过集中策略的设定，将操作系统中的系统功能进行定制（如：卸载、关闭、禁用），使之符合指定的规范。

-
- **个性化数据管理：**负责为每个用户独立保存相关的个性化数据和个性化桌面配置设定值。当用户登录到自己的本地计算机上时，其上运行的客户端专属虚拟机也会同时进行自动单点登录，此时会根据登录用户的账号寻找相应的个性化数据文件夹，然后自动将个性化桌面配置设定值应用到客户端专属虚拟机中的操作系统上，使得整个桌面调整到用户日常最习惯的桌面布局。同时自动将个性化数据连接到客户端专属虚拟机的操作系统中的指定位置（如我的文档、我的图片等）。这一过程对于用户来说完全是透明的。此模块用于管理所有用户的个性化数据的保存、同步、交换等工作。
 - **虚拟化应用管理：**负责将需要安装在客户端专属虚拟机操作系统中的应用程序/系统进行虚拟化打包。当用户登录到自己的本地计算机上时，其上运行的客户端专属虚拟机也会同时进行自动单点登录，此时会根据登录用户的账号和在此模块上设定的软件使用权限策略自动将应用程序的登录点推送到用户登录的客户端专属虚拟机操作系统的桌面环境中。当用户通过应用登录点启用应用时，此服务器会通过流的推送方式智能的将应用系统文件推送到客户端专属虚拟机上，从而确保应用的正常使用。应用虚拟化可以非常灵活快速的控制应用程序和用户使用权限的对应关系。换句话说，通过集中式策略管理方式，能够快速决定用户是否能够使用指定的应用程序，并且快速生效。同时使用应用虚拟化能够将客户端专属虚拟机镜像的准备工作变得更加简单，系统将更加灵活、稳定。
 - **用户操作行为策略管理：**用于集中管控客户端专属虚拟机上的用户行为。即在桌面环境中有哪些操作可以做，哪些不行。此组策略和用户账号相关。此模块用于设置各种策略规则，然后通过策略应用机制在客户端专属虚拟机上生效。
 - **操作系统行为管控：**用于集中管控客户端专属虚拟机上的操作系统行为。即在桌面环境中有哪些行为可以被系统执行，哪些不行。此组策略和操作系统相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在客户端专属虚拟机上生效。
 - **应用程序行为管控：**用于集中管控客户端专属虚拟机上的应用程序行为。即在桌面环境中有哪些应用程序可以被系统运行，哪些不行。此组策略和应用系程序相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在客户端专属虚拟机上生效。

- **数据安全：**用于集中管控虚拟桌面环境中的数据文件的生命周期的安全。确保数据文件在创建、编辑、保存、传输、销毁过程中的安全性。此模块用于设置各种策略规则，然后通过策略应用机制在客户端专属虚拟机上生效。
- **客户端专属虚拟机分发：**负责将客户端专属虚拟机镜像安装包推送到指定的用户客户端计算机上，并且进行相关的自动化安装配置工作。
- **虚拟桌面运行调度：**负责集中管理部署到客户端的虚拟机的运行状态。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，进行虚拟资源的划分、废除，运行权限授予、收回等运行状态管控的具体操作工作。
- **虚拟桌面操作交互：**客户端专属虚拟机最终需要被用户使用，虚拟桌面操作交互模块用于实现虚拟桌面环境与客户端本地操作系统环境进行融合和互动，从而展示给用户，然后由用户对虚拟桌面环境进行直接操作。如安装应用程序、开关虚拟机、在虚拟机中的系统环境中进行业务操作等。

3.2.4.4 远程共享应用环境



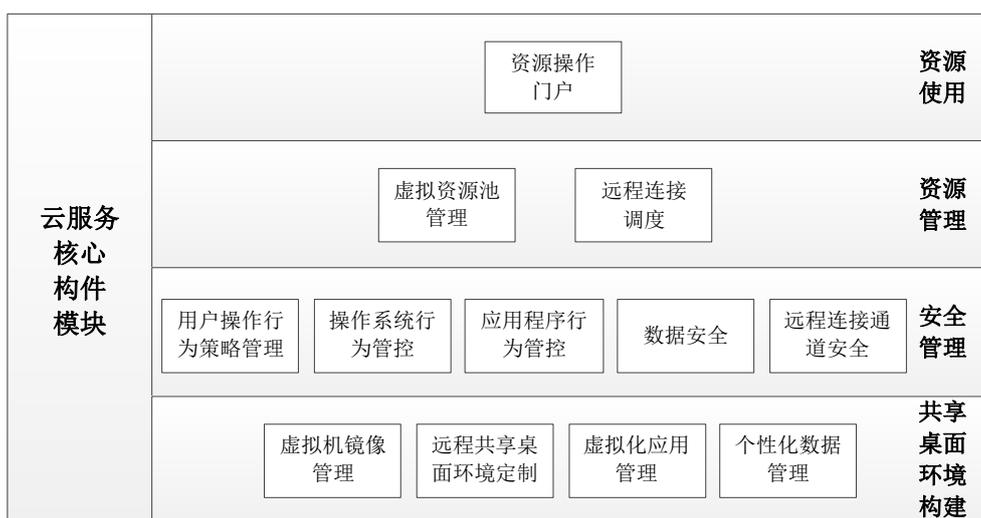
远程共享应用环境是通用虚拟桌面服务层中的一个服务项目，主要提供高密度的虚拟应用环境解决方案。当用户通过远程连接协议连接到服务器上时，服务器会为用户选择的应用创建一个相对独立的会话环境。用户对远程共享应用的操作体验和在本机安装的应用程序的体验基本相同。这种技术在单台服务器上承载的用户数量很大，是一种集中化管理、同时又节省建设成本的技术方案。换句话说，本服务会将指定的应用程序

进行集中部署和管理，然后用户通过远程访问的方式，在任意地点进行应用操作。非常便于维护人员的集中管理。每个远程共享应用会运行在一个相对独立的远程会话环境中。

- **虚拟机镜像管理：**负责对提供远程共享应用环境的服务器镜像安装包进行管理。包括分类保存、版本更新、补丁升级等工作。
- **远程共享应用环境定制：**负责对在提供远程共享应用的虚拟机系统环境中进行远程共享应用的配置工作。即决定哪些应用程序作为远程共享应用发布出去，对外提供服务。并且完成应用发布的相关配置工作。
- **个性化数据管理：**为每个用户独立保存相关的个性化数据。当用户连接到远程共享应用服务器上时，会根据登录用户的账号寻找相应的个性化数据文件夹，然后连接到用户的激活的应用程序所在的会话环境实例中。这一过程对于用户来说完全是透明的。此模块用于管理所有用户的个性化数据的保存、同步、交换等工作。
- **虚拟化应用管理：**用于将需要远程共享的应用程序/系统进行虚拟化打包。并将虚拟化的应用程序的登录点以共享应用的形式发布到远程共享应用服务器上。当用户具有实用此应用的权限，并通过应用登录点启用应用时，此模块会通过流的推送方式智能的将应用系统文件推送到会话环境中，从而确保应用的正常使用。使用应用虚拟化能够将远程共享应用服务器环境变得更加通用，系统将更加灵活、稳定。这样当远程共享应用服务器容量不够时，通过标准远程共享应用服务器模板能够快速准备出更多的服务器实例，加入服务器群组中提供服务输出。
- **用户操作行为策略管理：**用于集中管控用户在远程共享应用上的操作行为。即在共享应用环境中有哪些操作可以做，哪些不行。此组策略和用户账号相关。此模块用于设置各种策略规则，然后通过策略应用机制在远程共享应用服务器上生效。
- **远程连接通道安全：**用于集管控远程共享应用如何与远程访问终端进行交互的行为。从而避免数据通过远程连接通道产生异常流失。如数据是否下载到远程终端的机器上，数据是否能够从终端拷贝到服务器上，终端的移动存储是否能够被服务器看到等。
- **数据安全：**用于集中管控远程共享应用环境中的数据文件的生命周期的安全。确保数据文件在创建、编辑、保存、传输、销毁过程中的安全性。此模块用于设置各种策略规则，然后通过策略应用机制在远程共享应用服务器上生效。

- **虚拟资源池管理**：用于对所有的远程共享应用服务器进行统一管理。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，进行远程共享应用服务器资源的切分、归还，同时负责服务器资源的优化，对资源的各种变化和运行状态管控的具体操作工作。
- **远程连接调度**：用于集中管理用户与远程共享应用的连接情况。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，收回用户使用的远程共享应用连接。同时负责维护所有正在建立的会话连接，并对连接进行优化。
- **虚拟资源操作门户**：划分的远程共享应用最终需要被用户使用，虚拟资源操作门户提供一个统一的入口界面，用户可以在其上管理自己拥有权限的远程共享应用，并对其进行直接操作。

3.2.4.5 远程共享桌面环境



远程共享桌面环境是通用虚拟桌面服务层中的一个服务项目，主要提供高密度的虚拟桌面环境解决方案。当用户通过远程连接协议连接到服务器上时，服务器会为用户创建一个相对独立的桌面会话环境。用户在桌面会话环境中的操作体验和在本机登录的体验基本相同。这种技术在单台服务器上承载的用户数量很大，是一种集中化管理、同时又节省建设成本的技术方案。

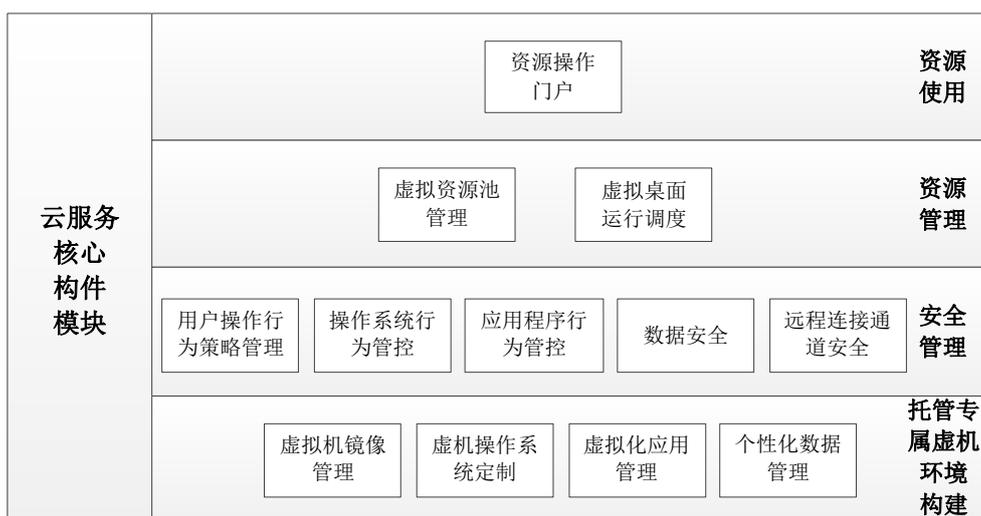
- **虚拟机镜像管理**：负责对提供远程共享桌面环境的服务器镜像安装包进行管理。包括分类保存、版本更新、补丁升级等工作。

-
- **远程共享桌面环境定制：**负责对在提供远程共享桌面的虚拟机系统环境中的操作系统进行定制。通过集中策略的设定，将操作系统中的系统功能进行定制（如：卸载、关闭、禁用），使之符合指定的规范。
 - **个性化数据管理：**负责为每个用户独立保存相关的个性化数据和个性化桌面配置设定值。当用户登录到远程共享桌面服务器上时，此模块会根据登录用户的账号寻找相应的个性化数据文件夹，然后自动将个性化桌面配置设定值应用到远程共享桌面会话环境中，使得整个桌面调整到用户日常最习惯的桌面布局。同时自动将个性化数据连接到远程共享桌面会话环境中的指定位置（如我的文档、我的图片等）。这一过程对于用户来说完全是透明的。此模块用于管理所有用户的个性化数据的保存、同步、交换等工作。
 - **虚拟化应用管理：**负责将需要安装在远程共享桌面服务器中的应用程序/系统进行虚拟化打包。当用户登录到远程共享桌面服务器上时，此模块会根据登录用户的账号和在此模块上设定的软件使用权限策略自动将应用程序的登录点推送到用户登录的远程共享桌面服务器上的桌面会话环境中。当用户通过应用登录点启用应用时，此模块会通过流的推送方式智能的将应用系统文件推送到远程共享桌面会话环境中，从而确保应用的正常使用。应用虚拟化可以非常灵活快速的控制应用程序和用户使用权限的对应关系。换句话说，通过集中式策略管理方式，能够快速决定用户是否能够使用指定的应用程序，并且快速生效。同时使用应用虚拟化能够将远程共享桌面服务器虚拟机镜像的准备工作变得更加简单，系统将更加灵活、稳定。
 - **用户操作行为策略管理：**用于集中管控远程共享桌面环境上的用户行为。即在桌面环境中有哪些操作可以做，哪些不行。此组策略和用户账号相关。此模块用于设置各种策略规则，然后通过策略应用机制在远程共享桌面环境上生效。
 - **操作系统行为管控：**用于集中管控远程共享桌面环境上的操作系统行为。即在桌面环境中有哪些行为可以被系统执行，哪些不行。此组策略和操作系统相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在远程共享桌面环境上生效。
 - **应用程序行为管控：**用于集中管控远程共享桌面环境上的应用程序行为。即在桌面环境中有哪些应用程序可以被系统运行，哪些不行。此组策略和应用系程序相关。

即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在远程共享桌面环境上生效。

- **数据安全：**用于集中管控虚拟桌面环境中的数据文件的生命周期的安全。确保数据文件在创建、编辑、保存、传输、销毁过程中的安全性。此模块用于设置各种策略规则，然后通过策略应用机制在远程共享桌面环境上生效。
- **远程连接调度：**用于集中管理用户与远程共享桌面的桌面会话连接情况。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，收回用户使用的远程共享桌面会话连接。同时负责维护所有正在建立的会话连接，并对连接进行优化。
- **虚拟资源池管理：**用于对所有的远程共享桌面服务器进行统一管理。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，进行远程共享桌面服务器资源的切分、归还，同时负责服务器资源的优化，对资源的各种变化和运行状态管控的具体操作工作。
- **虚拟资源操作门户：**划分的远程共享桌面最终需要被用户使用，虚拟资源操作门户提供一个统一的入口界面，用户可以在其上管理自己拥有权限的远程共享桌面，并对其进行直接操作。

3.2.4.6 托管专属虚拟机环境



托管专属虚拟机环境是通用虚拟桌面服务层中的一个服务项目，主要为每个用户提供完全独立的桌面运行环境。每个用户会独享一个虚拟机，并且不管其是否在使用，此

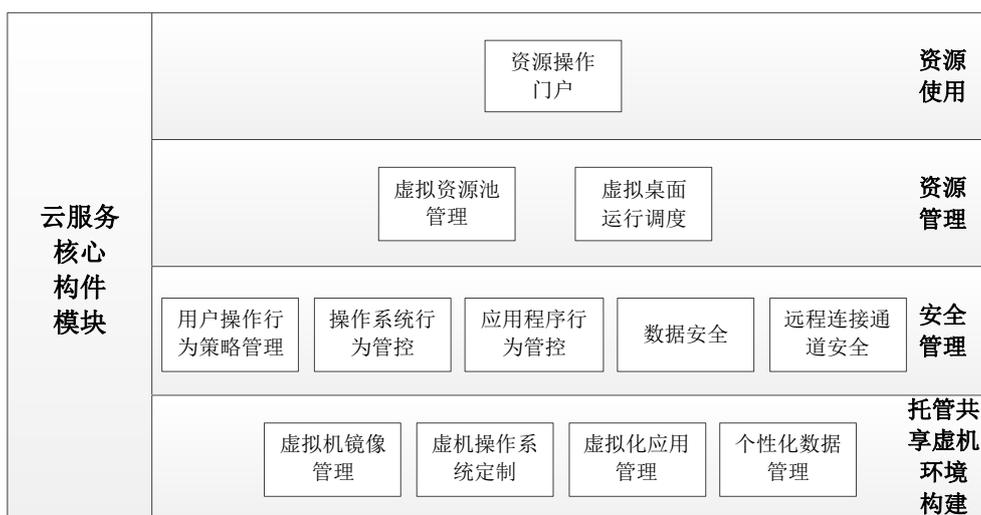
虚拟机都专属于此用户，即使处于关机状态。由于每个用户占有一个独立的虚拟操作系统环境和独立安装的应用程序，因此此技术的单台服务器上的用户集成密度不会很高。

- **虚拟机镜像管理：**负责对托管专属虚拟机镜像安装包进行管理。包括分类保存、版本更新、补丁升级等工作。
- **虚拟机操作系统定制：**负责对虚拟机的模板中的标准操作系统进行定制化。通过集中策略的设定，将操作系统中的系统功能进行定制（如：卸载、关闭、禁用），使之符合指定的规范。
- **个性化数据管理：**负责为每个用户独立保存相关的个性化数据和个性化桌面配置设定值。当用户登录到自己的专属虚拟机上时，此模块会根据登录用户的账号寻找相应的个性化数据文件夹，然后自动将个性化桌面配置设定值应用到托管专属虚拟机中的操作系统上，使得整个桌面调整到用户日常最习惯的桌面布局。同时自动将个性化数据连接到托管专属虚拟机的操作系统中的指定位置（如我的文档、我的图片等）。这一过程对于用户来说完全是透明的。此模块用于管理所有用户的个性化数据的保存、同步、交换等工作。
- **虚拟化应用管理：**负责将需要安装在托管专属虚拟机操作系统中的应用程序/系统进行虚拟化打包。当用户登录到自己的托管专属虚拟机上时，此模块会根据登录用户的账号和在此模块上设定的软件使用权限策略自动将应用程序的登录点推送到用户登录的托管专属虚拟机操作系统的桌面环境中。当用户通过应用登录点启用应用时，此模块会通过流的推送方式智能的将应用系统文件推送到托管专属虚拟机上，从而确保应用的正常使用。应用虚拟化可以非常灵活快速的控制应用程序和用户使用权限的对应关系。换句话说，通过集中式策略管理方式，能够快速决定用户是否能够使用指定的应用程序，并且快速生效。同时使用应用虚拟化能够将托管专属虚拟机镜像的准备工作变得更加简单，系统将更加灵活、稳定。
- **用户操作行为策略管理：**用于集中管控客户端专属虚拟机上的用户行为。即在桌面环境中有哪些操作可以做，哪些不行。此组策略和用户账号相关。此模块用于设置各种策略规则，然后通过策略应用机制在客户端专属虚拟机上生效。
- **操作系统行为管控：**用于集中管控托管专属虚拟机上的操作系统行为。即在桌面环境中有哪些行为可以被系统执行，哪些不行。此组策略和操作系统相关。即不管谁

登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在托管专属虚拟机上生效。

- **应用程序行为管控：**用于集中管控托管专属虚拟机上的应用程序行为。即在桌面环境中有哪些应用程序可以被系统运行，哪些不行。此组策略和应用系程序相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在托管专属虚拟机上生效。
- **数据安全：**用于集中管控虚拟桌面环境中的数据文件的生命周期的安全。确保数据文件在创建、编辑、保存、传输、销毁过程中的安全性。此模块用于设置各种策略规则，然后通过策略应用机制在托管专属虚拟机上生效。
- **远程连接调度：**用于集中管理用户与托管专属虚拟机的连接情况。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，收回用户使用的托管专属虚拟机连接。同时负责维护所有正在建立的会话连接，并对连接进行优化。
- **虚拟资源操作门户：**划分的托管专属虚拟机最终需要被用户使用，虚拟资源操作门户提供一个统一的入口界面，用户可以在其上管理自己拥有权限的托管专属虚拟机，并对其进行直接操作。如安装操作系统、开关虚拟机、在虚拟机中的系统环境中进行业务操作等。

3.2.4.7 托管共享虚机环境

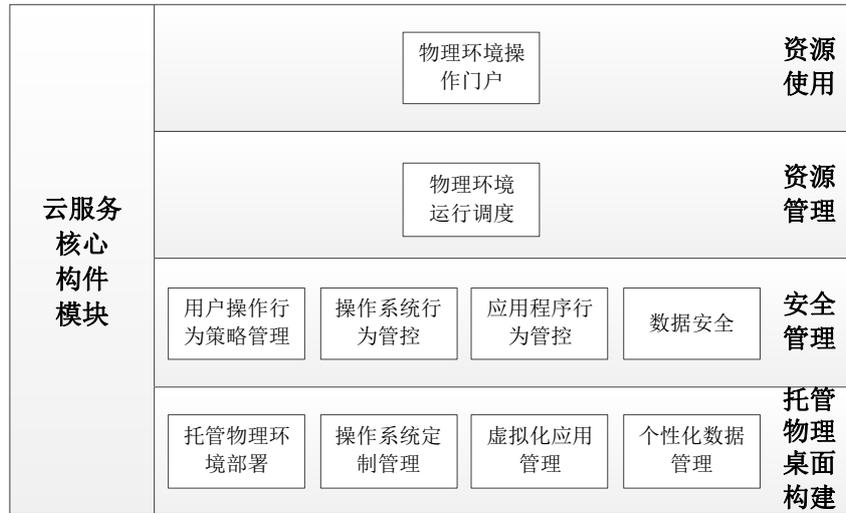


托管共享虚拟机环境是通用虚拟桌面服务层中的一个服务项目，主要为用户提供一组桌面运行环境。在用户登录使用之前，所有的虚拟机的运行环境是无状态的（没有和用户相关的个性化信息）。当用户登录到其中的某个虚拟机时，此虚拟机将会被此用户临时性独占，虚拟机的桌面环境将会因用户的操作而个性化变化（有状态）。当用户从虚拟机上退出时，虚拟机上的桌面环境将会回滚到用户登录前的初始桌面环境。

- **虚拟机镜像管理：**负责对托管共享虚拟机镜像安装包进行管理。包括分类保存、版本更新、补丁升级等工作。
- **虚拟机操作系统定制：**负责对虚拟机的模板中的标准操作系统进行定制化。通过集中策略的设定，将操作系统中的系统功能进行定制（如：卸载、关闭、禁用），使之符合指定的规范。
- **个性化数据管理：**负责为每个用户独立保存相关的个性化数据和个性化桌面配置设定值。当用户登录到共享虚拟机上时，此模块会根据登录用户的账号寻找相应的个性化数据文件夹，然后自动将个性化桌面配置设定值应用到连接的托管共享虚拟机中的操作系统上，使得整个桌面调整到用户日常最习惯的桌面布局。同时自动将个性化数据连接到托管共享虚拟机的操作系统中的指定位置（如我的文档、我的图片等）。这一过程对于用户来说完全是透明的。此模块用于管理所有用户的个性化数据的保存、同步、交换等工作。
- **虚拟化应用管理：**负责将需要安装在托管共享虚拟机操作系统中的应用程序/系统进行虚拟化打包。当用户登录到共享虚拟机上时，此模块会根据登录用户的账号和在此模块上设定的软件使用权限策略自动将应用程序的登录点推送到用户登录的托管共享虚拟机操作系统的桌面环境中。当用户通过应用登录点启用应用时，此模块会通过流的推送方式智能的将应用系统文件推送到连接的托管共享虚拟机上，从而确保应用的正常使用。应用虚拟化可以非常灵活快速的控制应用程序和用户使用权限的对应关系。换句话说，通过集中式策略管理方式，能够快速决定用户是否能够使用指定的应用程序，并且快速生效。同时使用应用虚拟化能够将托管共享虚拟机镜像的准备工作变得更加简单，系统将更加灵活、稳定。

-
- **用户操作行为策略管理：**用于集中管控客户端共享虚拟机上的用户行为。即在桌面环境中有哪些操作可以做，哪些不行。此组策略和用户账号相关。此模块用于设置各种策略规则，然后通过策略应用机制在客户端共享虚拟机上生效。
 - **操作系统行为管控：**用于集中管控托管共享虚拟机上的操作系统行为。即在桌面环境中有哪些行为可以被系统执行，哪些不行。此组策略和操作系统相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在托管共享虚拟机上生效。
 - **应用程序行为管控：**用于集中管控托管共享虚拟机上的应用程序行为。即在桌面环境中有哪些应用程序可以被系统运行，哪些不行。此组策略和应用系程序相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在托管共享虚拟机上生效。
 - **数据安全：**用于集中管控虚拟桌面环境中的数据文件的生命周期的安全。确保数据文件在创建、编辑、保存、传输、销毁过程中的安全性。此模块用于设置各种策略规则，然后通过策略应用机制在托管共享虚拟机上生效。
 - **远程连接调度：**用于集中管理用户与托管共享虚拟机的连接情况。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，收回用户使用的托管共享虚拟机连接。同时负责维护所有正在建立的会话连接，并对连接进行优化。
 - **虚拟资源操作门户：**划分的托管共享虚拟机最终需要被用户使用，虚拟资源操作门户提供一个统一的入口界面，用户可以在其上管理自己拥有权限的托管共享虚拟机，并对其进行直接操作。如安装操作系统、开关虚拟机、在虚拟机中的系统环境中进行业务操作等。

3.2.4.8 托管物理环境



托管物理环境是通用虚拟桌面服务层中的一个服务项目，主要为每个用户提供一组桌面运行环境。在用户登录使用之前，所有的物理服务器/工作站的运行环境是无状态的（没有和用户相关的个性化信息）。当用户登录到其中的某个物理服务器/工作站时，此物理服务器/工作站将会被此用户临时性独占，物理服务器/工作站的桌面环境将会因用户的操作而个性化变化（有状态）。当用户从物理服务器/工作站上退出时，物理服务器/工作站上的桌面环境将会重置到用户登录前的初始桌面环境。

- **托管物理环境部署：**负责将物理服务器/工作站配置成指定的托管物理桌面环境，以便供用户使用。包括桌面部署镜像管理、服务器/工作站的自动化部署、版本升级等工作。
- **虚拟机操作系统定制管理：**负责对托管物理环境部署中的标准操作系统进行定制化。通过集中策略的设定，将操作系统中的系统功能进行定制（如：卸载、关闭、禁用），使之符合指定的规范。
- **个性化数据管理：**负责为每个用户独立保存相关的个性化数据和个性化桌面配置设定值。当用户登录到自己的托管物理服务器/工作站上时，此模块会根据登录用户的账号寻找相应的个性化数据文件夹，然后自动将个性化桌面配置设定值应用到托管物理服务器/工作站中的操作系统上，使得整个桌面调整到用户日常最习惯的桌面布局。同时自动将个性化数据连接到托管物理服务器/工作站的操作系统中的指

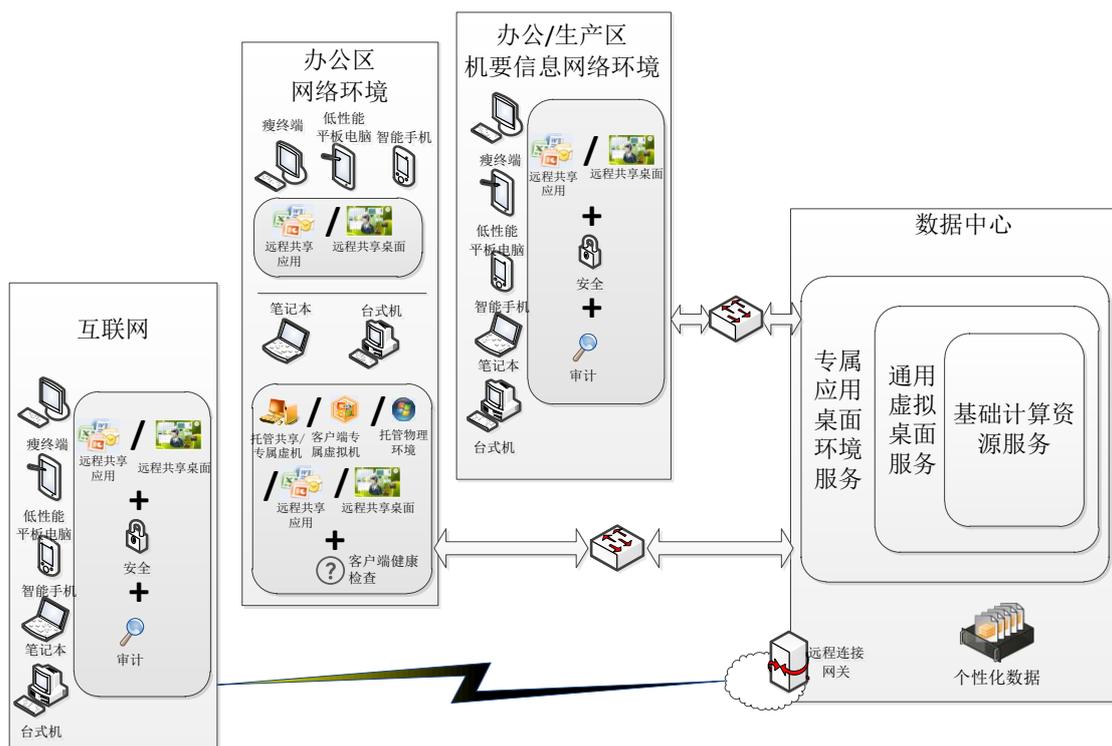
定位置（如我的文档、我的图片等）。这一过程对于用户来说完全是透明的。此模块用于管理所有用户的个性化数据的保存、同步、交换等工作。

- **虚拟化应用管理：**负责将需要安装在托管物理服务器/工作站操作系统中的应用程序/系统进行虚拟化打包。当用户登录到自己的托管物理服务器/工作站上时，此模块会根据登录用户的账号和在此模块上设定的软件使用权限策略自动将应用程序的登录点推送到用户登录的托管物理服务器/工作站操作系统的桌面环境中。当用户通过应用登录点启用应用时，此模块会通过流的推送方式智能的将应用系统文件推送到托管物理服务器/工作站上，从而确保应用的正常使用。应用虚拟化可以非常灵活快速的控制应用程序和用户使用权限的对应关系。换句话说，通过集中式策略管理方式，能够快速决定用户是否能够使用指定的应用程序，并且快速生效。同时使用应用虚拟化能够将客户端专属虚拟机镜像的准备工作变得更加简单，系统将更加灵活、稳定。
- **用户操作行为策略管理：**用于集中管控托管物理服务器/工作站上的用户行为。即在桌面环境中有哪些操作可以做，哪些不行。此组策略和用户账号相关。此模块用于设置各种策略规则，然后通过策略应用机制在托管物理服务器/工作站上生效。
- **操作系统行为管控：**用于集中管控托管物理服务器/工作站上的操作系统行为。即在桌面环境中有哪些行为可以被系统执行，哪些不行。此组策略和操作系统相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在托管物理服务器/工作站上生效。
- **应用程序行为管控：**用于集中管控托管物理服务器/工作站上的应用程序行为。即在桌面环境中有哪些应用程序可以被系统运行，哪些不行。此组策略和应用系程序相关。即不管谁登录，此模块限定的行为均生效。此模块用于设置各种策略规则，然后通过策略应用机制在托管物理服务器/工作站上生效。
- **数据安全：**用于集中管控虚拟桌面环境中的数据文件的生命周期的安全。确保数据文件在创建、编辑、保存、传输、销毁过程中的安全性。此模块用于设置各种策略规则，然后通过策略应用机制在托管物理服务器/工作站上生效。
- **物理环境运行调度：**负责集中管理托管物理服务器/工作站的运行状态。此模块负责根据云服务核心构件中的资源调度、业务流程、服务管理等模块的指令，进行托

管物理服务器/工作站的划分、废除，运行权限授予、收回等运行状态管控的具体操作工作。

- **物理环境操作门户：**划分的托管物理桌面最终需要被用户使用，物理环境操作门户提供一个统一的入口界面，用户可以在其上管理自己拥有权限的托管物理桌面，并对其进行直接操作。

3.2.4.9 用户端体验



整个桌面云系统全面考虑了将会使用到的终端系统以及访问过程中终端、桌面云环境以及其间数据的创建、访问、传输、保存的安全保护。桌面云的用户体验目标是：用户可以随时随地，通过任何设备进行办公/生产。桌面云会对台式 PC 机、笔记本、瘦终端、PAD、手机等设备类型广泛支持。用户基本可以做到用市面上可以获得的远程访问终端设备，与办公应用进行有效互动。图中阐述了访问桌面云的终端可能处在的网络类别以及相关的安全特性。

- **办公/生产区机要信息网络环境**

当用户需要访问企业规定的保密级别很高的办公/生产信息时，企业需要确保用户不会因为误操作或未经授权的情况下，将机密信息泄漏出去，让未经授权的人获得。因

此办公/生产环境必须存在于一个安全的环境中，并且用户行为进行相关的审计记录，同时信息的访问权限受到相应的约束。此类用户只能够在访问终端上，通过对展现层虚拟化技术远程传递过来的办公/生产应用的界面（GUI）或办公/生产桌面化境的桌面影像（GUI），进行互动操作来对办公/生产机要信息进行访问。而办公/生产应用程序只能运行在数据中心的各种虚拟桌面服务器上或者是客户端专属虚拟机环境中。同时办公/生产机要信息只允许停留在数据中心的虚拟桌面服务器上或客户端专属虚拟机中，在未经授权的情况下，绝对不允许信息复制到用户使用的访问终端上或通过邮件、文件网络复制等方式流传出去。

同时在用户使用的访问终端和数据中心虚拟桌面服务器/客户端专属虚拟机间的形成网络连接加密通道，确保数据的传输过程的安全性。而数据中心的虚拟桌面服务器/客户端专属虚拟机运行在有 IPsec 形成的安全网络环境中。

为了避免一旦机要信息泄露无法追查责任人的情况的出现，桌面云中必须具备用户行为审计功能，对用户通过远程连接进行操作的整个过程进行详细记录。

凡是能够进入办公/生产区机要信息网络环境的终端设备均为受控设备。即被企业 IT 系统管理着，从而确保其环境符合企业要求的健康和安全管理要求。

● 办公区网络环境

用户在办公网中进行典型的日常办公工作。信息的安全性没有机要信息区那样的严格。用户的 80% 以上的时间是在办公区网络环境中进行相关活动。通过使用托管共享/专属虚拟机，客户端专属虚拟机，托管物理环境，远程共享应用，远程共享桌面等技术，最大灵活度的为不同类型的用户提供最为恰当的虚拟化桌面环境。

大部分用户拥有自己的专属办公用终端，有些是台式机，有些是笔记本电脑。办公环境虚拟化在此种情况下可以有效的将办公环境和用户个人桌面环境进行隔离，从而确保对办公环境进行更为严格的标准化设置，降低办公环境出现问题的机率，减少维护人员的维护难度和工作量。在对办公环境进行虚拟化的同时，不会对用户的使用习惯和用户体验造成显著的差异感。即尽可能的让用户感知不到办公环境已被虚拟化。

对于那些只能在旧的客户端操作系统环境中工作，且需要离线操作的应用程序，本方案通过向用户的台式机或笔记本上推送客户端专属虚拟机环境，并确保虚拟机中应用程序使用体验与本地安装应用基本相同。从而解决旧程序和新的操作系统环境兼容性问题，实现旧系统在新的桌面环境安全规范下的稳定工作。

那些需要更强大的计算能力的应用程序来说，或由于某种原因需要临时借用其他员工的终端设备访问自己的办公环境时，可以通过使用托管共享/专属虚机（VDI 技术），为用户在数据中心服务器上提供更强劲的客户端虚拟机环境来满足相应需求，且用户使用的虚拟机桌面环境与其本机使用的办公环境基本相同。

对于那些受到严格约束的生产应用系统的用户，可以通过使用远程共享应用和远程共享桌面的方式加以实现。生产应用系统整个逻辑运算部分运行在数据中心的服务器中，用户只能够和远程传递过来的应用程序的界面（GUI）影像进行互动，从而确保应用系统运行环境和设置不被轻易破坏。

当然对于那些临时性需要查询企业信息/数据的情况，同样通过用远程共享应用，远程共享桌面的方式加以实现。生产应用系统整个逻辑运算部分运行在数据中心的服务器中，用户与远程传递过来的应用程序的界面（GUI）影像进行互动方式加以实现。

凡是能够进入办公区网络环境的终端设备均为受控设备。即被企业 IT 系统管理着，从而确保其环境符合企业要求的健康和安全管理要求

● 互联网

用户在临时出差在外，专属计算不在身边，又急需方法办公环境的情况，可以通过用远程共享应用，远程共享桌面，在具有加密通道的企业门户上提供办公环境的方式加以实现。从而实现在不安全的互联网上安全的访问办公应用/办公信息。

同样的为了避免办公信息的泄漏，此类用户操作需要进行详细的审计记录。

凡是能够进入互联网环境的终端设备均为非受控设备。即不受企业 IT 系统管理，无法确保其操作系统环境的安全性。

3.2.4.10 信息安全

● 访问终端自身安全

访问终端是用户与桌面云中虚拟桌面环境互动的主要交互工具，是最容易产生信息泄露、病毒侵害的地方。访问终端的安全主要从以下几个方面入手：

- **访问终端操作系统环境的安全保障：**最主要的保障手段是在访问终端的操作系统中安装杀毒软件，并且对病毒库进行及时的更新。
- **网络传输通道的管控控制：**最主要的手段是在访问终端环境中设置/安装双向防火墙，确保数据或病毒侵害停留在访问终端环境中，避免异常外泄。
- **访问终端桌面环境定制：**主要手段是对操作系统进行定制，将不必要的组件和功能进行卸载。还有就是通过策略将设立应用程序白名单和黑名单，从而限制可运行的应用程序，从而避免非法程序进行信息泄露。
- **访问终端所属信息审计：**将访问终端进行及时的记录，包括终端的型号、网址、时间等信息。

● 访问数据通道安全

访问终端设备会和虚拟桌面环境建立网络连接，进行数据交换。数据交换包括：操作行为指令、键盘输入数据信息，以及业务数据的双向传输。在网络上对数据通道进行监听，数据就会有泄漏的风险。通过在访问终端和虚拟桌面环境间建立加密通道(SSL)，然后所有数据在此通道中传输可以有效的解决此类数据泄漏风险。同时可以通过设定数据的传输方向，控制数据的是否可以上传或下载。

● 个性化/业务数据安全

个性化数据/业务数据是整个员工/企业最为需要保护的部分。数据包含了产生、保存、读取、传输、销毁五个状态。通过确保这五个阶段的安全就可以实现数据的安全保障。

- **产生：**数据在产生时主要停留在操作系统的内存空间中，要想保证内存空间中的数据不被泄漏，可以通过杀毒软件来实现操作系统实时防护。
- **保存：**数据的保存形式是以文件的形式保留在文件系统中，因此保护数据的保存主要通过文件系统的权限控制来加以实现。只有被授权的用户账号才能够对文件进行读取。同时通过杀毒软件来防护数据文件被病毒进行文件非法窃取。

同时通过文件加密技术对文件内容进行加密，从而确保即使数据被泄漏也无法正常读取文件内容实质。

- **读取：**将数据从文件中重新获取出来是数据安全的一个重要环节。数据的读取主要是通过文件系统的权限加以控制。同时通过应用程序黑/白名单功能限制操作系统中可运行的应用程序，从而禁止非法应用程序打开数据文件读取数据。
- **传输：**数据的传输主要形式是通过文件的传输方式进行。通过操作系统中的双向防火墙可以有效的约束文件的传输通道。
- **销毁：**数据文件的删除是数据销毁的主要途径。数据的完全删除是确保数据销毁的安全。

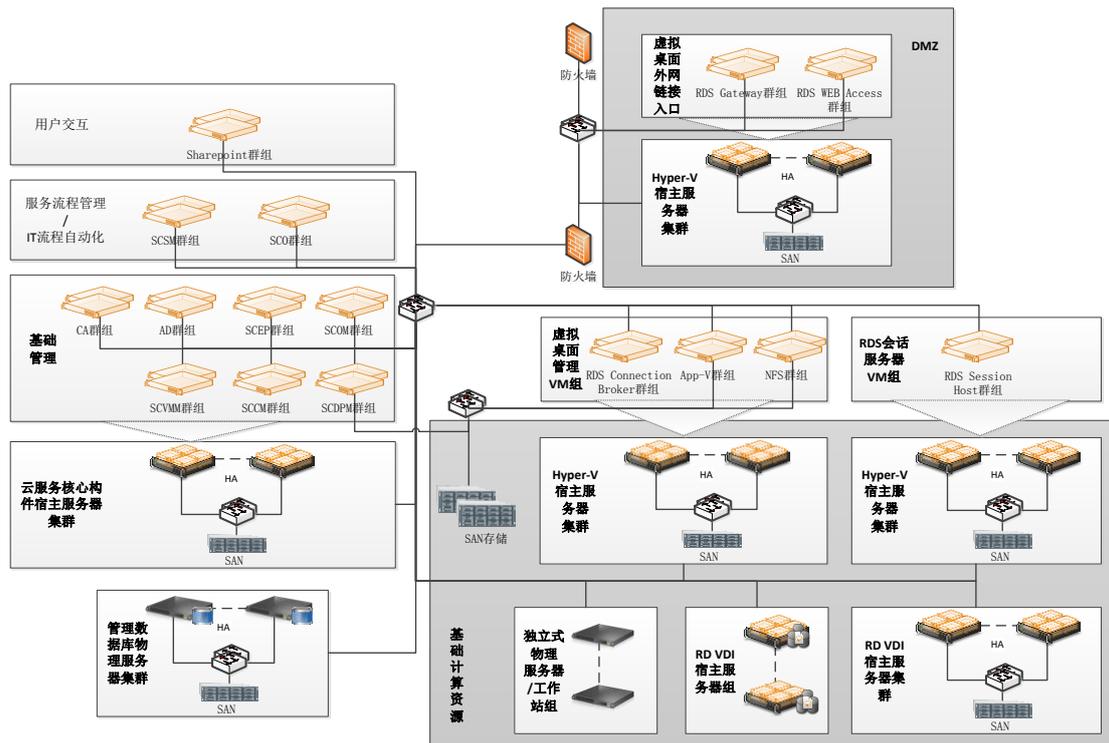
- **虚拟桌面服务自身安全**

数据主要会在虚拟桌面系统中运转因此系统自身应该提供足够的安全保障。虚拟桌面虚机的虚拟机文件保存时会通过加密的方式保存在宿主服务器上。宿主服务器自身也会通过杀毒、系统裁剪定制、防火墙的机制来确保服务器的安全。通过 IPSec 机制将系统环境运行在一个可靠的网络环境中。通过身份和授权机制来实现系统权限的管控。通过审计机制监察系统的可能出现的非法行为。虚拟机中操作系统同样可以进行杀毒、系统定制、防火墙的机制来确保其环境的安全。

- **用户行为安全管控**

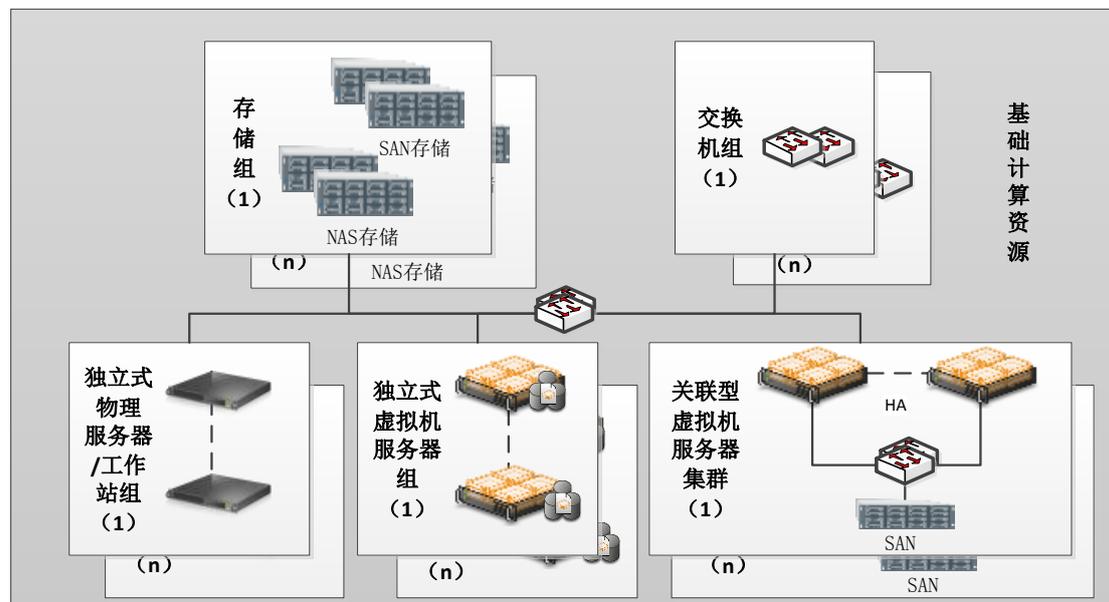
用户的误操作在信息泄漏上占有最大的比率。控制用户行为主要分为：通过黑白名单策略限制用户能够在操作系统中运行的应用程序；通过权限管控限制用户是否能够进行应用程序的安装卸载；通过移动硬盘加密策略确保数据传出系统时必须要进行数据加密，以防止意外丢失后的数据泄漏；通过文件系统权限控制约束用户是否能够对数据文件进行操作。同时通过审计工作，记录用户在操作系统上行为以便日后审计。

3.2.5 物理拓扑架构



3.2.6 拓扑结构组成

3.2.6.1 基础计算资源

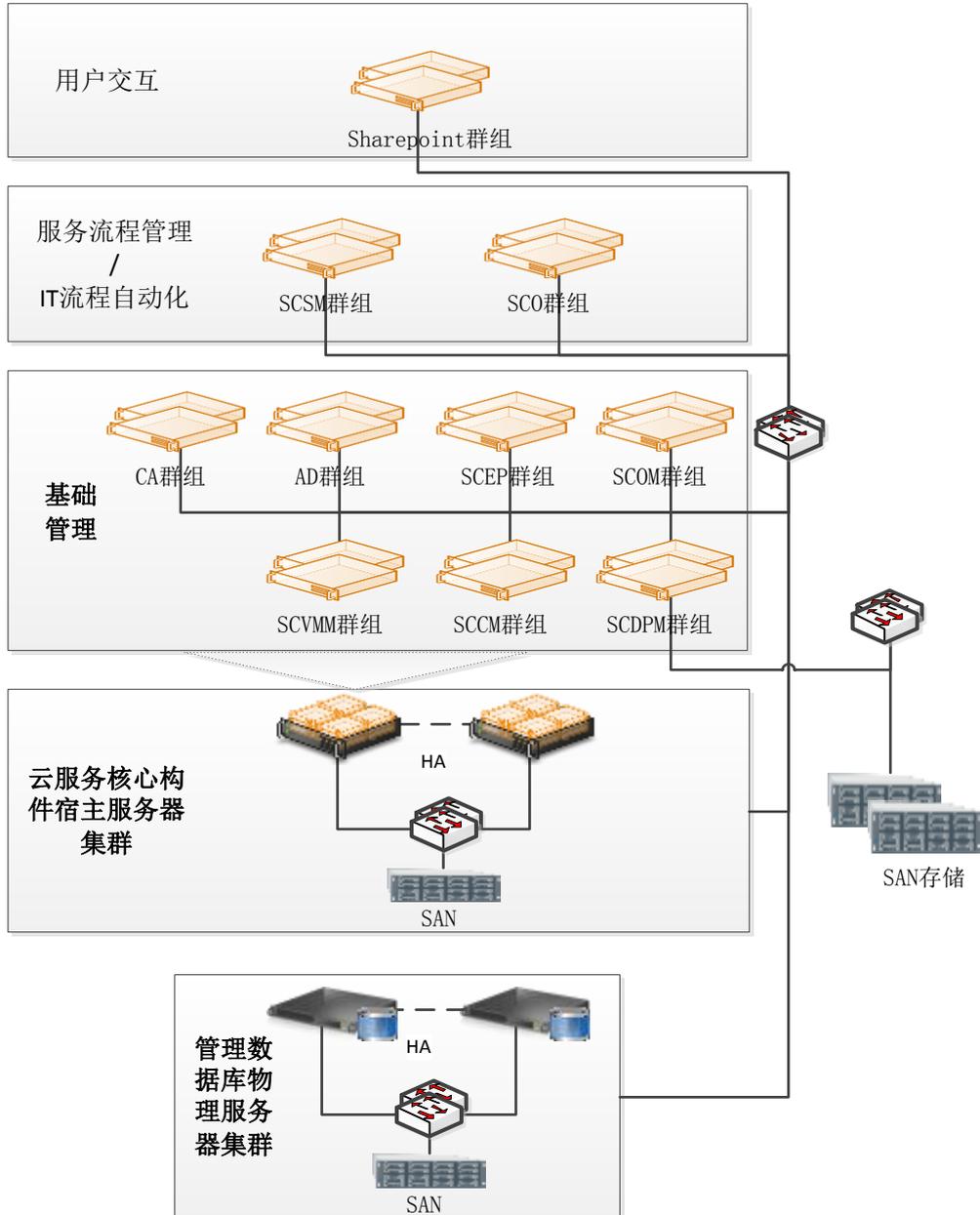


整个基础计算资源服务层中的物理设备根据地理位置、性能需求、建设成本等原因会由多种服务器/工作站类型和网络、存储设备组成多种资源池。图中对资源池的种类进行了分类：

- **独立式虚拟机服务器组：**是由独立运行的一组服务器虚拟化宿主服务器组成。在其上运行的虚拟机的虚拟磁盘文件将会直接存储在服务器的本地硬盘中。此类宿主服务器主要用来运行那些应用系统部署规模小，使用压力很低，允许短时间停止对外提供服务，进行离线维护处理的虚拟机。或者那种虚拟机中的应用系统本身具有良好的负载均衡/高可用性设计的。因为这种虚拟机需要资源池提供高可用性机制加以额外保护。这样设计是由于实际上有些需求确实不需要宿主服务器提供高可用性架构，同时又可以显著的降低系统建设成本。当然此服务器组中的宿主服务器又可以分成高性能、高配置的宿主服务器和低性能、低配置的宿主服务器，以便满足不同种类虚拟机性能输出的需求。此类服务器组很可能会在不同地理位置上存在部署需求，因此会从整个基础计算资源服务层角度上观察会存在若干个此类服务器组。
- **关联型虚拟机服务器组：**此类服务器组是由一组服务器虚拟化宿主服务器构建的集群。集群中的所有节点宿主服务器会通过光纤或 iSCSI 的方式共享一个 SAN 存储，从而形成服务器虚拟化的高可用环境，提供给其上运行的虚拟机快速恢复的能力。但是由于各服务器虚拟化软件厂商提供的产品的技术局限性，目前还不能构成集群中宿主服务器无限制数量扩展，因此集群必然是由固定数量的宿主服务器组成。而单一的一个集群不可能承载所有的虚拟资源需求。同时又可能因为需要部署到不同地理位置上等因素，从而在基础计算资源服务层中存在若干关联型虚拟机服务器组。由于此类服务器组提供了良好的 HA 架构，因此即使虚拟机自身没有 HA 架构设计时，也能帮助其形成较好的高可用性支撑。同时此类服务器组使用的是高性能物理设备，尤其是存储和网络，因此虚拟机的性能表现将会更佳，但此类服务器的构建成本也相当可观。
- **独立式物理服务器/工作站组：**此类服务器组是用来满足某些应用环境无法使用虚拟化资源的情况下提供整机租赁的服务。比如说某些地质分析、GIS 或 3D 设计应用等高性能需求的 3D 运算系统虚拟机可能无法满足需求，那么就可以通过提供物理桌面环境的方式加以满足。未来的使用场景肯定是当客户需要时，虚拟资源池管理

服务器会从此类服务器组中选出最适合客户需求的服务器/工作站，自动配置成用户需要的桌面环境，然后提供给用户使用。

3.2.6.2 云服务核心构件及用户交互层



此模块中展示的服务器是构建整个桌面云系统的核心部分。

- **管理数据库物理服务器集群：**是一组物理服务器构建的 MS cluster 集群。物理服务器上运行着 SQL Server。SQL server 利用 MS cluster 形成高可用架构，从而确保 SQL server 在异常情况下的快速恢复。SQL Server 中部署着云服务核心构件宿主服务器

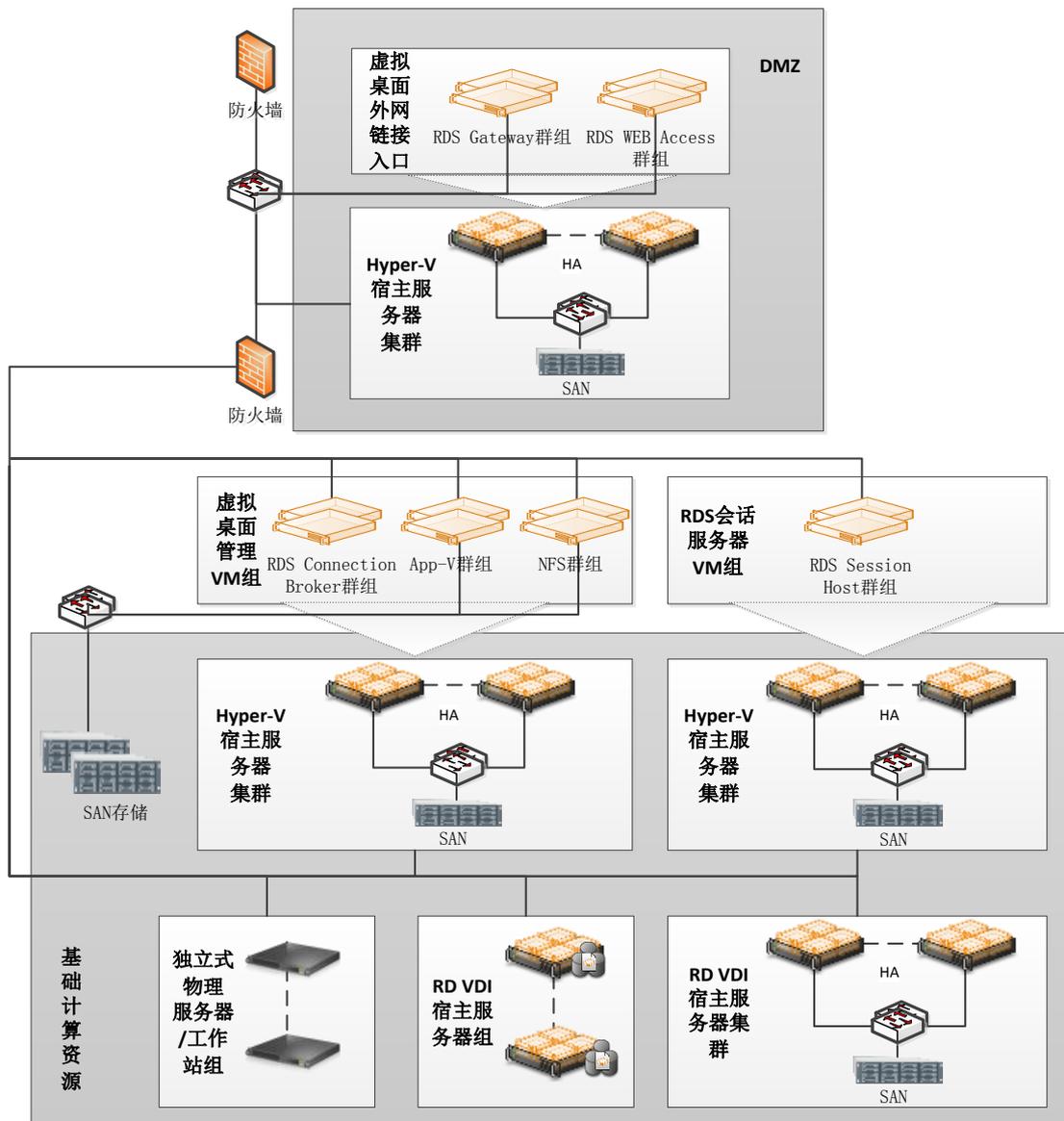
集群、基础管理、服务流程管理/IT 流程自动化、用户交互层中其它软件产品/定制开发应用所需的管理数据库。

- **云服务核心构件宿主服务器集群：**是一组物理服务器构建的 MS cluster 集群。集群中的每个物理服务器都是 Hyper-V 宿主服务器，并且通过 MS Cluster 构建成一个虚拟机资源池。云服务核心构件宿主服务器集群、基础管理、服务流程管理/IT 流程自动化、用户交互层中的所有软件产品/定制开发应用均会以虚拟机的形式运行在此组宿主服务器上。此组 Hyper-V 宿主服务器通过 MS Cluster 技术形成高可用环境，从而确保其上虚拟机在宿主服务器出现异常情况下的快速恢复。
- **SCVMM 群组：**是一组 SCVMM 2012 虚拟机，用于桌面云中虚拟资源的管理，并负责将物理设备转化成相关的虚拟资源。虚拟资源的动态优化和能源优化的具体操作也由 SCVMM 具体实现。随着管理虚拟资源数量的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCVMM 虚拟机。同时也实现相应的 SCVMM 高可用架构，确保能力的稳定输出。
- **SCCM 群组：**是一组 SCCM 2012 虚拟机，用于桌面云中资产状态跟踪、软件部署、系统升级等相关配置性工作。其中资产包括硬件设备信息、软件版本型号等。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会根据自身子系统的特征制定相关的系统配置、分发、补丁升级、资产状态跟踪的策略，然后部署到 SCCM 群组中，由 SCCM 群组中的服务器完成相关的工作。随着管理资产数量的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCCM 虚拟机。同时也实现相应的 SCCM 高可用架构，确保能力的稳定输出。
- **SCDPM 群组：**是一组 SCDPM 2012 虚拟机，用于桌面云中数据的备份/恢复工作。能够对虚拟机进行在线增量备份，可以对用户个性化数据进行增量备份，也能够对管理数据库进行增量备份。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会根据自身子系统的特征制定相关的系统备份和数据备份策略，然后部署到 SCDPM 群组中，由 SCDPM 群组中的服务器完成相关的工作。随着备份数据量的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCDPM 虚拟机。同时也实现相应的 SCDPM 高可用架构，确保能力的稳定输出。

-
- **CA 群组：**是一组 windows server CA 虚拟机，用于桌面云中相关证书认证的工作。随着证书数量的增加，系统会按照微软推荐的能力扩展架构搭建出多台 CA 虚拟机。同时也实现相应的 CA 高可用架构，确保能力的稳定输出。
 - **AD 群组：**是一组 Windows Server 构建的活动目录虚拟机，用于桌面云中身份认证和授权工作，同时也提供集中组策略管理功能。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境，用户互动层中的门户会根据自身子系统的特征制定相关的用户信息和身份认证策略，然后部署到 AD 群组中，由 AD 群组中的服务器完成相关的工作。同时通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会形成自己特有的用户操作行为、操作系统行为管控、应用程序行为管控、操作系统定制等管控策略，这些策略会以组策略的形式部署到 AD 群组中，然后由 AD 的组策略应用机制约束虚拟桌面环境上。随着用户数量和认证压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 AD 虚拟机。同时也实现相应的 AD 高可用架构，确保能力的稳定输出。
 - **SCEP 群组：**是一组 System Center Endpoint Protection 虚拟机，用于桌面云中系统病毒防护。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境，用户互动层中的门户，以及桌面云系统自身都需要进行病毒防护，从而确保整个桌面云环境的安全。System Center Endpoint Protection 负责此项工作。随着被防护环境的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCEP 虚拟机。同时也实现相应的 SCEP 高可用架构，确保能力的稳定输出。
 - **SCOM 群组：**是一组 System Center Operation Manager 虚拟机，用于桌面云中对系统进行运行状态和健康监控。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境，用户互动层中的门户，以及桌面云系统自身会根据自身子系统的特征制定健康、性能等监控策略，然后部署到 SCOM 群组中，由 SCOM 群组中的服务器完成相关的工作。随着监控信息和监控系统数量的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCOM 虚拟机。同时也实现相应的 SCOM 高可用架构，确保能力的稳定输出。

-
- **SCSM 群组：**是一组 System Center Service Manager 虚拟机，用于桌面云中服务流程管理、制作、执行，服务目录，事件处理，SLA 管理、CMDB 管理等桌面云核心构件。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会根据自身子系统的特征制定服务流程、服务目录、事件处理、服务管理等服务流程实例，然后部署到 SCSM 群组中，由 SCSM 群组中的服务器完成相关的工作。随着服务流程数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCSM 虚拟机。同时也实现相应的 SCSM 高可用架构，确保能力的稳定输出。
 - **SCO 群组：**是一组 System Center Orchestrator 虚拟机，用于桌面云中 IT 自动化流程的制作、执行、管理，是桌面云核心构件之一。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会根据自身子系统的特征制定 IT 自动化流程实例，然后部署到 SCO 群组中，由 SCO 群组中的服务器完成相关的工作。随着 IT 自动化流程实例数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SCO 虚拟机。同时也实现相应的 SCO 高可用架构，确保能力的稳定输出。
 - **SharePoint 群组：**是一组 SharePoint server 虚拟机，用于桌面云中用户交互层 2 大门户网站的实现。桌面云中基础计算资源服务层和通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会根据自身子系统的的需求会提供相应的门户入口页面和交互逻辑，这些都会部署到 SharePoint 群组中，由 SharePoint 群组中的服务器完成相关的工作。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 SharePoint 虚拟机。同时也实现相应的 SharePoint 高可用架构，确保能力的稳定输出。

3.2.6.3 虚拟化桌面技术组成



此部分的拓扑图展示的是桌面云中各种虚拟桌面技术的部署架构。

- **RDS Connection Broker 群组：**是一组 Windows Server 中 RD Connection Broker 虚拟机，用于保持用户远程连接客户端与桌面云中相应虚拟桌面环境连接持续性。桌面云中通用虚拟桌面服务中各虚拟桌面环境，专属应用桌面环境服务中的各专业桌面环境会将相应的虚拟桌面以 RDP 协议的形式提供给最终使用者，用户会通过远程连接程序在远程终端中通过 RDP 协议与虚拟化桌面提供的虚拟桌面建立连接。由于大多数虚拟桌面都依赖于网络，而网络会出现不稳定的情况，从而造成用户和虚拟桌面连接的中断。为了确保用户在网络恢复连接后，连接回同一个虚拟桌面继续之前

的工作。此服务器群组将会负责此部分功能。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 RDS Connection Broker 虚拟机。同时也实现相应的 RDS Connection Broker 高可用架构，确保能力的稳定输出。

- **App-V 群组：**是一组 App-V 虚拟机，用于桌面云中应用程序虚拟化包的制作、虚拟化应用的分发、用户使用权限控制等工作。本桌面云方案中虚拟桌面是由桌面操作系统环境虚拟化技术、应用虚拟化技术以及用户状态虚拟化技术等多种先进的虚拟化技术共同配合灵活搭建出用户能够使用的最终的虚拟桌面环境。这种多种技术组合方案能够使得虚拟桌面的构建和管理变得更加灵活。而 App-V 就是构建虚拟化桌面环境的组成技术中的一个。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 App-V 虚拟机。同时也实现相应的 App-V 高可用架构，确保能力的稳定输出。
- **NFS 群组：**是一组 Windows Server NFS 虚拟机，用于桌面云中用户状态和个性化信息保存工作。此服务器群组会和桌面操作系统环境虚拟化技术、应用虚拟化技术相互配合，搭建出用户能够使用的最终的虚拟桌面环境。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 NFS 虚拟机。同时也实现相应的 NFS 高可用架构，确保能力的稳定输出。
- **RDS Gateway 群组：**是一组由 Windows Server 中 RD Gateway 虚拟机，用于构建用户远程连接客户端与桌面云中相应虚拟桌面环境间连接通道的数据加密，同时也负责远程用户的认证和连接权限控制。此组服务器负责与用户使用的远程连接程序相互配合形成一个 SSL 的加密通道，用于传输 RDP 协议数据。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 Gateway 虚拟机。同时也实现相应的 Gateway 高可用架构，确保能力的稳定输出。
- **RDS Web Access 群组：**是一组由 Windows Server 中 RD Web Access 虚拟机，用于构建 Web 访问虚拟桌面的门户网站。用户可以使用自己的账号登录到此组服务器构建的门户网站，然后连接到自己的虚拟桌面上。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 Web Access 虚拟机。同时也实现相应的 Web Access 高可用架构，确保能力的稳定输出。
- **RDS Session Host 群组：**是一组由 Windows Server 中 RD Session Host 虚拟机，用于构建远程共享应用和远程共享桌面 2 个虚拟桌面类型中桌面操作系统环境的虚拟化

技术。此服务器群组会和应用虚拟化技术、用户状态虚拟化技术相互配合，搭建出用户能够使用的最终的远程共享应用和远程共享桌面环境。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 Session Host 虚拟机。同时也实现相应的 Session Host 高可用架构，确保能力的稳定输出。

- **RD VDI 宿主服务器组：**是一组安装了 Windows Server 中 RD Virtualization Host 的物理服务器群组，用于构建托管共享桌面和托管专属桌面 2 个虚拟桌面类型中桌面操作系统环境的虚拟化技术。此服务器群组会和应用虚拟化技术、用户状态虚拟化技术相互配合，搭建出用户能够使用的最终的托管共享桌面和托管专属桌面环境。此类物理服务器是从基础计算资源服务层中申请出来的独立服务器，然后由托管共享虚拟机环境或托管专属虚拟机环境中的相应模块将其自动安装 Windows Server RD Virtualization Host 环境。在此服务器组中运行的 VDI 虚拟机会直接使用服务器本地磁盘的存储空间。服务器之间彼此相互独立。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 Virtualization Host 物理服务器。
- **RD VDI 宿主服务器集群：**是一组安装了 Windows Server 中 RD Virtualization Host 的物理服务器集群，用于构建托管共享桌面和托管专属桌面 2 个虚拟桌面类型中桌面操作系统环境的虚拟化技术。此服务器群组会和应用虚拟化技术、用户状态虚拟化技术相互配合，搭建出用户能够使用的最终的托管共享桌面和托管专属桌面环境。此类物理服务器是从基础计算资源服务层中申请出来的服务器集群，然后由托管共享虚拟机环境或托管专属虚拟机环境中的相应模块将其自动安装 Windows Server RD Virtualization Host 环境。在此服务器组中运行的 VDI 虚拟机的虚拟磁盘文件会保存在集群共享的 SAN 存储上。服务器之间会搭建成 MS Cluster，从而形成高可用环境。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台 Virtualization Host 物理服务器。同时也实现相应的 Virtualization Host 高可用架构，确保能力的稳定输出。
- **独立式物理服务器/工作站组：**是一组安装了 Windows XP/Windows 7 等用户所需的操作系统的物理服务器/工作站，用于构建托管物理服环境中的桌面操作系统环境。此服务器/工作站群组会和应用虚拟化技术、用户状态虚拟化技术相互配合，搭建出用户能够使用的最终的托管物理服桌面环境。每个物理服务器/工作站在同一时

间只能供一个用户独占使用。随着用户数量和压力的增加，系统会按照微软推荐的能力扩展架构搭建出多台物理服务器/工作站。

3.2.6.4 通用虚拟桌面服务和基础计算资源服务层的关系

- **虚拟桌面管理 VM 组:** 此组虚拟机是各种虚拟桌面实现技术方案中通用的系统软件。这组服务器软件将会运行在从基础计算资源服务层中申请出来的虚拟机上。并由基础计算资源服务层负责虚拟机的稳定、高效运转。
- **客户端专属虚拟机环境:** 构建整个客户端专属虚拟机系统环境的所有服务器均运行在从基础计算资源服务层中申请出来的虚拟机上。并由基础计算资源服务层负责虚拟机的稳定、高效运转。
- **远程共享应用环境:** 构建整个远程共享应用的系统环境中所有服务器均运行在从基础计算资源服务层中申请出来的虚拟机上。并由基础计算资源服务层负责虚拟机的稳定、高效运转。远程共享应用系统根据用户压力的增加从基础计算资源服务层中动态增加虚拟机数量，然后转变成相应的系统服务器，从而提高远程共享应用服务的承载能力。
- **远程共享桌面环境:** 构建整个远程共享桌面的系统环境中所有服务器均运行在从基础计算资源服务层中申请出来的虚拟机上。并由基础计算资源服务层负责虚拟机的稳定、高效运转。远程共享桌面系统根据用户压力的增加从基础计算资源服务层中动态增加虚拟机数量，然后转变成相应的系统服务器，从而提高远程共享应用服务的承载能力。
- **托管专属虚拟机环境:** 构建托管专属虚拟机服务的系统环境可被分为 2 个部分，专属虚拟机的宿主服务器和其它系统组成部分。专属虚拟机的宿主服务器由专属虚拟机服务中的相关调度模块从基础计算资源服务层中申请相应的物理服务器，然后直接转化成宿主服务器融入专属虚拟机服务系统中对外提供能力输出。基础计算资源服务层负责此部分的物理服务器的稳定、高效运转。而专属虚拟机系统环境中的其它系统组成部分，则运行在从基础计算资源服务层中申请出来的虚拟机上，并由基础计算资源服务层负责虚拟机的稳定、高效运转。
- **托管共享虚拟机环境:** 构建托管共享虚拟机服务的系统环境可被分为 2 个部分，共享虚拟机的宿主服务器和其它系统组成部分。共享虚拟机的宿主服务器由共享虚拟机

服务中的相关调度模块从基础计算资源服务层中申请相应的物理服务器，然后直接转化成宿主服务器融入共享虚拟机服务系统中对外提供能力输出。基础计算资源服务层负责此部分的物理服务器的稳定、高效运转。而共享虚拟机系统环境中的其它系统组成部分，则运行在从基础计算资源服务层中申请出来的虚拟机上，并由基础计算资源服务层负责虚拟机的稳定、高效运转。

3.2.7 平台用户接入

3.2.7.1 身份认证

AD 域系统服务器：提供终端用户身份验证功能。

主要作用包括：

- AD 仅作为用户的身份认证服务器使用，其他的用户属性及组织机构信息放在数据库中。
- 在用户登录系统时，首先在 AD 中验证用户密码是否正确，之后根据用户名从数据库中获取该用户的中文名、附加码（动态手机密码）、所处部门、用户角色（即权限）等信息。

3.2.7.2 接入方式

用户接入虚拟桌面系统，有以下几种方式：

1) 普通方式

- 登录 PC 终端
- 在 Web 门户网站登录并获得虚拟终端
- 在虚拟终端中登录门户

2) 虚拟机快捷方式

在用户桌面实现发布虚拟机快捷方式

- 登录 PC 终端
- 在 PC 终端访问虚拟机快捷方式
- 在虚拟终端中登录门户

3) 应用嵌入

利用应用虚拟化技术，将门户中的应用以虚拟应用方式发布到门户上。用户在访问相关应用时，实际是通过虚拟应用的方式实现安全访问。

- 登录 PC 终端
- 在门户中以虚拟应用方式实现安全访问

3.2.8 虚拟桌面管理

确保办公环境符合企业和用户的复合需求，需要不断的对办公桌面环境进行管理和维护。微软使用 SCCM 和各种虚拟化技术实现办公环境的管理。

- 办公桌面环境标准化管理

使用 SCCM 可以按照企业的要求对企业级办公桌面环境进行标准化配置：如操作系统类型、操作系统相关优化配置、企业指定杀毒软件的安装和最新版本病毒库的更新、防火墙设定等。办公桌面环境的管理不仅仅是初始设定，还是个持续变化的过程。因为企业的要求会不断发生变化，使用 SCCM 可以很轻松的按照预先划分的用户类型进行局部或全面的标准化设定的升级操作。

- 办公桌面环境个性化管理：

系统通过使用微软提供的应用程序虚拟化技术—App-V 轻松实现个性化应用程序的管理。用户通过在自助门户网站上自行挑选需要的个性化应用程序。系统会在后台系统中进行相关的授权和配置工作，然后通过用户桌面环境中的 App-V 代理的配合，将用户挑选的应用程序快速的部署到客户端。使用 App-V 技术与传统软件的安装方式不同的地方在于软件的使用权限的授予和收回非常灵活，只需在 AD 中进行简单的配置即可轻松实现。

3.2.9 安全管理

3.2.9.1 用户数据的集中安全管理

为了确保用户数据的安全性，本方案提供多种安全机制。可以根据不同的需要通过使用其中一个单独的安全技术，或是多种技术进行组合来实现数据只被合法授权的用户读取。

- 文件/文件夹文件系统权限

微软在操作系统中提供一套非常成熟、完善的文件系统—NTFS。此文件系统能够很好的对其中保存的文件/文件夹进行访问权限的控制。当其他用户试图访问文件的时候，系统的权限验证机制判断访问者是否拥有对应的权限。如果没有权限，则无法获得相关文件的操作能力。

- 加密文件系统（EFS）用以对文件内容进行加密

加密文件系统 (EFS) 是 Windows 的一项功能，用于将信息以加密格式存储在硬盘上。加密是 Windows 所提供的保护信息安全的最强的保护措施。EFS 确保在未经授权的情况下，非法拷贝的文件无法正常获取其中有效信息。

EFS 以公钥加密为基础，并利用了 Windows Server 中的 CryptoAPI 体系结构。对用户所有的每个文件都是使用随机生成的文件加密密钥进行加密的，此密钥独立于用户的公钥/私钥对。

用户可以控制哪些人能够读取这些文件。在关闭文件时文件即被加密，但是当打开这些文件时，文件将会自动处于备用状态。

- 对整个磁盘进行加密的技术— BitLocker 驱动器加密

BitLocker 可以帮助保护安装了 Windows 的驱动器（操作系统驱动器）和固定数据驱动器（如内部硬盘驱动器）上存储的所有文件。使用 BitLocker To Go，可以帮助保护可移动数据驱动器（如外部硬盘驱动器或 USB 闪存驱动器）上存储的所有文件。

与用于加密单个文件的加密文件系统 (EFS) 不同，BitLocker 可加密整个驱动器。您可以正常登录和使用文件，但是 BitLocker 会帮助阻止黑客访问系统文件（黑客可根据这些系统文件找到您的密码），或访问您的驱动器（黑客通过从您的计算机删除该驱动器并将其安装到其他计算机上来实现此访问）。

在将新的文件添加到已使用 BitLocker 加密的驱动器时，BitLocker 会自动对这些文件进行加密。文件只有存储在加密驱动器中时才保持加密状态。复制到其他驱动器或计算机的文件将被解密。如果与其他用户共享文件（例如通过网络），则当这些文件存储在已加密驱动器上时仍将保持加密状态，但是授权用户通常可以访问这些文件。

如果对操作系统驱动器进行加密，BitLocker 将在启动过程中检查计算机是否存在任何可能具有安全风险的情况（例如，对 BIOS 或任何启动文件的更改）。如果检测到潜在的安全风险，BitLocker 将锁定操作系统驱动器，并且需要特殊的 BitLocker 恢复密钥才能对其解锁。请确保在第一次启用 BitLocker 时创建此恢复密钥；否则，您可能会永久失去对文件的访问权限。如果计算机具有受信任的平台模块 (TPM) 芯片，BitLocker 将使用它来密封用于对加密的操作系统驱动器解锁的密钥。启动计算机时，BitLocker 会要求 TPM 提供该驱动器的密钥并对其解锁。

如果对数据驱动器（固定或可移动）加密，则可以使用密码或智能卡解锁加密的驱动器，或者设置驱动器在登录计算机时自动解锁。

- 用户数据的备份

微软提供 SCDPM 可通过完整备份和增量备份相结合的方式保护磁盘上的数据。SCDPM 不仅能够对单独的文件/文件夹进行备份，同时也可以对正在运行的虚拟机实例进行在线备份。

SCDPM 利用受保护服务器上的 VSS 服务来创建与应用程序相适的备份映像，这样映像能够可靠地恢复。通过协调读取和写入与应用程序、文件系统服务、备份应用程序、快速恢复解决方案以及存储硬件之间的关系，VSS 可产生一致的影副本，并将它保留在受保护服务器上以跟踪更改并获取与应用程序相配的备份映像。

SCDPM 允许每 15 分钟进行一次增量备份，每小时进行一次完整备份。SCDPM 在同步的间隔期间，其代理仍会主动跟踪受保护服务器上的更改。

本方案通过使用 SCDPM 对用户的数据进行及时、集中备份，避免丢失。

3.2.9.2 访问客户端环境安全

本方案使用微软的网络访问保护(NAP) 技术有效的保证客户端桌面环境的健康状态，避免由于其环境被破坏，支持办公信息的泄漏。使用 NAP 技术可以根据需求进行相应的健康检查，实现远程访问的计算机操作系统环境只有在符合标准的情况下才能够访问办公应用和办公数据。

网络访问保护(NAP)可以防止不健康的计算机访问企业网络并危及网络的安全。利用 NAP 来配置、强制客户端的健康请求，并在连接到企业网络之前，更新或者纠正不符合的客户端计算机。NAP 也提供了一套 API，允许企业而不是微软将他们的软件整合到 NAP 平台。使用 NAP API，软件开发商和供应商可提供端到端解决方案，其可验证健康的客户端并及时纠正不符合的客户端。

3.2.9.3 访问数据通道安全

为了保证办公数据在网络上传输的安全性，本方案通过使用 SSL 或者是 IPSec 技术来加密远程访问设备和虚拟桌面间的数据通道安全。

企业的防火墙用来防护外来环境中可能带来的威胁，因此大多数企业会将网络端口尽可能的关闭掉。但多数企业都会保留 2 个网络端口：80 和 443。SSL 加密技术一般以 443 端口来进行数据沟通，通过非对称密钥算法生成动态对称密钥的方式对网络上的数据进行实施加密工作。

IPSec 同样会使用 SSL 技术对网络中的数据进行加密。但 IPSec 主要用于对企业内部网络环境进行有效划分，并对必要的网络范围内的传输的数据进行加密操作。

3.2.10 系统运维

3.2.10.1 基础资源管理

3.2.10.1.1 主机管理

3.2.10.1.1.1 裸机部署

使用 System Center Virtual Machine Manager 2012，可以实现从裸机设备引导启动开始、到操作系统的安装、到驱动程序的安装、到角色与功能的添加、到加域的管理、直到加入云系统的资源池等一系列的操作。

System Center Virtual Machine Manager 2012 通过主板管理控制器将新的品牌机部署为启用了虚拟化功能的虚拟化主机，自动将部署的服务器进行配置并将其加入到云系统之中，整个过程中确保主机使用了有效的 OS 配置完成部署过程，完全自动化的过程不需要管理员的干预。

System Center Virtual Machine Manager 2012 与裸机服务器上的 BMC 通信，并与 Windows Deployment Services (WDS) 集成，通过从 VHD 功能引导来部署 Windows Server 2008 R2。使用的 BMC 须支持以下协议之一：数据中心管理接口 (DCMI) 1.0；服务器硬件系统管理体系结构 (SMASH) 1.0；智能平台管理接口 (IPMI) 1.5 或 2.0；HP Integrated Lights-Out (iLO) 2.0。

VMM 2012 将与现有的 WDS 服务器集成。它仅响应对指定的主机的请求，使 WDS 能够继续为其他操作系统安装服务，也可为 VMM 配置单独的 WDS 服务器。

在将新主机配置为 Hyper-V 主机之后，然后可以在 VMM 中使用简单的向导进行创建群集操作。

3.2.10.1.1.2 异构虚拟主机资源管理

System Center Virtual Machine Manager 2012 在主机管理层面可管理多种虚拟机，实现 Hyper-V、VMware、Xen 异构虚拟化环境的统一管理。

在虚拟化平台方面，System Center Virtual Machine Manager 2012 支持 Windows Server 2008/2008 R2 环境中的 Hyper-V 角色(完全安装或服务器核心)，还支持 Hyper-V Server 2008 R2。它还通过 vCenter 支持 VMware vSphere 虚拟机监控程序(仅 4.1 版本)，并支持使用 ESXi/ESX 4.1 和 3.5 的主机(不再支持 ESX 3.0)。它现在支持带有功能包 1 的 Citrix XenServer 5.6 版。还有 Integration Suite 补充包来促进与 VMM 的集成。

在 VMM 与 VMware 环境的集成方面，新版本和旧版本的 VMM 存在一些差异，主要在客户反馈上。VMM 不再从 vCenter 导入、合并或同步主机和组的树结构。必须将需要的 ESX 服务器手动添加到 VMM 主机组中。如果把 VMware 模板导入到库中，它会将 .vmdk 文件留在 ESX 数据存储中，而是只复制元数据库和 ESX 主机之间的数据传输现在通过 HTTPS 进行，因此不需要启用对 ESX 主机的 Secure Shell (SSH) 访问。

Xen 和 VMM 集成是由 Citrix 和 Microsoft 联合开发的。可以在 VMM 2012 中管理 XenServer 池和主机，而不需要依赖 XenCenter 服务器。VMM 支持虚拟机监控程序虚拟化，还支持 XenServer 中的半虚拟化。它还支持 Citrix XenMotion。

3.2.10.1.2 存储管理

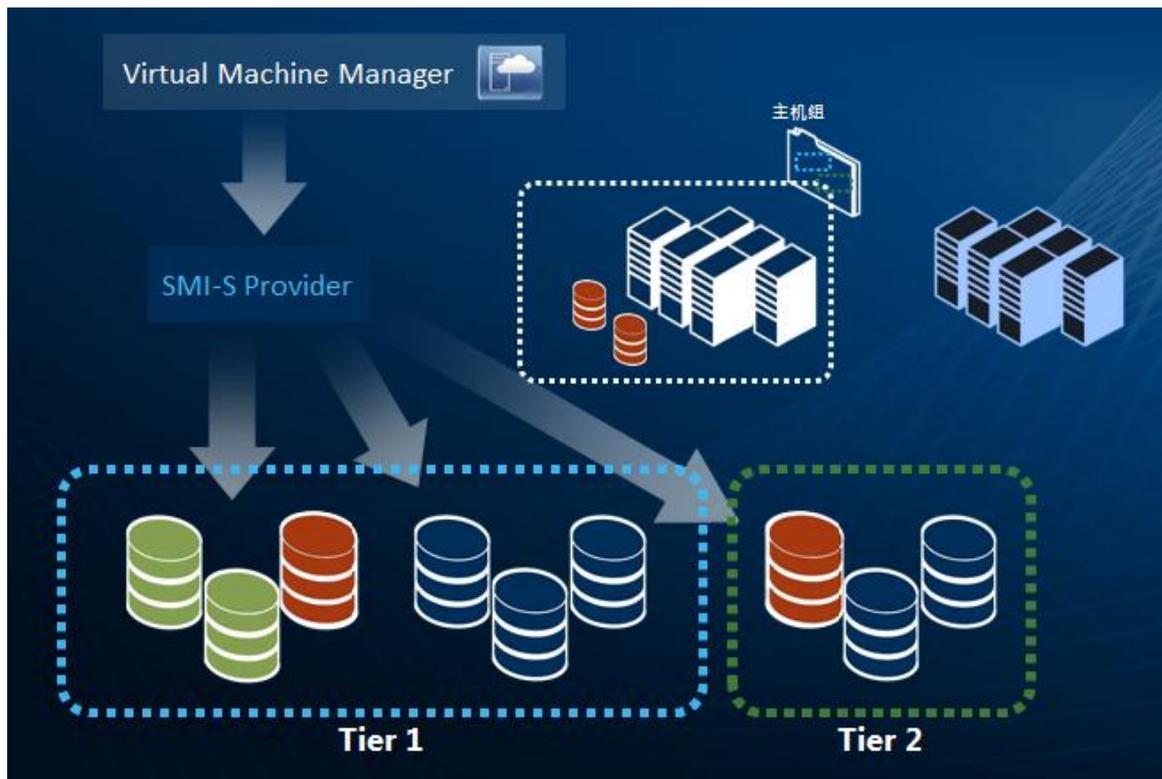
System Center Virtual Machine Manager 2012 在存储管理方面，使用 SMI-S 标准对存储资源进行管理，发现存储阵列的物理设备和存储池，根据吞吐率和容量对存储进行分类，并实现发现、配置 LUN，将其配置给主机与集群的操作，还可通过对 LUN 的快照克隆，实现虚拟机快速供应。可完全实现端到端的存储设备映射操作、存储资源的分配和指派、应用 SAN 资源给新的虚拟分配存储资源，并完成基于 SAN 的虚拟机迁移。

Virtual Machine Manager 2012 可通过存储管理计划规范 (SMI-S) 1.4 版协议发现环境中的 SAN 阵列并与其通信。因此您能够对可用存储进行分类，以便进行追溯。与存储供应商的软件配合使用时，VMM 能够创建逻辑单元 (GPT 和 MBR)，让您将存储空间作为群集共享卷 (CSV) 分配给主机或群集。

当前，VMM 支持的存储供应商产品包括 HP StorageWorks Enterprise Virtual Array (EVA)、NetApp FAS 以及 EMC Symmetrix 和 CLARiiON CX，将来还会不断增加。VMM 还支持 SAN 中的快照和克隆功能。这使管理员能够通过“支持 SAN 复制”的模板来复制 LUN，几乎瞬时地配置新虚拟机。这种集成仅适用于 Hyper-V 平台，对于 VMware 或 Citrix 则需要额外的配置步骤。

存储分配的过程如下图所示

- 通过 SMI-S provider 发现存储
- 创建存储池分级池并与存储进行关联
- 将存储分配到特定主机组
- 将现有的 LUN 指派到主机或者群集
- 从池中创建新的 LUN 并且将其关联到主机和群集



3.2.10.1.3 网络管理

在网络管理方面，微软云系统方案提出了逻辑网络的概念，同时它还支持网络负载均衡技术，包括软件网络负载均衡方案和基于硬件的网络负载均衡方案。我们将从逻辑网络管理和网络负载均衡管理方面展开了解方案的详细实现方法。

3.2.10.1.3.1 逻辑网络

System Center Virtual Machine Manager 2012 网络管理方面，可针对数据中心的每个位置，使用 VLAN 和子网定义逻辑网络，针对静态 IP、负载均衡虚拟 IP 以及 Mac 地址实现地址管理。逻辑网络为虚拟机分类可以访问的网络，将网络映射到拓扑，同时分配到主机和云。地址池从预配置的池中分配静态 IP 地址给虚拟机，创建 IP 地址池作为管理 IP 地址分配作用域，创建 MAC 地址池 作为管理 MAC 地址分配作用域。

System Center Virtual Machine Manager 2012 对一个或多个逻辑网络定义进行分组。每个定义包含 IP 子网 (IPv4 或 IPv6) 和 VLAN ID。它们还可在不同地理区域中表示，自助服务用户只需知道逻辑网络名称。当您配置虚拟机时，它与一个或多个逻辑网络关联。

Virtual Machine Manager 2012 将自动分配适当子网中的固定 IP 地址，以及 MAC 地址。如果您不希望使用 VMM 达到此目的，可使用动态主机配置协议 (DHCP)。地址池分成了 IP 地址池和 MAC 地址池。IP 地址池指派到虚拟机、主机以及虚拟 IP，在虚拟机模板创建时使用，在虚拟机创建的过程中签出并指派静态 IP 地址给虚拟机，在虚拟机删除后返还。MAC 地址池分配给虚拟机，在虚拟机模板创建时指定，在虚拟机创建时签出在虚拟机启动之前指派，在虚拟机删除后返还。

主机上的每个网络接口与 Trunk 模式或访问模式下的逻辑网络相关联。在 Trunk 模式下，NIC 仅使用单个 VLAN ID。在访问模式下，不同虚拟机使用不同 ID 进行网络连接。

3.2.10.1.3.2 网络负载均衡

System Center Virtual Machine Manager 2012 网络管理方面，可通过程序自动提供负载均衡。在服务部署中应用负载均衡能力的设置，通过使用设备厂商基于 PowerShell 的提供接口控制负载均衡，并通过创建虚拟 IP 模板统一负载均衡配置。

Virtual Machine Manager 2012 通过硬件提供接口连接到负载均衡器，然后指派给云、主机组和逻辑网络，配置负载均衡的方法并在服务部署时添加虚拟 IP。虚拟 IP 模板用来为服务部署时配置负载均衡指定预设的属性，指定负载均衡的方法—轮换，最少连接，快速响应。

System Center Virtual Machine Manager 2012 还能够让您创建虚拟 IP (VIP) 模板。这些模板指定负载均衡器的特征，可能是通用特征或针对特定模式的特征。设置包括控制 HTTP/HTTPS 流量、在负载均衡器上终止，还有可选的后端重新加密、持久性和负载均衡算法。

目前，对于硬件负载均衡设备，Virtual Machine Manager 2012 支持 F5 公司的 BIG-IP 和 Citrix Systems 公司的 NetScaler，以及 Brocade 公司的 ADX 负载均衡设备，但今后将能够识别更多负载均衡器。

3.2.10.1.4 主机群集

System Center Virtual Machine Manager 2012 能够为主机创建群集，而不再需要单独在 Hyper-V 上创建群集。推荐通过群集形成底层架构。群集的创建基于向导的操作体验，

支持群集验证，从管理的存储中分配群集磁盘，创建群集范围的虚拟网络。还可以通过 Virtual Machine Manager 2012 管理群集，如添加和删除节点，群集磁盘和虚拟网络，通过拖拽主机的方式实现群集节点的添加，监视群集的健康和状态。当然还可以通过 Virtual Machine Manager 2012 删除群集，此时群集的主机将成为单独的受管理主机，群集的磁盘将返回给受管理的存储。

通过主机集群，能够实现云平台的高可用性，以此来保证业务连续性。

3.2.10.2 基础资源优化

配置部署的云系统基础架构，投入生产运营之后必须提供一套完备的监视和操作机制才能够有效的实现稳定长周期的服务交付能力，同时云平台过程中的优化也将为数据中心的运营提供敏捷性和投入的节省。

3.2.10.2.1 基础架构优化

在 System Center 2012 中基础架构的优化能力不要体现在主机动态优化和主机电源优化两个方面：

3.2.10.2.1.1 主机动态优化

主机动态优化是 System Center Virtual Machine Manager 2012 的全新功能，以往的动态优化功能往往是在虚拟机宕机事件已经发生后，才能够进行自动迁移。全新改善的动态优化功能基于在线迁移避免虚拟机宕机，不需要与 System Center Operations Manager 相集成就可以独立完成，并支持 Hyper-V、VMware 和 Citrix XenServer 异构虚拟化环境的集群与迁移。

System Center Virtual Machine Manager 2012 可在系统中自动监控系统资源的使用状况，当资源使用率高于此前设置的阈值的时候，就开始执行优化操作。扫描系统资源的使用状况，并在系统判断是否进行优化的频次可以手动设置也可以自动设置，系统默认是 10 分钟为间隔进行一次扫描。

动态优化的基础由实时迁移、收管理的资源和管理选项组成。

- 实时迁移
 - 保证群集的平衡
 - 避免虚拟机的停机

-
- 支持异构的群集
 -
 - 受管理的资源
 - 考虑 CPU、内存、磁盘 IO、网络 IO
 - 当资源使用高于阈值时进行优化
 - 考虑整个群集的状态
 - 选项
 - 手动或自动优化
 - 用户可控制的频率
 - 可配置的主动范围

3.2.10.2.2 基础架构监视

基础架构的监视是确保云平台可靠和稳定运行的必备设施，也是优化操作的主要依据，在 System Center 2012 中提供了更全面的跨平台基础架构监视能力，这包括了从设备、操作系统一直到应用的纵向与全方位整体监视能力。

3.2.10.2.2.1 虚拟化监视

Microsoft System Center 2012 的组件 Operations Manager 提供了一种更简单的方式，可以查看云环境的全面、详细视图。作为基础架构管理员，需要直观、全面的方法来监控云平台的资源。最终的挑战是找到一种方法确定并主动修正计算、存储以及网络基础架构和资源方面的问题。理想的监控系统将提供一种方法，分析随时间发展的使用情况并找出趋势。

通过 Microsoft System Center 2012 的 Operations Manager 和 Virtual Machine Manager 之间的集成，可以在 Operations Manager 中看到 Virtual Machine Manager 中所有被管理的主机、虚拟机，包括他们的资源使用情况等信息。

3.2.10.2.2.2 跨平台监视

System Center Operations Manager 2012 体现了面向云的基础结构拓扑 Fabric 概念。这一特性扩展了它的可见性，包括底层网络和存储层，以及上层的应用层。

System Center Operations Manager 2012 显著增加了网络层的可见性，并且支持多平台、多协议网络设备监控。SCOM 2012 让您能够指定用于身份验证的 SNMP 字符串，然后利用简单网络管理协议和 Internet 控制消息协议在环境中发现网络设备。可以深入了解每个单独网络设备的详细运行状况信息，以及设备在一段时间内的运行情况。SCOM 2012 还推出了“近距离视图”。该视图显示具有两个网络跳跃的所有设备，提供一个网络地图，包括所有服务器、它们如何连接到网络以及它们如何相互连接。您可以查看这些网络连接的性能数据，以及它们对各项服务或应用程序性能的影响。

除了对网络设备的监控，System Center Operations Manager 2012 还支持通过可扩展的管理包实现对服务器硬件、存储设备、不间断供电电源设备的监控。如果有对应的管理包，甚至可以是实现对所有支持 SNMP 协议的设备监控。

3.2.10.2.3 容量监视

通过使用基于监视数据统计的报表，可以随时了解云平台的负载和容量使用情况，也能够对容量的使用预期及趋势做出比较准确的判断。

3.2.10.2.3.1 资源使用报表

利用 Microsoft 私有云和 System Center 2012 提供的报表功能，可以创建并共享报告和仪表盘，可以根据不同的租户和需求轻松地自定义报告和仪表盘。

云平台使用报表

Machine Group Forecasting Report

Description

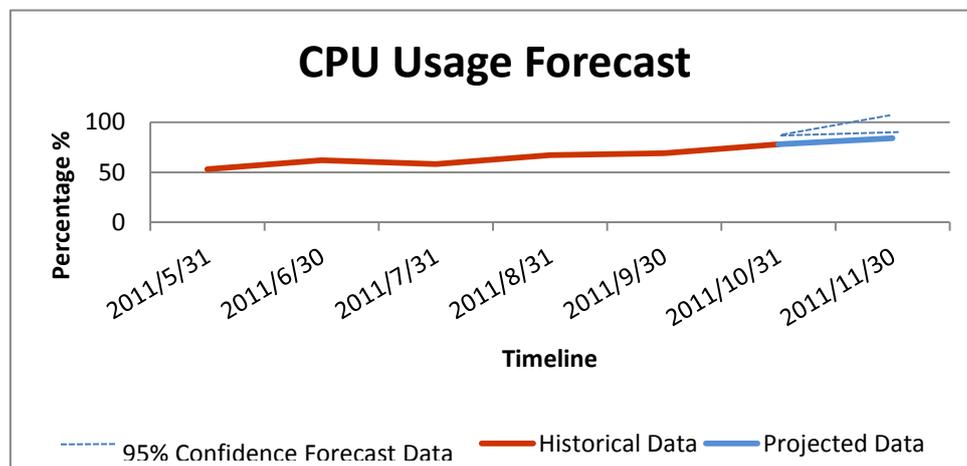
- Report Generated Time Label : 3/2/2011 10:57 AM
- Data Aggregation : Monthly
- Report Duration : 2/1/2011 10:56:00 AM - 3/2/2011 10:56:00 AM
- Object(s) Selected In Report : 2 objects selected in this report

Note: If historical data is not sufficient(at least 10 points), the forecasted confidence might be lower.

Performance Counters

- Disk Space Usage
- Memory Usage
- Disk Read/Write Forecast
- Network Input/Output Forecast
- CPU Usage Forecast

而且，还可以进行分析和假设预计。监视系统的使用以及随时间变化的数据，还可以分析历史数据，建立假设场景以得到将来的预计。



3.2.10.2.4 管理主机更新

System Center Virtual Machine Manager 2012 提供了主机的标准化更新，能够保持系统基础架构组件的最新状态。

通过设置基线，将软件更新按照合规评估的要求，再通过创建基线来实现逻辑分组，指派基线到主机组以评估合规性。然后通过扫描，根据指派的基线检测服务器的合规性，使用 Windows Update 代理应用和实现合规，根据需要或通过 PowerShell 自动执行扫描。第三步是修复，通过安装丢失的更新确保服务器符合要求，在 Virtual Machine Manager 控制台中跟踪状态，可以按需执行修复或者通过 PowerShell 自动执行。



3.2.10.2.4.1 主机电源优化

System Center Virtual Machine Manager 2012 在主机组启用动态优化功能后，可以激活电源优化。只要 Virtual Machine Manager 2012 能够直接与主机通信，它就能够在低负载时段撤离虚拟机并关闭组中的主机。在今后需要时，Virtual Machine Manager 2012 可重新打开主机。默认情况下，此功能全天候启用，也可以将其限定在特定的时间和日期。

电源优化的基础包括受管理的资源、用户定义的计划以及电源操作。

- 受管理的资源
 - 考虑 CPU、内存、磁盘 IO、网络 IO
 - 当资源使用低于阈值时，进行优化
 - 考虑整个群集的状态

- 用户定义的计划
 - 只有在每天特定的时间执行
 - 当动态优化设置为“自动”时启用

- 电源操作
 - 用实时迁移将虚拟机在主机关机前移开
 - 确保优化不会让剩余的系统过载
 - 确保关闭电源不会导致群集仲裁的失效
 - 利用带外管理执行电源操作

3.2.10.3 权限管理

3.2.10.3.1 用户资源权限控制

本方案推荐的系统中用户的相关操作的授权和权限认证均依赖于微软的活动目录（AD）。用户能够使用哪种虚拟化技术构建自己的虚拟化办公环境，个人办公数据的读写操作，自服务能力范围，必须先要明确用户和维护人员的身份。而身份的认证工作由微软的 AD 负责。各系统组成在彼此之间进行相互配合，或要依据用户的身份决定其功能使用范围时，需要和 AD 进行互动进行必要的身份判断工作。

3.2.10.3.2 维护管理权限的委派

本方案推荐的系统中维护人员的相关操作的授权和权限认证均依赖于微软的活动目录（AD）。维护人员的管理能力和管理范围的确定必须先要明确维护人员的身份。而

身份的认证工作由微软的 AD 负责。各系统组成在彼此之间进行相互配合，或要依据用户的身份决定其功能使用范围时，需要和 AD 进行互动进行必要的身份判断工作。

同时系统的各种服务和功能都支持权限的委派能力，从而将维护工作进行有效的分散，减轻每个维护人员的工作强度，同样也规避的权利过于集中所带来的安全隐患。

3.2.10.4 审计

3.2.10.4.1 用户操作审计

对于合法用户的利用合法操作授权进行不合理的行为（合规，审核的对象），传统的授权方法不能很好地解决。而利用虚拟桌面中自带的虚拟应用技术，基于相关功能模块，可以根据业务策略和安全规定，选择对特定用户使用特定应用时的所有行为进行全程录像，利用远程反问协议的基本原理和优势，一般性的业务操作录像，每天录像文件大小不会超过 30M 的数据量。通过这种技术可以对开发人员的全程行为监控：

- **事前通告**

被监控的用户在使用应用的时候，就会被告知，所有行为将会被录像。通过事先告知此种监控手段的存在，可以大大降低开发人员采取非法行为的动机和意愿，达到防患于未然的效果。

- **实时监控**

管理员可以从后台对开发人员正在进行的开发操作和工作进行实时的监控，一旦发生任何问题，管理人员可以第一时间发现问题并采取措施，防止产生任何不良的后果。

- **事后追溯**

如果一旦发生任何问题，造成不良后果，管理人员可以根据使用人员、应用和时间进行检索，调取录像，反向查找是什么人进行了什么非法操作，从而进行补救，并可以将其作为相关证据，辅助采取相关措施，保证企业利益。

3.2.10.4.2 系统维护操作审计

为了确保自身系统的安全、稳定运行，并且为了避免未来由于误操作或其它未知原因可能造成的系统运行不正常，加快问题定位和缩短系统恢复周期，系统的维护记录是

必要的。系统的每个功能模块都会产生操作日志，然后系统将使用微软的 System Center Operation Manager 软件进行审计日志的汇总、生产分析报告。

3.2.10.5 服务管理

3.2.10.5.1 工作流程自动化

云平台通过使用 System Center Orchestrator 2012 实现各种自动化流程。System Center Orchestrator 2012 采用一种精密的数据总线功能来实现 IT 流程（运行手册）中各个操作之间的双向信息交换，进而触发 IT 流程（运行手册）自动执行。通过对大批量的重复任务实现自动化，System Center Orchestrator 2012 能够为云平台中的大量自动化运维操作。

System Center Orchestrator 2012 通过提供多种自动化功能来实现云平台中各种流程的标准化，从而减少手动操作所导致的潜在问题和错误，和显著提高系统的工作效率。利用 System Center Orchestrator 2012 中内置的 Microsoft Silverlight 控制台，操作人员就可以启动和停止运行手册、监控运行手册的执行进度以及解决非正确执行的问题。

System Center Orchestrator 2012 同时提供易于使用的可视化制作与测试工具，利用内建的大量对象来构建出各种丰富而复杂运行手册。利用基于规则的智能分流技术，可以为这些内置的工作流赋予条件判断能力，以使其轻松适应云平台运维中将会出现的新的流程需求或已存流程的修改完善。而且，这些工作流既可被直接使用，也可在稍加修改后被使用，无需编写大量的脚本代码。

System Center Orchestrator 2012 实现了综合 IT 调度中心，将云平台中各个软硬件、系统组件连接在一起，完成更加复杂的运维或业务操作。

通过 System Center Orchestrator 2012 中的集成包内置一系列预构建的、可重复使用的操作，能够高效将各种现有的管理工具集以及诸如监控、预配置和服务管理等 System Center 功能集成到云平台中。这些集成包还包含针对一些知名厂商提供内置的互操作能力，这些厂商包括 HP、IBM、EMC、BMC、CA 和 VMware，它们均可无缝接入 System Center Orchestrator 2012。System Center 和第三方解决方案之间的互操作性

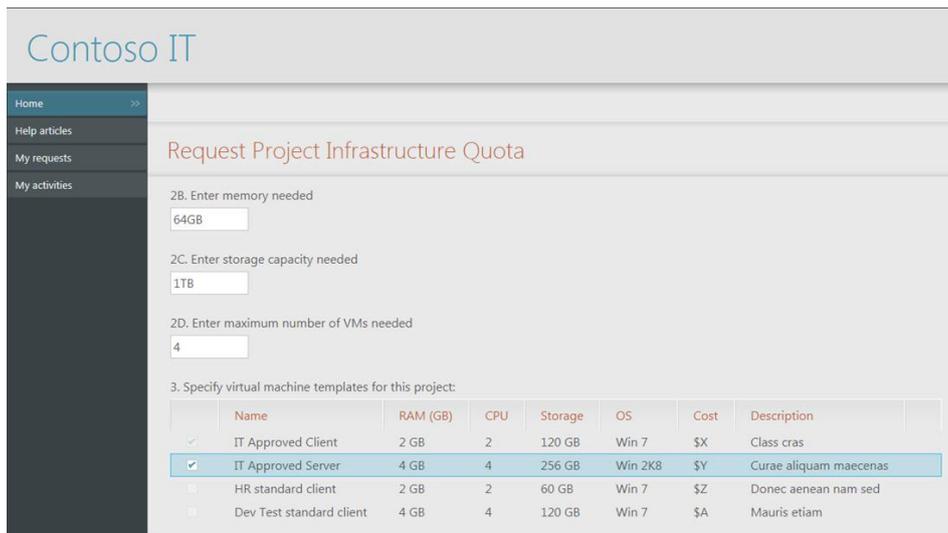
和集成性将通过基于标准化的 ODATA REST 的 Web 服务接口和对 PowerShell 的扩展支持来得以实现。有了 System Center Orchestrator 2012 如此强大的异构平台连接能力和扩展能力，能够更加快速、高效的完成云平台中的各种复杂流程，以及连接各种未来将要引入到平台中的软硬件。

3.2.10.5.2 业务流程管理

Service Manager 2012 提供强大的模板和工作流设计工具，可以帮助运维人员轻松制作和发布各种云平台的业务流程。

Service Manager 2012 内置一系列自动化工作流，这些工作流围绕事件管理、问题管理、SLA 管理以及实现对服务的请求。它们将帮助运维人员在云平台中实现可预期的有关运营上 SLA。

3.2.10.5.3 服务目录管理



云平台采用 Service Manager 2012 实现用户交互层中两大门户中的关键组成-服务目录。Service Manager 2012 中的服务目录实现，维护人员用目录的形式展示出云平台能够给用户提供的服务项目，而用户则能够通过服务目录自行找到自己想要使用的服务项目并从入口点进入服务项目享受服务。Service Manager 2012 可以配置各种基于角色的访问策略，以便有权限的用户可以看到并发起请求，然后 Service Manager 2012 就会自动触发后续的业务流程，随着业务流程步骤的依次执行，从而满足用户的要求。请求的目的多种多样，可以是相对简单的访问权，也可以是相对复杂的综合云服务项目。

Service Manager 2012 同时提供灵活、便捷的服务目录设计工具，从而帮助运维人员快速生成新的服务目录结构或对现存的目录进行调整。

服务目录将会以 WEB 页面的形式呈现给用户，因此云平台的两大门户网站中将会内嵌服务目录的 WEB 界面，使其和门户融为一体。

3.2.10.5.4 管理配置数据库

Service Manager 2012 的配置管理数据库 (CMDB) 可以对整个云平台中各种关系的捕获手段实现标准化，CMDB 就可以跟踪各种配置项，例如虚拟机模板、应用程序服务模板、虚拟机、物理主机以及应用程序服务。

Service Manager 2012 将简化 CMDB 的配置过程，让它可以从诸如活动目录和 System Center 2012 Configuration Manager 这样的数据源自动导入数据。同时提供编辑工具能够对配置项进行编辑。

3.2.11 方案特性

3.2.11.1 企业 Windows 桌面的最佳方案

目前企业中使用最为普遍的是微软 Windows 系列客户端操作系统，如 XP, Vista, Win7 等。微软在长久的开发、销售过程中收集了大量客户对于企业桌面操作系统的需求，并且通过 Windows 操作系统的版本的升级过程将客户的需求转变成产品的功能，从而不断满足企业当前对于桌面环境的需求变化。在微软 Windows 的发展过程中，不断出现用于企业桌面管理的优秀技术，如组策略、活动目录、双向防火墙、桌面自动化部署、桌面安全技术等。本方案中用于构建桌面云系统的所有软件产品都是微软经过长期积累形成的管理软件和虚拟化技术，它们彼此具有极佳的协同、联动能力，是最好的企业桌面云的解决方案。

3.2.11.2 最全面的桌面虚拟

微软提供的最为全面的桌面虚拟化实现技术，如托管桌面虚拟化 (VDI)、客户端桌面虚拟化 (MED-V)、展现层虚拟化 (RDS)、应用虚拟化 (App-V) 等。不同的虚拟化技术满足企业不同种桌面虚拟化场景需求。不同的桌面虚拟化技术在使用需求、建设成本、维护成本等各种企业关心的桌面云设计因素间上有各自特有的表现，企业可以根据自身的建设需求，选择最佳的技术组合构建自己的最佳桌面云系统。

3.2.11.3 强大的扩展能力

微软是个平台级厂商所有的微软产品都提供良好的开发框架、开发接口、以及平台的扩展框架。桌面云系统的建设者可以很方便的调用相应的编程接口与相关的软件产品进行控制、数据交互。同时也可以按照扩展框架的规范开发出专有系统模块，融入到微软产品之中，增强软件的额外能力。

3.2.11.4 异构系统的广泛支持

微软的产品提供良好的异构系统的支持能力。首先 SCOM 能够对各种服务器、网络设备以及 Windows、Linux 操作系统进行监控。并且通过相应的管理包监控更多地异构设备/软件环境。同时 SCVMM 能够对现有的市面上最主流的 3 大虚拟化厂商（微软、Wmware、Citrix）的虚拟化产品进行统一管理，并操控其上运行的虚拟机。SCO 能够轻松实现与任意系统、软硬件的自动化调度，只要这些系统和软硬件支持编程/脚本。

3.2.11.5 全面的监控能力

微软的 SCOM 是个开放的监控平台，主要用于对硬件设备、操作系统、应用程序进行全方位监控。SCOM 随着产品自带很多软硬件的监控能力。如服务器、网络、Windows、Linux 操作系统进行监控，同时可以根据其扩展框架开发出各种管理包（MP），从而将额外的监控能力融入到 SCOM 的监控框架中。SCOM 为企业提供了一个基于应用服务的监控能力。换句话说，就是把所有可能会影响到应用服务正常工作的因素全部监控起来，并且以树状结构展示其监控因素的相互影响/依赖关系。

3.2.11.6 融合微软云计算系统构建经验的强大产品

微软是全球知名的公有云提供商，并且拥有 10 年以上的云服务建设、运维管理经验。尤其是在最近几年，微软的公有云建设更加快速、投入力度更大。因此微软拥有大量的、先进的云计算建设、运维经验。微软将自己总结的云计算的建设经验以产品功能的形式融入到微软企业级软件产品之中。微软的 Windows Server 和 System Center 是企业建设私有云环境的核心产品体系。

3.2.11.7 通用型自动化流程引擎

微软的 SCO 是一个通用型自动化流程产品。所谓通用型是指 SCO 提供了一个解释型流程引擎，能够和任何提供编程/脚本互动能力的软硬件进行数据和控制交互。

3.2.11.8 灵活、强大的自动化流程制作平台

微软的 SCO 提供一个自动化流程设计工具，能够通过鼠标拖拽的方式很轻松的将各种自动化对象连接成自动化流程策略（Runbook），然后由 SCO 的引擎按照 Runbook 的描述逻辑自动运行。同时编辑工具提供调试环境，能够方便编写者跟踪自己编写的 Runbook 是否正确。

3.2.11.9 通用型业务流程制作引擎

微软的 SCSM 提供一套通用型业务流程引擎。此流程引擎具有良好的服务目录、业务流程、CMDB 联动框架。流程编辑者只需使用编辑工组创建自己的业务流程，流程将会非常顺畅的部署到引擎上，服务目录、流程等相关操作规则自动部署、一气呵成。业务流程本身没有任何行业、工种的限制。用户可以根据自身的需求制作企业业务、IT 业务、行业业务等流程。

3.2.11.10 ITIL 的最佳产品实现

ITIL 是国际公认的指导企业 IT 建设的指导方针。如何将这一指导方针落地是 ITIL 应用的关键之一。微软通过将 ITIL 中的概念转化成 System Center 产品功能的方式实现 ITIL 的落地。企业通过部署微软的 System Center 能够轻松实现 ITIL 在企业中的应用。