FS0001

金融行业桌面安全解决方案
技术建议书

文档版本 V1.0
发布日期 2013.11.1
作者 樊玉珂、孟冲

华为技术有限公司

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129
网址： http://www.huawei.com
客户服务邮箱： support@huawei.com
客户服务电话： 0755-28560000 4008302118
客户服务传真： 0755-28560111

目 录

图表目录

1 文档说明

1.1 文档目的

本文从技术角度，对金融行业桌面安全ICT建设进行规划设计和建议，目的如下：

1） 对金融行业桌面安全所需的主要ICT系统进行整体分析设计，明确客户总体需求，阐明设计思路，给出总体设计方案，界定金融行业桌面安全建设所需的各个子系统；

2） 对金融行业桌面安全建设所需的各个子系统进行细化设计，明确子系统功能、组网方案、关键指标、部署建议和设备选型。

1.2 文档范围及结构

本文分14章，各个章节的内容简要介绍如下：

第1章：文档介绍，包括文档的目的、文档范围和结构。

第2章：项目概述，包括项目背景、项目的客户痛点。

第3章：客户项目需求分析，包括客户的业务需求和规划，以及业务对ICT的需求。

第4-11章：金融行业桌面安全总体方案设计，包含逻辑架构、物理架构、接口描述和总体方案亮点。金融行业桌面安全各子系统方案设计，包含华为桌面云、华为安全沙箱、华为PolicyCenter、华为文档安全管理、华为OIC文件信息管控中心子方案介绍。各子系统涉及的主要产品及特点。

第12章：华为合作伙伴统一运维审计子解决方案介绍。

第13章：华为金融行业桌面安全方案的典型成功案例。

第14章：缩略语。

2 项目概述

2.1 项目背景

随着金融机构业务发展和应用扩大，组织和网络规模的扩充、分行网络接入点的不断增加，使得网络中的安全风险成倍的增加，更好的服务客户的同时其安全风险也变得更加严重和复杂。单台终端安全事故引起的损害可能传播到其他终端和系统，引起大范围的瘫痪；缺乏安全控制机制和对网络安全政策及防护意识的认识不足，各类安全风险正日益加剧。

- 内网信息泄密已成为首恶之源，严重威胁金融机构的信息安全。

根据加利福尼亚州旧金山的计算机安全协会(CSI)的观点，大约60%到80%的滥用事件起源于企业内部。在金融机构内部网络中，任何一台终端的安全状态都将直接影响到整个网络的安全。员工安全意识薄弱，安全策略难以实施，网络病毒泛滥；网络资源的不合理使用，行为规范难以管控，工作效率下降；各种外设滥用，高密区数据访问缺乏管控，信息泄漏频繁等问题极大的困扰着金融机构高层管理人员和IT部门。在金融机构当前复杂的网络环境下，如何有效保证接入网络的终端的安全可信，成为了信息安

全建设的重中之重。身份认证、安全检查、补丁管理、重要网络资源的安全防护、终端行为管理、资产管理等一系列归一化的完整终端安全解决，成为金融机构IT安全管理人员追求的重要目标。

- 内网安全管控同时需要兼顾办公效率，在安全和效率之间取得有效平衡。

同时随着金融业务不断发展，金融监管逐步放开，金融机构竞争越来越激烈，促使金融机构不断提升自身运营效率。而金融业务本身信息化程度高，保密等级高，在提升效率同时，如何平衡安全风险防范，面临很大挑战。桌面安全解决方案为金融机构在效率和安全之间找到很好平衡点，对业务进行防泄密，敏感操作进行审计安全防护，同时通过集中管理和高体验来提高效率，也提升金融行业信息系统等级保护政策要求合规性，以及健全金融机构内部信息安全管控体系建设。

2.2 主要客户痛点

1. 数据泄露，防不胜防
   a) USB介质携带方便，大部分员工有正常文件交换需求，但也有少部分离职员工，外部人员通过USB介质拷贝泄密。
   b) 海量合作伙伴，供应商，外包人员及终端随意接入内网，导致内部网络的安全性岌岌可危，泄露客户账户等关键信息。钓鱼木马等窃取账户信息。
   c) 非法外联行为严重，经常通过调制解调器、ISDN 拨号设备、ADSL 拨号设备、无线网卡等网络设备非法接入互联网，给网络的安全性等带来了极大的隐患；
   d) 办公网络没有进行准入控制，任何终端只要插入网络就能够自由的访问整个网络，存在大量非法接入和非授权访问的状况，有可能导致办公系统的破坏，以及关键信息资产的泄漏，已经成为了办公网需要解决的重要风险。
2. 特权泄密，无法追溯
   a) 对服务器构成的安全风险中，有近80%是发生在系统内部。服务器的应用相当复杂，维护起来非常困难，当然服务器操作系统也是一样的复杂，配置和管理都需要充足的专业知识。在管理和维护的过程中，难免会有不当的操作。或是给服务器的安全留下隐患，或是对服务器运行造成影响。更可怕的还有商业间谍可能伪装成第三方厂商维护人员，从而轻易的从系统内部窃取商业机密，造成巨大的损失。
   b) 分散的多点登录管理方式，无法准确的身份认证和授权控制。多点登录的分散管理方式无法进行强有效的授权控制，致使用户的登录操作难以管理、难以审计。
   c) 有规范、规章制度，但没有相应的过程监控手段去监督。虽然企业内部制定了一系列的操作规范和管理制度，但管理人员有没有严格地按照规范、规章去执行，我们无从知道。当发生安全事件时无法进行责任鉴定和事件追溯。
3. 海量终端和桌面，难以管理
   a) 目前大多数终端部署防病毒软件，但没有集中管理，对于感染病毒和木马的终端无法进行控制其访问，只能通过管理手段要求分员工对终端进行杀毒等等，并且该工作是事后的工作，当一个未知病毒大面积爆发时有可以造成整个网络无法使用，对网络的安全稳定运行造成非常大的影响；
   b) 没有部署强制的补丁管理系统进行补丁统一管理，各终端不打、漏打系统补丁状况严重，而且没有办法强制安装，导致一旦某台终端感染病毒或恶意代码，则很快就会在内网泛滥；
   c) 员工安全意识薄弱， 安全策略难以实施。主要表现在私自安装软件的情况比较严重，无法对终端的非法软件安装情况等进行检测和控制。

3 总体需求

3.1 需求场景

为充分了解金融机构（后面简称金融机构）各部门对现有终端的安全使用情况，用户习惯和对项目实施后的安全期望，特开展此调研，总结出防泄密、可审计、集中管理三大类需求。

3.1.1 典型场景业务操作调研

金融机构各业务场景常涉及的业务操作有下面几类：

- ✧ 办公网日常办公：
  - ■ WINDOWS XP/Windows 7操作系统。
  - ■ 需要使用OFFICE，Outlook，Project,IE，Adobe Reader,Media Player视频播放软件,金融机构通讯软件,常用输入法，微星阅读器，支持视频直播和点播，画面流畅；
  - ■ 用户虚拟桌面颜色至少32位以上，保证图像显示质量；
  - ■ 支持PC机、瘦客户机访问虚拟机桌面平台；
  - ■ 支持在同一桌面使用不同版本的应用软件；包括office文档编辑，收发邮件，内网网站，internet访问等。
- ✧ 开发测试
  - ■ 具有安全OA办公用户所有的功能；
  - ■ 使用VDI，能够安装使用Visual Studio/My Eclipse/MENTOR/ALTUIM/VC/MATLAB/等软件
- ✧ 办公网生产网文件交换：
  - ■ 金融机构办公网与生产网一般为逻辑或物理隔离
  - ■ 通过办公网与生产网之间的文件服务器进行文件交换；
- ✧ 生产办公：
  - ■ 高密级生产业务，客户账户及交易敏感信息。
  - ■ 某某业务流程处理
- ✧ 运维
  - ■ 服务及应用系统主机监控，巡检，配置管理。

各业务场景安全等级及业务操作如下表：

图表 1 业务场景操作对应表

序号	场景	安全等级	日常办公（office/mail/网站）	办公网生产网文件交换	内部文件共享	特有业务
1	办公网网办公	2级	√			电子流审批，公文查阅。公文流转，ERP系统，内部通信，internet访问。
2	开发测试	2级	√		√	办公系统，生产系统开发
3	生产业务	3级	√	√		生产业务操作

4	运维	2~3级	√			生产运维系统为3级、其他OA/ERP办公系统、网络运维、开发测试系统运维为2级

3.1.2 金融机构业务风险分析

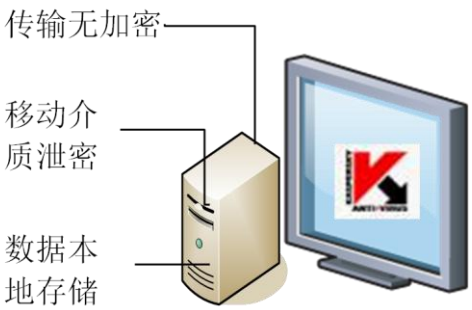
根据金融机构各业务场景的业务操作总结分析，涉及的风险主要为终端泄密，及文件交换无审计、运维无审计风险，终端未集中管理。

3.1.2.1 终端泄密风险

终端存在较大泄密风险，主要有：

1) 办公网终端保存工作文件，有泄密到 internet 风险，不符合行业主管机关要求；
2) 办公终端和生产终端复用，存在泄密隐患；
3) 非法外联以及非授权资产等的接入不可控；
4) 移动终端设备（PAD/智能手机）接入，存在泄密隐患；
5) 移动介质接入不能全面可控；
6) 移动介质拷贝文件交换无加密、无留痕，使用和管理存在泄密隐患

图表 2 终端数据泄密风险图



3.1.2.2 文件交换无审计

文件交换无审计风险主要有：

1) 文件交换无法审计、留痕；
2) 外包人员无行为审计功能；
3) 业务邮件，敏感文件通过外网邮件外发未审计、留痕和归档，存在泄密隐患。

3.1.2.3 终端未集中管理

金融机构终端管理现状：

1) 每个员工自己管理终端，安全策略无统一管理；
2) 敏感数据存放在本地终端；
3) 接入无法控制和管理；

出于安全管理考虑，需要对金融机构终端进行集中管理，包含安全策略集中管理，数据集中管理和风险防范，缩小风险扩散范围，降低信息安全风险。

3.1.2.4 风险与业务场景对应

安全风险对应到各业务场景：

图表 3 场景与安全风险对应表

序号	场景	终端泄密风险	文件交换无审计	终端未集中管理	特殊说明
	办公网办公	√	√	√	
	开发测试	√	√	√	
	生产业务	√	√	√	
	运维	√	√	√	

3.1.3 合规要求

依据《信息安全技术-信息系统安全等级保护基本要求(GB/T22239-2008)》，对金融机构终端安全进行优化改进，主要要求有：身份鉴别（S3）（7.1.3.1.），访问控制（S3）（7.1.3.2.），安全审计（G3）（7.1.3.3.），数据保密性（S3）（7.1.5.2.），介质管理（G3）（7.2.5.3.）等。

3.2 需求总结

3.2.1 安全需求

3.2.1.1 防泄密需求

1）数据不落在终端
2）移动介质管控
3）禁止非法接入
4）防止非法外联
5）移动办公终端接入安全

3.2.1.2 可审计需求

1）文档审计
2）敏感业务操作审计

3.2.1.3 集中管理需求

1）需要将终端进行集中管理，并使之简单化、标准化；
2）敏感数据集中管理，加强文件交换的管理，防止敏感数据泄密。
3）信息安全策略集中管理
4）系统运维集中管理

3.2.2 用户范围及规模

涉及金融机构所有内网终端办公用户，包含金融机构员工和外包员工。用户规模

见下表：

图表 4 桌面云用户规模

办公网和生产网数据交换用户规模为某某个，移动办公接入用户规模为某某个。

应用场景	规模	规格	主存储	预留扩容	操作系统	备注
OA办公用户		2U4G	XXG系统盘+XXG数据盘	XX T	Win7	
开发用户桌面		4U8G	XXG系统盘+XXG数据盘		Win7	
运维用户		2U4G	XXG系统盘+XXG数据盘		Win7	

3.2.3 非功能性需求

除了上述安全及系统资源需求，还包含下面非功能性需求。

1) 系统规划设计具有高性能、高可靠性、易管理性、高可运维性，同时考虑在实施时迁移及用户体验的需求。
2) 可靠性需求：
   - 内网日常办公使用主机，能在出现故障后能快速恢复；
   - 个人办公数据高可靠；
   - 运维场景下，运维出现故障，需要快速切换和恢复。
3) 易管理需求：
   - 低运营成本、低维护成本。从架构设计、维护技术等方面考虑总体设计，降低后期维护成本；
   - 快速部署、终端自动修复、自动化补丁和软件部署，减轻 IT 管理员的工作强度，降低 IT 运维成本。
   - 支持运维的自动化操作、用户的自助化服务，并为将来的整体自动化调度系统预留接口。
4) 迁移需求
   - 系统上线、终端迁移不影响现有业务连续性，对用户的切换工作量降到最低，保证业务数据完整迁移；
   - 终端安全系统需对用户主机资源占用较少，不影响日常业务操作交互；
   - 在进行终端安全改进同时，兼容用户现有业务操作体验；
   - 建立新技术的宣传灌输策略，增强用户对新技术认同感。
5) 用户体验需求
   - 提供端到端的性能和用户体验优化方案，并建立性能基线库和验收标准，达到基于业务场景的最优的性价比；
   - 提供简便的用户体验优化工具，最终实施方应在兼容性案例和端到端的优化方案有较多的积累和经验；
   - 开发环境下，不影响用户主机资源占用高的操作，如重载测试、编译、调试；
   - 在大规模用户上线使用时，不降低用户体验；

4 总体方案设计

4.1 设计原则

在桌面安全中，设计终端安全改进系统时，遵循以下原则：

1) **安全性：**从终端、隔离、核心层，办公外网、生产网进行立体安全设计，数据不落在终端，访问及操作记录要留痕审计，集中管理。
2) **体验：**桌面云系统提供最佳的访问体验，用户不再受PC、Windows系统的频繁故障的影响。实现不同网络环境的一致访问体验，提升桌面的可用性与连续性。桌面云系统简单，易用，并提供友好用户界面与自助维护界面。
3) **可靠性：**采用先进虚拟化技术，资源池化，所有设备均应经过大规模组网运行验证。系统的业务、管理、存储功能应该由独立的平面承载，所有设备、模块节点具备冗余部署能力，确保系统及业务的可靠运行，并且系统应具有平滑扩容的能力。
4) **可服务性：**降低运维成本，提高工作效率，减轻管理维护人员的工作强度与不必要的的重复劳动。桌面云系统将应用、桌面的升级、变更、维护等工作交由后台统一管理与运行；具备良好的综合定位分析及故障恢复能力，从而降低对业务的影响。供应商具备为项目长期服务和保障的能力。
5) **可扩展性：**系统将来覆盖延伸扩容方便，扩展成本小，后期新增应用可随时、简便的接入办公运维系统，新业务新用户接入对整体影响小。

4.2 方案概述

针对金融机构终端办公网办公，生产网办公，系统运维场景的防泄密（介质管控，接入管控防止非法外联，终端数据管控等），可审计（文档审计，敏感业务操作审计，运维过程审计），集中管理（终端管理，安全策略，文件及敏感数据等）需求，设计本方案。

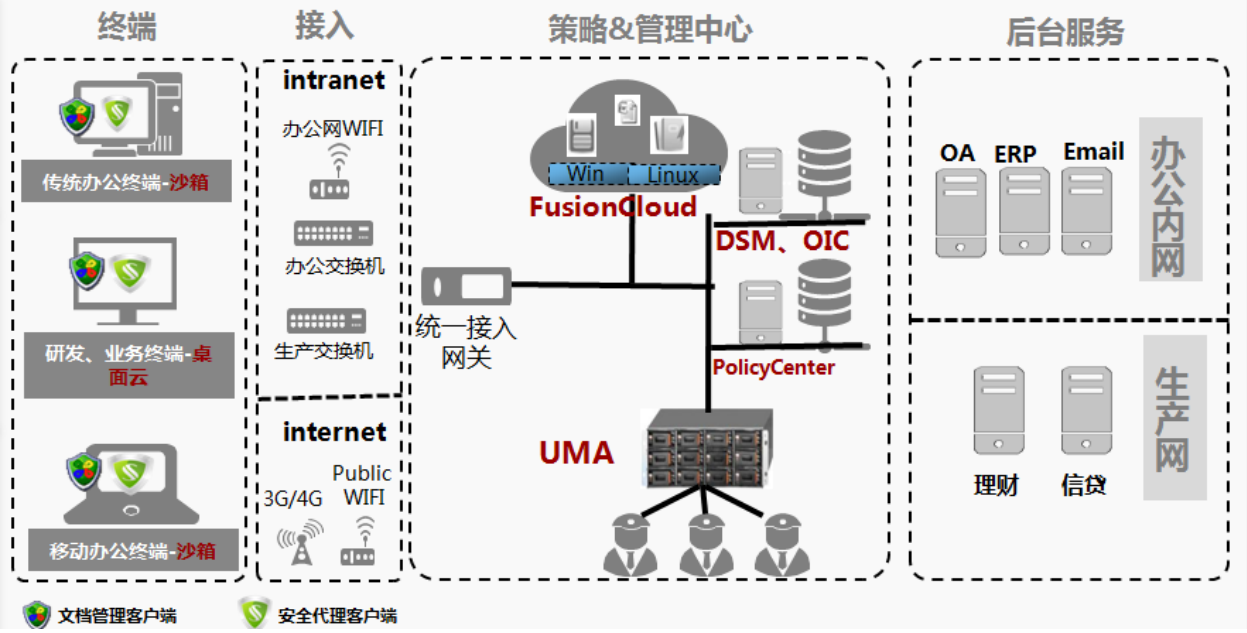
办公网办公（OA，开发测试）：针对内网办公进行OA办公（office文档，邮件），同时访问多个办公业务系统，操作数据密级度高，设计桌面云方案，一个终端对应多套虚拟机（为办公，每种业务独立发放虚拟机，虚拟机之间隔离），集中管理用户桌面，数据不落在本地，使用安全TC管控外设和存储介质；设计安全数传跨网/终端之间数据交换进行权限控制和审计，保证数据安全。同时也满足虚拟机安全策略统一管理需求。

运维（办公网OA，生产网业务）：针对运维多入口，服务器账号分散，高密级服务器（交易主机）密码共享，无审计等情况，设计统一运维审计进行运维管控，控制运维入口，集中管理运维账号，控制运维权限，并对运维操作进行日志记录和录频，满足运维集中管理和审计需求，大大降低了高密级服务器运维风险。

集中管理（所有场景）：针对金融机构本身安全管理和合规需求，设计AD域管理统一进行办公账号和身份认证，对终端账号和计算机策略进行统一管理；设计PolicyCenter，统一管理终端桌面安全策略，控制PC外设和存储介质，管理用户行为，防护木马病毒；满足合规要求及安全策略统一管理需求，有效降低了安全风险。

4.3 总体方案架构图

图表 5 桌面安全总体架构图



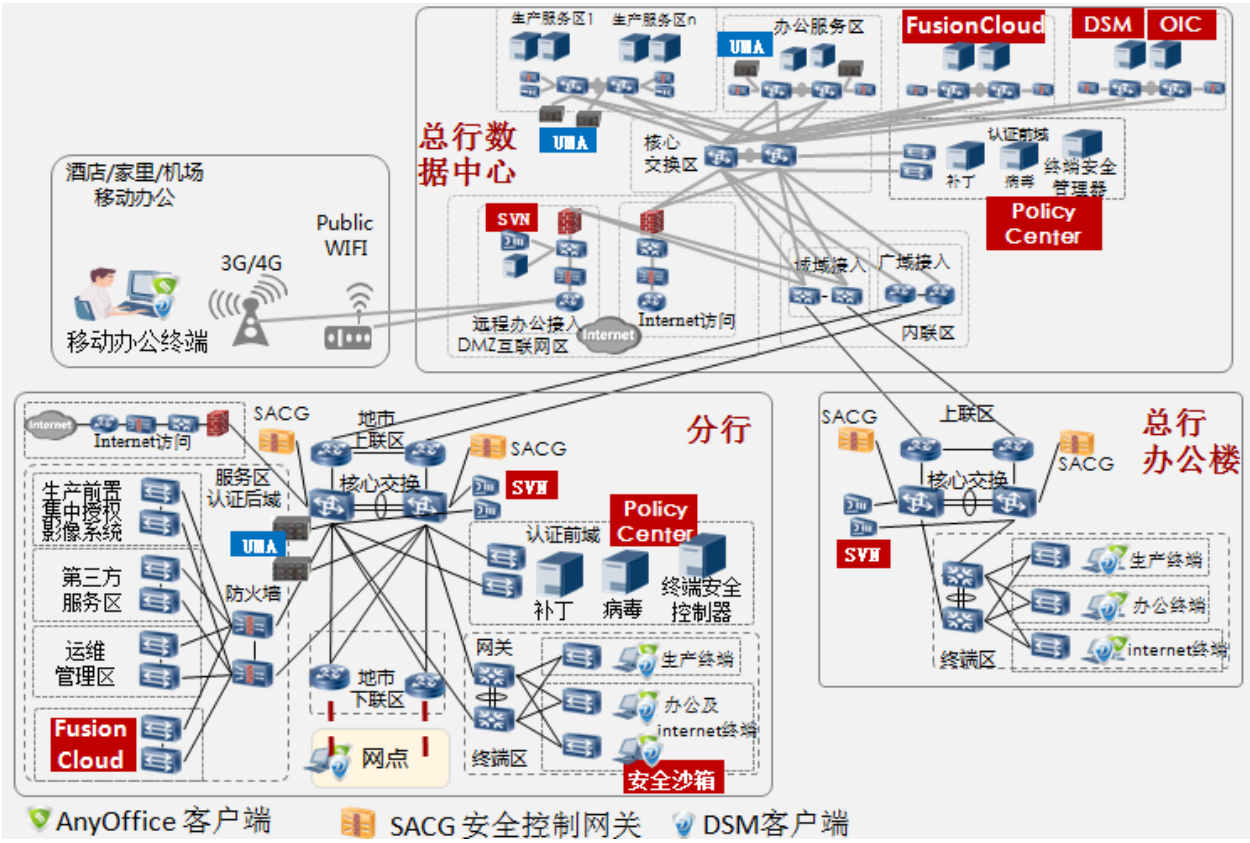
方案子系统包含桌面云FusionCloud，安全沙箱，策略中心(PolicyCenter)，统一运维审计（UMA），移动办公,文档安全管理（DSM），文件信息管控中心（OIC）子系统。

这些子系统中统一运维审计为合作伙伴产品，其他的子系统为华为产品和方案。

图表 6涉及解决方案及产品

4.4 物理部署图

图表 7 桌面安全总体架构图



方案包含桌面云，PolicyCenter，安全沙箱，文档安全管理（DSM），文件信息管控中心（OIC），统一运维审计（UMA）六大子方案。

在办公场景应用桌面云、安全沙箱、PolicyCenter，文档安全管理（DSM）、文件信息管控中心（OIC）子方案；生产场景应用桌面云、PolicyCenter、堡垒机（UMA）、文档安全管理（DSM）、文件信息管控中心（OIC）子方案；运维场景应用PolicyCenter、堡垒机（UMA）子方案。

✧ 桌面云：

华为桌面云解决方案是基于华为FusionCloud云平台的一种虚拟桌面应用，通过在云平台上部署软、硬件，使终端用户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，以及整个客户桌面。桌面云使用PolicyCenter进行安全加固，主要用于办公PC和便携PC，以及桌面云的虚拟桌面，桌面云的安全TC自身有非常多的安全防护，无须使用PolicyCenter加固。

✧ PolicyCenter：

为了解决金融机构办公网终端安全、桌面安全管理问题，有效保障内部网络的畅通、终端的安全和公司信息数据的安全，PolicyCenter方案有效的帮助金融机构提供整合的内网安全管理思路，实现从终端到业务系统的控制和管理功能。

PolicyCenter方案将试图访问金融机构网络资源的用户进行身份认证和强制实施安全认证，通过双重检查保证接入网络终端的安全性，对不满足需求的终端自动引导进行安全修

复和补丁安装，对满足需求的终端接入网络后，对其网络和终端行为进行实时监测和审计，保护终端软硬件资产，防止信息泄密，最大程度保障金融机构终端、桌面、信息的全面安全。

✧ 安全沙箱：

安全沙箱子系统中在不同业务区域之间部署安全接入网关， 所有跨区域访问的终端接受该安全接入网关的管理和控制，跨区域访问时，终端和安全接入网关之间的数据传输进行安全加密。当终端需要进行跨区域访问时，首先需登录安全接入网关，接受安全接入网关的接入认证。认证通过后，接入终端在桌面系统中创建一个安全桌面，和本地真实桌面进行逻辑隔离。

隔离的数据进行交换时，必须通过网关进行安全数传。网关对传输进行权限控制和策略管理，对传输的数据进行加密，并记录日志，方便审计。

安全沙箱主要用于办公，同时进行internet访问的场景。所有的internet访问必须在安全沙箱里进行，物理桌面无法访问这些文件，防止病毒、木马传播到办公环境。

✧ DSM：

文档安全管理须 “技术与管理”并重，才能从根本上杜绝内部人员泄密问题。

在管理上，一是要建立一整套规范的安全保密制度并严格执行；二是要加强员工的保密教育，使他们认识到保密工作的重要意义；三是要有奖惩制度，对保密先进个人、单位予以嘉奖，对于泄密事故加大惩处力度，做到以儆效尤。

在技术上，一是利用加密等信息安全技术对公司内部的机密文档进行加密和合理的授权，防止主动泄密事件的发生；二是对内部人员的使用计算机接入企业内网的行为进行监控和审计，若有泄密事件发生可以找到泄密渠道。

文档安全管理（DSM, Document Security Management）系统是针对机密文档、防止主动泄密的一款安全软件产品。通过对企业的重要文档进行加密和实时权限控制，可为企业提供安全授权下的机密信息共享机制，使信息所有者能够定义信息的访问者、访问方式和时间等，并记录文档操作日志。有效控制因不受权限限制的阅读、修改、分发文件导致的信息泄密。

✧ OIC：

OIC文件信息管控中心方案，从文件采集、集中管理共享、检索、加密管控、流转发布、审批审计等各生命周期阶段的信息管控平台，防止信息通过网络、计算机、移动存储介质等途径泄密，同时促进协同工作及信息共享。

可以集中管理多来源信息，防止流失：可以手工上传、标准协议传输、开放接口等方式可集中各业务系统、个人PC等多来源信息数据，提供海量存储空间集中管理共享。按照整个机构、不同部门、团队等各范围灵活赋权，实现不同范围内的共享服务；提供灵活便捷的数据存取方式，可以通过WEB和本地网络磁盘两种方式访问，操作符合本地Windows操作系统使用习惯，集中存储管理机构资产，防止信息流失。

同时集中控制涉密信息传播，保障安全：为满足信息资产长期安全保存并防止信息资产泄密的需要，系统需要支持文件集中管控手段，如在线查阅：自动转换文档为标准flash格式在线查阅，防止网页复制，实现可控下载。集中加密：支持自动加密和实时权限控制，机密信息仅被获权用户下载，传播后也仅能被具备权限的指定员工阅读。审批审计：支持审批流程和文件操作生命周期日志审计，做到发生误删等操作时有据可查。

另外，OIC还集中提供多种增值服务，提升效率：提供与GOOGLE类似的全文检索平台，能够在海量历史知识资产中快速准确的定位所需要的内容；检索技术需和机构内部信息资产获权匹配，严格保障合适的人获得合适的信息；支持面向个人和团队分别提供存储空间，支持全格式文件在线编辑、信息在线分享等多种增值服务能力。

✧ UMA：

华为合作伙伴桑威UMA统一运维审计系统，作为金融机构IT核心资源的统一接入控制和运维审计解决方案，通过对核心业务系统、主机、数据库、网络设备等各种IT资源的帐号、认证、授权和审计的集中管理和控制，可有效解决IT运维管理问题，满足相关法规、标准要求，完善IT管理体系。UMA统一运维审计提供服务器统一操作管理平台，隔离“人（操作者）”和“主机设备等重要资源（操作对象）”直接连接，规范服务器操作管理行为，将管理、维护数据流和业务数据流分离，统一操作管理接口，完成和谐、规范、有序网络构建和资源使用行为控制，为随后的“集中认证”、“访问控制”、“权限控制”和“操作审计”打下坚实基础。

UMA主要应用于各业务运维及桌面云运维场景，进行统一运维管理和审计。

各子方案适用应用场景如下：

图表 8　子方案适用场景

子方案	特点	典型场景	说明
桌面云	1.桌面虚拟化，数据不落终端 2.资源弹性调度，最大化利用 3.集中运维，低成本	OA办公，网点柜面服务，研发，呼叫中心，培训，运维等	密集办公场景特别适用
安全沙箱	1.沙箱技术，安全隔离数据 2.多沙箱，多个安全工作空间	OA与internet办公，OA与研发办公等	同一终端多个不同密级别的工作空间适用
PolicyCenter	1.接入认证 2.合规检查和修复 3.外设及介质管控，防泄密	OA办公，柜面服务，研发，呼叫中心，运维，培训等	不同人员，不同业务可以使用不同安全策略
文档安全管理	1.文档加密和权限控制 2.文档操作审计	OA，研发，运维，培训等	涉及机密的文档管理
文件信息管控中心	1.文档集中保存和授权 2.文档流向跟踪，使用审计	信息管理，OA，研发，培训，运维	知识共享可控
统一运维审计	1.统一运维入口 2.运维操作审计	运维	管理员特权管控

典型业务场景应用：

图表 9　业务场景应用方案

场景	主要挑战和需求	子方案	特点

OA	普通办公	部分机密文档，防泄漏 安全管控同时兼顾效率 终端数量多，维护难度大	桌面云 PolicyCenter 文档安全管理 文档信息管控	数据不落终端，用户行为可控，文档加密，零泄密 桌面、文档集中，高效管理
	Internet 访问	同一办公终端访问 internet，防止数据泄密，网络入侵，需安全加固	安全沙箱 PolicyCenter 文档安全管理	沙箱隔离 internet 空间，用户行为可控，文档加密，安全办公 对现有系统改变较小
	移动办公	移动终端管控更难，更易泄密 同时保障移动办公体验	桌面云 PolicyCenter 文档安全管理	数据不落终端，传输加密，用户行为可控，文档加密，零泄密 不同终端，一个工作桌面，保证体验
研发		高密级研发代码文档，防泄密 代码编写，编译调试，要求高性能，支持串并口外设	桌面云 PolicyCenter 文档安全管理 文档信息管控	数据不落终端，用户行为可控，文档加密，零泄密 高性能虚拟机，外设映射，保证体验 桌面、文档集中，高效管理
运维		共用用户和密码，权限易滥用 操作无审计留痕，无法追溯 多点接入，难管控	堡垒机 PolicyCenter	密码托管，操作审计，防特权泄密 统一运维入口 旁挂，对现有系统改变较小

4.5 方案亮点

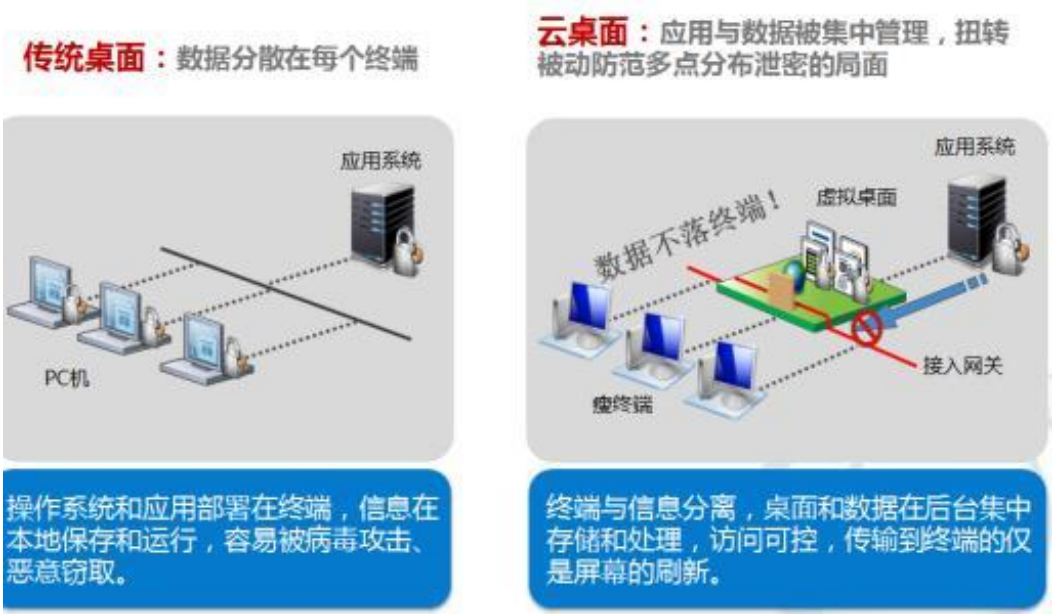
4.5.1 全面安全防护

华为内网终端安全改进解决方案从终端、接入传输、网络系统及运维管理层逐层安全加固，全方位进行信息安全防护，防止数据泄密，满足等级保护身份鉴别，接入控制，安全审计，介质管控等要求。

✧ 防泄密：

办公外网终端：与办公内网环境的文件传输进行策略控制、传输加密，更好防范信息泄密。数据与终端分离，终端不落工作数据，有效防止敏感信息从终端泄露。

图表 10 传统桌面与云桌面数据存放对比



办公内网及交易网终端：TC瘦终端从硬件和软件设计上，采用了多种安全机制，有效防止泄密。硬件芯片ID与ROM加密绑定；限制BIOS只能从内置加密存储引导；定制OS，无存储驱动，只开放ICA及TCM网络端口，禁止任意安装程序等。

接入及传输网络：通过网络平面隔离、引入证书认证，传输加密等手段，保证业务运行和维护安全。

✧ 可审计：

对于数据传输，可以记录数据传输的操作日志及文件，对这些日志和文件进行审计，防范主动泄密，追溯泄密责任。

桌面云操作日志记录了用户对系统所做的操作以及操作的结果，用于跟踪和审计。记录操作日志，可以快速定位系统是否遭受恶意的操作和攻击。

统一运维审计对服务器、主机系统进行统一运维审计，对操作进行录频回放，防范恶意操作，提高系统的安全程度。

✧ 集中管理：

通过AD域对用户账户进行集中管理，用户统一进行域认证，可以按照用户组进行安全策略集中管理，提升安全管理水平，同时也带来良好的用户体验。

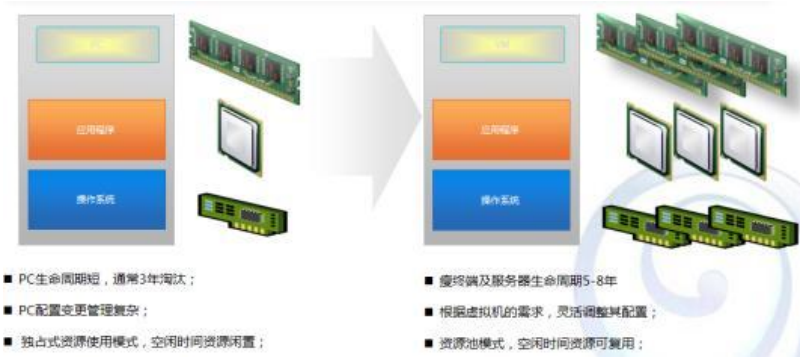
对用户桌面数据统一集中在桌面云，终端只能远程通过ICA访问桌面，数据不落在终端，可以防止非法外泄。对用户桌面统一进行安装、分配、回收，集中管理和运营，提高了维护效率，更合理利用资源，降低长期桌面采购成本。

通过对桌面云业务维护系统和运维管理系统管理员区分权限，对被访问的数据区分权限，限制管理员访问系统的范围，保证系统的安全。

4.5.2 资源高效利用，降低总体采购成本

计算资源复用，设备生命周期延长，降低总体采购成本。虚拟机资源配置可动态调整，减少浪费。

图表 11　桌面云资源高效调度



4.5.3 维护效率提升

传统PC桌面终端分散，标准不统一，维护效率低下。桌面云集中管理桌面，人均维护效率可以提升2-4倍，对维护人员技能发展空间也更大。

图表 12　桌面云终端集中管理

4.5.4 提升办公效率

办公内网内桌面漫游，实现敏捷办公； 允许认证用户通过认证设备可以在任意时间、地点接入。研发人员可以在研发区域内进行漫游办公，还可以跨区域漫游。运维人员还可以移动办公，在出差或家里进行远程接入运维。

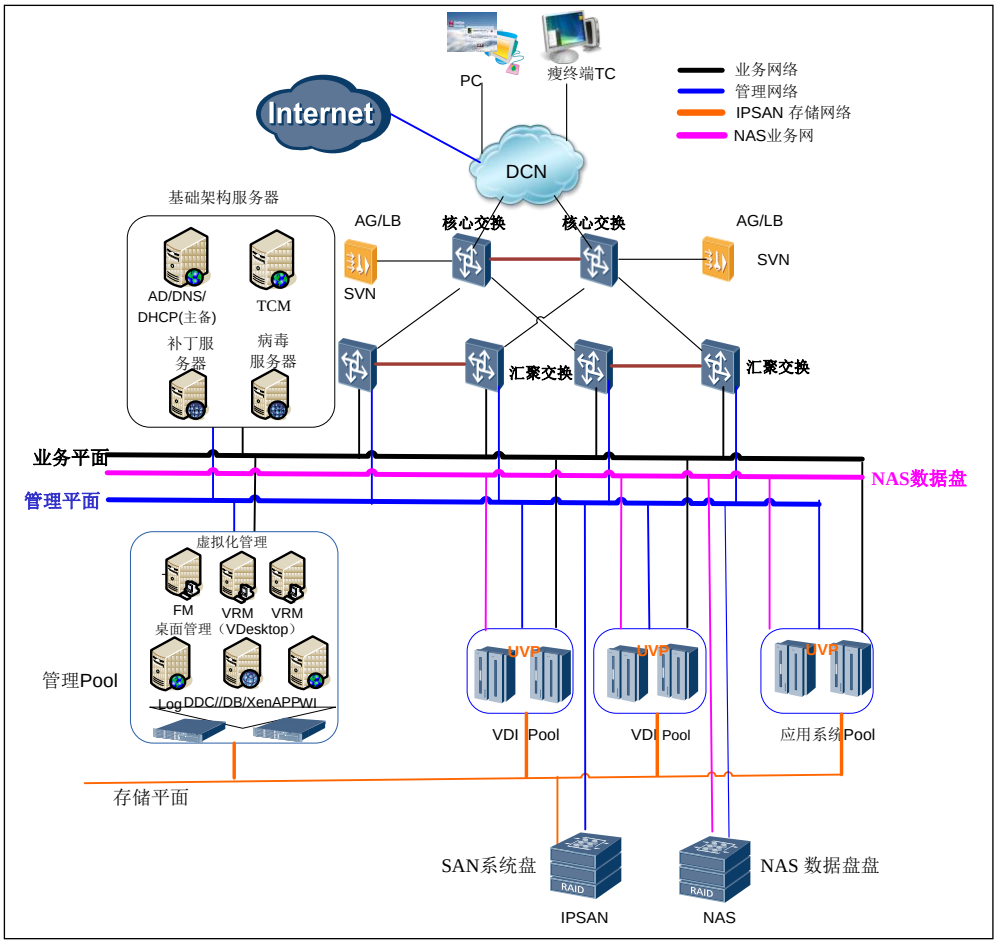
图表 13　桌面云敏捷办公

5 华为桌面云子方案

5.1 总体技术方案

桌面云总体技术方案如下图所示：

图表 14 总体技术方案示意图



本项目为了实现高安全、高可靠、高性能、易远程集中运维、平滑扩容的目标，采用业界主流成熟的虚拟化技术，实现虚拟桌面、应用发布、服务器虚拟化等要求。本项目方案主要以下方面考虑：

资源池设计：根据本项目的需求，服务器上安装华为的虚拟化软件，将服务器池化。池化后VDI桌面、应用虚拟化、服务器虚拟化的服务器分别组成集群。池化后服务器上运行虚拟机便于管理、监控。虚拟机在集群里可以实现定制策略迁移、手动热迁移、故障热迁移。资源池的设计具有高可靠、平滑扩容特性。

桌面管理：华为虚拟桌面管理软件FusionAccess，提供高性能且可靠的桌面投送。

虚拟化管理：为了便于硬件设备（服务器、存储、交换机）、虚拟资源的集中管理，采用华为的虚拟化管理软件FusionSphere。FusionSphere采用B/S架构，可以远程统一管理本项目中VDI桌面、应用虚拟化、服务器虚拟化三个资源池。FusionSphere可管理、监控硬件资源、虚拟资源；支持虚拟机的快速部署、定制化策略调度。

- 计算资源池

计算资源池为用户提供CPU、内存计算资源。在服务器上安装华为的虚拟化软件，

可以在一台服务器上虚拟出多个台虚拟机，提供弹性规格的虚拟桌面。这几个资源池归属同一朵桌面云管理系统。

➢ 存储资源

存储资源主要为虚拟桌面提供系统盘空间、还有桌面云管理系统所需要的空间。这些存储都在主用存储上。主存储根据数据类型的不同，划分不同的数据LUN。这里的数据类型主要包括 管理数据、Windows系统数据、用户数据。

NAS存储主要用于，保存用户个性化数据，表现形式为数据盘。

5.2 桌面云架构与组件介绍

FusionAccess桌面云以服务器虚拟化为基础，允许多个用户桌面以虚拟机的形式独立运行，同时共享 CPU、内存、网络连接和存储器等底层物理硬件资源。这种架构将虚机彼此隔离开来，同时可以实现精确的资源分配，并能保护用户免受由其他用户活动所造成的应用程序崩溃和操作系统故障的影响。

FusionAccess采用业界最优的ICA桌面协议，将访问带宽要求降到最低，并可将授权用户安全连接至集中式虚拟桌面。它与 FusionSphere协同工作，可提供一个完整的端到端桌面云解决方案，此解决方案不仅能增强控制能力和可管理性，还可以提供与PC一致的桌面体验，FusionAccess能简化虚拟桌面的管理、调配和部署。用户能够通过FusionAccess安全而方便地访问虚拟桌面，升级和修补工作都从单个控制台集中进行，因此可以有效地管理数百甚至数千个桌面，从而节约时间和资源。数据、信息和知识财产将保留在数据中心内，而且永远不外流。配备FusionAccess桌面云方案具备下列优势：

- ✧ 集控制能力和可管理性于一身：由于桌面在数据中心运行，因此管理员可以更轻松地对其进行部署、管理和维护。
- ✧ 与PC一致的体验：用户可以灵活访问与普通 PC 桌面功能相同的个性化虚拟桌面。
- ✧ 降低总体拥有成本 (TCO)：桌面云可以减低其管理和资源成本。

FusionAccess各部件简要介绍如下：

➢ 瘦终端TC/SC

为用户提供用户桌面的显示输出，以及键盘鼠标输入，TC/SC通过桌面接入网关代理访问对应的桌面，同桌面接入网关之间采用SSL加密的ICA协议进行信息传递，可以通过策略开放或者禁止TC/SC USB等外设至虚拟机的重新定向；用户通过在TC/SC上输入域用户名和密码访问对应桌面。

➢ 接入网关

接入网关主要提供两个功能，一是对WI节点提供负载均衡；另一个是对桌面ICAOver SSL 提供加密功能。

➢ 桌面软件FusionAccess

FusionAccess是华为提供的桌面管理与投送软件，包括以下组件，所有组件均安全在Windows 2008 R2系统上。

Web Interface：采用2台虚拟机负荷分担方式部署。Web Interface（WI）负责显示基于Web的界面，当用户顺利通过身份验证后可以看到自己可用的虚拟桌面和虚拟应用。

DDC(Desktop Delivery Controller)：（1+1主备方式）负责即桌面传输控制器，安装在虚拟机上，负责新虚拟桌面的注册、将虚拟桌面的请求指向可用的系统、以及代理

用户和虚拟桌面之间的连接。它控制桌面的状态，根据需要和管理配置启动和停止虚拟桌面。采用虚拟机1+1热备方式部署。

DB节点：用于存储桌面云的数据，包括ITA、DDC和XenApp所需要的数据库SQL Server 2008 R2。采用虚拟机1+1热备方式部署。

ITA节点：桌面云解决方案对金融机构IT资产管理系统提供的接口。IT系统可通过IT适配器完成对桌面云的虚拟机管理、虚拟机镜像管理、虚拟机分配管理、系统运行维护管理等操作。采用虚拟机1+1热备方式部署。

License节点：桌面云License的管理与发放系统，License服务器用于控制器接入桌面云的用户数。

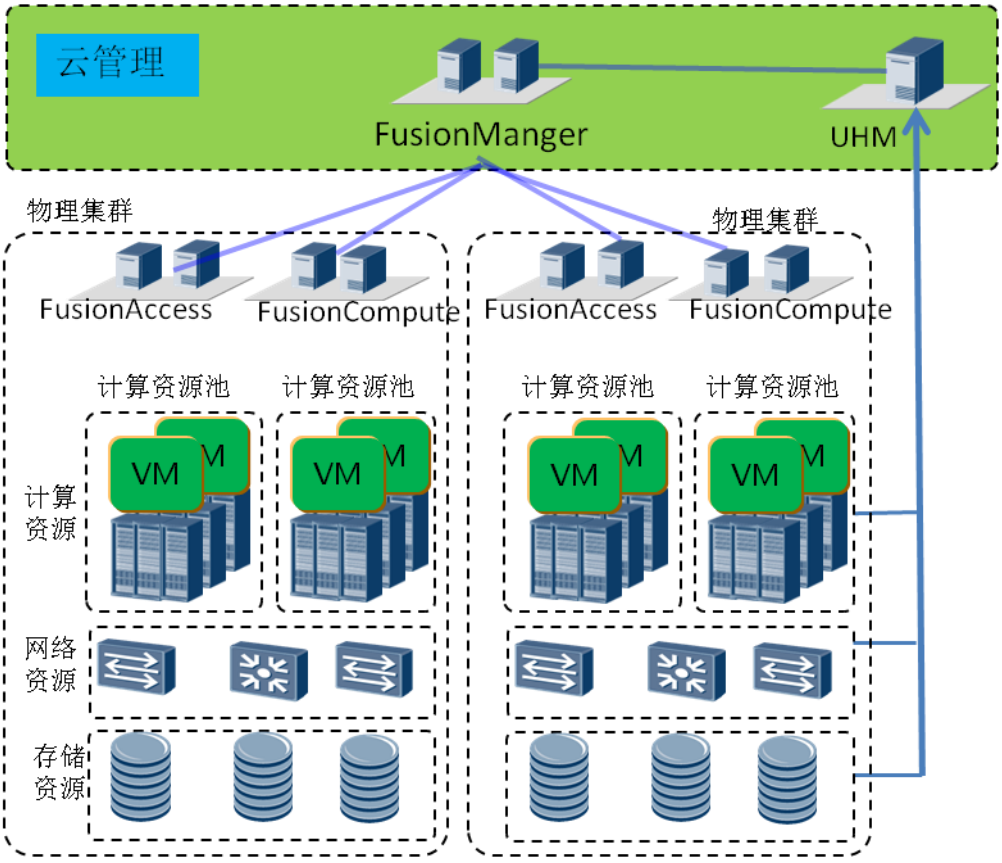
TC管理（TCM）：对瘦终端进行集中管理，包括版本升级、状态管理、信息监控、日志管理等。License\TCM组件合一部署在一台虚拟机上。

AD/DNS/DHCP：AD域控用于用户登录鉴权，DHCP用于域内IP分配。DNS用于域内计算机名、桌面云登录域名的解析。采用虚拟机1+1热备方式部署。

XenApp应用虚拟化：后台基于Windows Server 2003或2008服务器，使用XenApp发布虚拟机的桌面或应用（如IE、VNC）给几十用户同时访问，配置严格的组策略保护共享的服务器工作环境。

5.3 云基础平台架构与组件介绍

图表 15　桌面云平台组件架构



华为云平台FusionSphere主要有虚拟化基础引擎FusionCompute、云管理

FusionManager两个节点组成。一套云平台部署一对FusionManager主备节点，FusionManager通过自动发现功能发现其管辖下的物理设备资源（包括机框、服务器、刀片、存储设备、交换机）以及他们的组网关系；提供虚拟资源与物理资源管理功能（统一拓扑、统一告警、统一监控、容量管理、用量计费、性能报表、关联分析，生命周期），并且对外提供统一的管理Portal。

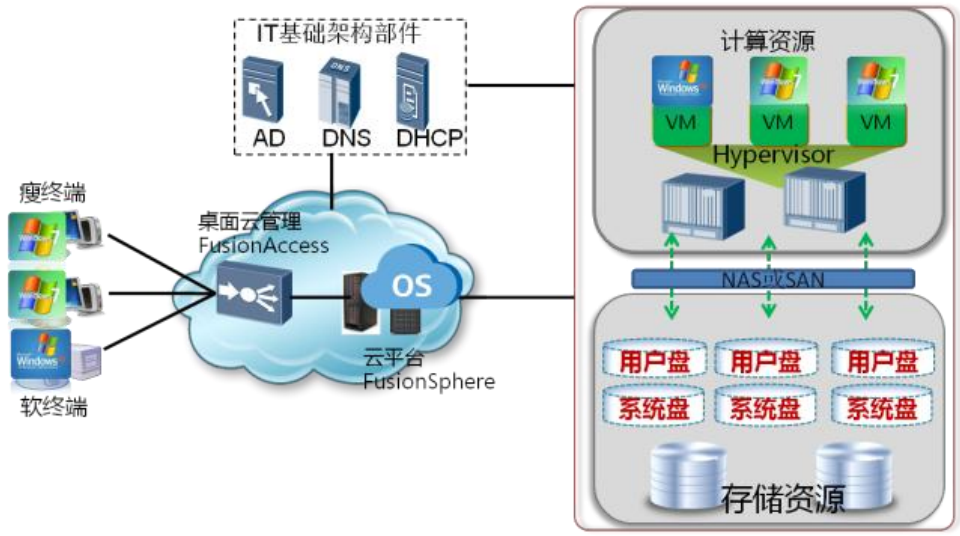
FusionManager还包括统一硬件管理UHM（Unified Hardware Management）功能，UHM提供对硬件自动发现，硬件自动配置、统一监控（带内和带外）、硬件统一告警、硬件拓扑、异构硬件支持。

FusionCompute提供基础的虚拟化功能，提供服务器、存储、网络的虚拟化功能，并向上对FusionCompute提供接口。每套FusionCompute主要由一对主备管理节点VRM组成。一对VRM对应一个物理集群(或者叫站点)。一个物理集群中可以把多台服务器划分成一个资源集群（又叫HA资源池），一个计算资源池有相同的调度策略，为了使用热迁移相关的调度策略要求资源池主机CPU同制。计算资源池不包括网络资源与存储资源。一个物理集群中可以包含多个资源集群。

多个物理集群（此时对应多对VRM）可以级联，由FusionManager统一管理。友商的虚拟化集群（如：VMware Vsphere集群），也可以交由FusionManager统一管理。

5.4 完整复制桌面云方案说明

图表 16 完整复制桌面云方案说明



本次金融机构要求个性化桌面云，也就是完整复制桌面云模式。

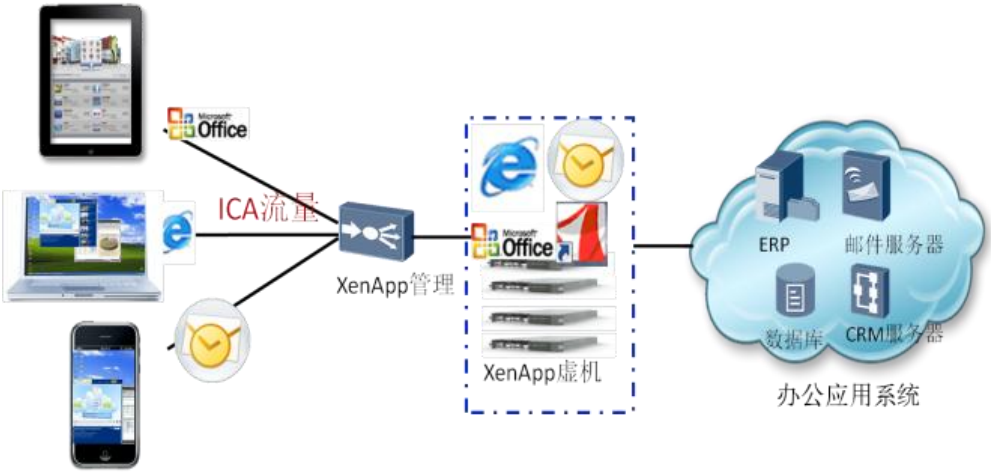
完整复制桌面云桌面利用虚拟化技术与远程桌面投送技术。在桌面云中心，利用虚拟化技术把服务器与存储虚拟成一台台弹性的虚拟主机。完完整复制虚拟桌面在创建时，系统会给这个虚拟桌面分配一份独立系统盘空间，并将虚拟机模板完整复制到系统盘上。这样每个完整复制虚拟桌面都有单独的系统盘与用户数据盘。基于虚拟机级别的隔离；安全性高；个性化强；外设支持类型丰富；用户体验与传统PC一致，可以按照用户的工作负荷弹性修改虚拟机规格。每个用户都有一个独立的虚拟机，虚拟机系统盘和数据盘都通过集中的存储设备加载。存储设备支持SAN与NAS设备。

用户通过本地瘦终端，或软终端可以远程登录虚拟机。虚拟机采用业界性能最优、带宽最低的ICA协议将虚拟机桌面显示投送到用户终端上。瘦终端的无本地存储、USB可

管控，功耗低。办公环境相对PC环境更简洁，无噪音。

5.5 基于 XenApp 的应用虚拟化方案说明

图表 17 应用虚拟化应用场景



本次金融机构要求满足200用户的应用虚拟化需求，主要用于移动办公场景和普通办公场景。

XenApp可以将在Windows Server 2008R2系统上的安装的应用软件与Windows Server桌面发布出来。这些Windows的应用软件可以在服务器侧集中管理和发布。所有XenApp服务器及其他配套组件服务器均部署在FusionSphere云平台上，可进行弹性调度、热迁移、故障迁移，大大地提高了可靠性。

XenApp发布的用户访问界面如下图所示；用户在终端（Pad/手机）用户不需要在本地安装这些应用软件，可通过ICA协议访问后台的这些应用软件与应用系统，充分利用后台的计算资源。用户可以通过IE、Outlook直接访问后台各种应用系统，进行公文审批、邮件浏览。应用系统的访问客户端不用经过任何改造。用户就可以获得类似PC的办公体验。用户终端与虚拟机之间采用加密ICA协议，保障了访问的安全，有效减小访问带宽。

- XenApp应用虚拟化的优势：

简化IT管理：将应用和数据从个人设备转移到数据中心，XenApp将应用程序集中在数据中心，可以降低管理成本，提高IT向分散用户交付应用的响应速度，加强应用和数据的安全性。

简化用户使用：将应用和数据从个人设备转移到数据中心后，所有应用和数据都在一个安全的位置进行维护、备份和管理。分散用户不再需要投入应用维护、数据备份、应用和数据的管理。

按需访问：用户可以通过TC、PAD、智能终端等多种设备即时、按需地使用应用。

应用虚拟化特点：

- ✧ 对应用程序要求支持在Windows 2008 R2上运行，并且支持多实例；
- ✧ 基于会话（Session）的隔离，用户使用之间会有影响，安全性弱于VDI；
- ✧ 用户体验与PC有不同；对外设的支持比VDI模式的差；

XenApp支持个人配置数据漫游和统一用户数据存储。支持用户登录到不同的XenApp服务器上可使用相同的用户配置文件。使用windows Terminal Service Roaming Profile技术，来实现用户配置信息的漫游设置。

本项目中用户个性化配置文件通过在AD上配置重定向统一存储在文件服务器上。并在AD上设置组策略的方法禁止用户访问XenApp服务器磁盘。每用户增加一个NAS网盘，用于保存用户个性化数据。

XenApp的主要应用可发布桌面与应用，本次采用发布共享应用。

- XenApp方式共享应用

将应用软件安装在XenApp服务器上，发布给用户，完成共享应用的功能。如下图样例：

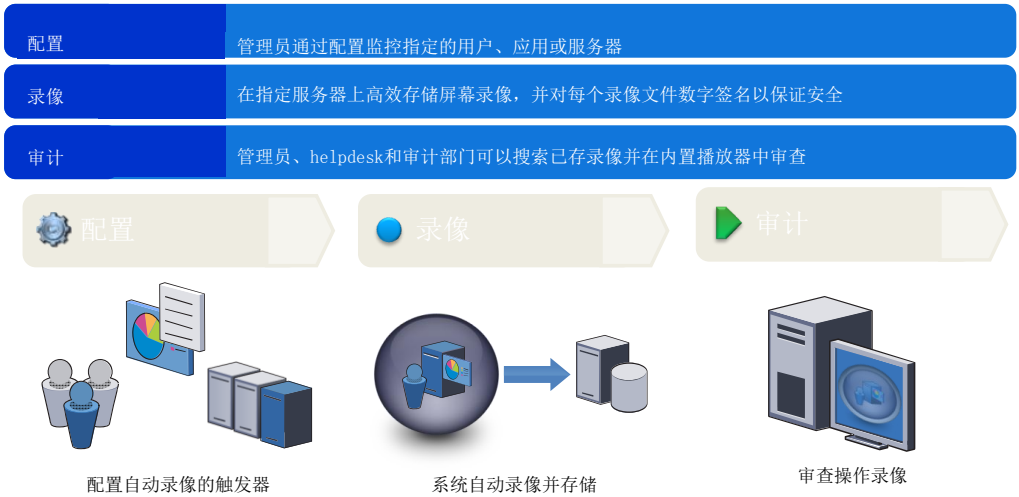
图表 18 发布应用

当用户访问应用虚拟化平台，任何用户使用应用的过程都可以被全程监控，强化审计和监控。

当用户使用应用虚拟化平台的应用时，用户的操作行为及显示器上的内容变化都可以被全程录像并可以保存在磁盘上，然后在需要的时候像看电影一样回放。并可以以用户、时间、角色、应用名称、位置等搜索并回放符合条件的录像内容。

可以配置指定的用户、应用或服务器对其进行监控录像，并且只有指定的用户才具有回放录像的权限。

图表 19 智能审计

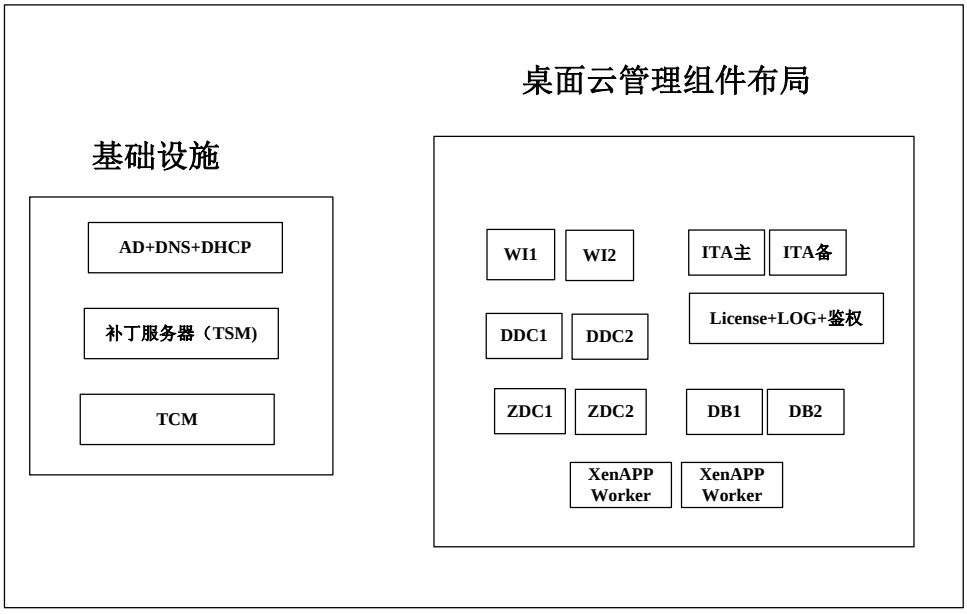


5.6 桌面云方案设计

5.6.1 FusionAccess 规划

金融机构一共规划1套FusionAccess，部署图如下：

图表 20 FusionAccess 部署图



ITA部署一台，license服务器部署一台，其他组件单独部署。

每套基础架构组件主要包括：

- WI ：2 台
- DB(SQL server) ：2 台
- DDC 主备 ：2 台
- ITA/WIA ：2 台
- License 日志服务器/鉴证服务器 ：1 台（每朵云配置一台）
- DHCP/DNS/AD ：2 台
- XenAPP DC：2 台
- XenAPP worker：6 台

域名规划：用户访问桌面云主域名、DDC-VDA域名、LOG server域名、VNC LB域名、IT portal。

DG规划原则：每个DG一般创建100台VM。

IT资源规划：

- OU 资源：基础架构服务器 OU 和用户虚拟机 OU
- 域名：系统管理员域帐号、DDC 主机域帐号、SQL Server 主机域帐号、WI 域帐号、ITA/WIA 域帐号、License Server 域帐号、TCM 的管理服务器、日志服务器账号；
- 证书申请：包括 LB 和 AG 、TC/SC 证书
- NTP/DNS/DHCP/win7 激活资源
- 数据库账号：FusionAccess 数据库、ITA 数据库、TCM 数据库

图表 21 FusionAccess 组件的虚拟机的套餐规格

部件部署	磁盘空间	IOPS	VCPU	内存	网卡	系统	备注
WI1+ITA1+DB1+DDC1	30GB+20GB	60	4	8	2	Windows 2008 R2 sp1	主
LOG+LIC+Witness	30GB+20GB	60	2	2	2	Windows 2008 R2 sp1	N/A
DNS1+AD1+DHCP1	30GB+20GB	60	2	2	2	Windows 2008 R2 sp1	主
WI2+ITA2+DB2+DDC2	30GB+20GB	60	4	8	2	Windows 2008 R2 sp1	备
DNS2+AD2+DHCP2	30GB+20GB	60	2	2	2	Windows 2008 R2 sp1	备
TCM	30GB+300GB	60	4	4	2	Windows 2008 R2 sp1	主

系统盘规划：30GB

数据盘规划如下：

- TCM 服务器挂载一个 300GB 的数据盘。
- 其他服务器挂载一个 20GB 的数据盘。

5.6.2 FusionSphere 集群规划

部署一套FusionSphere云平台，一朵云，共一个管理集群，X个用户集群，X个应用虚拟化集群。

管理集群部署如下，FusionAccess基础架构和云平台管理节点全部采用虚拟机部署：

图表 22 管理虚拟机的套餐规格

部件部署	磁盘空间	IOPS	VCPU	内存	网卡	系统
TCM	330	60	4	4	2	Windows 2008 R2 sp1
VRM	50	100	4	8	2	Suse
VRM	50	100	4	8	2	Suse
VRM	50	100	4	8	2	Suse
VRM	50	100	4	8	2	Suse
VRM	50	100	4	8	2	Suse
VRM	50	100	4	8	2	Suse
GM/UHM	280	100	4	8	2	Suse
GM/UHM	280	100	4	8	2	Suse
合计	1440	1160	36	68		

用户集群分布如下：

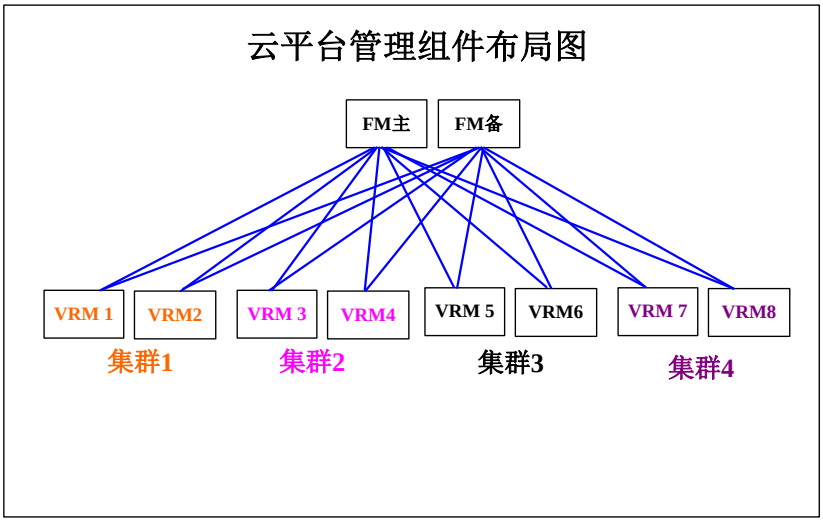
集群1：管理集群

集群2：OA办公用户集群

集群2：开发用户集群

集群4：应用虚拟化用户集群

图表 23 FusionSphere 云平台管理组件布局图

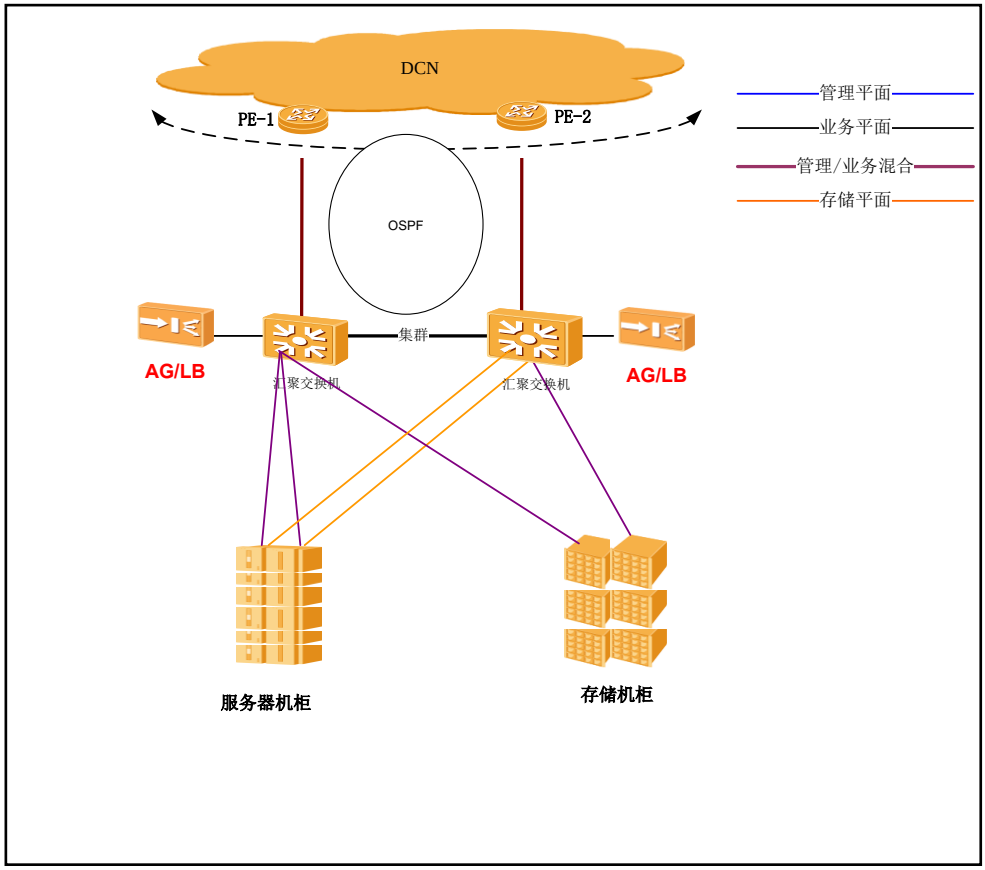


5.7 网络设计方案

5.7.1 桌面云物理组网图

桌面云物理组网示意图如下图所示：

图表 24 桌面物理组网示意图



具体方案说明如下：

所有的服务器同时接入管理、业务、存储网络。

每个桌面云用户可以在办公位上使用TC、或者PC接入到桌面云中心。瘦终端放在每个用户的办公位，每个位子提供百兆或千兆GE网口就可以。

桌面云部署在客户的数据中心机房中；需要与客户的核心交换机对接。考虑后续扩展性，采用2*10GE(请实际项目选择)上行到客户核心交换机。桌面云网络通信平面划分为业务网、存储网和管理网。三个网络之间是隔离的，保证最终用户不能破坏基础平台。

存储网络：存储网络通过多路径确保链路冗余，服务器与存储设备通过存储网络二层直接互通。存储设备为虚拟机提供存储资源，但不直接与虚拟机通信，而通过虚拟化平台转化。

业务网络：为用户提供业务通道，为虚拟机虚拟网卡的通信平面，对外提供业务应用。ICA协议与虚拟机访问外部应用系统都是经过这个网络。各业务部门可以细分VLAN进行访问隔离。

管理网络：负责整个云计算系统的管理、业务部署、系统加载等流量的通信。BMC平面主要负责服务器的管理，BMC平面可以和管理平面隔离，也可以不进行隔离。

服务器采用户GE组网，每刀片采用2个业务与管理网口+2个存储网口方式进行组网，业务、管理平面通过两网口聚合确保链路冗余。

整体网络划分为两层，分别为接入层、核心层。

接入层：

本次采用E6000框式刀片服务器，自带板载接入交换机，在接入交换机划分VLAN，将管理、业务、存储三个平面逻辑隔离。接入交换机再上行汇聚到核心交换机。

核心层：

华为云桌面通过内部的接入交换机汇聚后，接到客户核心交换机。

安全接入：配置SVN安全网关，主要有2个作用，接入负载均衡和安全网关

5.7.2 机柜部署方案

E6000的额定功率大约3900W（配置E5-2690 CPU），目前金融机构的机柜功率为6KW，因此一个机柜只能够部署1框E6000，因此一共配置4个服务器机柜。

图表 25　服务器机柜物理部署图

		服务器机柜 （4*10GE光口+2*GE电口）											
46	1U											1U	46
45	1U											1U	45
44	1U	配线架										1U	44
43	1U											1U	43
42	1U											1U	42
41	1U											1U	41
40	1U											1U	40
39	1U											1U	39
38	1U											1U	38
37	1U											1U	37
36	1U											1U	36
35	1U											1U	35
34	1U											1U	34
33	1U											1U	33
32	1U											1U	32
31	1U											1U	31
30	1U											1U	30
29	1U											1U	29
28	1U											1U	28
27	1U											1U	27
26	1U											1U	26
25	1U											1U	25
24	1U											1U	24
23	1U											1U	23
22	1U											1U	22
21	1U											1U	21
20	1U											1U	20
19	1U											1U	19
18	1U											1U	18
17	1U	Filler Panel										1U	17
16	8U	1	2	3	4	5	6	7	8	9	10	8U	16
15		BH622	BH622	BH622	BH622	BH622	BH622	BH622	BH622	BH622	BH622		15
14													14
13													13
12													12
11													11
10													10
9													9
8	1U	Filler Panel										1U	8
7	1U											1U	7
6	1U	Filler Panel										1U	6
5	1U											1U	5
4	1U	Filler Panel										1U	4
3	1U	Filler Panel										1U	3
2	1U											1U	2
1	1U	Filler Panel										1U	1

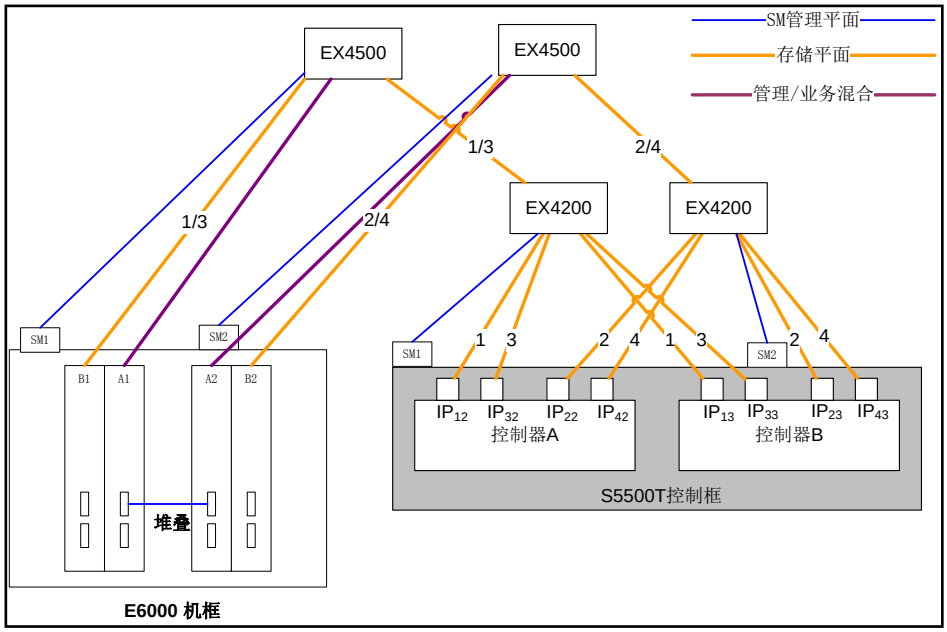
存储方面：一共需要3套S5500T，每套都为1拖2，功率大约1200W，因此存储机柜需要一个。

图表 26　存储机柜物理部署图

		存储机柜(S5500T方案) (2*10GE光口)		
46	1U		1U	46
45	1U		1U	45
44	1U	配线架	1U	44
43	1U		1U	43
42	1U	EX4200	1U	42
41	1U	Cabling Through	1U	41
40	1U	EX4200	1U	40
39	1U	Cabling Through	1U	39
38	1U		1U	38
37	1U		1U	37
36	1U		1U	36
35	1U		1U	35
34	1U		1U	34
33	1U		1U	33
32	1U		1U	32
31	1U	Filler Panel	1U	31
30 29	2U	S5500T（硬盘框）	2U	30 29
28	1U	Filler Panel	1U	28
27 26	2U	S5500T（硬盘框）	2U	27 26
25	1U	Filler Panel	1U	25
24 23	2U	S5500T（控制框）	2U	24 23
22 21	2U	Filler Panel	2U	22 21
20 19	2U	S5500T（硬盘框）	2U	20 19
18	1U	Filler Panel	1U	18
17 16	2U	S5500T（硬盘框）	2U	17 16
15	1U	Filler Panel	1U	15
14 13	2U	S5500T（控制框）	2U	14 13
12 11	2U	Filler Panel	2U	12 11
10 9	2U	S5500T（硬盘框）	2U	10 9
8	1U	Filler Panel	1U	8
7 6	2U	S5500T（硬盘框）	2U	7 6
5	1U	Filler Panel	1U	5
4 3	2U	S5500T（控制框）	2U	4 3
2 1	2U	Filler Panel	2U	2 1

5.7.3 主存储组网方案

图表 27　主存储组网图



说明如下：

E6000 配置4个交换板（机），A1/A2堆叠，管理和业务共用A1/A2，存储单独共用一个平面（B1/B2）。

S5500T一共2个控制器，每个控制出4个业务口，一个管理口。

5.7.4 设备上行接口说明

每框E6000上行4个10GE口+2个GE电口（硬件管理）

每套IPSAN 上行8个GE口+2个GE电口（管理）

鉴于存储机柜上行口太多，至少都是10个端口，一般的机柜不会有这么多光跳线接口。存储机柜配置2台接入交换机。

5.7.5 带宽需求

几种典型应用带宽需求情况如下：

- 空闲：5K～20Kbps;
- Office(Word/Excel)办公应用： 20K～120Kbps;
- Internet /WWW浏览（纯文字）: 50K～150Kbps;
- 呼叫中心客服应用(旁路/分离方案)：100~150 Kbps;
- PPT/图片应用： 200~300Kbps;
- 打印：500~800Kbps;
- 标清视频(320P，原始窗口)： 1~5Mbps；带宽至少按4M算;
- 高清视频(480P,720P,1080P原始窗口)： 2~15Mbps；带宽至少按10M算;

根据客户业务需求、以及业务模型带宽经验值分析，带宽需求分析如下

图表 28 带宽需求表

参数	带宽需求(kbps)	值	备注
空闲	15	20%	表示同时有20%的用户空闲。

参数	带宽需求(kbps)	值	备注
互联网浏览	100	19%	表示同时有29%的用户都会进行互联网浏览操作。
文档编辑	100	40%	表示同时有70%的用户在进行文档编辑。
PPT/图片浏览	250	20	表示同时有20%的用户在进行PPT/图片浏览。
视频浏览	4000	1%	表示1%的用户都在进行视频播放需求。
带宽利用率	-	80%	-

每用户平均带宽需求＝（15kbps*20%(空闲) ＋100kbps×19%(互联网浏览)＋100kbps×40%（文档编辑）＋250kbps×20%（PPT/图片浏览）＋4000kbps×1%（视频浏览））/70%＝218kbps。

也就是金融机构旧大楼办公的用户访问新大楼的桌面虚拟机，总占用带宽约为：218×某某Kbps。

5.7.6 网络 QoS 设计

本项目的虚拟化平台方案设计需要承载网络有一定的带宽保证和基本的QoS保证，确保虚拟桌面OA办公业务的正常使用，虚拟桌面TC—VM之间的网络质量可以分为以下级别:

图表 29 网络质量级别表

网络质量等级	包丢失率	抖动(ms)	单向时延(ms)
良好	≤0.1%	≤5	≤25
一般	0.1%～1%	5～20	25～50
较差	1%～5%	20～60	50～200
特别差	≥5%	≥60	≥200

根据上述表格：

1、OA办公桌面的网络QoS的要求达到时延<25ms，抖动<5ms，丢包<0.1%。

2、在VoIP语音的场景下,网络QoS要求丢包<0.1%、时延<10ms，语音质量PESQ>3.0 语音延时<800ms（TC到TC）。

- 桌面云数据中心内部通过以下方式保证QoS：

二层网络启用802.1P，进行流分类，标识出ICA流量；

启用PQ队列调度，避免拥塞，优先转发ICA流量；

➢ 传输网络需要启用区分服务保证QoS：

根据RDP/ICA的优先级表示，进行不同的DSCP标记，设置为EF或者AF级别，进行优先转发，保证网络拥塞后的RDP/ICA流量优先转发；

➢ 对于TC接入网络，做类似处理，保证接入侧优先级；

二层网络启用802.1P和PQ队列；

三层接入部分采用DSCP区分服务；

5.7.7 网络设备

配置2台Juniper EX4500万兆交换机和2台Juniper EX4200 千兆交换机。

5.7.8 负载均衡与接入网关

结合用户数以及桌面云出口带宽，配置2台SVN5530。

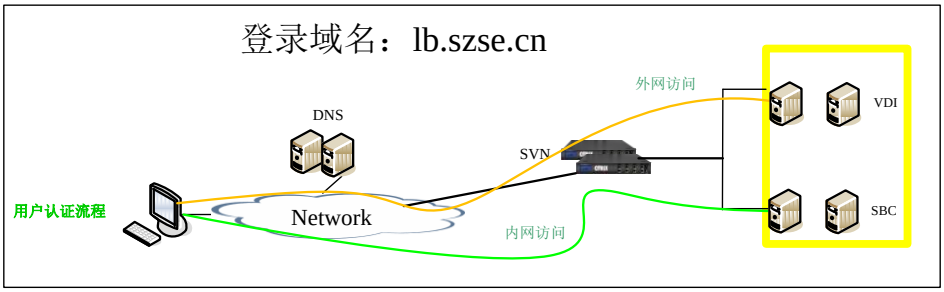
为了实现用户连接负载均衡要求以及接入安全需求，需要配置桌面云网关设备，可以起到下面两个作用：

功能一：网络负载均衡器（LB）：将某一应用的流量根据负载均衡算法重定向到多台WI服务器上，并能监控服务器的可用性；

功能二：接入网关（AG）：集中所有用户的认证、单点登录；负责瘦终端和服务器之间的ICA连接安全，实现ICA Over SSL功能。

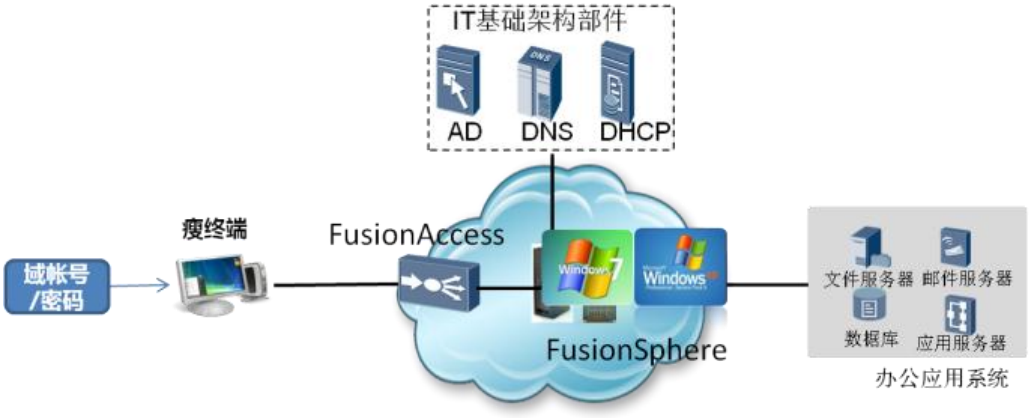
金融机构桌面云采用统一域名，一个入口。所有VDI/SBC应用都共用一个入口。

图表 30 LB 部署图



5.8 桌面云安全接入方案

图表 31 桌面云安全接入组网图



本次金融机构项目桌面云采用AD域帐号+域密码方式进行身份认证。用户输入AD域帐号与密码，登录时到AD服务器进行认证。认证成功即可以进入用户虚拟桌面。在虚拟机里Ctrl+Alt+Del就可以锁屏，输入域密码解锁。

5.9 安全部署方案

为保障数据中心安全，云计算采用了完整的安全架构，避免出现安全真空，强化了网络隔离和虚拟化隔离。此安全架构层面主要采用了分层和纵深防御的思想。

分层防御（Layered Defense）：分层防御旨在采用多种方法，在网络中多个区域执行安全性策略，从而确保网络中没有单点安全故障发生。

纵深防御（Defense in Depth）：纵深防御思想使用多重防御策略来管理风险，以便在一层防御不够时，另一层防御将会阻止完全的破坏。

云数据中心安全框架从分层、纵深防御思想出发，根据网络层次分为物理、主机/虚拟化、网络、业务和数据、管理维护等几个层面，同时整体上考虑满足合规性等需求，用来指导数据中心安全解决方案的部署。

根据云计算面临的威胁与挑战，华为提供桌面云安全解决方案。

华为桌面云从防范非法用户和恶意系统管理员角度进行系统的防范，保证存放桌面云数据中心的数据做到非法用户“进不来”，即使进入系统数据也“拿不走”，即使进入系统机密敏感数据也“打不开”，非法人员作案后“赖不掉”，机密数据“丢不了”。各分层采用安全措施介绍如下：

1. 终端安全

采用精简加固Linux嵌入OS，TC无本地存储，接入桌面云系经时对TC进行合法性认证、TC绑定虚拟机、USB读写禁用可控、802.1X认证防止非法终端接入等方式保证终端安全。

2. 接入与认证管理安全

提供丰富的安全用户身份认证，确保接入用户的合法性。

3. 网络安全

通过VLAN隔离；引入防火墙做ACL访问控制；

客户端用户通过WI登录虚拟桌面时，认证数据采用HTTPS加密传输；

客户端用户通过ICA协议连接虚拟桌面时，桌面访问采用传输加密（ICA over SSL）等手段，保证业务运行和维护安全；

管理员使用Web管理系统时，客户端数据采用HTTPS加密传输。

4. 虚拟化安全

根据虚拟化机制，做到CPU调度、内存、网络访问、磁盘IO、存储空间的隔离，保证虚拟机隔离安全；避免虚拟机之间的数据窃取或恶意攻击，保证虚拟机的资源使用不受周边虚拟机的影响。

5. 数据安全

从数据完整性、身份认证、数据访问隔离控制、数据机密性等方面保证用户数据的安全。系统进行资源回收时，剩余数据清零。

6. 管理安全

用户接入桌面云，在桌面云的接入网关、认证系统和VM都有完善的日志记录，便于追查责任事故。

从帐号、密码、管理员和用户权限、日志等方面日常管理方面安全措施。管理员采用HTTPS加密保证管理访问安全，通过分权分域管理，确认管事员的权限制得制约。

完善的日志审计：各桌面云管理业务Portal、各操作系统、硬件设备都提供完善的日

志，保证所有管理员的操作都有日志记录，供事后审计；

管理员分权分域管理，回收超级管理员权限，通过设置不同权限、不同管理范围的管理员，实现分权分域管理。

7. 基础设施和物理安全

通过操作系统加固、数据库加固、安装安全补丁、防病毒等手段保证基础设施的安全。主要加固措施：关闭不必要的通信端口、服务进程、限制系统访问权限、各账号严格控制权限、开启安全日志审计功能、避免黑客通过漏洞攻击系统。

8. 用户虚拟机安全

在用户虚拟机上部署防病毒软件，防止用户虚拟桌面遭受病毒攻击。虚拟机运行时，可采用PolicyCenter安全系统提供网络访问控制、USB读写加密与管控、员工行为监控、补丁管理、软件分发等功能，保证用户虚拟机运行安全。

5.10 数据迁移方案

桌面云数据迁移方案有2种，一种是文件直接拷贝，另外一种是利用华为的迁移平台进行自动化的数据迁移。

5.10.1 直接迁移方案

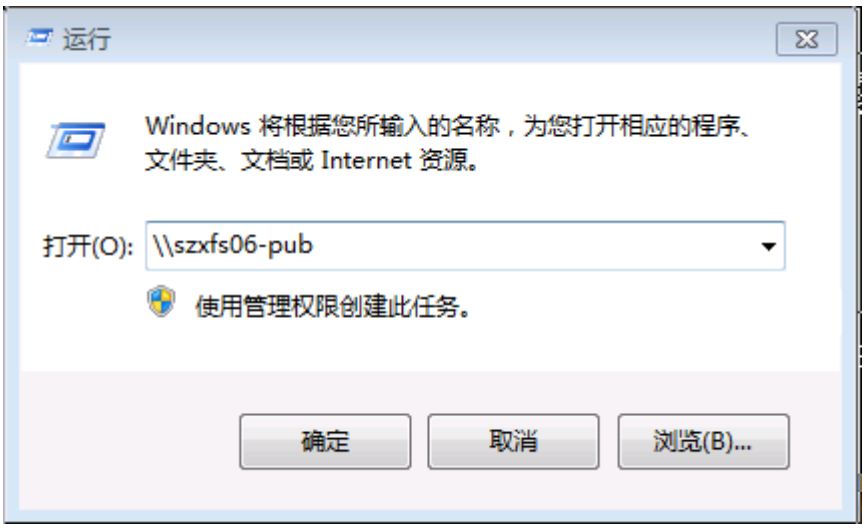
业务数据迁移采取直接迁移的方案，在同一网段下可以直接访问，跨网段需要在路由器上路由，及开放netbios协议端口139和445。

本次为每用户提供了100G的NAS数据盘空间，可以提前做数据迁移。

网络条件具备后，用户就可以自己进行数据文件的迁移拷贝了，详细步骤如下：

- 在 PC 机上通过 IE 登录虚拟机，点击虚拟机开始菜单—>点击运行(输入 cmd)—>弹出的 DOS 窗口中输入 ipconfig，即可看到虚拟机 IP 地址登录虚拟机，查看虚拟机的 IP。
- 在 PC 机上选择“开始”->“运行”（输入：\\NAS 业务 IP 地址或者域名），如下图：

图表 32 办公数据迁移图例 1

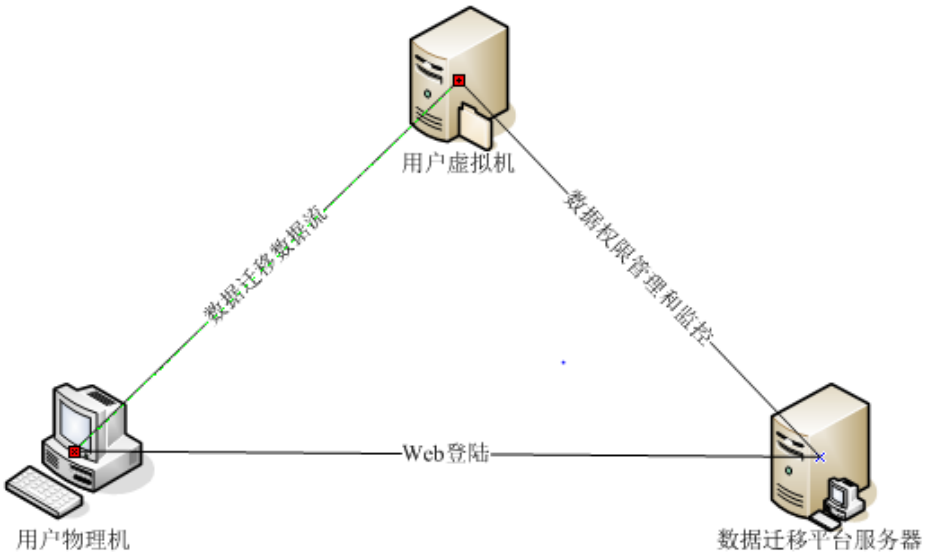


回车，打开虚拟机上的对应磁盘，如果提示输入密码，请输入域账户和密码：

- 将 PC 机上需要拷贝的文件复制（拖动）到虚拟机对应的 NAS 数据盘可。

5.10.2 迁移平台方案

图表 33　迁移平台方案示意图



图表 34 迁移方案示意图

华为公司为了满足大规模用户实现自动迁移，特开发了迁移平台。该平台的主要功能有：支持增量复制、支持断点续传、支持网络QOS控制等等。

此次使用的数据迁移工具使用web服务器的方式支持用户通过web访问的方式管理数据迁移过程，数据迁移平台搭建在Linux操作系统之上，包含Apache、脚本语言PHP、python以及数据库软件Mysql。

数据迁移工具组网由用户PC，数据迁移平台服务器和用户虚拟机组成，迁移的基本过程是：用户使用PC通过web访问数据迁移平台服务器，首先下载并安装客户端软件，然后定制自己的数据迁移任务。

对于直接迁移到虚拟机的场景，数据迁移工具服务器的检测程序，将在用户指定的时间内，向安装在用户PC内的客户端软件发起拷贝指令。客户端软件使用网络文件共享协议（CIFS），将用户数据从个人PC直接拷贝到用户虚拟机，完成数据迁移的自动化操作。在整个迁移过程中，用户可以登录数据迁移平台服务器查看任务的拷贝进度，并完成任务的新增，删除以及反馈问题和意见等操作。

迁移工具主要有三部分组成，在数据迁移平台上部署服务器端，用户PC上部署SpeedMonitor客户端，中转服务器上需要安装相应组件，每一部分的安装要求如下。

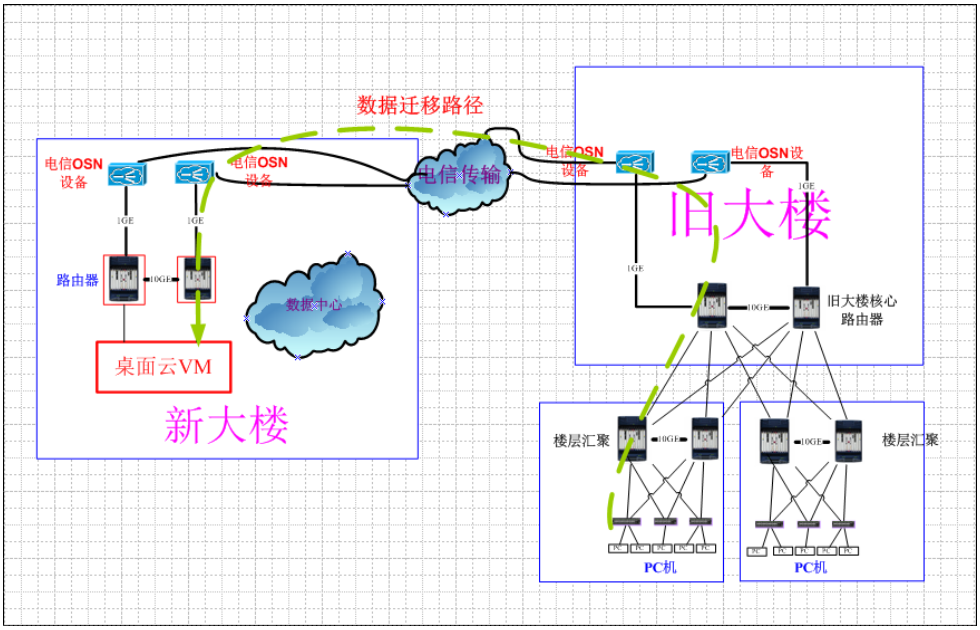
数据迁移平台服务器为linux操作系统，以虚拟机的形式运行，配置4VCPU，12G内存，80GB硬盘，100Mbps网卡等，具体要求见下表：

图表 35 数据迁移平台服务器安装要求

数据迁移平台服务器安装要求	
是否支持虚拟机安装	是
操作系统	linux
CPU	4 VCPU
内存	12GB
硬盘	80GB
网卡	≥100Mbps
其他要求	开启 80 端口提供 http 服务

5.10.3 迁移组网及流量分析

图表 36 迁移物理组网图



说明：

用户物理机在金融机构旧楼，而用户虚拟机和数据迁移平台位于在新楼

用户物理机与数据迁移平台之间的 web 流；用户物理机和用户虚拟机之间的数据流都需要经过承载网传输

数据迁移平台和用户虚拟机之间的监控流只在新大楼的局域网内传输。

5.10.4 迁移模型分析

迁移模型：

- 平均每用户数据：100GB
- 迁移总用户数：1200
- 每月迁移时间：（24*7+8*23）=352 小时（周末全天，平时 8 小时）
- 迁移最大带宽为 10Gbps
- 迁移时间利用率：70%
- 迁移时带宽占用率：70%

则可以计算出迁移的用户数为：

每个月迁移用户数= 352*0.7*3600*0.7*10*1000/(100*1024*8)=7579 人，大约每周迁移1900人，仅考虑流量，初步估算，1200人大约需要1周时间。

5.11 高可靠性方案

桌面云平台通过在系统的各个层面采用相应的可靠性技术来保障业务提供的可用性，具体来说，包括：

5.11.1 服务器可靠性设计

服务器可靠性包括内存、硬盘、电源等多个层面的内容。

- 提供BIOS内存自检和ECC纠错技术。

- 支持硬盘热插拔和RAID功能，提供硬盘在线故障检测和预警。
- 支持电源1+1冗余和热插拔。
- 支持对CPU，内存，风扇，电源，硬盘等热关键器件的温度实时监控，设备故障时会产生告警，可以灵活对支持热插拔设备进行在线更换，不支持热插拔设备提前安排好业务后进行下电更换。配合智能的风扇调速和监控，确保系统运行的可靠性。
- 多台服务器组成计算资源池，支持虚拟机的热迁移、HA功能。

5.11.2 存储可靠性设计

- 存储多路径

每个计算节点与存储集群之间，至少配置两个完全冗余的路径，从而提供存储的多路径访问功能。多条路径间的故障切换由软件自动提供，从而避免单点故障带来的存储访问问题。

- 存储数据的冗余备份

采用SAN作为存储设备，在SAN高可靠性的基础之上，配置热备盘做冗余备份，保证数据不丢失和故障快速恢复。

- 存储冷迁移

在虚拟机关机情况下，通过管理员手动操作，将虚拟机的卷迁移至其他的存储单元中，可以在同一个VRM管理下的同一个存储设备内，不同存储设备间，块设备和存储虚拟化之间进行迁移。

- 存储热迁移

在虚拟机正常运行时，通过管理员手动操作，将虚拟机的卷迁移至其他存储单元中，可以在VRM管理下的同一个存储设备内、不同存储设备间，块设备和存储虚拟化之间进行迁移。

- 存储动态资源调度(DRS：Dynamic Resource Scheduler)

在存储热迁移的基础上，可以进一步提供存储DRS功能。虚拟化平台通过相关的数据采集（数据存储的空间使用率和IO延时），并制定采集的数据制定相应的存储自动调度计划，以保证业务连续性的情况下根据设置的参数来实现存储资源的合理调度，使得集群下的存储资源在使用率和IO性能上达到一定的均衡优化效果。

5.11.3 网络可靠性设计

- 网络路径全冗余

核心层交换设备通过使用交换机集群技术，保证对外与防火墙/NAT和对内汇聚交换机连接的冗余。

汇聚层交换设备通过使用交换机集群技术，保证对外与核心层交换设备和数据中心内接入层交换机连接的冗余。

接入交换机通过使用交换机堆叠技术，保证对外与汇聚层交换设备和对内虚拟网络层连接的冗余。

虚拟网络层通过采用多网卡绑定等技术避免单个网卡故障引发的业务中断。

- 网络分平面通信

系统通信平面划分为业务平面、存储平面和管理平面。为了保证各种网络平面数据的可靠性，不同平面间采用VLAN等技术进行隔离，单个平面故障不影响其余两个平面的正常工作。

业务平面：主要为虚拟机虚拟网卡的通信平面，对外提供业务应用。

存储平面：主要为iSCSI存储提供通信平面，并为虚拟机提供存储资源，但不直接与虚拟机通信，而通过虚拟化平台转换。

管理平面：负责整个云计算系统的管理、业务部署、系统加载等流量的通信。

- 网卡负荷分担

对于各通信平面（业务、存储、管理）均采用双网卡，双网卡采用了Bonding模式，两网卡被绑定成逻辑上的“一块网卡”后，同步一起工作。既能对服务器的访问流量进行负荷分担，又能保证其中一块发生故障的时候，另外的网卡立刻接管全部负载，过程是无缝的，服务不会中断。

5.11.4 虚拟化可靠性

- 虚拟机热迁移

提供虚拟机的自动迁移和手动迁移方案，当前计算节点出现故障或者计算节点负载过高时，可以把虚拟机迁移到正常的计算节点或者负载相对较低的计算节点上，保证虚拟机的正常运行。

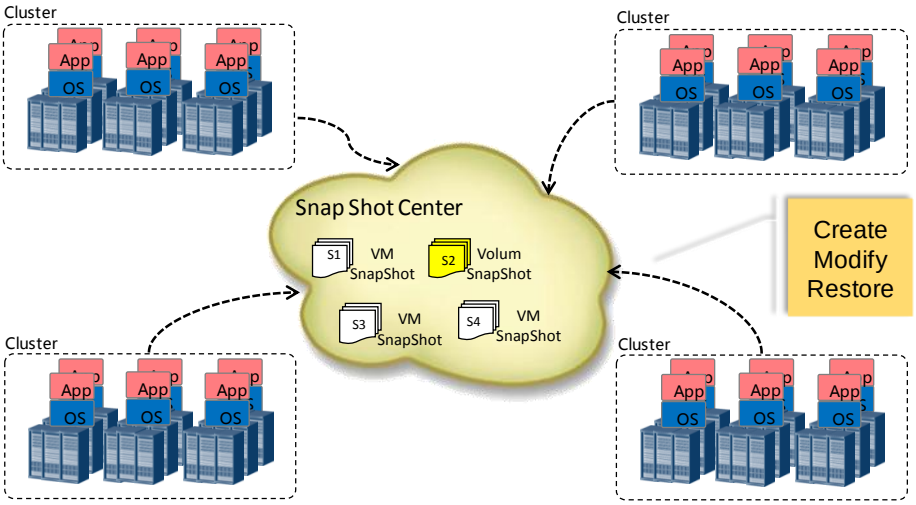
- 虚拟机HA

虚拟机高可用性（HA）是虚拟机的一个特性，当虚拟机所在的物理服务器故障（如宕机、掉电等）或重启后，虚拟机可以自动在其他物理服务器上运行，保证虚拟机能够快速恢复，它可以保护用户的业务程序对外提供不间断的服务，把因软件/硬件/人为造成的故障对业务的影响降低到最小程度。

- 快照

系统提供虚拟机、卷快照功能，系统正常状态下，可以触发一个系统快照，用于在系统出现故障的时候还原系统。

图表 37 虚拟机、卷快照示意图



5.11.5 管理可靠性

- 配置数据自动备份

桌面云提供管理系统配置数据自动备份机制，在系统配置数据意外损坏或丢失时，可快速恢复备份的系统配置数据，尽快恢复桌面云系统的正常运行。

- 计算和存储集群分离

通过采用计算集群和存储集群相分离的架构，提升系统的可靠性。计算集群完成虚拟机的按需分配以及集群内的热迁移，存储集群完成虚拟机的系统卷和用户卷的按需分配以及跨磁盘的存放。

- 管理节点HA

管理软件均采用1+1备份或负载均衡的方式运行。当一个管理节点的软件出现故障的

时候，系统自动切换到备用节点，保证整个系统不间断运行。

- 故障检测

华为虚拟桌面系统提供了一个故障信息收集和存储集群节点可用性度量的功能，同时它包括了在Web浏览器中显示这些数据的工具，一旦集群进入正常状态，系统提供使用数据可视化工具观察集群管理和分配负载的功能，这可以帮助用户确定是否有负载均衡问题、失控进程或硬件性能下降的趋势，将对合理调整、分配系统资源，提高系统整体性能起到重要作用。历史记录允许你查看集群每日的、每周的，甚至是每年消耗的硬件资源。

通过在每个被监控的节点上运行探针程序，华为虚拟桌面系统可以收集它运行的机器的核心指标如CPU使用情况、基础网络流量和内存数据等，检测到诸如进程崩溃、管理和存储链路异常，节点宕机、系统资源过载等各种异常，使系统具备完善的故障检测能力。

- 黑匣子

管理节点和计算节点引入电信领域“黑匣子”技术，在系统出现异常时自动存储内核日志、系统快照、内核诊断信息及临终遗言，并保存至非易失性存储设备（计算节点）或自动传送至网络服务器（例如日志服务器），以便系统故障后，导出分析定位。

- 数据一致性审计

系统提供数据一致性审计功能，定时审计VM及其卷文件的相关数据和状态的一致性。当发现有异常的时候，会自动记录下来，以便维护人员做相应的判断和恢复措施，从而保证了系统内部各种相互关联的数据的一致性。

5.12 系统扩容方案

5.12.1 集群内主机可扩展性

桌面云平台中每个FusionManager最大支持256个VRM集群，4096个主机服务器、8000个虚拟机支持。每VRM集群支持的服务器数量最大可达到256台，每VRM集群支持32个HA资源池。每HA资源池内支持的服务器数量最多可扩展至128台服务器，可轻松满足未来桌面的平滑扩容需求。

单用户可扩展性设计：单用户支持vCPU个数最大可以扩展到64个，内存可以扩展到1024GB，支持的虚拟网卡数最多可以支持8个，可充分满足虚拟机规格的弹性伸缩。

5.12.2 虚拟桌面管理节点可扩展性

虚拟桌面管理节点可分布式平滑扩展。一套虚拟桌面最大支持5000桌面用户，当超过5000用户容量后，需要新增加一套虚拟桌面管理节点，虚拟桌面管理节点之间属于分布式，相互之间完全独立。

5.12.3 存储扩展性

根据存储需求增长，可以实现存储在线平滑扩容，根据规划可以在线扩展磁盘、磁盘框、控制框。

5.12.4 虚拟桌面/虚拟应用扩展

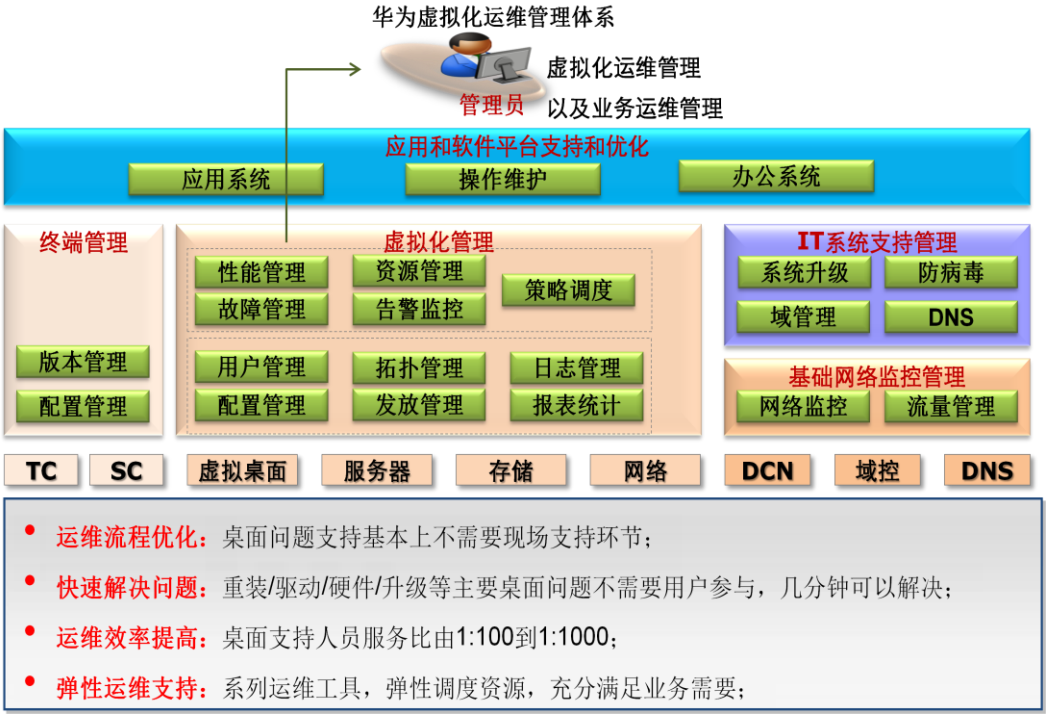
在桌面云平台中，一个用户既可以单独拥有虚拟桌面功能，或单独拥有虚拟应用的功能，同时有可以同时拥有虚拟桌面和虚拟应用的功能。针对适合在虚拟桌面的应用，可以由虚拟桌面扩展到虚拟应用的方式使用。也可以将在虚拟应用方式下的所有应用全部转换到虚拟桌面方式下使用。

5.13 运维管理方案

5.13.1 总体架构

华为桌面云运维服务管理，基于B/S架构，提供远程集中运维管理，全中文界面。华为运维管理参考ITIL标准，基于统一维护，可运营、可管理的理念，设计了符合虚拟化产品特点，易运维的管理系统。支持友好的WebUI维护界面，统一管理所有硬件资源与虚拟化资源，VDI桌面，提供基于定制化策略的自动化运维系统。运维系统架构如下：

图表 38 华为虚拟化桌面运维体系



桌面云系统运维和维护管理主要由“FusionSphere运维管理系统”提供，“桌面云业务维护系统”提供部分辅助功能。运维系统基于Web架构，用户可通过IE、Firefox浏览器访问，无需安装本地客户端。

图表 39 虚拟桌面维护系统登陆页

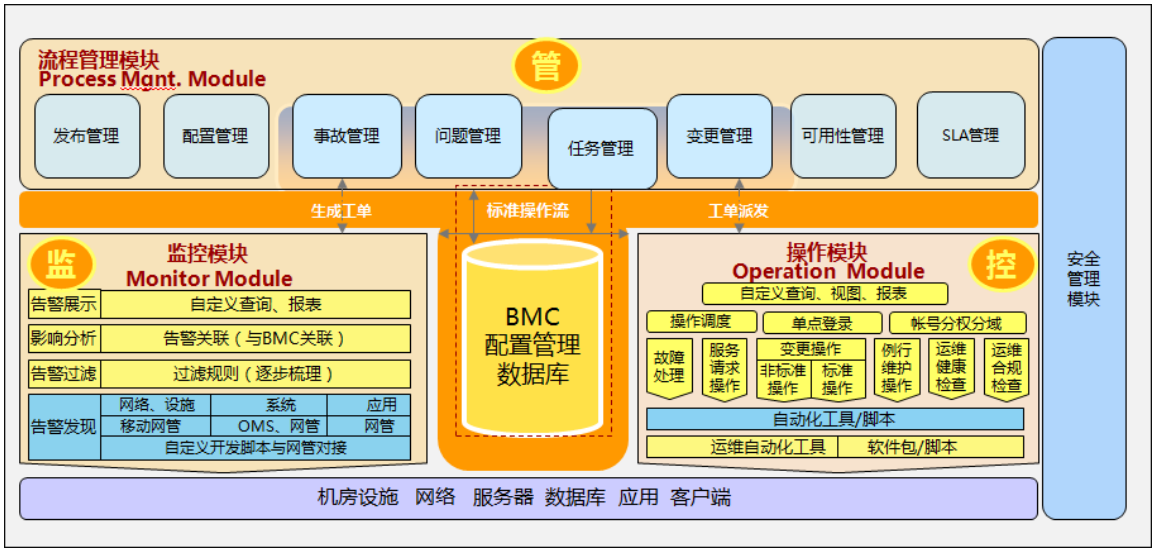
图表 40虚拟桌面维护系统主页

5.13.2 运维对接方案

桌面云需要纳入金融机构IPolicyCenter管理系统，实现IT维护的可视化、可控化、自动化。如下图所示：

桌面云所属的机房设施、网络、服务器、数据库、应用及客户端统一纳入金融机构的IPolicyCenter管理系统。

图表 41 运维对接方案



a) 桌面云需要加入 IT 管理系统（IPolicyCenter），主要有配置管理，变更管理，可用性管理，SLA 管理，资产管理，问题管理等。要求桌面云可以提供北向接口（标准 REST 或 SOAP 接口），将监控和告警信息通过相关北向接口上报给 IPolicyCenter 系统。

b) IT 管理系统从桌面云平台运维管理系统上，通过 FTP 下载日志文件(用户访问日志、操作日志、事件告警日志、系统运行日志（syslog）、审计日志等)。管理员在 IT 服务支撑平台上查看日志。

c) 桌面云管理服务器、Hypervisor 主机、IPSAN 管理及 BMC 带外管理均在管理网内部，与业务网的边界采用防火墙隔离。

d) 桌面云使用的所有硬件（服务器、存储、网络、安全网关等）都支持标准的监控接口，比如 SNMP、IPMI 等等，可以直接将监控和高级集成到现有的 IPolicyCenter 系统中。

e) 厂家提供统一的监控和告警平台，可以实现桌面云后台系统所有软硬件的一体化监控和告警

f) 监控策略及过滤：

服务级别：0级运维人员提供7*24服务，收到告警邮件后电话知会1级运维人员。

监控周期：每5分钟轮询1次，2次失败后即告警。

告警邮件：3级以上告警参数发给0级运维人员，3级以下直接发给一级运维人员。

5.13.3 桌面云运维团队

如下图所示，桌面云运维团队分成4个等级：

0级：IT热线，一般外包承担，主要工作是负责处理用户的问题及投诉，可以解决一般的桌面云常见用户问题，可以查看一般的监控告警邮件，一旦有重大告警或集中的用户问题反馈或投诉，需要及时发邮件或打电话给一级运维人员，一般工作8小时（上班时间），同时至少需要安排一位运维人员值晚班（主要负责下班时间紧急的系统告警和用户问题）。

一级：IT运维人员，主要负责解决0级技术支持上报的用户问题处理，包括

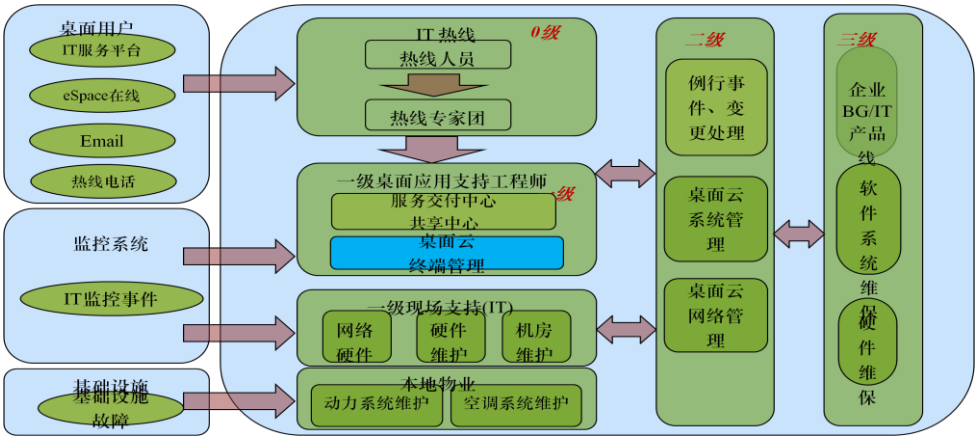
日常的硬件维护（机房维护、硬件维护、网络硬件维护），同时负责日常

的监控及告警处理，负责日常的系统升级或扩容，一般要求24小时响应

二级：原厂技术服务支持，主要处理IT运维人员上报的疑难用户问题或产品问题，协助客户进行系统升级或扩容，一般要求24小时响应，对于重大问题，要求4小时内到现场支持。

三级：原厂研发支持，主要处理原厂服务人员无法快速解决的疑难产品问题或用户问题，同时需要支持现场紧急问题处理和定位，提高问题处理效率，减少业务中断时间，一般要求24小时响应，对于重大问题，要求2小时内到现场支持。

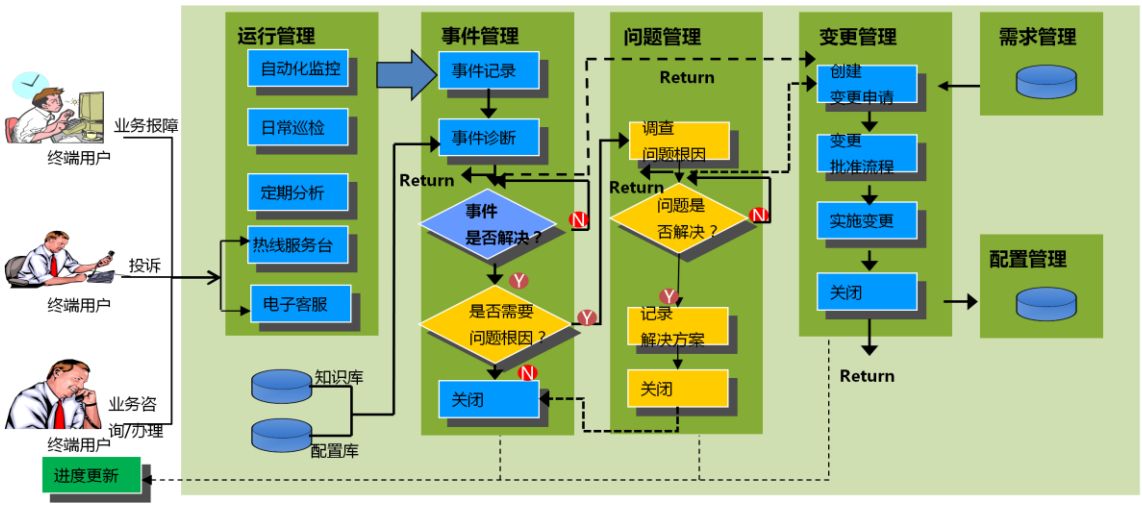
图表 42桌面云运维等级



5.13.4 桌面云运维流程

桌面云运维支持标准的ITIL流程，如下图所示：

图表 43 桌面云运维流程



所有用户业务报障、投诉、业务咨询可以通过IT热线、电子客户等多种途径上报。

单一云管理平台可以实现对所有软硬件进行日常自动化巡检、自动化监控、自动化告警。

所有的桌面云事件记录、配置信息（CI）、知识库、事件诊断都必须纳入CMDB数据库。

桌面云必须纳入所有的事件管理、问题管理、变更管理和需求管理的ITIL标准流程

中。

5.13.5 运维解决方案特点

华为FusionAccess的统一资源发放WEB PORTAL，业务发放更灵活、更高效。强大的OM运维能力，支持用户分权分域管理，安全性高。管理员可通过Portal快速地进行业务发放、桌面管理、模板管理、权限管理、资源管理、监控管理、告警管理、拓扑管理、日志管理、任务管理、统计管理。

管理员登录支持SSL、数据加密、用户密码加密保存，确保用户数据安全。

桌面管理支持虚拟桌面生命周期管理、快照、使用快照创建虚拟机和恢复虚拟机。为用户数据提供备份功能。

拓扑管理能让管理员非常直观地看到系统的部署情况、运行情况。

告警管理支持告警转E-Mail、短信的即时通知，使用户及时了解系统。

日志管理支持操作日志、运行日志记录，便于审计和故障处理。FusionAccess支持集中日志，用户桌面日志、管理日志进行集中收集和分析；

统计管理支持灵活配置、报表统计分析。

桌面云系统支持软件HA，高可靠性，减少故障对系统和业务的影响。

支持系统配置自动备份，避免系统数据丢失。

支持动态节能，例如：虚拟机长时间未用则自动休眠、用户再次使用时自动恢复虚拟机使用；虚拟机自动调度包括定时迁移关闭启动虚拟机、将虚拟机集中运行在某些服务器并下电其他服务器。

5.13.6 虚拟桌面管理

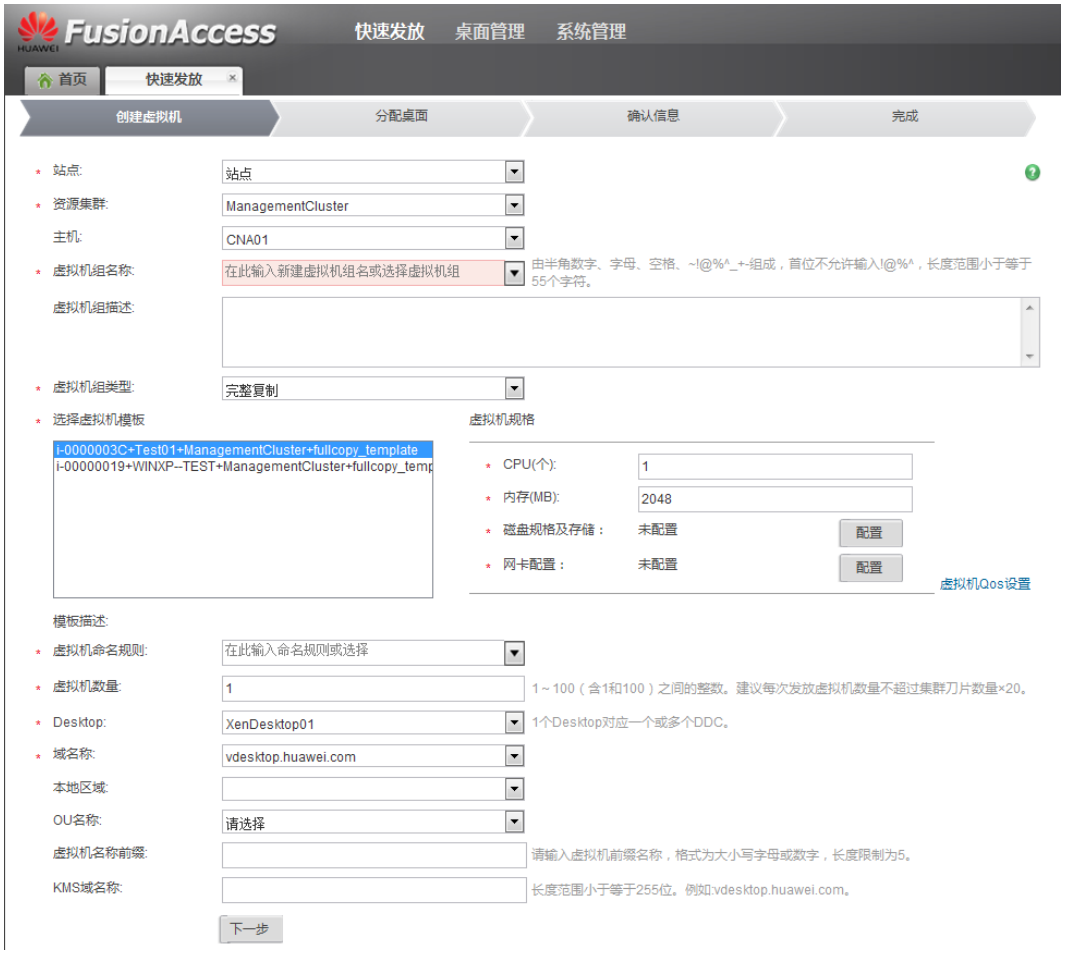
虚拟桌面运营管理由FusionAccess提供，该系统基于Web架构，用户可通过IE、Firefox浏览器访问，无需安装本地客户端。并且支持管理员分级分域管理。

- 虚拟机发放

管理员可以Portal发放裸虚拟机，完整复制，链接克隆虚拟机。

支持虚拟机的单个发放或批量发放。批量发放可以发放给一批人，批量创建后的虚拟机有系统盘、用户盘，关联到AD域帐号。如下图是批量发放虚拟机截图。

图表 44　虚拟机发放界面



虚拟机发放给用户即绑定用户，只有绑定用户才能访问虚拟机。支持发放时自动绑定、手动绑定。

一个虚拟机可以绑定给一个用户，也可以绑定给多个用户。多个虚拟机组成的资源池，可以共享绑定给多个用户。适用于多种用户场景，例如个人办公虚拟机则一一绑定，公用虚拟机则一对多或多对多绑定。

桌面管理应用于用户进行虚拟桌面的发放和维护场景。用户通过桌面管理主要完成以下三大维护管理模块：

➢ 虚拟机管理

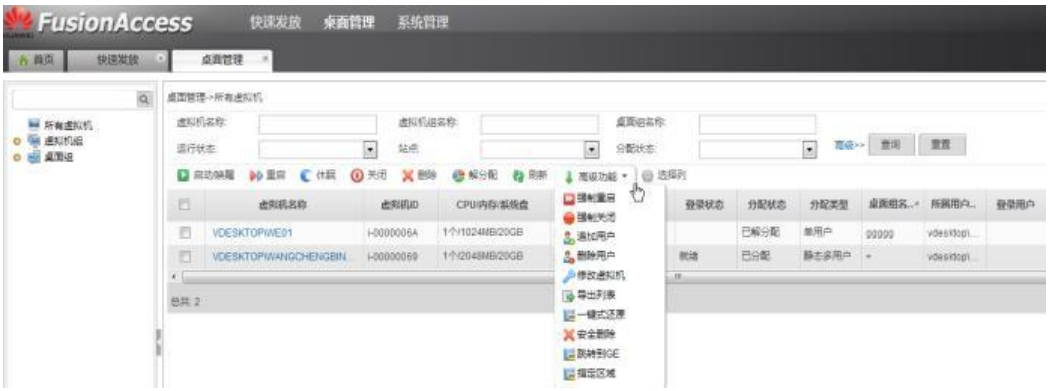
该模块可完成虚拟机的启动/唤醒、重启、休眠、关闭、删除、解分配、以及高级功能（强制重启、强制关闭、追加用户、删除用户、虚拟机配置调整、链接克隆虚拟机一键还原、安全删除）等操作。

修改虚拟机可以修改虚拟机的业务类型、CPU、内存以及描述。

一键式还原针对链接克隆虚拟机，强制还原虚拟桌面系统到初始状态。

安全删除功能把虚拟机删除后，但磁盘空间不会立即可用，会在后台进行磁盘空间的清“0”处理，磁盘空间清“0”后会自动加入可用的存储资源池。

图表 45　虚拟机管理界面



➢ 虚拟机模板和镜像管理

支持虚拟机模板的创建、修改、删除、查看。虚拟机模板参数包括：虚拟机规格（CPU、内存、系统磁盘大小）、镜像、虚拟机QoS（是否HA、服务质量级别）等。

➢ 虚拟机组管理

每个虚拟机都必须归属于某个虚拟机组。该模块可完成虚拟机组的创建、编辑、删除、添加虚拟机、更新链接克隆组软件以及一键式还原。

➢ 桌面组管理

每个虚拟桌面都必须归属于某个桌面组，该模块可完成桌面组的创建、编辑、删除、分配虚拟机、批量分配虚拟机以及一键式还原。

5.13.7 权限管理

权限管理可以创建和管理FusionAccess系统中管理员帐号、管理员所承担的角色和管理员管理区域，实现FusionAccess系统的分权分域的功能。FusionAccess系统支持对用户进行访问控制，支持用户组、分权、分域、密码管理，便于维护团队内分职责共同有序地维护系统。

➢ 帐号管理

创建、修改、删除管理员帐号；修改管理密码。

图表 46　用户管理界面

➢ 角色管理

角色指具有相同分权功能的管理员分组。管理员可以按实际需要创建相应的角色。缺省的角色包括：

超级管理员：具有全部操作维护权限和管理其他用户的权限。

操作维护管理员：具有超级管理员授予的操作和查看权限。

只读管理员：具有超级管理员授予的查看权限。

图表 47　角色管理界面

➢ 分域管理

监控功能支持对操作维护管理员和只读管理员用户进行分集群域的授权管理。

用户分域管理：授予用户各自的集群权限。集群可对应不同部门（如营业厅、客服中心）、不同地区（如东城区、西城区）的虚拟桌面。分域管理员仅对属于自己管理范围的虚拟桌面具有管理权限，包括虚拟机的查看、分配、回收、登录、关闭、重启等。

➢ 密码管理

支持设置密码策略，确保密码的保密性。密码策略包括：密码长度、密码是否含特

殊字符、密码有效时长、密码到期提前多长时间提醒用户、修改密码时不允许使用最近几次的密码、是否强制用户第一次登录时修改密码等。

虚拟机用户账号管理采用AD的方式管理，包括创建域用户账号、域组用户账号、用户漫游及强制配置文件等。

5.13.8 软件管理

软件系统包括：云平台系统软件、桌面接入系统软件、用户虚拟机软件。为了方便客户管理软件，软件系统具有如下特点：

- 软件预安装和预置

发货前，桌面接入系统及操作系统补丁，已预置在基础服务器镜像中，在现场可直接快速创建虚拟机。

用户虚拟机支持将用户应用软件预置到虚拟机模板中，使用虚拟机模板安装虚拟机。

- 软件自动化批量安装

云平台软件：支持统一安装界面，一次性导入所有服务器的信息，多节点同时加载安装，安装效率高。

桌面接入系统软件：支持统一安装界面，便于安装管理。

用户虚拟机软件：通过虚拟机模板方式，创建虚拟机并安装应用软件，且支持批量创建虚拟机，大大减少了用户操作和操作难度。

- 升级、打补丁及回退自动化

云平台软件支持升级、打补丁有工具支撑，实现了自动化健康检查、分发软件、升级/打补丁、校验、回退。且支持静默升级，即升级/打补丁不影响业务。

- 用户虚拟机软件管理集中化

支持使用工具快速将用户数据从原来的物理机迁移到虚拟机、虚拟机间数据迁移。

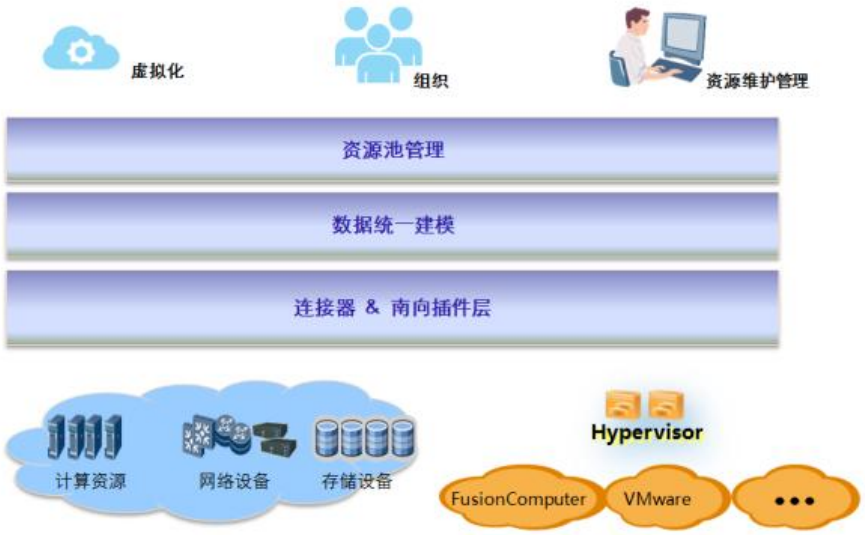
用户虚拟机操作系统，通过补丁服务器打补丁，方便安全。

通过AD域控管理用户虚拟机的应用软件，具有准入控制、安全策略管理、员工行为管理、软件分发功能。

5.13.9 资源管理

FusionManager云管理平台，通过对各种物理资源、虚拟化资源数据统一建模，将资源以用户可见的资源池形式提供给上层应用。

图表 48　统一资源管理模型图



统一资源管理，支持发现其管辖范围内的物理设备（包括机框、服务器、存储设备、交换机）以及它们的组网关系。支持将这些物理设备进行池化管理，提供给应用管理模块使用。对于虚拟化一体机场景支持自动发现物理设备，基础设施虚拟化场景需要手工导入物理设备，对服务器、存储设备和交换机进行集中管理，对物理资源进行池化管理，给上层的业务发放屏蔽物理设备的差异。

虚拟化资源管理可以统一管理不同系统提供的不同的虚拟资源，包括虚拟机资源、虚拟网络资源、虚拟存储资源的管理等。

通过资源池管理，提高基础设施资源的利用率和灵活性，提供统一的虚拟化资源管理能力，对上层应用发放屏蔽差异；实现虚拟资源集中管理提升管理效率，降低运维成本。

采用南向插件机制，使FusionManager可以快速、便捷、可定制的实现不同硬件和虚拟化系统的对接。

➢ 物理资源管理

对于华为自研的物理设备可自动发现； 第三方厂家设备支持单条设备接入或批量设备接入。

服务器资源管理能够发现服务器的配置信息，可以实现服务器的监控，监控信息包括CPU占用率，内存占用率，网络流出、流入，磁盘I/O写入、读出，可以按周、月、年及自定义时段查询性能监控结果。服务器设备的维护能力：上电，下电，安全重启，安全下电，强制下电，进入维护模式，退出维护模式，一键式上电、下电所有服务器；

网络设备管理能够发现交换机的配置信息，显示交换机端口的连接状态，状态信息包括连接与否、发送、接收速率，发送、接收丢包率，发送、接收错误率。另外还可以对本系统的网络模式及网络配置进行管理。

存储设备管理能够发现存储设备，查看存储设备的配置信息，信息包括存储设备位置，产品型号，状态，管理IP地址，磁盘数量。可以查询存储设备的总容量和可用容量，以便用户知道是否要扩容存储设备。支持IP SAN、FC SAN、NAS、服务器本地存储。

资源集群管理，集群的创建、删除、扩容、减容，对集群进行性能监控，配置集群的资源调度策略，调度策略可以设置为手动和自动，实现虚拟机根据系统负荷在不同服务器上迁移。

图表 49　物理设备资源管理

➢ 虚拟资源管理

虚拟化资源管理支持对计算虚拟化、网络虚拟化、存储虚拟化的管理。

虚拟机生命周期管理：业务管理员通过应用对虚拟机进行创建、销毁操作，对虚拟机的日常维护包括：启动、重启、迁移、关闭、修复、快照、虚拟机资源调整和监控；

虚拟化网络管理：虚拟网络管理负责管理系统的虚拟交换机及虚拟交换机分配的子网。虚拟网络对应的是DVS(分布式虚拟交换机)和PortGroup（端口组）。分布式虚拟交换机支持系统管理员对一至多台主机上的虚拟交换机的上行链路和虚拟端口进行配置与维护。对子网、VLAN和端口组的管理；可对端口组进行限速设置、上限带宽、优先级和DHCP隔离配置。

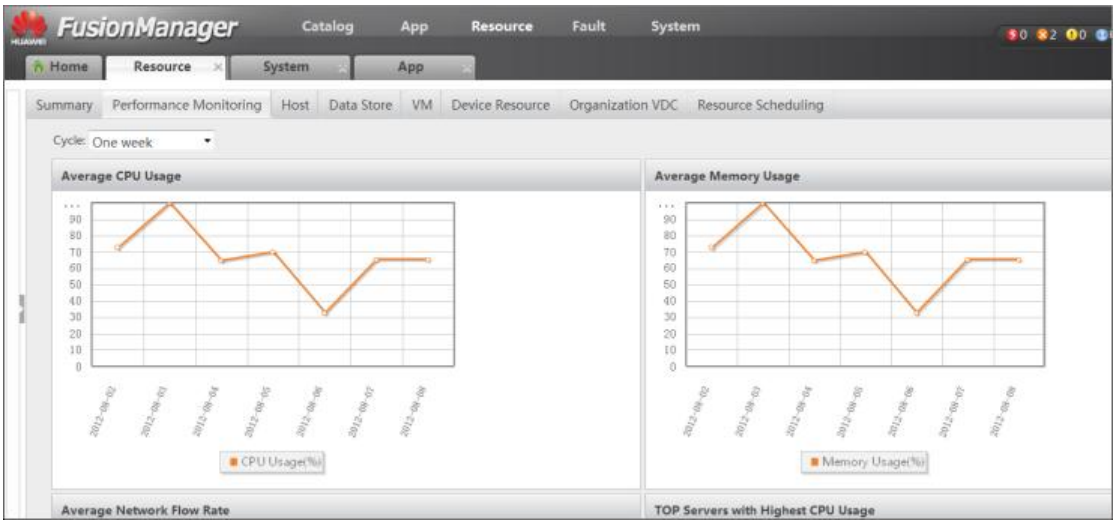
虚拟化存储管理：可以管理IP SAN、FusionStorage、FC SAN、NAS上的存储资源，以数据存储为单位分配给资源集群使用。数据存储是虚拟机卷所在的存储空间，其对应的物理概念是：SAN的存储资源池、FusionStorage的内部资源池。

可以向存储资源池中增加、删除数据存储，已经存在的数据存储可以进行扩容。支持多级存储

图表 50　虚拟化资源管理

5.13.10 监控管理

图表 51 监控管理



监控主要针对云平台、计算集群、计算服务器、虚拟机、存储、交换机等进行监控。

云平台的监控信息包括：云的整体CPU平均占用率、内存平均占用率、存储平均占用率、故障服务器数量、虚拟机CPU分配情况、虚拟内存分配情况、存储资源分配情况等。

计算集群的监控信息包括：计算集群的CPU平均占用率、内存平均占用率、故障服务器数量、虚拟机CPU分配情况、虚拟内存分配情况等。

计算服务器的监控信息包括：服务器的CPU占用率、内存占用率、虚拟机数量、服务器基本信息、虚拟机CPU分配情况、虚拟内存分配情况等。

虚拟机的监控信息包括：虚拟机的CPU占用率、内存占用率、磁盘读写次数、网络流入流出流量、状态等。

网络交换机监控：监控信息包括流入流出速率、端口信息状态、端口数据流量等信息。

存储监控：监控信息包括存储的总容量、已分配容量、实际可用容量等信息。

总之，监控主要分为：硬件部分和软件部分。

1、硬件部分监控

服务器（状态、CPU、内存、磁盘、网络连接）

存储（磁盘状态、网络连接）

交换机（端口状态、流量）

接入网关（端口、流量）

接入终端（TC状态、CPU、内存、磁盘、文件系统）

2、软件部分s

FusionSphere系统软件（软件进程状态、性能）

FusionAcess系统软件（软件进程状态、性能）

接入网关软件（软件进程状态、性能）

TC终端软件（软件进程状态、性能）

虚拟机（状态、CPU、内存、磁盘、文件系统）

3、系统提供的对外监控接口包括：

SNMP ：网络、存储等硬件设备

SOAP 协议接口：虚拟机。

5.13.11 告警管理

图表 52 告警管理操作界面

“FusionManager故障管理”模块，提供了云平台系统管理功能。“FusionAccess系统告警”模块，提供了桌面云系统管理功能，便于运维人员进行故障定位，保证系统稳定运行。故障管理是确保系统正常运行的重要活动，包括：系统故障预防设计、故障检测和处理。告警管理是故障管理的重要部分。

- 系统故障预防设计

系统设计时，考虑到部件故障时的系统自动处理，确保故障不影响系统正常运行和业务正常使用，降低了故障危害。包括：

硬件RAID、硬件HA和软件HA。

系统数据自动备份、用户数据备份容灾方案。

虚拟机HA、虚拟机快照、虚拟机迁移、存储迁移。

故障处理时，支持对故障服务器进行隔离，避免业务消息发到故障服务器。

- 故障检测和处理

系统支持故障的自动检测，及时上报告警。告警管理具体如下：

告警对象：硬件、虚拟桌面软件、虚拟机。

告警级别：支持四种告警级别，标识不同严重程度的告警。

告警的声光显示：根据用户的设置，云管理可通过不同的声音、颜色标识不同级别的告警，呈现给维护人员。

告警查看：支持活动告警浏览和历史告警查询。通过设置浏览参数，管理员可以实时监控自己关注的活动告警，例如查看“重要”级别的实时告警。

Email和短信通知告警功能：告警产生和恢复时，系统会自动给运维人员发Email和短信，及时告知。通过订阅重要的告警，实现在无人值守的环境下，仍能实时掌握全网节点的运行状态。

告警阈值可配：管理员可根据实际情况，配置告警阈值。

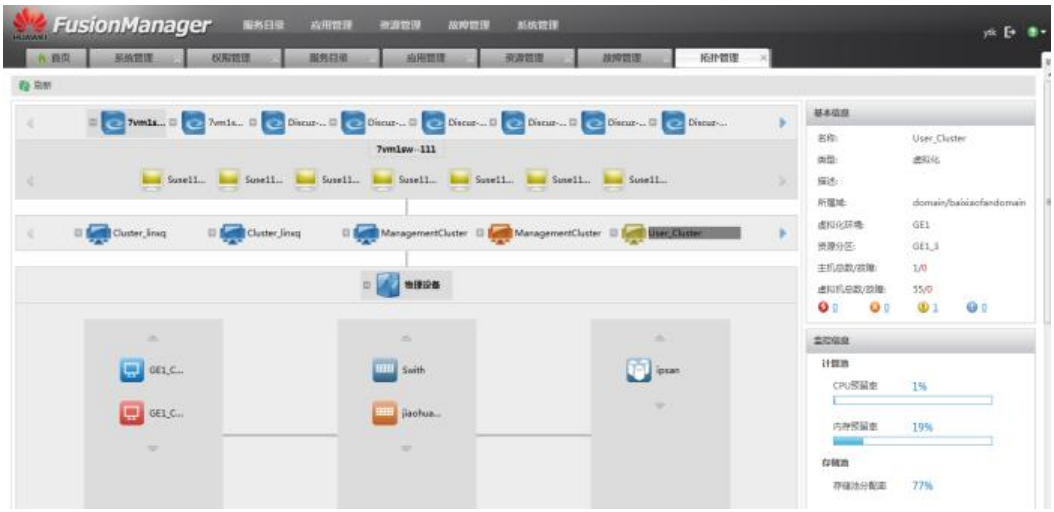
告警北向接口：云管理提供标准的告警北向接口能力，供上层网管对接。

支持第三方设备告警接入到云平台管理系统。

5.13.12 拓扑管理

拓扑管理提供一个可视化界面，呈现全系统的所有资源信息，无需管理员手动干预。拓扑图整体上分为三个层次：物理资源视图、集群视图和应用视图以及层间关联关系。

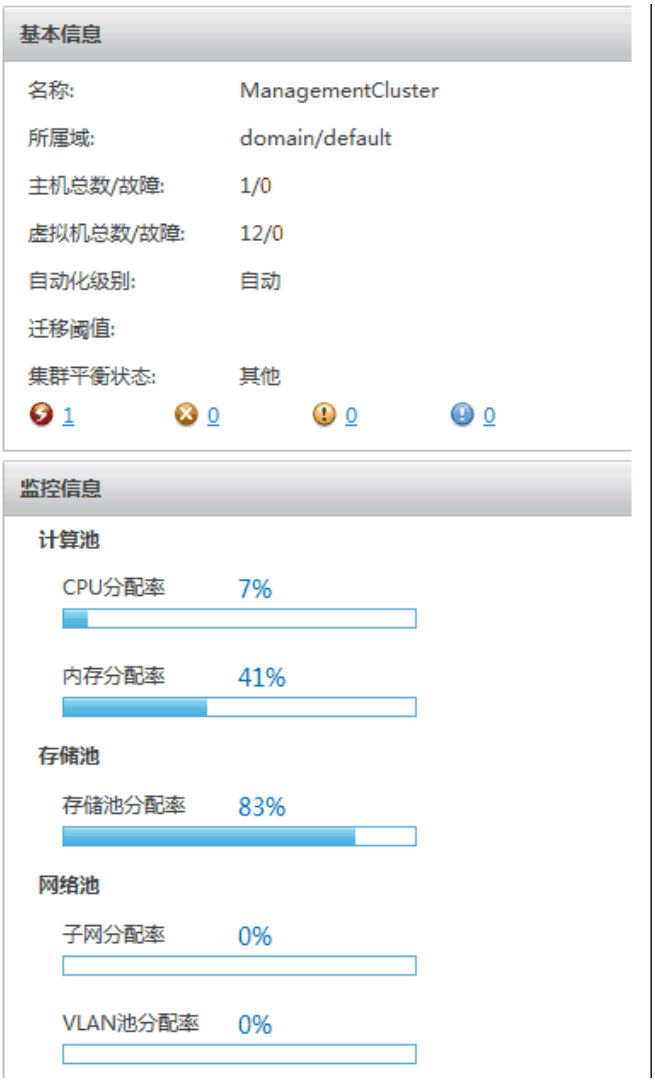
图表 53 拓扑管理呈现



通过拓扑视图可以查看物理硬件资源视图，应用部署以及虚拟机资源视图，即通过拓扑视图可以了解计算、存储、网络以及虚拟资源的逻辑视图。获取硬件资源（计算硬件、存储硬件、网络硬件）、应用部署情况（例如，数据库服务器部署在哪台虚拟机上，虚拟机位于哪台主机上）、虚拟机属性。

拓扑节点会和告警中心关联，即使呈现对象当前的监控状态。拓扑管理呈现选中的集群资源占用和监控状态。

图表 54 对象当前的监控状态



5.13.13 配置管理

配置管理包括组策略配置、系统配置管理。

图表 55 配置管理界面

1. 用户组策略配置管理

采用windows Server的组策略管理控制台实现可视化的组策略管理，在AD(活动目录）提供组策略管理，实现组策略的一站式管理。

组策略管理以组对象（GPO）为基本操作单元，实现组策略的导入/导出；实现组策略的建模/部署、备份/恢复、拷贝/粘贴等操作以及生成GPO设置与策略结果集

（RSoP）数据的 HTML 报表。

组策略管理以组对象（GPO）为基本操作单元，

2. 系统配置管理

系统配置支持初始配置和配置调整，支持系统配置的保存和备份，具体配置如下表所示。

图表 56 配置管理配置项

配置项	说明
AD域服务器	当AD服务器中的以下域信息发生了变化，需要在FusionAccess中同步修改域信息，以确保发放虚拟机时，FusionAccess能够重新获取AD服务器的域信息。
Desktop组件信息	配置Desktop组件信息，包括DDC、WI和License信息。
NTP时钟同步	调整与上层时钟源同步。
告警转Email和短信	配置告警Email和短信通知的地址
License配置	加载License
虚拟机命名规则	配置虚拟机命名规则
配置模板类型	配置模板类型为桌面链接克隆模板、Personal vDisk模板、桌面完整复制模板、桌面快速封装模板。
WI登录界面信息	配置WI登录界面信息，可修改WI超时时间，更换WI背景Logo和图片，更新WI界面每日提醒。
虚拟机登录登出方式	配置当用户登录WI后可自动登录到虚拟机的功能。单虚拟机用户在WI登录界面上输入用户名和密码后，系统默认直接访问到虚拟机桌面。
重定向策略	配置串口、并口、USB、打印机、TWAIN设备、本地磁盘驱动器、设备端口重定向策略；配置Flash重定向策略、QoS策略。
用户和TC的绑定关系。	绑定关系配置后，被绑定用户只能使用绑定的TC登录虚拟机。
告警阈值 第三方设备管理	故障管理。

5.13.14 日志管理

图表 57日志管理界面

日志管理包括日志记录、查看、审计。支持的日志包括：

- 用户访问日志

用户访问虚拟桌面日志。包括虚拟机用户登录、关闭、重启虚拟机。

- 操作日志

管理员访问运维管理平台日志，即管理员的操作日志，包括管理员登录、修改配置、查看告警监控等所有用户操作的日志。操作日志内容包括操作用户、操作类型、用户IP、操作时间、操作结果、操作失败原因、详细信息。

- 系统运行日志。

运行日志用于记录各业务节点的运行情况。系统支持运行日志加密功能，确保运行日志的安全。

黑匣子日志：用于业务和系统异常的故障定位。

5.13.15 统计管理

资源统计可以让管理员查看虚拟机登录、分配以及运行状态信息。包括：

- 查看柱状图显示TOP 10的CPU及内存超过80%的用户。以列表的形式分页显示用户的性能数据。
- 查看虚拟机历史注册异常统计信息。
- 查看最近一个月用户的在线人数，按时间显示在线人数的折线图。
- 查看用户使用虚拟机的时间，
- 查看用户登录信息，以用户列表形式排列显示。
- 查看最近一个月内未使用的虚拟机信息。

系统支持各种统计报表和运行分析报告，支持根据配置字段进行统计，支持保存为EXCEL格式，支持柱状图、折线图和饼状图显示。

图表 58 统计报表界面

5.13.16 智能调度管理

资源统一调度，支持设置集群资源的调度策略，根据管理员设置的调度策略。

根据应用场景，可以分为三种策略类型：组内自动伸缩策略、组间资源回收策略和时间计划策略。

1. 组内自动伸缩策略

针对单独的应用而言，应用根据应用的当前负载动态的调整应用实际使用的资源，当一个应用资源负载较高时，自动添加虚拟机并且安装应用软件；当应用的资源负载很低时，自动释放相应的资源。

2. 组间资源回收策略

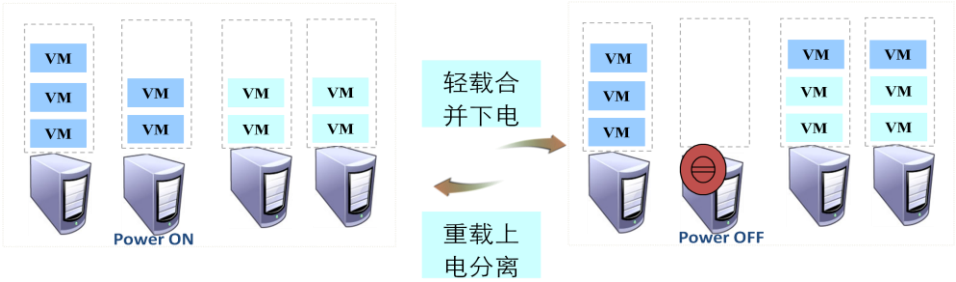
当系统资源不足的情况下，系统可以根据组间设置的资源复用策略， 优先使优先级高的应用使用资源，使优先级低的应用释放资源，以供优先级高的应用使用。

3. 时间计划策略

时间计划策略允许用户对于不同的应用实现资源的分时复用。用户可以设置计划策略，使得不同的应用分时段的使用系统资源，比如说白天让办公用户的虚拟机使用系统资源，到了晚间可以让一些公共的虚拟机占用资源。

4. 节能降耗

图表 59 智能节能调度策略



上图是的调整策略，可以实现节能降耗，实现轻载合并下电，重载分离上电。

- 系统负荷不大时，各VM占用CPU较低，部分VM关机了，可以将某些服务器上的虚拟机自动迁移到其他节点，对这个服务器进行休眠或下电，实施系统节能策略。
- 系统重载时，再让部分物理机上电，并迁移VM到新物理机，保证用户感受。
- 系统需分析并选择合适的物理机上下电，减小迁移的VM数目。
- 为了快速响应，系统保证小部分物理机处理休眠态。

图表 60 计划调度策略

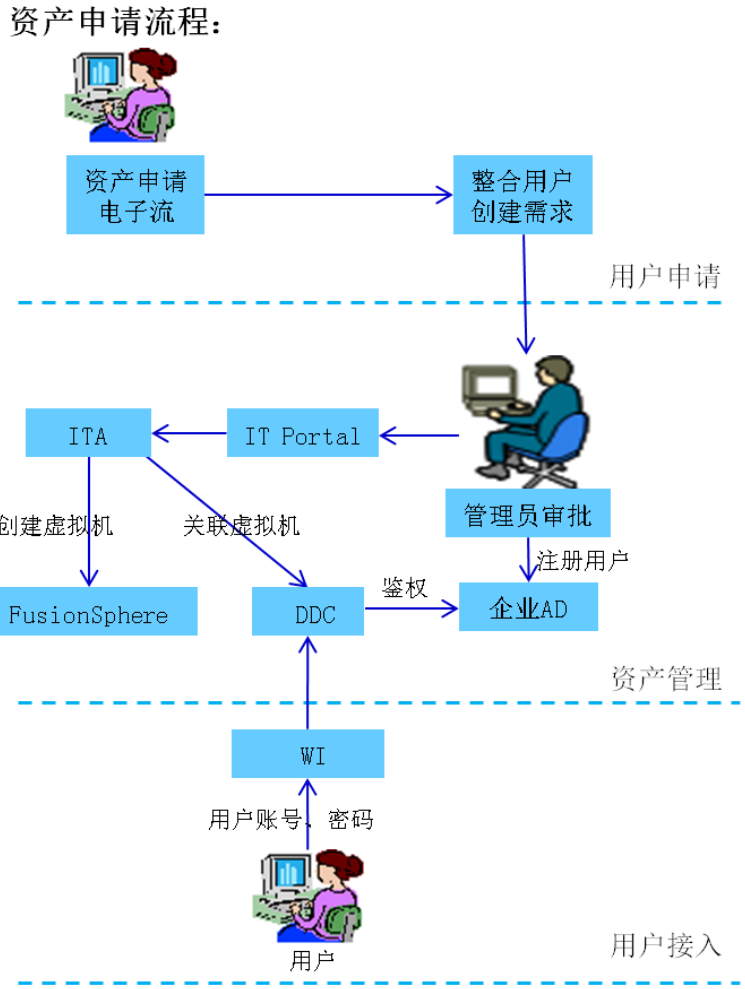
图表 61 组间伸缩策略

5.13.17 开放接口管理

支持通过ITA提供开放接口，客户通过调用接口实现自己的定制化需求，例如虚拟机管理、虚拟机磁盘管理、虚拟机关联、网络管理、告警、开户。

以下是基本的业务流程：

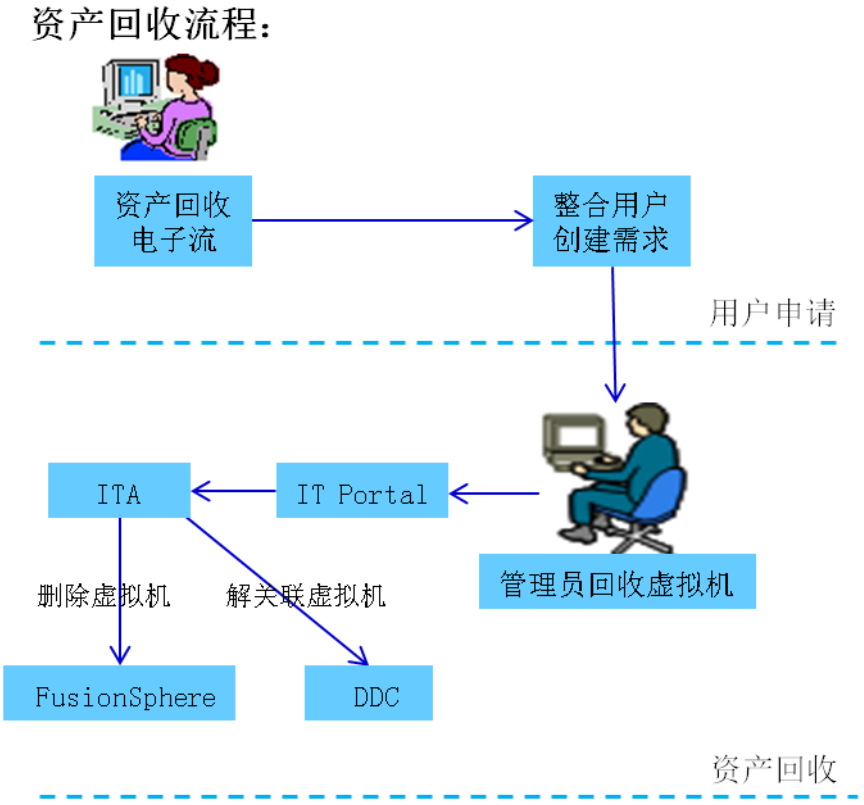
图表 62 自助请求流程



通过与ITA接口的对接，客户可以定制化开发自己的云计算IT资产管理系统，实现对员工域账号、虚拟桌面的完全对接，资产回收完全自动化。

以下是基本的业务流程：

图表 63 资产回收流程



5.13.18 TC 统一管理

华为的所有瘦终端都可通过统一的管理系统进行管理。它是一套基于Browser/Server的管理系统，支持客户机的远程管理操作。同时，对于其他厂家的客户机，以及安装了Windows XP操作系统的PC，只要符合华为的通讯和界面规范，仍可实现联合管理。

桌面管理系统包含如下几个管理功能：

- 基本管理：

该模块是进行主要的客户机管理操作的模块，同时监测客户机运行状况和操作行为，对可能影响系统安全的问题进行警报处理。瘦客户端远程电源控制功能，包括瘦客户端的开机、关机、注销和远程唤醒等操作。

对瘦客户端各项性能进行监控，方便跟踪瘦客户端的运行状况，对突发状况进行及时的处理。同时，通过报表的分析统计，使用户对瘦客户端性能有全局的了解。

- 部署管理：

高级操作指南中的操作主要会涉及到这个模块，主要实现是部署、升级相关的操作。

- 公共管理：

通用的模块。包括对管理员权限的管理、管理员的操作日志和管理工具的基本配置。管理系统用户管理，提供用户建立、删除、审批新用户申请、角色管理、角色分配等通常的功能。

对管理员、瘦客户端的活动进行了记录和统计，以日志的形式进行存档和管理；使用户对系统操作情况有全局的了解。

- 作业管理：

对瘦客户端设备的管理操作进行调度，为一些繁琐重复长时间的管理操作建立作业，制定作业的执行策略，任务之间的依赖关系，帮助系统管理员完成无人值守的管理操作。

- 消息管理：

为管理员和瘦客户端用户提供一个实时消息交互通道，方便系统管理员与瘦客户端用户进行在线实时交流。

图表 64 终端管理系统界面

华为瘦终端统一管理软件有如下特色优势：

- 支持TC终端零配置，降低用户使用门槛

通过终端管理系统，统一能够对TC的配置信息进行下发，无需终端用户自行进行设置，降低用户使用门槛，也便于管理员统一管理。

- 支持TC自动升级和开机强制升级

能够对于已下电的TC，在其下次开机时会进行强制升级，保证所有的TC都能够升级到目标版本。

- TC用户的权限控制

TCM对TC的配置信息，可以根据用户类型不同，发放不同的权限让用户进行修改，这样可以区别对待不同的用户群体。

5.14 可服务性解决方案

5.14.1 软件自动化安装部署

桌面管理系统各个部件能自动化安装部署。桌面管理系统涉及部件很多，如果不能够统一的、自动化的方式来安装部署，安装将变得非常复杂。

- FusionSphere 虚拟化平台自动化安装

自动化安装：基础的MN管理节点安装完成后，其它管理节点的安装自动化完成。自动化的部署模式，可大大减化部署难度。提供预安装与现场安装两种方式：

✧ 预安装模式：

整套设备在供应商发货之前，完成FusionSphere虚拟平台预安装。设备到达现场后，可以直接开始进行FusionAccess桌面管理软件的安装和配置，可大大缩短现场部

署周期。

✧ 现场安装模式:

在现场完成虚拟平台的安装，整个安装过程也高度自动化。

- FusionAccess 桌面管理自动化安装

FusionAccess桌面管理系统支持一键式自动安装部署。管理系统各组件在安装过程中，提供直观的进度状态提示信息。可以随时停止、推出安装过程。

5.14.2 用户自助维护通道

员工通过VNC自助维护通道访问属于本已的虚拟机，可以解决由于员工误操作、或应用程序导致虚拟机网卡禁用，ICA服务被停止等导致无法正常登录问题。还可与虚拟机BIOS执行过程、操作系统启动过程进行交互，也可以解决操作系统启动过程中的异常。

图表 65 VNC登陆界面

5.14.3 桌面云自助连接检修工具

为了提高用户自助解决桌面云问题，华为特开发了桌面自动检修工具，用户可以傻瓜式解决桌面云问题。

1、“桌面云自助连接检修工具”，如下图所示：

图表 66 桌面云自助连接检修工具

2、“一键检修”按钮，对“检修项目”中的每一项进行先检查后修复，修复完一项后进行下一项。检修结果如下图所示：

图表 67 一键检修结果

图示说明：

诊断结果　　修复结果

“ ✔ ✔ ”表示诊断是没有问题的，当然也就无需修复，修复结果也是 OK 的。

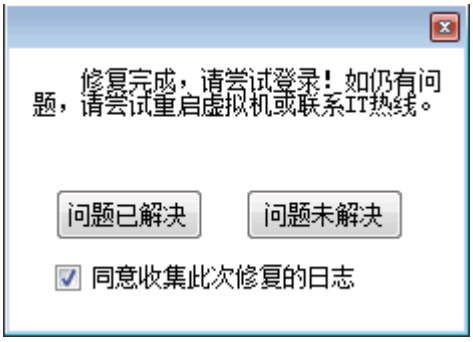
“ ⚠ ✔ ”表示诊断是有问题的，已修复。

“ ⚠ ✘ ”表示诊断是有问题的，工具无法修复，需要联系 IT 热线。

说明：修复过程中无法修复的项会弹出对话框，请点击“确定”继续执行，若点击“取消”则停止修复。

检修完成，有问题是否解决的反馈，如下图所示：

图表 68 一键检修完成



1、 以将步骤2分开处理，即先“ 诊断 ”后“ 立即修复 ”。

图表 69 诊断与立即修复

5.14.4 健康检查工具

健康检查工具是虚拟桌面平台为技术支持工程师和维护工程师提供的一套日常检查工具，并能输出各部件健康检查报告。方便技术支持工程师和维护工程师快速了解系统的健康状况。通过检查系统当前信息和运行状态，反映系统健康或亚健康状态，在开局、巡检、升级等维护场景中使用。

目前健康检查工具可以检测整机PDU健康状态，交换机健康状态，IPSAN健康状态：FusionSphere健康状态（FM健康状态，VM节点健康状态，CAN节点健康状态），FusionAccess健康状态。

- 健康检查工具

健康检查工具是桌面云平台为技术支持工程师和维护工程师提供的一套日常检查工具，并能输出各部件健康检查报告。方便技术支持工程师和维护工程师快速了解系统的健康状况。通过检查系统当前信息和运行状态，反映系统健康或亚健康状态，在开局、巡检、升级等维护场景中使用。

目前健康检查工具可以检测整机PDU健康状态，交换机健康状态，IPSAN健康状态：FusionSphere健康状态（ESC节点健康状态，CRM节点健康状态，CAN节点健康状态），FusionAccess健康状态。

- 健康检查工具输出报告

图表 70健康检查报告

环境整体运行情况		ok	
检查部件	检查项	是否OK	备注（当出现异常时，需要详细描述，出现重大问题需要写成文档的word）
硬件			
E6000服务器			
	刀片面整灯是否正常	ok	
	SMM板告警灯是否正常	NOK	P16B6000_01， P16B6000_02，出现SMM板告警，查看日志发现还是和上次一样的问题，电源告警，需要申硬实施定位
	硬盘Active灯是否正常	ok	
	硬盘Fault灯是否常亮或有闪烁	ok	
	服务器上所有网口是否正常	ok	
	电源灯是否正常	ok	
	风扇是否正常	NOK	P16B6000_01， P16B6000_02，风扇告警
整机			
PDU			
	PDU的电压以及电流是否过载（电流过大时需要记录）	ok	
	PDU插槽指示灯是否正常	ok	
交换机			
	所有端口指示灯是否正常	ok	
IPSAN			
	电源，电池是否正常	ok	
	网口灯是否正常	ok	
	告警灯是否亮	ok	
软件			
OMMx			
ESC节点			
	tomcat进程是否正常	ok	
	PostgreSQL进程是否正常（备用节点没有）	ok	
	ldap数据库是否正常（备节点没有）	ok	
	8443端口是否正常	ok	
	8773端口是否正常	ok	
	8773端口上是否有CLOSE_WAIT状态	ok	
	DRBD进程是否正常（备节点没有启用）	ok	
	ci进程是否正常（备节点没有启动）	ok	
	日志进程rsyslogd是否正常	ok	
	查看服务器CPU占用率是否飙高	ok	
CRM节点			
	DRBD进程是否正常（备节点未启动）	ok	
	PostgreSQL进程是否正常（备用节点没有）	ok	
	8774端口是否正常	ok	
	8559端口是否正常	ok	
	3551端口是否正常	ok	
	3552端口是否正常	ok	
	8774端口上是否有CLOSE_WAIT	ok	
	DRBD进程是否正常（备节点没有启用）	ok	
	服务器CPU占用率是否飙高	ok	
	日志进程rsyslogd是否正常	ok	
	ci进程是否正常（备节点没有）	ok	
CAN节点			
	zookeeper进程是否正常	ok	
	8553端口是否正常	ok	
	8554端口是否正常	ok	
	8555端口是否正常	ok	
	8775端口是否正常	ok	
	8776端口上是否有CLOSE_WAIT状态	ok	
	dom0的CPU占用率是否飙高	ok	
	日志进程rsyslogd是否正常	ok	
	nc进程是否正常	ok	
VDeskTop			
	检查DDC中Citrix Delivery Service Console进程中虚拟机的状态	ok	
	DDC服务器中service里面Citrix相关服务没有停止	ok	
	DDC服务器中操作系统日志没有Citrix的相关错误，警告	ok	
	DDC服务器中查看系统进程，CPU不会持续飙高，内存保持在正常范围一般都没有超过10	ok	

5.14.5 用户体验优化工具

桌面云用户体验优化工具从风险检查、系统优化、语音质量优化、历史案例库以及软件兼容性检查几个方面来进行用户虚拟机的风险漏洞检测、系统配置的优化。并配置大量局点的攻关案例来帮助用户解决桌面使用过程中的问题，有效管理已发放出去的云桌面性能，提升最终用户自主改善桌面云操作系统用户体验能力 。

图表 71　用户体验优化

5.14.6 故障信息采集工具

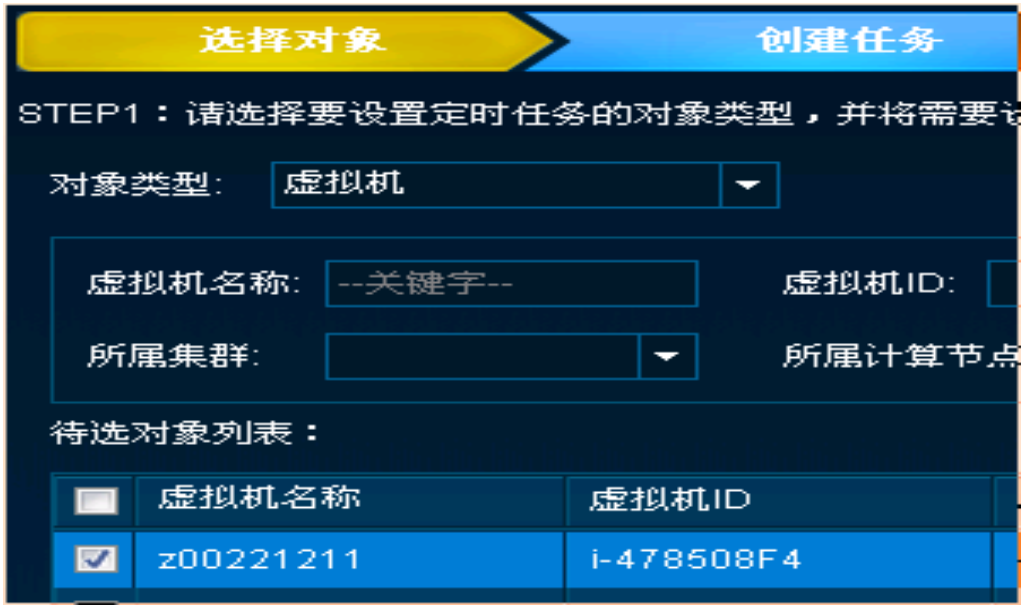
华为桌面云提供的故障信息采集工具主要为了采集故障信息，方便后方快速定位，修复问题。因此采集工具会采集公共的OS运行环境，软硬件版本信息，运行日志，性能测量数据，黑匣子日志等数据。还会根据各模块调试定位的需要采集日志及可能被客户修改的必需的配置数据等内容。原则是包含完整调试信息，但尽量排除不必要的数据以控制数据大小。实现一键式收集整理局点故障信息，简化维护人员的信息收集工作，方便后方研发人员定位故障。

5.14.7 定时任务（应对开机风暴和创建虚拟机风暴）

为了应对开机风暴，华为特开发了定时任务功能：可以制定定时任务，将所有的桌面虚拟机在早上上班之前全部分配定时启动，错峰启动，减少了对存储的冲击。

也可以定时创建虚拟机，按照不同规格预留一定资源，减少用户申请时间，非工作时间执行，防止网络风暴。

图表 72 定时任务



5.14.8 数据一致性审计

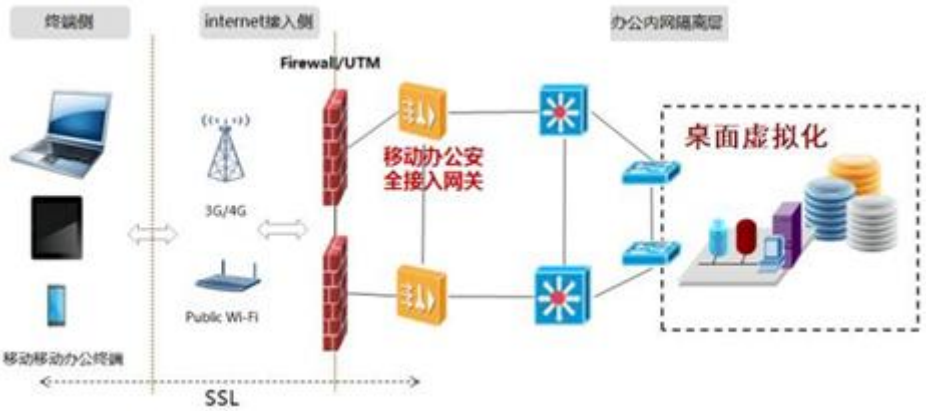
FusionCloud提供了数据一致性审计功能，定时审计VM及其卷文件的相关数据和状态的一致性，当发现有异常的时候，会自动记录下来，以便维护人员做相应的判断和恢复措施，从而保证了系统内部各种相互关联的数据的一致性

5.15 移动办公

5.15.1 移动办公接入方案组网图

针对金融机构员工差旅酒店、家庭或其他场所办公人员的远程接入需求，设计安全、便捷、高效、易管理的远程接入解决方案。

图表 73 移动办公接入组网图



金融机构的员工使用笔记本和Pad移动办公时，在互联网通过3G/LTE、公共场所或家庭Wi-Fi接入金融机构办公内网隔离区SVN移动安全接入网关，所有的管理流量和业

务流量都经过SVN移动安全接入网关。

终端和移动办公接入网关之间的传输通过SSL进行加密。

5.15.2 移动办公接入网关主要功能

1) 身份鉴权

为保证移动接入用户的合法性，数据交换网关SVN支持多种身份鉴权方式。

移动办公接入网关SVN自身支持VPNDB（Virtual Private Network Database）认证方式，即在安全数据交换网关SVN上建立本地用户数据库，对用户名、密码进行严格认证，用户无需另外建立认证系统。同时，针对已建设起相对完善的认证体系，移动办公接入网关SVN还支持以下外部认证系统：

- 第三方认证服务器，包括与符合RADIUS（Remote Authentication Dial in User Service）、LDAP（Light Directory Access Protocol）、AD（Active Directory）、SecurID等标准协议的认证服务器对接。
- 数字证书认证，包括多级证书，且支持证书的CRL（Certificate Revocation List）和OCSP（Online Certificate Status Protocol）检测，保证证书的有效和安全。

2) 角色授权:

角色是系统一系列资源/权限的组合。不同的角色可以绑定不同的资源/权限的组合。

通过角色绑定，我们可以为接入用户分配不同的权限和可访问的资源。场景包括：

- 绑定不同角色的两个用户；
- 绑定不同角色的两个用户组的组内用户；

通过角色的定义和识别，我们为用户提供基于群组的访问权限控制。移动办公接入网关SVN提供基于角色/资源关联的授权方式。可访问的内网资源被关联到不同的用户角色上，属于某角色的用户可以访问该角色关联的内网资源。通过将可访问资源与具体用户剥离，可灵活应对金融机构组织架构中人员的调整，减少管理员权限管理的工作量。

移动办公接入网关SVN提供外部组的授权映射，能够和金融机构已有的用户管理系统完美对接。移动办公接入网关SVN提供外部组映射功能，通过这个功能，管理员能够将保存在LDAP、RADIUS等认证服务器中用户组/组织机构等信息映射到移动办公接入网关SVN中，移动办公接入网关SVN将这些用户/用户组信息和具体的可访问资源关联起来完成移动办公接入网关SVN用户的访问授权。

移动办公接入网关SVN提供基于接入终端安全等级的动态授权方式。管理员可以配置在远程用户移动办公接入网关SVN之前先进行接入终端的安全检查，并将安全检查结果作为获得用户角色的条件。

3) 数据传输使用高强度加密的 SSL VPN 通道传输

用户访问内部网络时，用户桌面会与移动办公接入网关SVN建立高强度的SSL VPN通道，确保数据在传输过程中的安全、可靠。

4) 桌面访问更安全

禁止对桌面云客户端的截屏操作；禁止其他主机二次跳转到运行桌面虚拟机客户端的PC ； 接入认证使得直接攻击WI的路径被阻断。

5.15.3 设备选型方案

设备选型为华为SVN5530安全网关。详细说明请见3.8章节华为SVN安全接入网关介

绍。

5.16 设备选型方案

5.16.1 服务器选型方案

✧ Huawei Tecal E6000 服务器

图表 74 E6000服务器

本次管理服务器和资源服务器拟采用华为刀片服务器E6000。E6000服务器具有如下特点：

➢ 散热好：

华为刀片散热架构先进：每个模块独享风道；刀片采用“对称布局”设计，相对“影子布局”，散热更均匀。

➢ 可靠性

架构可靠性高：背板采用无源背板；全冗余设计；所有模块（刀片/硬盘/交换/管理/风扇/电源）支持在线热插拔；

➢ 管理维护简单

“免下架”维护：机箱上架后，终生“免下架”维护。机箱所有模块拔出后，只剩下免维护的无源背板和结构件。ZeroTouch零接触管理，所有管理维护操作都可以远程完成。

➢ 技术规格

图表 75 E6000技术规格

系统	类别	描述
E6000主机	尺寸	8U机架（HxWxD：353mm×447mm×810mm）
	刀片槽位	10
	交换机模	6，可配置为6个GE交换机或4个GE交换机+ 2个FC交换机

	块	
	电源	6个 110V/220V 80plus电源
	风扇	9个热插拔风扇模块
BH622 V2 刀片	CPU	2路四核/六核/八核Intel Sandy Bridge-EP Xeon E5-2600系列处理器，支持130W、115W、95W、80W系列；
	内存	24个DDR3 DIMM插槽，最大支持768GB内存（采用32GB内存条）；
	硬盘	2个2.5英寸SAS或SATA或SSD硬盘；
	扩展	板载2个GE口，采用Intel 82580；支持扩展2个PCIe 接口模块；
管理	管理	板上支持单板管理模块BMC提供对服务器的智能监控功能，符合IPMI2.0标准； 支持远程KVM，虚拟媒体等功能；

5.16.2 存储选型方案

✧ OceanStor S5500T

图表 76 OceanStor S5500T 存储-2.5寸盘

图表 77 OceanStor S5500T 存储-3.5寸盘

2U控制框：

4U硬盘框：

针对本次项目需求分析，我们拟采用OceanStor S5500T存储为用户提供系统空间和数据空间。华为自研的中高端存储S5500T在实现了文件和块的统一、协议的统一和管理界面的统一的基础上，以业界领先的性能为支撑，融合了高密硬盘设计、TurboModule 接口模块及热插拔设计、TurboBoost 三级性能加速技术、多重数据保护等高端技术，能够满足大型数据库OLTP（On-Line Transaction Processing）、高性能计算、数字媒体、互联网运营、集中存储、备份、容灾、数据迁移等不同业务应用的需求，有效保证用户业务安全

性与连续性。S5500T存储特点如下：

高性能、高扩展性

高速部件/高速总线：配备64位多核处理器以及高速大容量缓存，最高36GB/s的系统内部交换带宽，支持SAS2.0宽端口后端通道。

支持多种不同种类的硬盘：SAS/SATA/SSD。

支持最大2块I/O接口卡。支持8Gb FC、1/10G Ethernet、10G FCoE与6Gb SAS2.0接口。

三重性能加速技术：依靠强大硬件支撑的固有性能，使用SmartCache技术持续监测系统热点数据并缓存至SSD盘片，最高可获得数倍的读性能提升；利用纯SSD将系统性能再次大幅提高。三重性能加速机制，稳固按需提升系统性能，全面降低整体拥有成本。

高镜像带宽：双控之间的Cache镜像采用专用高速8GB/s通道，消除双控间数据交换的瓶颈。

高可靠、高可用性

接口模块化热插拔设计： TurboModule技术使得I/O接口卡可在线热插拔而无需关闭存储控制器，对业务主机完全透明，实现真正的在线I/O扩容

掉电数据保护：系统掉电后内置电池模组自动将Cache数据写入数据保险箱，保证数据不丢失。

硬盘预拷贝技术：提前发现即将故障的硬盘，主动迁移故障盘数据，规避系统降级的风险，有效降数据丢失的风险。

硬盘坏道修复技术：最大限度修复硬盘坏道，将硬盘故障率降低50％以上，延长硬盘的可使用周期。

高级数据保护技术：利用HyperImage以及HostAgent实现针对应用系统数据的一致性快照，并能从快照中瞬间恢复数据；跨存储平台卷拷贝技术实现异构存储间的数据保护。远程复制技术实现数据异地备份容灾保护。

低总体拥有成本

统一的IO接口模块：本系列全线产品使用统一的IO模块，极大降低总体拥有成本。

24盘位高密设计：2U/4U高密度硬盘框（24块/框），平均1U空间最高可容纳12块硬盘（2.5英寸），相对于低密度盘框设计来讲，扩容成本降低60％。

易用的管理维护工具：通过ISM统一管理界面，5步即可完成基本配置。支持声音、灯光、手机短信、邮件等多种告警手段；一键式双控在线Firmware升级，有效地降低用户运维成本。

绿色节能

绿色节能设计提供了多种节能减排措施，包括：CPU智能调频、风扇精细化智能调速、硬盘智能休眠技术等。

不仅如此，华为公司还提供了可对OceanStor系列存储设备进行统一管理的集成存储管理软件OceanStor™ ISM（以下简称ISM）。该软件可通过安全便捷的GUI管理界面对存储设备进行引导式业务配置、一键式升级以及告警上报等人性化的运维管理。

图表 78 OceanStor S5500T技术规格

型号	S5500T
硬件特性	
存储处理器	多核多处理器组
缓存	8GB、16GB、32GB
控制器数	2
前端通道端口类型	8 Gb FC，1 Gb iSCSI，10 Gb iSCSI（TOE），10Gb FCoE
后端通道端口类型	24Gb SAS宽端口

板载IO端口数	2*4*8Gb 前端FC、2*1*管理网口，2*1*维护网口，2*1*串口，以及4×24Gb 后端SAS宽端口
最大IO模块数	2个4*8Gb FC IO模块,或 2个4*10GE IO模块 或 2个4*1GE IO模块 或 2个4*10GE FCoE IO模块
最大硬盘数量	528
硬盘规格	3.5″或2.5″ SAS、SATA、SSD
软件特性	
RAID 支持	0,1,3,5,6,10,50
连接主机数量	512
LUN	2048
支持快照数量	1024
TurboBoost	支持
TurboModule	支持
其他功能软件	HyperImage（快照）、HyperCopy（LUN拷贝）、HyperMirror（同步/异步远程复制）、HostAgent（主机端快照/复制管理模块）、UltraPath（多路径软件）、Diskguard（主机端数据保护软件）、SmartCache（TurboBoost中的动态数据缓存技术）

图表 79 OceanStor Dorado2100G2 SSD存储

针对本次项目需求分析，采用OceanStor Dorado2100G2 SSD存储为用户提供系统空间，可提供卓越性能，带来极速用户体验。华为自研的固态存储Dorado2100G2 可提供行业领先的性能、真正的可靠性、多维可扩展性以及无与伦比的投资保护。Dorado2100G2 能够满足大型数据库、高性能计算、OLTP（On-Line Transaction Processing）、集中存储、备份、容灾、数据迁移等不同业务应用的需求，有效保证业务的安全性与连续性。产品特点如下：

高性能、高扩展性

业界领先的硬件规格：配备64 位多核处理器以及高速大容量缓存。支持6Gbit/s SAS2.0（Serial Attached SCSI）宽端口后端通道。

支持金融机构级的SSD（Solid State Drive）硬盘：将SSD 硬盘作为存储介质，可解决数据读写性能的瓶颈，提供低延迟和高吞吐量。

支持最大2块I/O接口：支持8Gbit/s FC（Fiber Channel）；10GE TOE接口；40Gb IB接口。支持6Gbit/s SAS2.0 后端接口。

高可靠、高可用性

模块化热插拔设计：TurboModule 技术使得控制器、风扇、电源、接口模块、硬盘模块、BBU 模块均可在线热插拔而无需重新启动存储控制器，对业务主机完全透明，实现真正的在线扩容。

高可靠性：Dorado2100G2存储系统主要采用主机路径冗余保护、FRU（Field Replaceable Unit）器件1+1 冗余设计、热插拔技术、硬盘双端口技术以及硬盘多路径技

术实现存储高可靠性。

掉电数据保护：系统掉电后内置电池模组自动将Cache数据写入数据保险箱，保证数据不丢失。

硬盘预拷贝技术：提前发现即将故障的硬盘，主动迁移故障盘数据，规避系统降级的风险，有效降低数据丢失的风险。

硬盘坏道修复技术：最大限度修复硬盘坏道，将硬盘故障率降低50％以上，延长硬盘的可使用周期。

高效、易用

统一的IO接口模块：本系列全线产品使用统一的IO模块，极大降低总体拥有成本。

25盘位高密设计：2U高密度硬盘框（25块/框），平均1U空间最高可容纳12.5块硬盘（2.5英寸），相对于低密度盘框设计来讲，扩容成本降低60％。

易用的管理维护工具：通过ISM统一管理界面，5步即可完成基本配置。支持声音、灯光、手机短信、邮件等多种告警手段；一键式双控在线Firmware升级，有效地降低用户运维成本。

绿色节能

绿色节能设计提供了多种节能减排措施，包括：CPU智能调频、风扇精细化智能调速、硬盘智能休眠技术等。

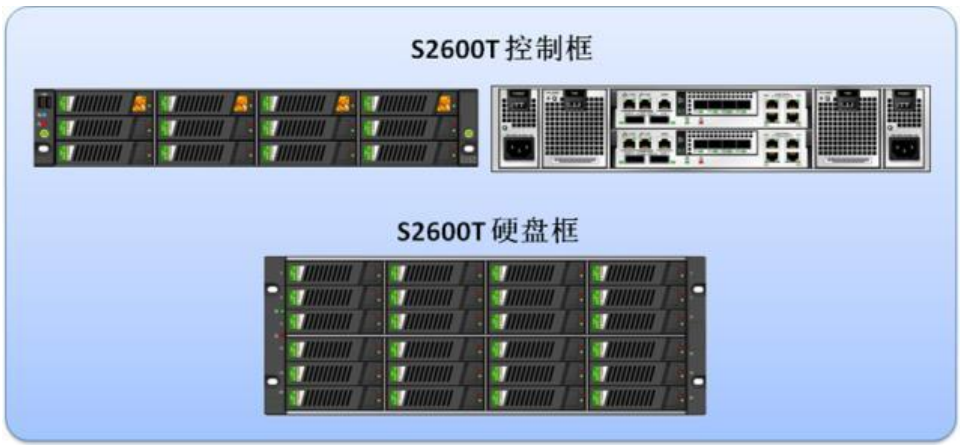
不仅如此，华为公司还提供了可对OceanStor系列存储设备进行统一管理的集成存储管理软件OceanStor™ ISM（以下简称ISM）。该软件可通过安全便捷的GUI管理界面对存储设备进行引导式业务配置、一键式升级以及告警上报等人性化的运维管理。

图表 80 Dorado 2100G2 SSD存储技术规格

型号	Dorado 2100G2
硬件特性	
存储处理器	多核多处理器组
缓存	48GB
控制器数	2
前端通道端口类型	8 Gb FC， 10 Gb iSCSI（TOE），40Gb IB
后端通道端口类型	24Gb SAS宽端口
板载IO端口数	2*4*8Gb 前端FC、2*1*管理网口，2*1*维护网口，2*1*串口，以及4×24Gb 后端SAS宽端口
最大IO模块数	2个4*8Gb FC IO模块,或 2个4*10GE IO模块或2个2*40Gb IB模块
最大硬盘数量	100
硬盘规格	2.5″ SSD
软件特性	
RAID 支持	0,5,10
连接主机数量	512
LUN	2048
TurboBoost	支持
TurboModule	支持

Thin LUN	支持
其他功能软件	HostAgent（主机端快照/复制管理模块）、UltraPath（多路径软件）、Diskguard（主机端数据保护软件）

图表 81 OceanStor S2600T存储



针对本次项目需求分析，我们拟采用OceanStor S2600T存储为用户提供系统空间和数据空间。该产品是面向低端市场应用的新一代金融机构入门级存储系统，以强大的硬件规格为支撑，融合了全冗余架构设计、IO模块热插拔以及多重数据保护等高端技术，能够以入门级的价格满足规模不断增大并且存储要求日益复杂的数据库，数字媒体，互联网运营，集中存储，备份，容灾，数据迁移等不同业务应用的需求，有效保证用户业务安全性与连续性。

S2600T有以下特点：

高性能、高扩展性

采用业界领先的硬件：配备64位多核处理器以及高速大容量缓存，高达20GB/s的系统内部交换带宽，支持SAS2.0宽端口后端通道，充分消除了硬件瓶颈

硬盘类型选择灵活：6Gbps SAS/NL SAS/SATA/SSD

按需进行初始配置和扩展：从小规模起步，随着存储需求的增长进行适当扩展。独创的TurboModule技术使得单框I/O接口密度大幅提高，支持4/8Gb FC，1/10Gb Ethernet与6Gb SAS2.0接口，高达24个I/O接口（包括前端与后端接口）。根据数据重要性和安全级别，选择SAS/NL SAS/SATA/SSD硬盘，实现数据按需存储，极大降低维护成本

TurboBoost按需提升系统性能：依靠业界领先的硬件支撑的固有性能，使用SmartCache技术持续监测系统热点数据并缓存至SSD盘片，最高可获得数倍的读性能提升；利用纯SSD RAID组将系统性能再次大幅提高。三级性能加速机制，稳固按需提升系统性能，全面降低整体拥有成本

高可靠、高可用性

模块化热插拔设计： TurboModule技术使得控制器、风扇、电源、I/O模块、备电模块、硬盘等模块均可在线热插拔而无需重新启动存储控制器，对业务应用服务器完全透明，实现真正的在线扩容

断电保护技术：系统断电后内置的电池模组自动将Cache数据写入数据保险箱，保证数据不丢失

硬盘预拷贝技术：提前发现即将故障的硬盘，主动迁移故障盘数据，规避系统降级的风险，有效降低数据丢失的风险

硬盘坏道修复技术：最大限度修复硬盘坏道，将硬盘故障率降低50％以上，延长硬盘的可使用周期

高级数据保护技术：利用HyperImage与HostAgent实现针对应用系统数据的一致性快照，并能从快照中瞬间恢复数据； HyperClone、HyperCopy实现本地数据备份恢复；跨存储平台卷拷贝技术实现异构存储间的数据保护；远程复制技术实现数据异地备份容灾保护。

高效，经济，易用

自动精简配置：HyperThin技术支持容量自动扩展，提高磁盘利用效率，实现用户按需购买，降低初次购买成本和TCO

易用的管理维护工具：通过ISM统一管理界面，5步即可完成基本配置；支持声音，灯光，手机短信，邮件等多种告警手段；一键式双控在线Firmware升级，有效地降低用户运维成本

绿色节能

硬盘节能技术：依据业务负载，实现硬盘智能休眠，可降低40%的能耗

16档智能风扇调速技术：根据系统当前温度智能调节风扇转速，降低风扇功耗及噪音(风扇占整机功耗15%左右)，增强设备环境适应能力

CPU智能变频：根据业务负载智能调节CPU工作频率，在业务负载小时，降低CPU工作频率，大大降低系统功耗

图表 82 OceanStor S2600T产品规格

型号	S2600T
硬件特性	
存储处理器	多核多处理器组
Cache容量	8GB / 16GB
控制器数	2
前端通道端口类型	1Gb iSCSI、10Gb TOE和8Gb FC主机接口模块
后端通道端口类型	SAS2.0宽端口
板载I/O端口数	2*4*1Gb iSCSI、2*1*管理网口，2*1*维护网口，2*1*串口，以及2*2*6G后端SAS宽端口
最大I/O模块数	2*4*8Gb FC接口模块 或 2*4*1Gb iSCSI接口 或 2*4*10Gb TOE接口模块
最大盘位数	276
支持的硬盘类型	4U 硬盘框 3.5寸 SSD、SATA、NL SAS、SAS
软件特性	
RAID 支持	0,1,3,5,6,10,50
支持应用服务器数量	256
支持LUN数量	1024
支持快照数量	512
TurboBoost	支持
TurboModule	支持
其他功能软件	HyperImage（快照），HyperCopy（卷拷贝），HyperClone（卷克隆），HyperMirror（同步/异步远程复制），HyperThin（自动精简配置），HostAgent（应用服务器端快照/复制管理模块），UltraPath（多路径软件），DiskGuard（应用服务器端数据保护软

	件），SmartCache（TurboBoost中的动态数据缓存技术）
操作系统兼容	AIX，HP-UX，Solaris，Linux，Windows，VMware VAAI等
物理特性	
尺寸	2U控制框（长宽高）：582mm×446mm×86.1mm
	4U硬盘框（长宽高）：412mm×446mm×175mm
重量	2U控制框≤23.9kg
	4U硬盘框≤25.2kg
电源	交流：100V ～ 127V 或200V ～240V 直流：-48V ～-60V
功耗	2U控制框≤539W（含24 SAS 盘） 4U硬盘框（满配600GB SAS）≤441W

图表 83 OceanStor N8300 NAS引擎

图表 84 OceanStor N8500 NAS引擎

OceanStor N8300/N8500 是面向中高端NAS和统一存储市场。满足电信，数字媒体，高性能计算，政府教育等客户对存储系统高性能，可扩展能力，高效数据管理和统一存储的业务需求

图表 85 OceanStor N8300/N8500 NAS技术规格

型号	N8300	N8500
系统架构	多节点全Active集群架构。后端存储支持：S2600T/S5500T/S5600T/S5800T/S6800T	
节点数	2 ～ 6个	2 ～ 24个

最大系统容量	7 PB	15 PB
缓存/节点	标准版：标配16GB,可扩展至24GB 金融机构版：标配16GB,可扩展至32GB,48GB	基础版：16GB；标准版：24GB 金融机构版：48GB; 增强版：标配96GB，可扩展至192GB
以太网支持	1GE 和 10 GE	
协议支持	NFS, CIFS, FCP, iSCSI, FTP, HTTP, NDMP	
最大文件系统大小	256 TB	
主要特性	主要体现在高可靠性、高性能、SmartCache(动态数据缓存技术) 支持多种客户端操作系统 支持动态分级存储 支持业务网口绑定 支持用户配额管理 支持文件系统、卷级快照，支持存储单元虚拟快照 支持文件系统的在线扩容，HyperThin(自动精简配置) 支持基于LAN的备份，支持NDMP、NBU 备份方式，内置Symantec NetBackup Client 支持文件系统多重镜像，HyperClone (分裂镜像) 支持NFS和CIFS协议的共享、支持NAS&SAN 一体化、支持FTP协议访问 支持AD、NIS、LDAP、Domain 域环境 支持文件系统远程复制、支持文件块级增量远程复制 支持重复数据删除 支持EV归档 支持存储单元LUN拷贝 支持存储单元后台格式化 支持存储单元远程复制、同步/异步远程复制 支持动态添加、删除镜像卷	
磁盘类型	SSD,FC, SAS, SATA, NL-SAS	

5.16.3 接入网关设备选型方案

设备选型为华为SVN5530安全网关。详细说明请见6.3-6.7章节 SVN安全接入网关介绍。

5.16.4 瘦终端选型方案

华为瘦终端支持虚拟化桌面、XenApp应用虚拟化，设备精巧，让办公环境更加简洁。

- 专利技术，独特体验

USB映射、双向语音映射、位图加速，专利技术带给您独有的用户体验。

- 高度集成，时尚外观

结构紧凑、精致灵巧的产品形态，加上行业领先的无风扇设计，把视觉压力、听觉压力远远地抛在脑后；双屏双显的绝美应用，让工作更加得心应手。

- 随心摆放，更自如

产品拥有超强的环境适应、协调能力：可背挂于显示器后，支持VESA国际标准背挂方式；可立于桌面上。让您动动手指，就能随心所欲改变办公环境。

图表 86 瘦终端选型

特性概述

- 高性能、低功耗

  采用Intel Cedarview平台，搭载Intel D2550 1.86GHz CPU，超强性能；整机功耗小于12W，TDP小于10W，带给您急速体验的同时，彰显您的节能主张。

- 超强多媒体体验

  拥有出色的图形处理能力和多媒体播放能力，支持本地硬解、1080P高清视频播放，带给您更炫更快的多媒体新体验。

- 丰富外设，强大扩展
  - 支持 4 个串口、1 个并口、4 个 USB2.0 接口，行业外设接口最丰富，最大化地满足客户需求。

- 双屏双显，静音设计

  双屏双显的绝美应用，让工作更加得心应手。采用行业领先的无风扇设计，把视觉压力、听觉压力远远地抛在脑后。

- 背挂摆放，别样空间体验

  产品支持 VESA 国际标准背挂方式，可背挂于显示器后、可立放桌面上，让您轻轻松松改变办公环境。

图表 87 瘦终端技术规格

接口示意图

正面

1. 电源按钮
2. 音频接口(输入/输出)
3. USB 2.0 接口
4. IC 卡插槽（可选）

背面

1. 电源接口
2. PS2 接口
3. 串口
4. 并口
5. DVI-I 接口
6. USB 2.0 接口
7. 10/100/1000 以太网 RJ-45 接口

技术规格		
处理器	CPU	Intel D2550 1.86GHz
内存	系统内存	2GB DDR3（最高支持4GB）
存储	DOM	8G SATA（可扩展硬盘）
输入/输出/外设支持	键盘	PS/2键盘
	鼠标	PS/2鼠标
	显示	DVI/VGA视频输出
I/O端口	串口	1转4串口辫子线扩展
	并口	1个
	网口	2个千兆(RJ-45)
	USB 2.0端口	6个(前面板2个，后面板4个)
	DVI-I接口	1个
	耳机插孔	1个
	麦克风插孔	1个
网络	LAN	10/100/1000以太网(RJ-45)
	网络启动方式	PXE、RPL
显示支持	分辨率	本地最大支持32位真彩色显示, VGA：最大分辨率1920x1200@60Hz DVI：最大分辨率1920x1200@60Hz
操作系统 / 语言	WES7	中文、英文
	Linux	中文、英文
包含的软件	操作系统	WES7
	RDP	V7.1
	管理浏览器	CDMS V3.6.2(升腾曦帆桌面管理系统)
	本地媒体播放	安装 IE 9.0

		Windows Media Player V12.0
外形尺寸(长x宽x高)：	机身	206×249×49mm
电源	适配器	外置12V/3A DC直流电源
重量	毛重	待测
	净重	待测
工作环境	工作温度范围	0℃－40℃
	湿度(无凝结)	30%-90%

环保规格		
能耗	TDP	10W
	整机功耗	桌面：8.17W 最大：11.42W
散热	无风扇设计	
产品认证	CCC 、CE、FCC、VCCI、RoHS	
材料利用	本产品不包含超过规定限值的以下任何物质： • 石棉 • 某些含氮着色剂 • 某些溴化阻燃剂 — 禁止在塑料中作为阻烯剂使用 • 镉 • 氯代烃类 • 氯化石蜡 • 卤化二苯基甲烷 • 用户经常接触或持握的外表面禁止使用的镍磨光 • 破坏臭氧的物质 • 多溴联苯(PBB) • 多溴二苯醚（PBDE) • 多氯联苯(PCB) • 多氯三联笨(PCT) • 聚氯乙烯(PVC) — 接线与电缆除外 • 放射性物质 • 三丁基锡(TBT)、三苯基锡(TPT)、氧化三丁基锡(TBTO)	
包装	升腾遵循以下指导原则，降低产品包装对环境的影响： • 包装材料中不包含已被禁用的铅、铬、汞和镉 • 在包装材料中不使用消耗臭氧的物质(ODS) • 设计的包装材料易于拆卸 • 在包装材料中充分利用回收材料 • 使用易于回收的包装材料，例如纸和波纹材料 • 减小包装的尺寸与重量，以提高运输的燃油利用率•	

5.17 桌面云方案配置清单

图表 88 桌面云配置清单

设备类型	型号	单位	数量	备注
计算服务器1	E6000服务器（2路8核CPU、256G内存）	台		普通办公
计算服务器2	E6000服务器（2路8核CPU、384G内存）	台		开发
计算服务器3	E6000服务器（2路6核CPU、192G内存）	台		应用虚拟化
管理服务器	E6000服务器（包括桌面会话管理FusionAcess和虚拟化管理FusionSphere）	台		管理节点
接入交换机	Juniper EX4200	台		存储接入
汇聚交换机	Juniper EX4500	台		汇聚
存储	S5500T（配置216块600G SAS硬盘）	套		系统盘存储
云终端	TC	台		
机柜	IDCU机柜(2路32A交流220V输入)	个		
桌面云软件	桌面云金融机构版每用户	个		标准VDI
桌面云软件	桌面云金融机构增强版每用户	个		应用虚拟化
桌面云接入软件（SVN）	云接入并发用户-含华为通用安全平台软件	个		含移动办公
移动办公桌面云接入网关	SVN5530	台		移动办公

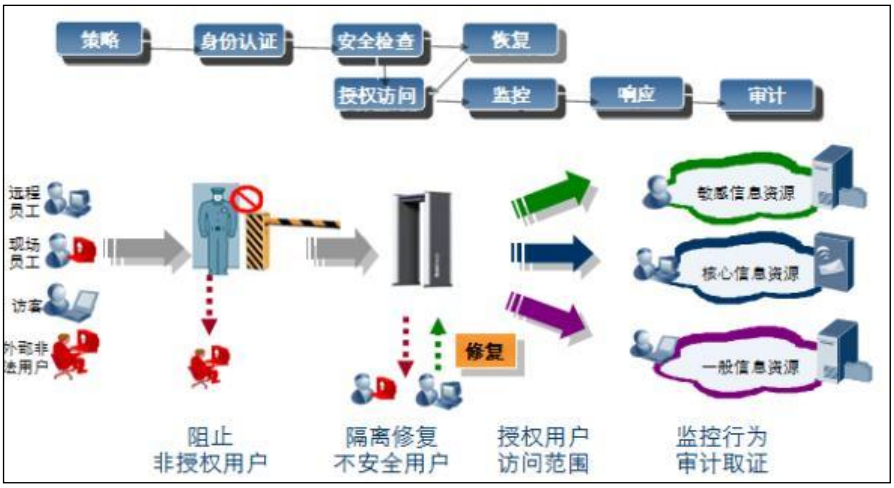
6 华为 PolicyCenter 子方案

6.1 概述

内网安全解决方案将试图访问金融机构网络资源的用户进行身份认证和强制实施安全认证，通过双重检查保证接入网络终端的安全性，对不满足需求的终端自动引导进行安全修复和补丁安装，对满足需求的终端接入网络后，对其网络和终端行为进行实时监测和审计，保护终端软硬件资产，防止信息泄密，最大程度保障金融机构信息安全。

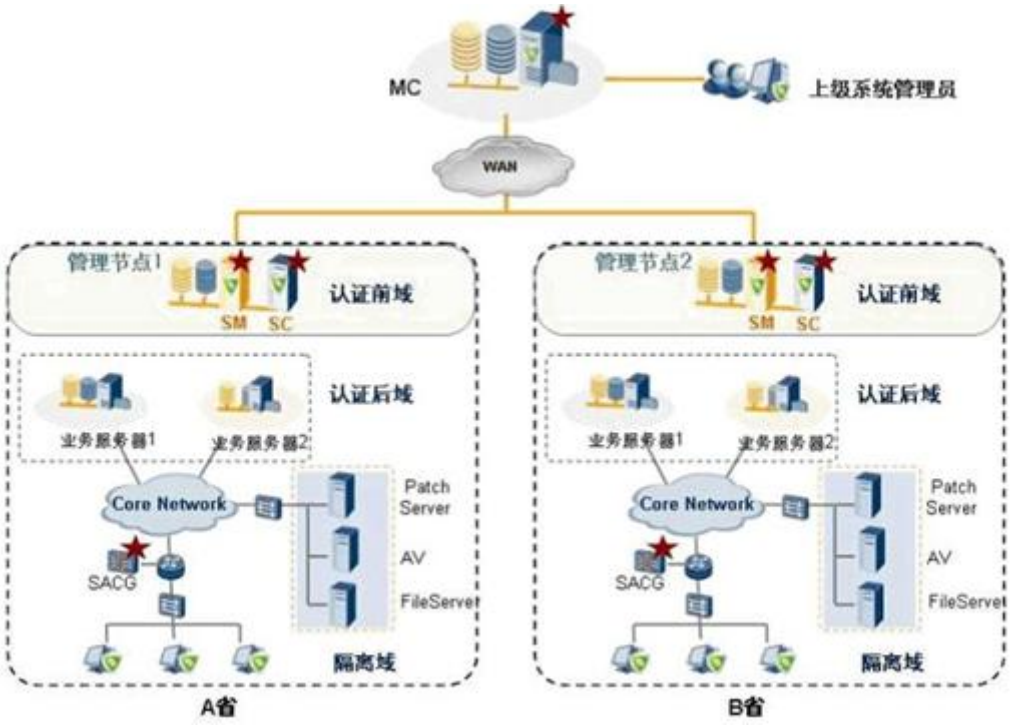
终端接入金融机构内网的管理流程如下所示：

图表 89 终端接入管理流程



6.2 PolicyCenter 系统组成介绍

图表 90 PolicyCenter终端安全系统结构图



PolicyCenterPolicyCenter系统由如下几个部分组成：

1. MC管理中心

分级管理部署时使用，作为PolicyCenter的管理中心，负责制定总体的安全策略，下发给各个PolicyCenter管理节点，并且对PolicyCenter管理节点实施情况进行监控。

2. PolicyCenter管理服务器SM

系统管理员通过WEB管理界面，可以完成终端用户管理、安全策略配置等业务管理工作。通过该操作界面，系统管理员可以查询终端的安全状态和违规的历史记录和报表。

此外，作为管理服务器，将管理其下的各个PolicyCenter控制服务器SC的连接状态，向已经连接的各个SC控制节点发送实时指令，完成各种业务。

3. PolicyCenter控制服务器SC

SC主要负责完成如下几项业务：

- 与802.1X联动，当身份认证通过后，根据终端的安装状态，通知802.1X交换机开放网络端口或者切换VLAN。
- 与SACG联动，当身份认证通过后，通过私有协议，根据终端的安全状态，对于安全检查不通过的终端，通知SACG切换到隔离域。对于安全检查通过的终端，通知SACG切换到认证后域。
- 作为与PolicyCenter安全代理SA交互的控制点，完成身份认证、安全策略下发、数据上报等任务。

4. 网络准入控制设备

有三种可选的网络准入：

1）802.1X交换机

2）安全准入控制网关SACG

3）基于终端主机防火墙的软件准入控制

通过准入控制设备，把企业的网络资源划分为一个认证前域，若干个隔离域，以及若干个认证后域。终端在身份认证前，只能访问认证前域；当终端通过身份认证，没有通过安全认证的时候，只能访问该终端用户所属的隔离域；当终端通过身份认证，并且通过安全认证，根据终端用户的身份，切换到该用户对应的认证后域，达到最小授权访问控制的目的。

5. PolicyCenter安全代理SA

PolicyCenter安全代理是一个安装在终端PC上的应用程序，当终端PC启动后，终端用户输入用户名+口令，执行身份认证和安全检查操作，并且把检查的结果作为安全认证开通网络访问权限的依据。在代理执行的过程中，监控终端的行为，包括监视和控制两个部分，如禁止使用USB接口以及监视用户所有网络访问的WEB URL，并且把审计的结果上报服务器，作为分析和统计的数据来源和审计的证据。PolicyCenter安全代理提供补丁管理、软件分发、资产管理、公告下发，以及远程协助等IT管理辅助功能。PolicyCenter安全代理全面支持多种Windows操作系统，如Windows XP、VISTA、Windows 7等，全面支持64位Windows操作系统，满足复杂环境下PolicyCenter需求。

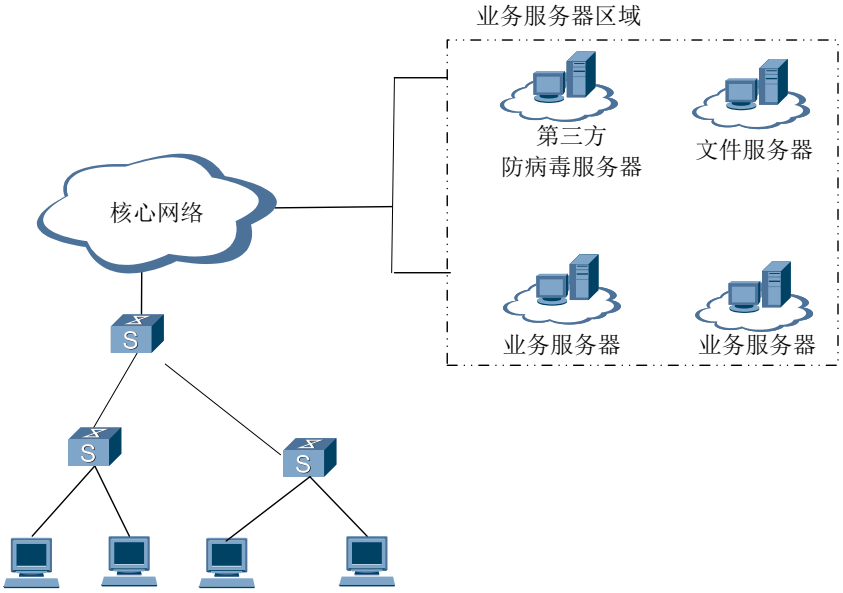
6. 基于ActiveX技术的WEBAGENT认证客户端

PolicyCenterPolicyCenter提供无需在终端安装代理软件的安全解决方案，通过基于ActiveX技术的WEB认证客户端，提供身份认证和安全检查操作，并且把检查的结果作为安全认证开通网络访问权限的依据。

6.3 部署方案

金融机构网络拓扑结构如图所示：

图表 91金融机构网络拓扑结构图

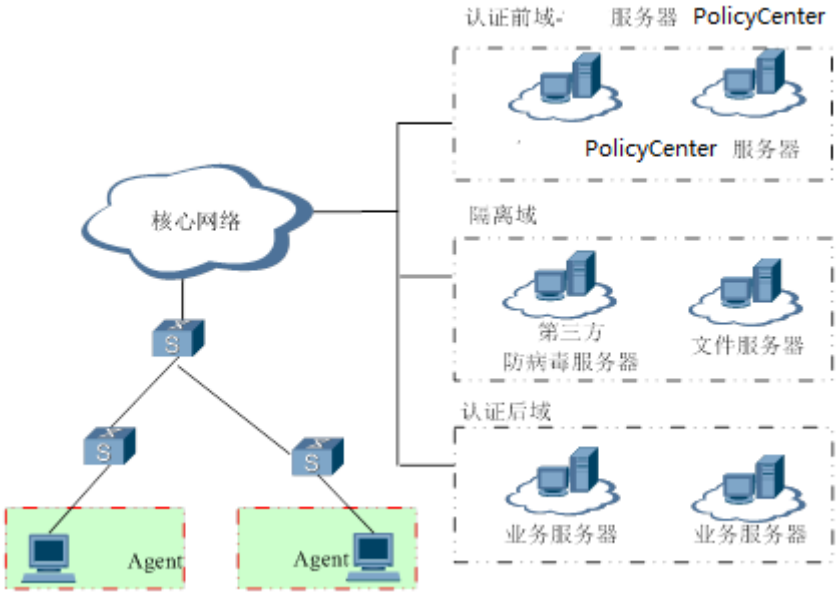


其网络架构特点如下：

- 结合桌面云部署，终端桌面较为集中，桌面统一部署在数据中心；

根据方案设计依据和设计原则，结合XX金融机构现网拓扑架构和客户的具体需求，建议PolicyCenter系统采取集中式部署，部署示意图如下：

图表 92 金融机构PolicyCenter系统部署示意图



部署说明：

1） 在所有接入终端安装PolicyCenter系统的客户端Agent；

2） PolicyCenter系统服务器部署在现有业务系统区域，保证与所有终端路由可达；

3） 在PolicyCenter系统管理界面启用基于主机防火墙的准入控制功能，并将现有网络资源按照业务和安全等级划分为3个安全域：

- 认证前域：终端在身份认证和安全检查通过前能够访问的网络资源，包括 DHCP 服务器、PolicyCenter 系统服务器等；
- 隔离域：终端在通过身份认证但没有通过安全检查时处于被隔离状态，此时仅能够进行安全修复操作，包括防病毒软件病毒库升级服务器、补丁服务器等；
- 认证后域：终端在通过身份认证和安全检查后能够访问的网络资源，管理员可根据工作相关

性和最小授权原则，将不同的终端用户授权访问相应的网络资源，有效防止非法访问和越权访问。

此部署方案中，需要在所有接入终端安装PolicyCenter系统的客户端Agent，通过PolicyCenter Agent集成的主机防火墙对终端接入网络进行准入控制。PolicyCenter服务器根据终端身份认证和安全检查的结果，通知终端上的客户端Agent允许或拒绝接入金融机构网络，从而实现对终端接入网络的控制。

6.4 PolicyCenter 方案

6.4.1 终端加固管理

企业内网终端众多，员工的计算机水平和信息安全意思参差不齐，由于操作系统安全设置不当而引起的安全风险越来越明显，仅通过目前行政管理手段无法保证所有终端的安全性，建议加强对操作系统的安全加固管理，具体管理方案如下：

- 防病毒软件安全策略

目前XX公司内网的办公终端绝大多数已经安装了防病毒软件，但由于强制检查，导致终端长期不更新病毒库和病毒引擎版本，使得防病毒软件形同虚设，没有发挥其重要的终端保护能力。

因此，建议通过PolicyCenter系统的防病毒管理策略实现终端的安全防护，PolicyCenter配合企业自身的防病毒软件，通过检查终端是否安装、运行状态以及防病毒软件的更新状态，作为判断终端当前安全状态的一个依据，阻止或提示没有部署杀毒软件的终端或者杀毒软件长期不更新的终端接入网络。保证企业内网运行的终端杀毒软件能够及时更新并且有效运行，减少病毒感染和扩散的风险。

- 强化补丁安装

加强操作系统和应用程序的安全漏洞检查，把补丁的检查作为一个重要的检查项，检查操作系统补丁、IE的SP补丁、OFFICE的SP补丁等，当检查到终端没有部署必须的补丁的时候，PolicyCenter系统能够协助终端快速完成补丁的修复。

- 超时自动锁屏

通过屏幕保护策略检查终端的屏幕保护是否启用，屏幕保护程序密码是否设置以及屏幕保护启动时间是否符合企业安全要求的安全检查，保证终端在空闲一定时间后屏幕保护程序自启动的安全要求，满足企业终端桌面管理规范。当终端屏幕保护设置不符合规范时，进行自修复。

- 注册表配置管理

通过对系统注册表键值检查，完成终端注册表键值存在与否的安全性检查。支持对终端的自动修复功能，对于要求存在的键值，如果该键值不存在，则添加该键值；对于不允许存在的键值，如果该键值存在，则删除该键值。

- 冗余账号检查

通过检查系统冗余账号，PolicyCenter系统能够协助管理员发现终端长期未使用的临时账号，降低企业PolicyCenter风险。

- 检查账号安全

通过账号的弱口令检查、账号群组检查、本地密码策略包括密码长度最小值，密码最长存留期属性检查等，保证终端操作系统账号的安全；

- 检查端口策略

通过检查终端口策略，有效保证对于接入网络的终端，及时提醒个人用户关掉无用端口，保证无用服务的最小化使用原则；

- 网络共享管理

Window操作系统默认情况下对共享文件夹和共享打印机设置为Everyone权限，如果终端用户安

全意识不高的情况下，就会带来较大的安全隐患。一方面，网络内任意终端可能在未获得授权的情况下直接窃取共享信息；另一方面，公开的共享目录也给病毒的传播提供了温床。PolicyCenter的系统安全管理功能，能够及时协助终端用户发现并且清理不安全的共享账号。

- 监控非法应用和服务

通过检查终端的软件安装情况和监控终端软件程序的运行情况，阻止终端安装和运行非法应用程序。如果发现安装或使用了非法软件、进程和服务，可以通过与准入控制设备的联动提示或阻止该终端接入网络，也可以拦截非法软件、进程和服务的使用，规范员工的行为。同时，管理员可通过审计软件的安装和使用情况，从而及时了解安全状态。

6.4.2 终端行为管理

法律规定了很多网站是非法的，比如有色情、迷信和犯罪相关的等等。使用宽带接入互联网后，企业内部网络某种程度上成了一种“公共”上网场所，很多与法律相违背的行为都有可能发生在内部网中。这些事情难以追查，给企业带来的法律法规方面的风险。因此，建议对员工的网络访问行为进行管理，具体管理方案如下：

- 监控网站访问

通过对WEB访问的监控，记录终端用户的WEB网站访问信息，由管理员进行统一管理和审计。通过这样的手段，一方面可以管理员工的上网行为，上班时间屏蔽一些与工作无关的网站；另一方面，提供审计和责任追溯的途径。

- 软件安装标准化

通过软件黑白名单检查，检查终端安装软件的列表，可以定义软件黑名单的违规软件列表和软件白名单的合法的软件列表，也可以通过检查软件黑白名单规定只能安装列表中的软件或者必须安装的软件，加强企业桌面软件统一安装的标准性。

- IP 访问和网络应用程序监控

通过对终端的IP访问控制和网络应用程序访问控制功能，对于一些安全性要求比较高的业务系统，允许定义基于时间段的IP访问规则，允许配置特定用户群在下班时间后不能访问一些关键的业务系统，防止对这些关键服务器可能造成的危害。允许定义网络应用程序访问规则，控制IM等聊天工具在上班时间的使用。此外，提供网络流量监控功能，能够协助管理员发现流量异常的终端。

- 终端入网审计

提供终端登录内部网络的日志上下线记录，管理员可以通过日志及时查询哪些用户在什么时间登录的企业内网安全网络，同时对长期没有登录的账号也提供检索查询；

6.4.3 信息防泄密管理

目前企业办公终端数量较多，员工的办公终端里存储大量涉及企业机密的敏感信息，时常发生员工通过终端外设，如刻录光盘、U盘拷贝、打印等方式将敏感信息外泄，目前通过人工管理方式不仅耗时费力，而且效果并不明显。针对此种状况，建议加强对终端外设接口的监控，具体管理方案如下：

- 外设接口管理

关闭终端上不需要光驱、刻录机、软驱、打印机等外部设备以及串口、并口、红外、蓝牙、PCMCIA卡、1394、SD/MMC控制器等计算机外设接口，通过关闭不必要的外设和接口，从而在一定程度上防范信息泄漏。

- 监控 USB 设备使用

在不影响USB鼠标/键盘的情况下， 对USB设备的管理支持放行、监控、禁用、只读和写加密四种状态。

USB监控属性：对USB存储设备的文件操作进行监控，识别和记录创建文件、拷入U盘、拷出U盘、内部复制、删除文件等操作的审计记录；

USB禁用属性：禁止终端使用USB设备；

USB只读属性：对USB存储设备进行只读控制，防止终端用户将本地硬盘上的数据拷贝至USB存储设备上；

USB写加密属性：允许终端正常使用USB设备，当终端用户从本地硬盘将文件拷贝到USB设备时，系统自动对拷入文件进行加密，从而保证拷入的文件只允许在企业终端机上使用；

- 拨号连接管理

通过管理Modem、3G上网卡、ISDN、PPPOE拨号设备，管理员可以通过提供的安全策略监控或阻断终端的拨号行为，系统自动记录拨号的开始时间和结束时间或者禁止终端用户使用拨号设备，有效阻止终端绕过企业的监管连接互联网，避免企业内网直接面对来自互联网的攻击。

- 防止违规假设 PROXY/路由器等外联设备

监视内网私自架设PROXY服务器的非法外联行为，当发现违规架设PROXY服务器，可以记录违规PROXY服务器的地址/端口信息，上报服务器，由管理人员进行跟踪和处理。确保企业的所有互联网出口流量都经过统一架设的出口网关，通过出口网关过滤不安全的网络访问，保障企业内网安全。

- 文件操作审计

通过文件名和通配符的方式自定义需要监控的文件记录，提供文件的新建、删除、编辑、复制、重命名等操作日志记录，方便安全事件的追溯。

6.4.4 网络安全防护

- 监控网络异常流量

蠕虫病毒的爆发一般都伴随着大量的异常网络流量。通过对网络异常流量的监控，PolicyCenter系统能够协助管理员发现流量异常的终端，并针对超过流量阈值的终端进行告警或阻断。

- ARP 防护

启用ARP防护功能，对已经安装了PolicyCenter安全代理的终端，进行ARP报文过滤，阻止终端发出的ARP欺骗报文，以及ARP泛洪报文。学习和绑定网关的IP/MAC关系，过滤各种伪造网关的ARP报文。通过该防护方案，即使网络中存在少量没有部署PolicyCenter安全代理的终端感染了ARP病毒，也不会导致局域网范围内ARP报文泛滥对网络造成的影响。

- 拨号连接管理

通过管理Modem、3G上网卡、ISDN、PPPOE拨号设备，管理员可以通过提供的安全策略监控或阻断终端的拨号行为，系统自动记录拨号的开始时间和结束时间或者禁止终端用户使用拨号设备，有效阻止终端绕过企业的监管连接互联网，避免企业内网直接面对来自互联网的攻击。

- 防止违规假设 PROXY/路由器等外联设备

监视内网私自架设PROXY服务器的非法外联行为，当发现违规架设PROXY服务器，可以记录违规PROXY服务器的地址/端口信息，上报服务器，由管理人员进行跟踪和处理。确保企业的所有互联网出口流量都经过统一架设的出口网关，通过出口网关过滤不安全的网络访问，保障企业内网安全。

- DHCP 强制管理

当企业网络规划强制终端要求通过DHCP方式获取IP地址时，为了避免终端通过静态IP获取网络资源时，在终端接入网络过程中，对其违规行为进行记录，同时提供自修复功能；

6.4.5 USB 存储设备接入管理

现网当中有大量的USB存储设备在使用，这些存储设备在方便数据传递的同时，增加了安全管理的风险，大量外来USB存储设备容易引起病毒的传播、内部数据的泄密等。要解决USB存储介质的管理问题，首先解决未注册的USB存储设备的接入问题，需要将所有在公司内部使用的USB存储设备都纳入安全管理体系，要对已注册和未注册的USB存储设备使用的权限进行控制，要能通过身份认证明确终端使用人员的信息，员工对已注册和未注册的USB存储设备具有不同的使用权限，通过策略可限制员工对注册USB存储设备和非注册USB存储设备的使用权限。

- USB 存储设备的注册审批流程管理

由于在企业内部使用未注册的USB存储设备会受到限制，员工在使用USB存储设备前，需要通过PolicyCenter代理提交注册申请。根据员工提交注册申请所使用的账号是否具有自动审批权限，所提交的注册申请的审批过程有所不同。

如果提交注册申请的员工具有自动审批权限，则该注册申请自动审批通过，无需管理员审批。

如果提交注册申请的员工不具有自动审批权限，则该申请提交到管理员处等待审批，管理员审核员工提交的申请，当申请属实时批准申请，当申请不属实或注册申请填写错误时拒绝申请。

审批通过后的USB存储设备即成为已注册的USB存储设备。

➢ USB 存储设备权限策略管理

USB存储设备管理功能通过监控USB存储设备策略，实现对已注册和未注册的USB存储设备使用权限的控制，员工对已注册和未注册的USB存储设备具有不同的使用权限。

可供选择的权限包括禁用、只读、监控、写加密。写加密：在启用加密写功能后，终端用户拷贝到U盘的文件都是经过加密的，只有该企业的用户并且安装了PolicyCenter安全代理的终端，才能使用这些加密文件，加密文件从U盘拷贝到本地硬件自动解密。通过写加密控制，即可以保证正常的USB存储设备拷贝资料的需要，有可 有效防止由于USB存储设备遗失和私自拷贝资料到公司外引起的信息泄密。

➢ 日志审计

从USB存储设备的管理角度出发，要求USB存储介质管理系统能对相关的USB存储介质的使用情况进行审计，能够监控USB存储设备的违规信息和使用记录，通过USB存储介质的使用帐号、PC的MAC、IP的信息对存在违规操作的已注册USB存储设备进行定位统计。提供完善的安全审计方案，包括USB存储设备安全违规报表和系统日志管理。通过严格的USB存储设备使用状态审计和检查，减少内部安全威胁，有效强化内部信息安全的管理，将公司的信息安全管理规定通过IT的手段得到落实。

6.5 桌面运维管理方案

6.5.1 补丁管理

Windows操作系统的安全漏洞是企业内网安全的一个关键因素。如果企业内网有大量没有部署关键补丁的终端，将会导致企业内网的漏洞攻击。只有当终端及时安装安全补丁，才能大大减少病毒在网络中大面积传播的可能。PolicyCenter系统的补丁管理方案可以有效的帮助安全管理员和终端及时解决严重关键级别补丁的安装任务，确保接入企业网络的终端的安全可信。

PolicyCenter支持以下两种补丁管理方式：

支持与WSUS联动；

内建补丁管理功能；

➢ PolicyCenter 与 WSUS 联动

企业内网已经部署了微软的WSUS服务器做补丁管理，但实际使用中却无法彻底解决终端的补丁管理问题，遇到的困扰如下：

配置自动更新方式虽然可以解决终端的补丁安全问题，所有补丁不加选择的全部安装，势必影响终端业务等正常工作；

选择其它更新方式，如果终端安全意识不高，不去下载或更新补丁，随意接入企业网络将会为内网带来安全隐患；

为了解决WSUS做补丁管理引起的问题，本方案中建议采用PolicyCenter系统与WSUS联动来加强WSUS的补丁管理：PolicyCenter负责判断终端的安全性，安全则顺利接入网络，不安全则调用WSUS客户端接口，实现管理员指定的关键重要补丁的安装工作。

PolicyCenter与WSUS联动过程如下：

在PolicyCenter管理平台上，由管理员配置终端的操作系统补丁策略，指定终端需要安装的补

丁等级和特殊补丁号，作为安全与否的判断标准。

当PolicyCenter终端进行网络接入认证时，进行身份认证和安全检查。安全检查前PolicyCenter安全代理先从服务器上更新补丁检查策略参数，与终端未安装的补丁列表进行比对，当发现有符合条件的未安装的补丁（即满足安全策略定义的严重补丁漏洞）时，强制终端的网络隔离并调用WSUS接口提供补丁自动修复任务；

用户点击修复窗口，调用WSUS接口实现终端关键补丁的自动安装和修复任务，安装完成后，重新认证，实现终端安全状态下的接入。

- 补丁管理功能

建议通过PolicyCenter系统自带的补丁自动管理功能和补丁策略检查配合实现，彻底解决企业补丁管理的问题。具体方案如下：

补丁来源和模板管理

安全补丁获取建议从微软网站自动下载补丁，系统自动提取补丁的相关信息。

管理员按照补丁的安全级别、补丁号自定义操作系统补丁分发的策略模板，不同的用户组可以分配不同的补丁管理策略模板。PolicyCenter系统可以根据管理员制订的补丁模板分发策略自动或手动向终端分发操作系统的补丁。

系统支持补丁列表的导入和导出操作。

补丁测试管理

当微软发布新的安全补丁时，管理员可以先挑选小范围的终端部署这些补丁，验证补丁的安全性；当小范围终端验证通过，确认安全性和兼容性后，再挑选更大范围（如全网）的终端部署和验证补丁，最终实现补丁的统一部署。管理员也可在系统提供的补丁报表里查看补丁的分发状态，监控补丁的分发进展。

关键补丁的准入管理

补丁的自动管理能够很好地解决在线终端的补丁安装问题，对经常离线（如长期出差）的终端建议通过补丁检查策略在接入企业内网时进行补丁检查，当检查到终端没有部署关键的补丁时，可以协助终端快速完成补丁的修复。对于特别重要的安全补丁，管理员可通过补丁检查策略与接入控制进行联动，强制接入企业网络的终端进行补丁检查，对于未按照企业要求安装指定补丁的终端禁止接入企业网络。通过此方式，从技术上保证了网络的安全性，并能够有效提高员工的安全意识，防范安全事件的大规模发生。

补丁分发状态管理

管理员在补丁分发任务管理界面上，可以查看指定终端安装补丁的情况，以及每个补丁的终端部署情况。

6.5.2 资产管理

随着企业业务的不断扩展，内网办公终端与日俱增，仅仅依靠纯手工的资产管理方式远不能满足需求，PolicyCenter系统的资产管理功能提供企业资产的全生命周期管理。

通过自动化的资产采集功能，及时收集终端的软硬件信息，为企业的管理者提供一个全局的视图，了解企业终端当前配置的状况，为企业更新终端配置提供一些决策上的统计数据。

PolicyCenter系统能够跟踪资产变更的情况，记录资产变更的详细信息，并且提供资产变更告警功能。PolicyCenter资产管理采用硬件信息标识一台计算机，即使重新安装了操作系统，PolicyCenter系统的资产管理模块也能够自动识别回原来的设备，避免因为重新安装操作系统导致大量冗余的无效资产数据，简化管理员的日常维护工作。

资产管理提供两种模式：

人工资产编号模式：系统中的每一个资产，都有明确的资产编码，终端用户在客户端程序上输入资产编码，实现资产注册，完成设备与资产编号和资产描述信息的关联。

自动资产编号模式：当管理员只希望管理终端的软硬件配置信息，以及跟踪软硬件变化的时候，

可以采用资产编号模式。系统将根据管理员设定的规则，对资产进行自动编号。

6.5.3 软件分发

能够协助IT管理人员分发企业内的标准软件，避免IT人员到每一台计算机设备安装应用软件，减少软件初次安装时的工作量。PolicyCenter系统的软件分发功能支持局域网范围内的快速下载，能够大大减少对网络带宽的占用。

6.5.4 公告下发

公告下发功能能够帮助企业IT管理员针对不同部门，不同人员下发公告通知，减少企业运维压力。

6.5.5 远程协助

远程协助功能能够帮助企业IT管理员及时响应终端用户的需求，无须东奔西跑的现场解决，从而提高问题解决的效率和业务部门的满意度。

6.5.6 安全审计报表

多维度的网络安全报表的平台化管理功能，通过预置报表模板完成整网安全的可视化管理。通过报表饼图,直观感受全网被管理终端接入网络的状态;通过趋势图获取终端接入网络的安全走势;通过柱状图，可快速定位违规终端的TOPN排行等;

6.6 PolicyCenter 可靠性介绍

6.6.1 操作安全性

PolicyCenter系统采用基于管理角色的操作权限控制,并记录管理员的操作日志保证提高操作安全性和可追溯性。PolicyCenter系统支持管理员、操作员、审计员权限分离。通过权限分离，实现系统管理的安全性，有效防止权限乱用。

6.6.2 数据安全性

PolicyCenter系统提供完善的数据安全解决方案。

数据传输方面：

- PolicyCenter 系统服务器之间的数据传输采用华为私有协议进行加密;
- 代理程序与服务器之间的通讯通过 SSL 协议加密;
- 补丁和软件的分发均支持数据完整性检查和断点续传功能,充分保证数据传输的安全性;

数据存储方面：

- PolicyCenter 系统通过数据库保存终端的违规日志信息，支持数据镜像和增量备份功能;
- 系统管理员通过管理界面进行日志管理时无法删除任何的违规信息，保证存储数据的完整性和原始性;

6.6.3 系统可靠性方案

➢ 逃生通道

PolicyCenter系统特有功能的逃生通道功能,当服务器发生故障无法执行身份认证和安全认证时，系统自动启动业务优先下的逃生功能。

逃生通道支持自动开启和关闭。如果企业偏重业务的安全性，则可以选择不开启此功能。

➢ SACG 故障方案

PolicyCenter的接入控制功能主要是通过接入控制设备SACG实现,终端计算机访问内网资源的上行数据都需要经过SACG设备,如果SACG故障将带来严重后果,因此SACG部署的可靠性性也很重要。

为避免单点故障的隐患，一般建议都采取双机备份方案来保证SACG部署的可靠性。

➢ 服务器多资源池备份方案

单台服务器能够处理一万并发用户数，可以通过增加服务器的方式实现后续扩容。服务器以资源池的方案提供负载分担功能，。当终端代理检测到当前区域内的主用服务器故障时或者无法连接时，自动关联下一台备用服务器继续进行认证。

6.7 子方案亮点

➢ 集中统一的认证、授权管理

管理员不在需要费尽脑汁去配置网络中的各个设备，去完成相应的访问控制机制，所有的安全策略都由PolicyCenter服务器统一的进行配置和下发，无论对于安全策略的定义、执行还是故障排查，都提供了很大的方便性。

➢ 融合的网络安全方案

充分利用已有的网络安全建设，将各个孤立的解决方案实现最佳的融合。PolicyCenter将内部网络的网络访问控制解决方案、防病毒解决方案、补丁管理解决方案、身份认证解决方案、资产管理解决方案结合一起，实现了对终端安全方案的强制执行，不符合终端安全策略的用户，将会在网络访问中受到限制，对网络访问的方案增强到基于网络标识、用户标识和终端状况等因素的集中授权。

➢ 灵活丰富的安全检查

包含了业界最多的终端安全检查策略，并且在用户访问的整个过程当中都可以进行检查，一旦发现于预定义的策略不符，系统可以改变该用户的权限，或者禁用用户。

➢ 安全管理

采用基于管理角色的操作权限控制,并记录管理员的操作日志保证提高操作安全性和可追溯性;支持管理员、操作员、审计员权限分离,通过权限分离，实现系统管理的安全性，有效防止权限乱用；在数据安全性方面，系统内部所有通讯均采用加密手段传输，充分保证数据传输的安全性；数据存储支持数据镜像和增量备份功能，保证存储数据的完整性和原始性。

➢ 高可靠性

重要组件均提供主备和负载均衡，提供独有的逃生通道功能，在服务器发生宕机等极端情况下能够自动暂时放开网络访问控制，以免影响正常业务；

6.8 配置清单

根据XX的网络情况和终端数量，这里推荐配置的服务器具体使用及说明如下表：

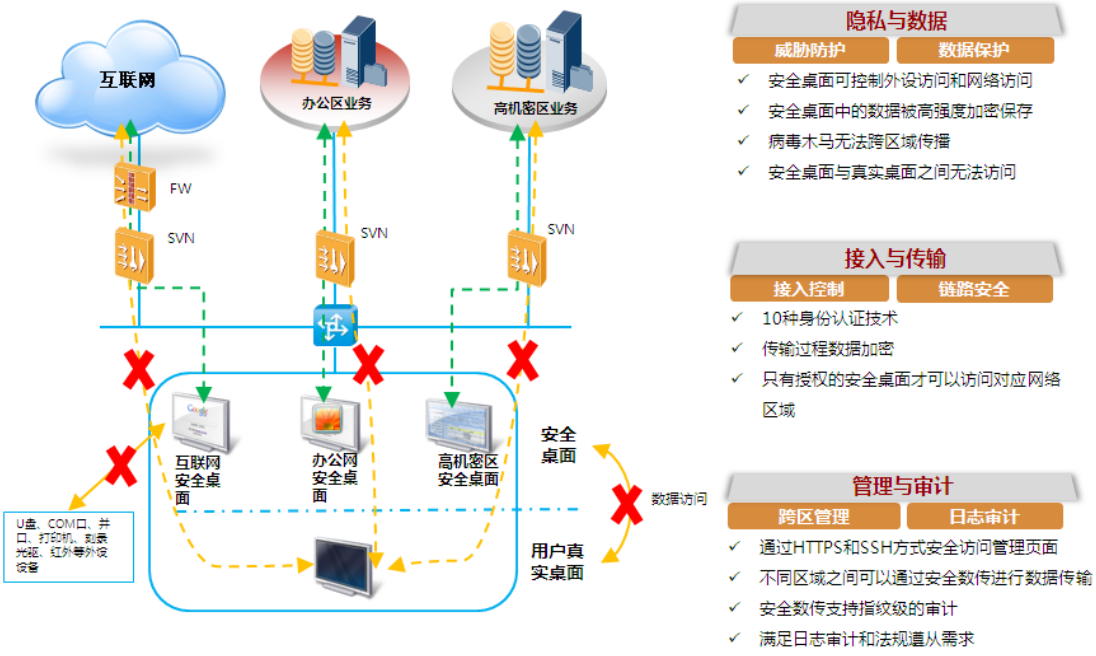
部署位置	数量（台）	说明
总部	2	分别安装PolicyCenter系统SM、SC和SQL Server 2005数据库组件，两台服务器之间互为主备；由总部管理员统一对全网终端进行安全管理

XX 分 公 司	1	安装PolicyCenter系统SC组件，负责XX分公司本地500终端的安全接入控制；当上海服务器宕机时，上海分公司的终端连接到总部SC服务器上进行认证

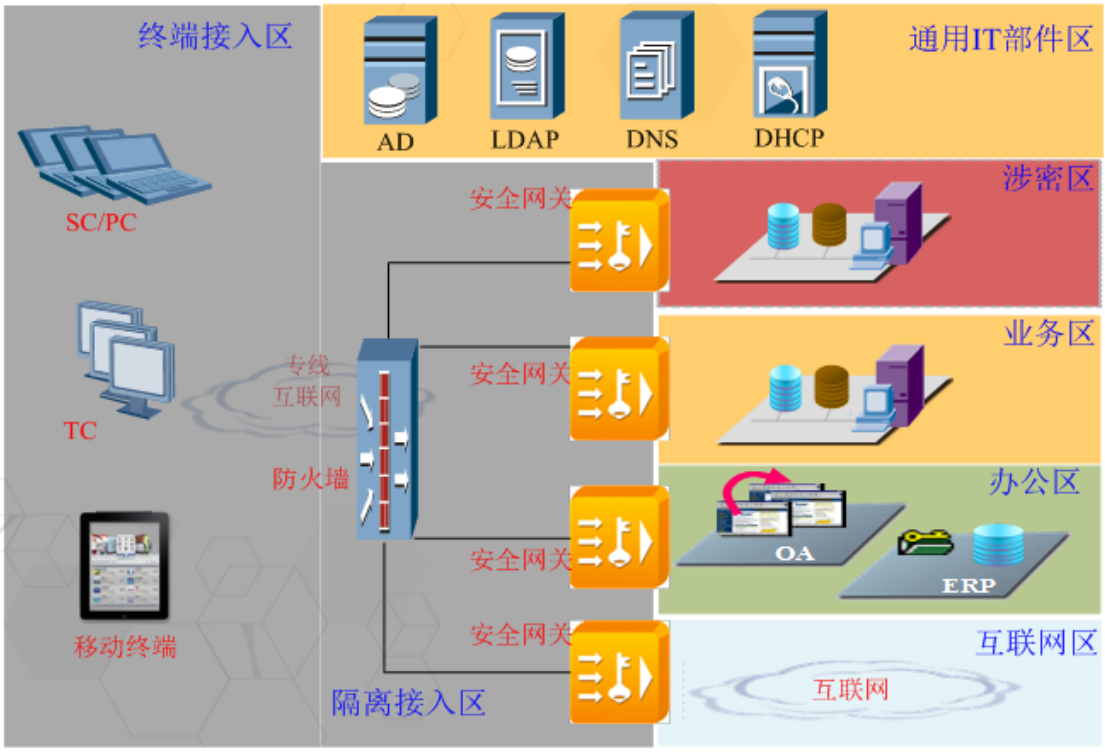
7 华为安全沙箱子方案

7.1 方案概述

安全沙箱方案中需要在不同业务区域之间部署安全接入网关， 所有跨区域访问的终端接受该安全接入网关的管理和控制，跨区域访问时，终端和安全接入网关之间的数据传输进行安全加密。当终端需要进行跨区域访问时，首先需登录安全接入网关，接受安全接入网关的接入认证。认证通过后，接入终端在真实桌面系统中创建一个虚拟安全桌面，和本地真实桌面进行安全隔离。



7.2 区域智慧隔离解决方案架构



区域智慧隔离方案中需要在不同业务区域之间部署安全接入网关，所有跨区域访问的终端接受该安全接入网关的管理和控制，跨区域访问时，终端和安全接入网关之间的数据传输进行安全加密。当终端需要进行跨区域访问时，首先需登录安全接入网关，接受安全接入网关的接入认证。认证通过后，接入终端在真实桌面系统中创建一个虚拟安全桌面，和本地真实桌面进行安全隔离。

通过安全沙箱方案总体部署后，能够实现不同密级区域间信息安全互访，不同安全级别安全区域间访问将达到以下效果：

- **跨区域访问接入控制，包括用户认证控制和终端认证控制；**
  1) 用户认证控制：用户进行跨区域访问时，需要登录安全接入网关，接受用户认证。安全沙箱支持多种丰富的认证方式，包括本地用户认证、Radius 认证、SecurID 认证 LDAP 认证、AD 认证、数字证书认证、短信密码辅助认证、图形验证码辅助认证；
  2) 终端认证控制：安全接入网关在用户登录时，除了对用户身份进行认证外，还可以对接入终端进行准入检查，可检查的内容包括：操作系统版本号、操作系统补丁、防病毒软件、防火墙软件、关键文件、网络通信端口、注册表、关键进程等，只有满足安全接入网关定义的安全策略的终端才能够被允许接入。
- **安全桌面推送及控制策略下发**

在用户认证及终端认证通过之后，安全桌面将被自动推送到用户终端，并下发安全桌面控制策略。安全桌面控制策略包括：可执行文件控制、文件访问控制、注册表控制、外设及端口禁用、网络访问控制、命令行控制等。在安全桌面启用及控制策略下发完成之前，用户终端被限制不能进行跨区域访问。

- **用户跨区域获取数据仅限于安全桌面，退出后清除**

安全桌面内保持与真实桌面的操作习惯一致，使用过程中跨区域获取的数据文件重定向加密存储在虚拟空间中，退出安全桌面后，安全桌面内遗留的文件、对计算机终端做的任何修改都会被清除，用户终端将被还原成为启用安全桌面之前的状态。

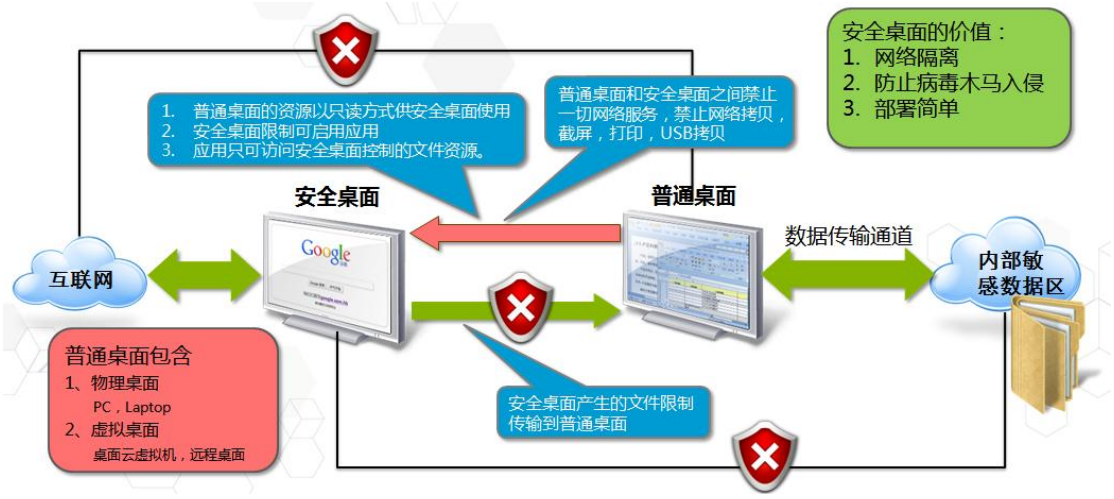
- **特权用户跨区域受控安全数据传输，“数据指纹级”安全审计**

特权用户在需要进行跨区域文件传输时，管理员可开通安全数传权限，允许其进行跨区域文件传输，并对其传输文件名及文件内容进行摘要或转存。通过细粒度的审计控制，实现用户跨区传输的防抵赖、可追溯，实现区域隔离系统的可控、可管、可查。

7.3 办公区访问互联网场景

办公内网中的业务人员有时需要进行互联网查阅资料，了解业界动态，如果直接允许办公网终端直接访问互联网，可能会使终端被黑客入侵、被植入木马后门等恶意程序导致办公网机密数据泄露。

通过在互联网出口部署 SVN 安全接入网关，办公网终端通过与互联网边界安全接入网关建立加密通道，并启用安全桌面访问互联网。



安全桌面中可以设置真实系统中磁盘空间对虚拟系统进行隐藏，因此在虚拟安全桌面环境下将无法访问真实硬盘中的文件，以防止数据泄露。而互联网访问过程中可能潜伏于虚拟磁盘空间中的病毒、木马等恶意程序，由于在安全桌面退出时会对虚拟空间中的重定向数据进行清除，因此可以保证没有任何恶意程序残留在真实系统。

办公网用户访问互联网时，有时需保留一些从互联网上获得的资料，而在安全桌面中是默认无法保留任何文件的，因此也会带来了不便，为了能让业务人员更好开展工作，管理员可以对安全桌面用户可以配置控制策略，为用户开启文件传输隧道。终端用户可以把安全桌面中的指定文件，通过手工的方式从虚拟环境中导出到真实桌面，从而可以不受限制地应用在本地的计算机中。通过“文件摆渡”方式的传输，避免了基于 TCP/UDP 的木马控制和攻击，同时传输文件内容需要通过安全审查和内容过滤，以确保文件安全。

办公网访问互联网场景应用特点：

- 禁止安全桌面下虚拟系统访问真实操作系统下本地磁盘，防止真实系统数据泄露
    - 安全桌面退出时，清除虚拟系统中重定向数据，防止恶意程序残留真实操作系统

允许特权用户开启文件传输通道，将虚拟系统中指定文件导出到真实操作系统

1.1 华为区域智慧隔离方案亮点

1.1.1丰富的终端接入控制

用户进行跨区域访问时，需要登录安全接入网关，接受用户认证。区域智慧隔离支持多种丰富的认证方式，包括

1) 本地用户名、密码认证
2) Radius认证
3) SecurID认证
4) LDAP认证
5) AD认证
6) 数字证书认证（UKey认证）
7) 短信密码辅助认证
8) 图形验证码辅助认证

安全接入网关在用户登录时，除了对用户身份进行认证外，还可以对接入终端进行准入检查，可检查的内容包括：

1) 操作系统版本号、补丁
2) 防病毒软件
3) 防火墙软件
4) 关键文件
5) 网络通信端口
6) Windows系统注册表
7) 关键进程

只有满足安全接入网关定义的安全策略的终端才能够被允许接入。

1.1.2完备的数据防泄露机制

区域智慧隔离解决方案具备完善的数据防泄露机制，满足用户通过安全桌面访问低密级区域和高密级区域场景。

文件访问控制

管理员可对安全桌面进行配置，指定安全桌面下允许用户访问的操作真实系统中的文件夹和目录。

文件重定向

使用安全桌面过程中跨区域获取的数据文件重定向加密存储在虚拟空间中，退出安全桌面后，安全桌面内遗留的文件、对计算机终端做的任何修改都会被清除，用户终端将被还原成为启用安全桌面之前的状态。

外设及网络访问控制

当安全桌面内保存有机密数据时，如果不对终端的外设进行访问控制，恶意用户将有可能通过打印、U盘拷贝及网络文件传输等方式将机密数据带离安全桌面，为了防止此类行为发生，区域智慧隔离方案提供配置选项，使得管理员可禁止安全桌面内访问终端外设及网络文件传输。

透明加解密

在安全桌面中，所有被修改过的文件、安全桌面内产生的数据都将被加密保存，真实桌面下无法正常打开和运行。加密算法采用强度最高的AES256，加密密钥动态生成，保存在安全接入网关中，并按周期进行更新。

防截屏、防粘贴板拷贝

通过对安全桌面截屏（屏幕拷贝）、系统粘贴板拷贝的方式，也可能导致关键信息的泄漏，区域智慧隔离解决方案通过对屏蔽截屏操作、虚拟化粘贴板等措施，防止机密数据泄露。

1.1.3 安全高效的办公能力

区域智慧隔离解决方案在保障跨区域的业务访问安全性的基础上，提供了丰富的高级特性，以提高办公效率，包括安全桌面保持功能、离线模式、安全数据传输、安全桌面协作等特性。

安全桌面保持

默认情况下，用户在安全桌面内所做的一切操作，在用户退出安全桌面之后都被清除，这种实现方式的安全性最高，但是影响办公效率，例如当用户在安全桌面内进行作业，当工作未完成但也不得不中断时（参加重要会议、下班等情况），此时保存在安全桌面内的工作成果如果不能保存将严重影响工作效率。

针对上述情况，管理员可配置“安全桌面保持”功能。启动安全桌面保持功能后，用户在安全桌面的工作成果，在退出安全桌面时，自动以高强度加密的方式保存在磁盘上。这些加密数据只有在相同用户重新进入安全桌面后才能重新打开。

离线模式

办公网用户在安全桌面下访问业务过程中，可能出现某项工作无法在工作时间内完成，如编辑文档或制作数据表格，直接退出安全桌面会导致数据全部被清除。这时可以将安全桌面切换到离线模式，离线模式安全桌面对数据的隔离保护依然有效，用户可以将工作带回家完成。当与SVN安全接入网关网络连接恢复后，将工作模式重新切回到在线模式。

安全数据传输

用户在安全桌面内编辑保存的数据文件，如果需要跨区域传递到另外一个业务区域， 用户可将该文件通过网络上传到一个特性的共享文件夹下。用户切换到真实桌面后可通过安全接入网关从共享文件夹下载所需的文件。

安全文件传输对于用户来说稍稍增加了复杂性，但是对于企业管理员来说极大了增强了安全性。首先管理员可配置用户所允许上传文件的共享文件夹、可配置用户所允许下载的共享文件夹、可配置用户上传下载文件格式、文件关键字过滤等。

用户通过“安全文件传输”功能上传下载文件的操作都会被详细的记录，管理员可根据记录定期审计用户行为，回溯用户的非授权操作。

安全桌面协作

当存在多用户协作场景时，通过安全桌面协作功能可支撑该工作方式。

默认情况下，用户起用安全桌面后，将和本地网络内的其他终端之间进行网络隔离，也就是说用户在安全桌面内无法访问到本地局域网内的其他用户终端。当一项工作需要多人完成时，该用户的工作成果无法传递给其他同事继续完成。通过“安全桌面协作”功能，可允许该用户在安全桌面内和另外一个用户的安全桌面进行网络通信，并且在网络中传递的工作成果以加密的方式保存避免网络窃密。

1.1.4 灵活易用的操作方式

由于终端操作人员 IT 技能水平良莠不齐，区域智慧隔离解决方案提供良好的易用性，避免因为操作复杂、管理复杂、维护复杂而影响到业务效率。

安全桌面下操作方式与真实桌面一致

认证结束之后，在计算机终端自动开启虚拟系统空间，对于终端用户来说是呈现出一个新的桌面，称之为安全桌面。在这个安全桌面内，操作性和原本的默认桌面是一致的，所以用户可以在安全桌面内保持其原有的操作习惯，无需对终端操作人员进行培训。

单机两安全桌面，同时访问两个安全区域

在超过两个业务区域隔离的情况下，例如企业同时存在办公网、业务网、安防监控网等业务区域，如果存在同一个终端要求能够同时接入两个不同的业务区域时，可在终端上启动两个安全桌面，除本地桌面连接本地业务网络外，每一个安全桌面可连接一个不同的业务区域。

多桌面任意切换，定制桌面背景

用户在终端上启动多个工作桌面后，可在不同桌面之间切换。区域智慧隔离解决方案中用户可在终端屏幕上方浮动的导航条上进行屏幕切换。

为了区分不同的工作桌面，管理员可在安全接入网关上对所有用户的安全桌面的背景图片进行统一定值，当用户在不同桌面间切换时，通过不同的桌面背景即可快速确定是否位于安全桌面。

跨桌面消息通知，不错过重要信息

对于一些及时通信软件，例如 QQ、MSN 等，当其运行在一个工作桌面环境内，而用户在另外一个工作桌面内作业， 为了保证及时通信软件的消息“及时性”，区域智慧隔离解决方案的安全桌面可允许即使通信软件的消息跨桌面通知，例如真实桌面内的 QQ 软件接收到即使消息后，可在安全桌面内以可见的方式提示用户。

7.4 安全沙箱产品选型

图表 93 华为安全沙箱产品选型

	SVN5530	SVN5560
SSL最大并发用户数	12000	20000
IPSec最大并发用户数	12000	20000
硬件		
固定接口	5×GE(RJ45)+4×GE(combo)+2×USB	
扩展插槽	1×FIC	
功能特性		
SSLVPN	支持Web代理、文件共享、端口转发、网络扩展等 支持访问Web资源、C/S资源、多媒体资源、基于IPv4的资源、基于IPv6的资源	

	支持虚拟桌面功能、安全浏览器、安全PushMail
数据保护	数据隔离功能、数据加密保存、缓存清除、安全桌面
VPN类型	SSLVPN、IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN
用户认证	支持本地口令认证(VPNDB)、AD认证、Radius认证、LDAP认证、SecurID认证、证书认证、USBKEY证书认证、短信认证、终端标识码校验、图形码校验等 支持单点登录、软键盘功能
权限控制	基于角色的授权、外部组的授权映射 基于接入终端安全等级的动态授权 基于IP、端口、URL的细粒度访问控制
终端安全	支持终端主机检查、缓存清除、终端标识码绑定、安全桌面功能
虚拟网关	支持多个虚拟网关，服务虚拟化、网络虚拟化，认证、授权、业务、资源实现完全独立管理
防火墙	支持访问控制、NAT、攻击防范等，支持虚拟防火墙
网络协议	支持IPv4和IPv6
部署及可靠性	支持单臂、双臂模式部署，支持主/备模式
整机规格	
尺寸（W×D×H）mm	442×560×43.6
满配重量	13 kg
电源AC	100V～240V（50Hz/60Hz），支持冗余
电源DC	-48～-60V，支持冗余
工作环境	温度：0℃～45℃ / 湿度：10%～90%
非工作环境	温度：-5℃～50℃ / 湿度：5%～95%

7.5 配置清单

图表 94 移动办公接入网关配置清单

设备类型	型号	单位	数量
安全沙箱接入网关	深信服VPN-7050	台	
安全沙箱软件	安全沙箱并发用户-含桑威合作伙伴深信服通用安全平台软件	个	

8 华为文档安全管理子方案

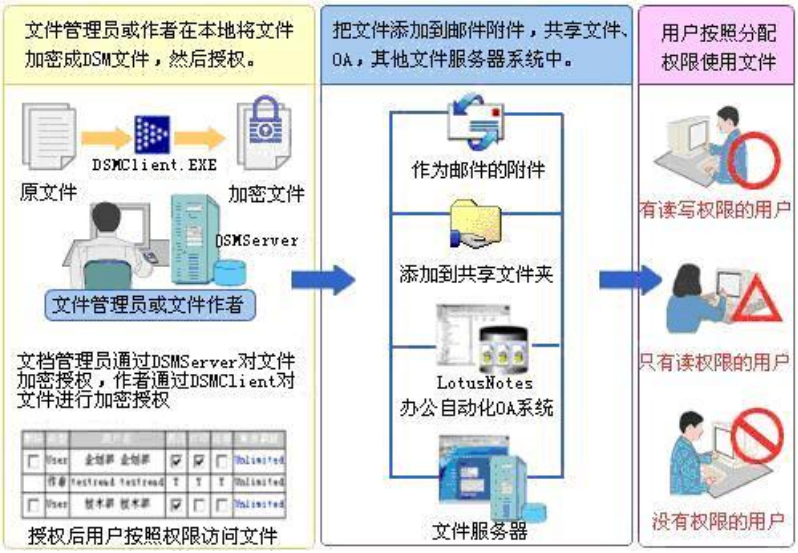
8.1 方案概述

DSM系统解决方案通过分散管理用户文件，保证安全控制服务器可以高效率处理用户身份验证、存储加密数据信息等操作，不但极大提高每个前端单独访问服务器的速度，同时极大提高许多前端并发访问服务器的速度。文件操作在用户客户端完成，使得在并发用户很多时整个安全控制系统的处理绝对性能不会下降。

另外，DSM系统解决方案通过分散管理文件，有效地让用户根据自身权限对文件进行灵活操作，只要通过服务器身份验证，能随时对文件进行操作。

DSM系统可以给每个部门分配一个或多个文档管理员，可以限制文档管理员管理的文档类型，大部门的文档管理员可以给小部门分配管理员，也可以回收小部门的文档管理员权限，对大金融机构应用来说，提供了很好的管理功能。

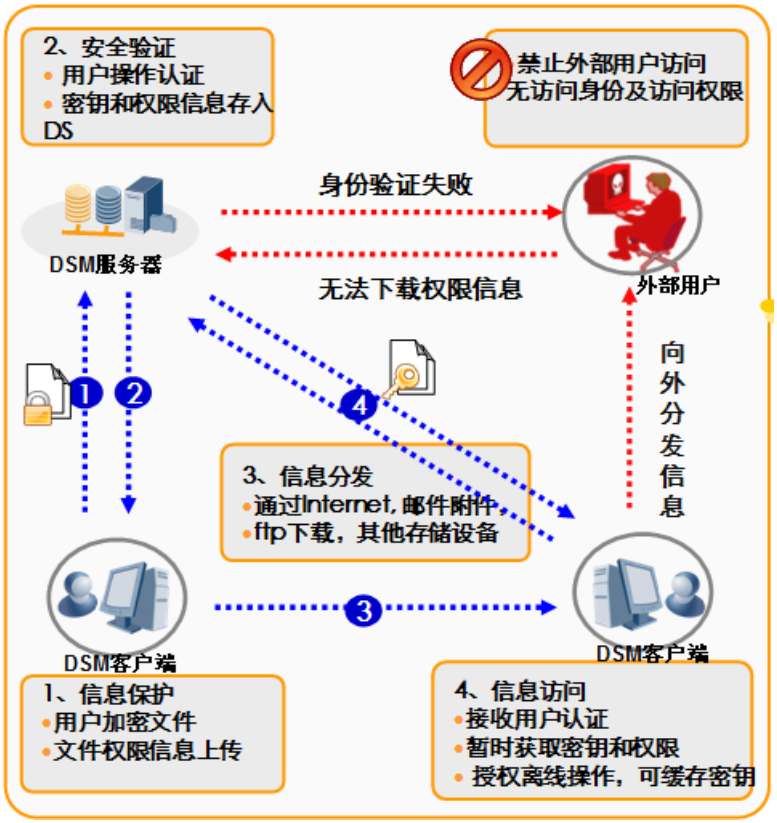
图表 95 分散管理文件，集中管理信息



8.1.1 文档加密过程

- 用户通过客户端软件加密文件，把文件密钥上传给服务器，同时文件作者可以对其他用户打印，阅读，保存，有效时间等权限进行授权。
- 其他用户获取到加密文件（通过文件共享或 email 等方式）
- 其他用户通过身份认证之后，可按权限使用文件。

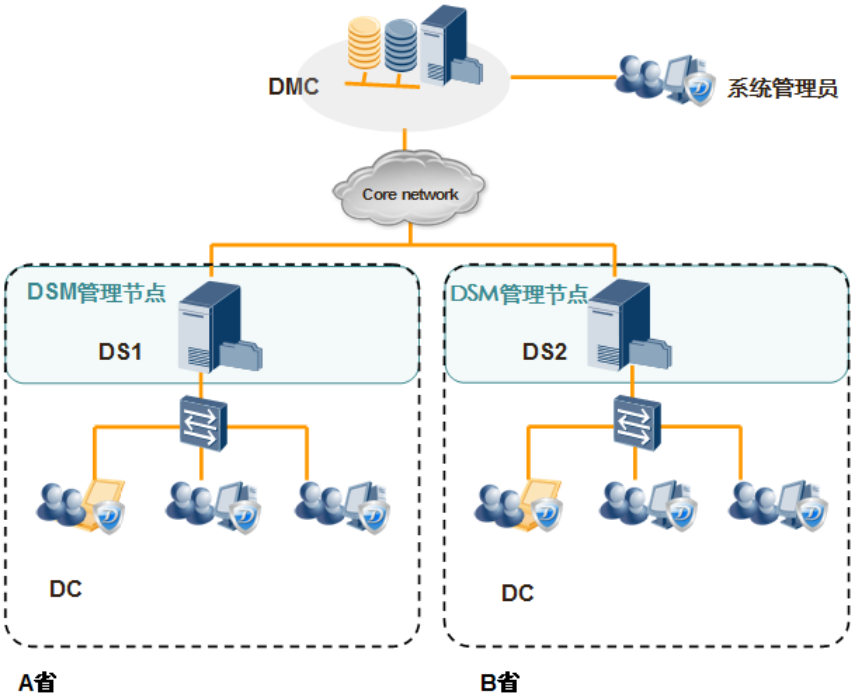
图表 96 DSM 系统工作流程图



8.2 系统部署架构

本次项目中，由于XX终端用户较为集中，推荐使用集中式部署方式实施文档安全管理系统。集中式部署方式中需要部署一套DSM系统，其组件主要由DSM服务器、客户端组成。DSM服务器群由至少一台服务器组成，当由三台或以上服务器组成时，DSM系统可以实现数据库热备、服务器冗余备份、负载均衡的功能。DSM服务器用于处理终端用户的请求，进行文档权限的统一管理。

图表 97 DSM分级分布式部署示意图



本次项目中，由于XX终端数较多，且有分支机构，因此建议分布式部署DSM文档安全管理系统。

DSM文档安全管理系统在部署上主要分两级架构，第一级为管理中心DMC，第二级为DSM管理节点，管理中心统一对下面的DSM管理节点进行系统管理，指派管理节点的文档管理员等。DSM服务器用于处理终端用户的请求，进行文档权限的统一管理。分级架构理论上提供了无限的人数扩展功能，支持用户的漫游和权限的跨系统（DSM管理节点）授权。

在分级部署中，每一套DSM管理节点就是一个完整的“独立部署方式下的DSM系统”，只是为了支持大规模的应用把各个DSM系统使用一个一级的DSM管理中心进行统一的管理而已，另外，跨DSM二级系统授权和用户漫游也需要DSM管理中心的支持。

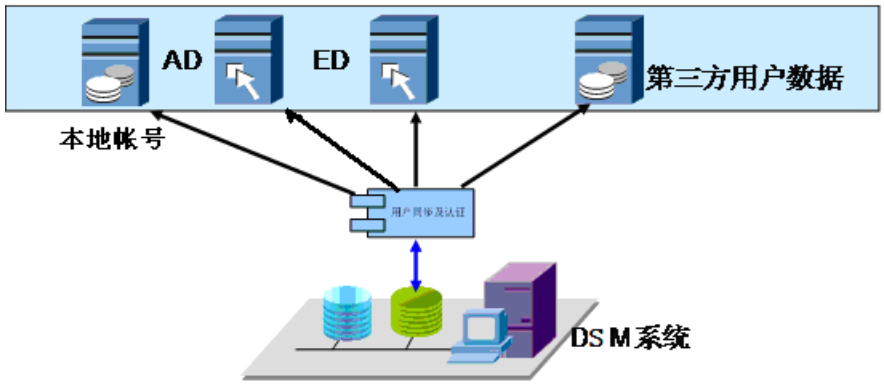
8.3 用户管理方案

8.3.1 账号管理方案

管理员可以在本地创建用户账号，还支持从其它身份管理系统AD和ED中同步用户信息。系统定时增量从第三方身份管理系统同步数据，从而保证最小带宽的用户账号同步数据。 独立的用户同步及认证模块，方便快速满足对第三方的用户数据定制联动。

考虑到账号的安全性，DSM系统以UUID作为用户的唯一标识，用户文档权限通过UUID进行关联，后续即使再创建被删除账号一样的同名账号，对于新生成的UUID，对以前设置的文档权限也不会有任何影响，保证了文档权限的安全性。

图表 98用户管理示意图



8.3.2 离线用户文档控制方案

DSM采用文档与权限分离的方式保证了加密文档权限的实时联机获取和更新，权限信息保存在DSM的服务器端，用户对文件的打开操作需要与DSM服务器通信。当网络被隔离或者用户出差等原因无法连接DSM服务器时，用户将无法连接DSM服务上申请加密文档的权限，这就意味着用户将无法打开被加密的文档。

针对以上场景，DSM系统为用户提供了离线操作功能。当用户要阅读曾经在自己机器上打开过并且具有离线操作权限的加密文档时，可以在此计算机上直接打开该文档。系统支持当用户对某个文档具有离线权限时，无需连接服务器获取权限，就可以对文档进行离线操作。离线操作功能与硬件绑定，保证了只允许在这台计算机上打开文档。同时支持离线时间和阅读次数的设置，充分保证离线文档的操作控制。

- **硬件绑定：**加密文件在与用户电脑绑定时会在服务器中记录用户电脑 CPU 的序列号，该文件只可以在这台电脑中进行阅读，不可以在其它电脑上使用；
- **允许离线时间：**保存到用户电脑中的已绑定的加密文件，其有效时间受加密文件绑定生成时有效时间设定的限制，该时间限制不会因为用户修改电脑时间而改变；
- **文档阅读次数：**可以给文档设置阅读的次数，在离线打开文档时也计算这个次数,阅读次数超过设置次数后无论在线或者离线都无法打开文档；

8.3.3 漫游用户文档控制方案

对于分级部署方案而言，各个地区都有属于自己的DSM管理节点，各个地区保存着各个地区用户的认证信息和文档的权限信息。

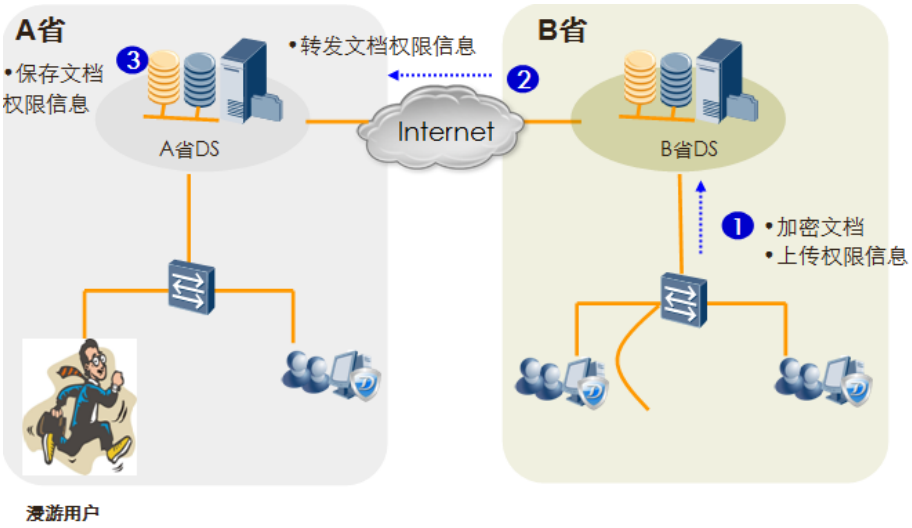
漫游用户是指一个用户从归属地区出差到另外一个地区时，无法接入到用户归属地区的DSM管理节点A，只能接入到出差目的地所在的DSM管理节点B，对于目的地DSM管理节点B而言，这些用户就是所谓的漫游用户。

为了方便文档权限的统一管理，满足用户身份信息和文档权限用户归属地集中管理的要求。漫游用户制作的所有加密文档的信息和权限都应该存储在用户归属地所在的DSM管理节点 A上，而不会存储在漫游所在地的DSM管理节点 B上。

漫游的方案如下：

- 用户身份认证，通过系统 DSM 管理节点 A 与 B 之间的通讯，把用户的认证信息发送到用户所属的 DSM 管理节点 A 上进行认证；
- 制作文档的权限信息，通过系统 DSM 管理节点 A 与 B 之间通讯，转发并保存在用户归属地的 DSM 管理节点 A 上；

图表 99 用户漫游示意图

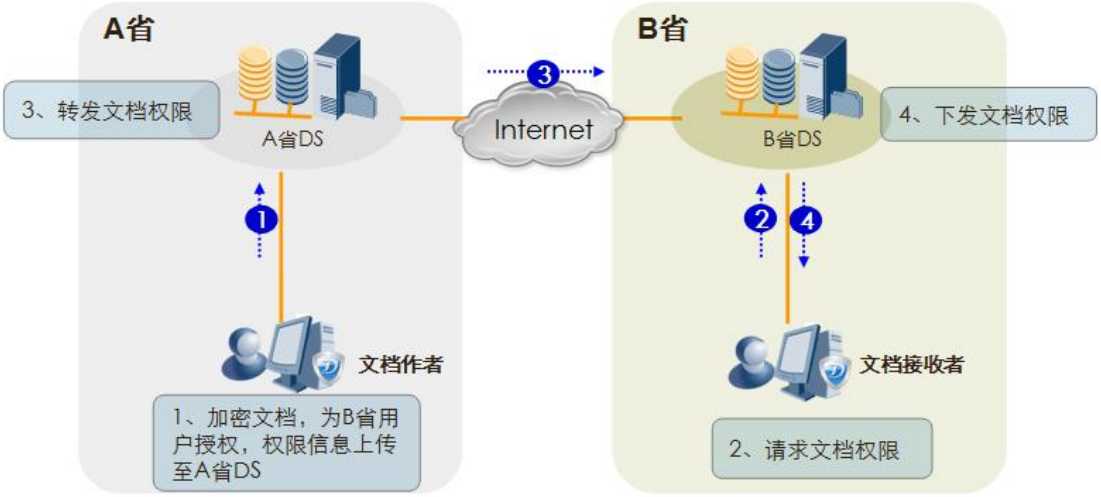


8.3.4 跨地区用户授权

对于分级部署方案而言，各个地区都有属于自己的DSM管理节点，各个地区保存着各个地区用户的认证信息和文档的权限信息。

文档的跨地区授权是指一个地区的用户A制作好加密文档后，给另外一个地区的用户B授予一些权限（例如读），另外一个地区的用户B拿到文档后，可以进行对应的操作（例如读）。用户B所在的DSM管理节点自动转发文档的权限信息到用户A所在的DSM管理节点，再通过DSM管理节点之间的通讯，将用户B的文档权限信息进行下发。跨地区的权限授于过程对用户B是透明且无感知的。

图表 100 跨地区授权示意图



8.4 系统冗余备份方案

系统冗余备份方案包括DSM服务器的备份和数据库的备份。

- DSM 服务器采用主备方式，通过协议实现冗余备份。当主服务器崩溃后备服务器可以继续提供主服务器相关服务。
- 使用镜像技术实现数据库备份，通过见证服务器实现数据库故障的自动转移。当主数据库服务器崩溃后，备数据库服务器可以正常进行服务。

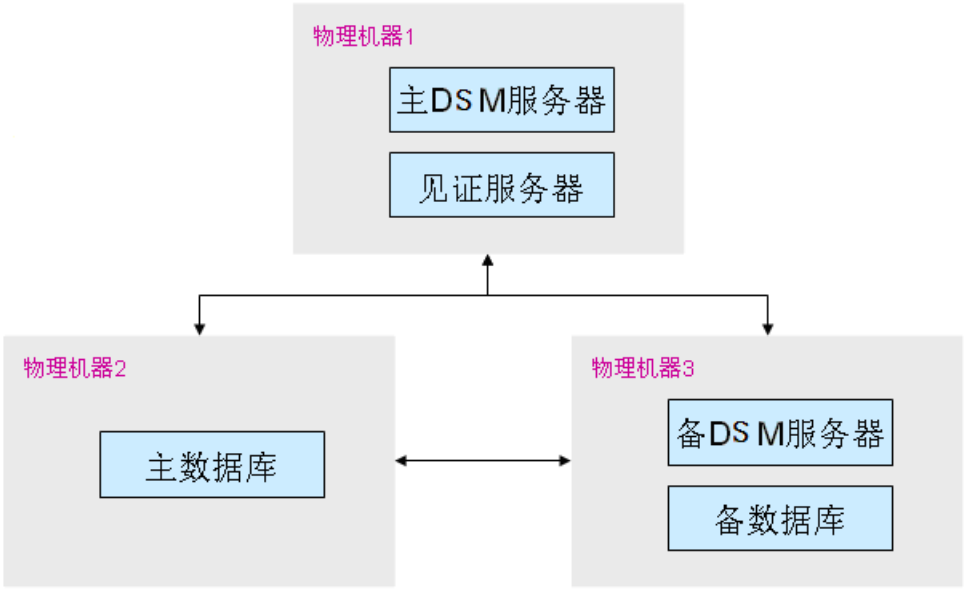
建议使用数据维护计划，使用镜像技术定期把数据库数据备份到磁盘，再通过手工方式把备

份的数据库文件存放到其它地方，保证数据的最大可靠性。

为了节约成本可以将备份的DSM服务器和备份的镜像数据库部署在同一台机器上面。同时，见证服务器对系统资源要求较低，可以部署到主DSM服务器上面。

服务器备份结构如下：

图表 101 服务器备份部署结构示意图



8.5 客户端软件部署模式

可以通过第三方工具实现客户端软件的部署，再通过手工方式实现安装，安装过程需要使用管理员组中的账号完成。推荐使用以下方式进行部署：

- 域控制服务器

如果客户已经部署AD域管理服务器，可以配置域服务器的用户域登录脚本，添加代理安装程序。

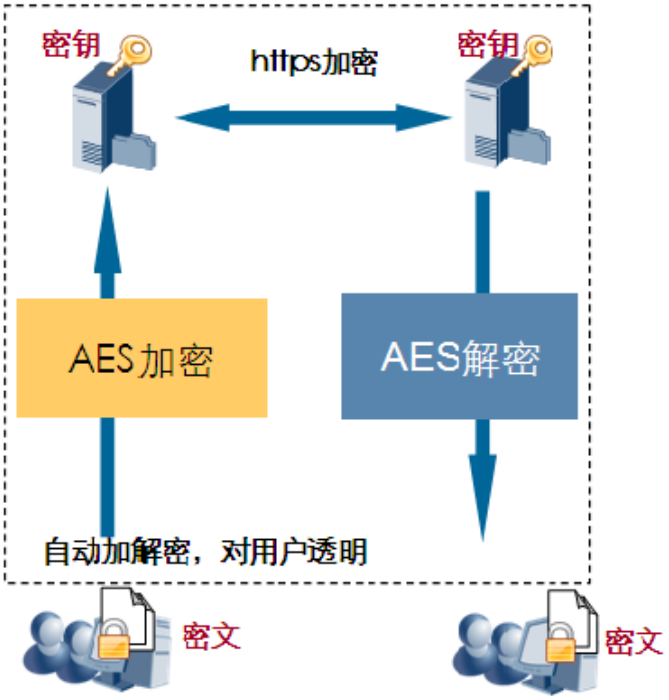
- 第三方工具

如果客户已经部署邮件系统或者其他文件传送工具，也可发送代理安装程序到终端用户桌面。

8.6 方案特点

8.6.1 强大的动态加密技术

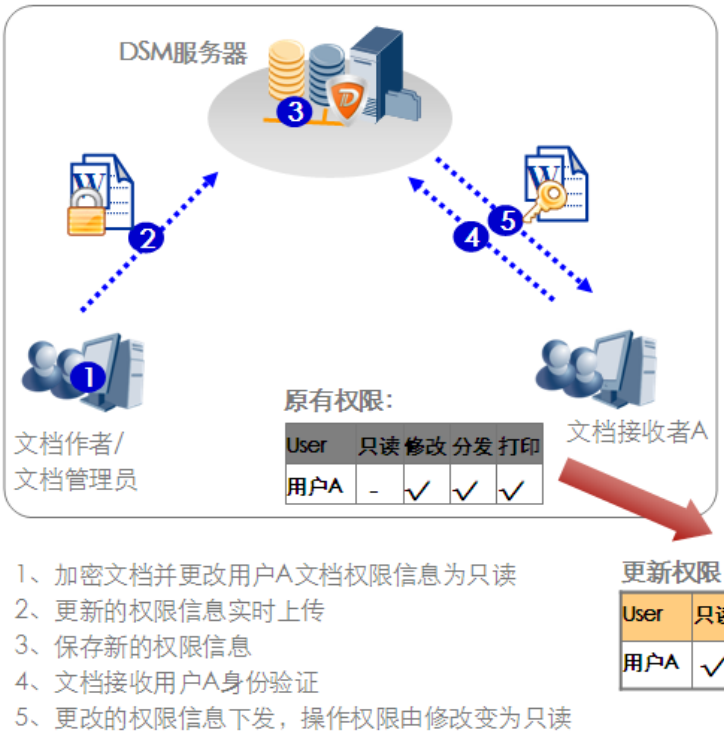
图表 102 DSM系统动态加密示意图



- 强大的 AES 动态加解密技术；
- 驱动层与应用层加解密结合；
- 密钥与内容分离：分散管理文件、集中管理加密信息。不仅极大地降低了服务器工作负载，而且确保了信息系统内用户能够灵活操作文件；
- 高效快速加密文档：只须单击加密按钮并设置权限，避免复杂人为操作；1MB 以内大小的文档加解密时间在3秒以内完成；
- 透明加解密，对使用者完全透明，不改变文档使用习惯；

8.6.2 实时的权限管理方式

图表 103 DSM系统权限管理示意图



- 只有经过授权的用户才能在权限范围下访问机密文件，在文档存放和传输过程中持久保护文档安全；
- 无论文档分发、保存到何处，文档所有者都可以实时动态更改和回收权限，控制使用者的访问权限；
- 文档接收者可实时在线通过 email 申请文档访问权限。文档所有者收到权限请求，点击授权链接，即可实现一键授权，灵活、易用性高；
- 支持跨系统授权和用户漫游，提供持续的访问保护

8.6.3 完善的权限管理

系统支持对阅读、打印、编辑、复制、权限分发、离线、完全控制等基本权限的控制。为了方便用户进行授权操作，系统将权限分为读取、编辑、完全控制三种级别，用户通过权限级别对文档进行授权，可根据需要调整每种级别的可选权限。

DSM系统中用户管理以个人和部门为单位，根据文档管理的需要，用户还可以灵活定义文档权限分类，定义细化到用户和部门的具体上述权限。所有权限都可以灵活更改，具体包括实时设置/更改/回收相应用户或部门的授权。

8.6.4 全面日志审计

- 跟踪记录所有文件操作日志，包括创建、阅读和修改等；
- 跟踪记录所有离线文件操作日志；
- 日志审计，满足法律、法规要求，提供追溯泄密渠道的依据；

8.6.5 系统高可靠、可扩展，高性能

- 高可靠：支持数据库备份、服务器双机热备和密钥备份和恢复；
- 良好的扩展性：提供 com 接口给第三方应用程序调用，进行文档加密，权限设置和修改；
- 高性能：

单套服务器支持最大用户数20000个；
支持最大用户并发数200个；
系统吞吐量：2000个用户/分钟；

8.7 产品主要性能指标参数

8.7.1 DSM 安全管理系统性能

图表 104 DSM 性能说明列表

性能项目	性能指标	说明
单服务器最大本地用户数	20000个	一套DSM服务器所能容纳的最大本地用户个数
支持并发数	200	同一个时间点接入的用户数量
系统吞吐量	2000个业务/分钟	系统每分钟支持完成2000个客户端业务
制作单个文档最长时间	15秒	在业务高峰期，每个文档的制作时间不超过15秒（不包括用户界面操作停留时间）
打开单个文档最长时间	15秒	在业务高峰期，与未加密时相比，打开文档速度（包括服务器响应时间）最大不能超过15秒

8.8 产品运行环境软硬件需求

8.8.1 DSM 服务器

硬件环境：
- Xeon 双核 1.6GHz×2
- 4GB ECC RAM
- 146GB 以上可用硬盘空间用于软件安装和数据库
- 2 张 1GB 以太网卡(安装有 TCP/IP 协议)
- 支持 1024 768 分辨率或更高的显示器

软件环境：
- 操作系统 Microsoft Windows Server 2003 R2-中文版-标准版
- 数据库系统 Microsoft SQL Server 2005-中文版-标准版-10 用户

8.8.2 DSM 客户端

硬件环境：
- Pentium III 900 MHz 或更高
- 512 MB RAM (或更高)
- 一张 10/100M(或更高)以太网卡(安装有 TCP/IP 协议)

- 支持 1024　768 分辨率或更高的显示器

软件环境：

- 操作系统　Windows xp sp1/sp2

9 华为 OIC 文件信息管控中心子方案

9.1 方案概述

华为OIC文件信息管控中心解决方案（以下简称OIC）基于云计算技术，能协助用户建立安全可靠、灵活可扩展的信息管控平台，建立统一数据防护体系，提供文件集中存储、管理共享、安全管控、安全审计、检索等增值服务等几个方面的功能，实现内部公开数据在线查阅可控下载、涉密数据强制加密权限细分，防止信息通过网络、计算机、移动存储介质等途径泄密。

图表 105 OIC解决方案架构图

OIC部署时通过分布式内容管理节点DCMN（Distributed Content Management Node，以下简称DCMN节点）及分布式计算节点DCN（Distributed Computing Node，以下简称DCN节点）承载应用业务，组成业务网络。同时OIC提供服务时运行管理组件SEM（Service Environment Manager，以下简称SEM管理服务），为OIC文件管控业务的正常安装、系统运维、监控配置等提供全生命周期的管理服务。

DCMN节点为计算存储节点，用于承载OIC文件信息管控业务和文件信息的集中存储，在无存储系统配合的场景中，可实现OIC管控业务功能和数据集中存储能力；DCMN节点分为500和1000两种型号，分别提供5TB和10TB的有效存储空间。

DCN为计算节点，可在大型组网环境（一般是大于4台DCMN节点时）单独部署独立承载SEM运行管理业务和负载均衡业务；具体组网参见部署方案部分。

9.2 部署方案

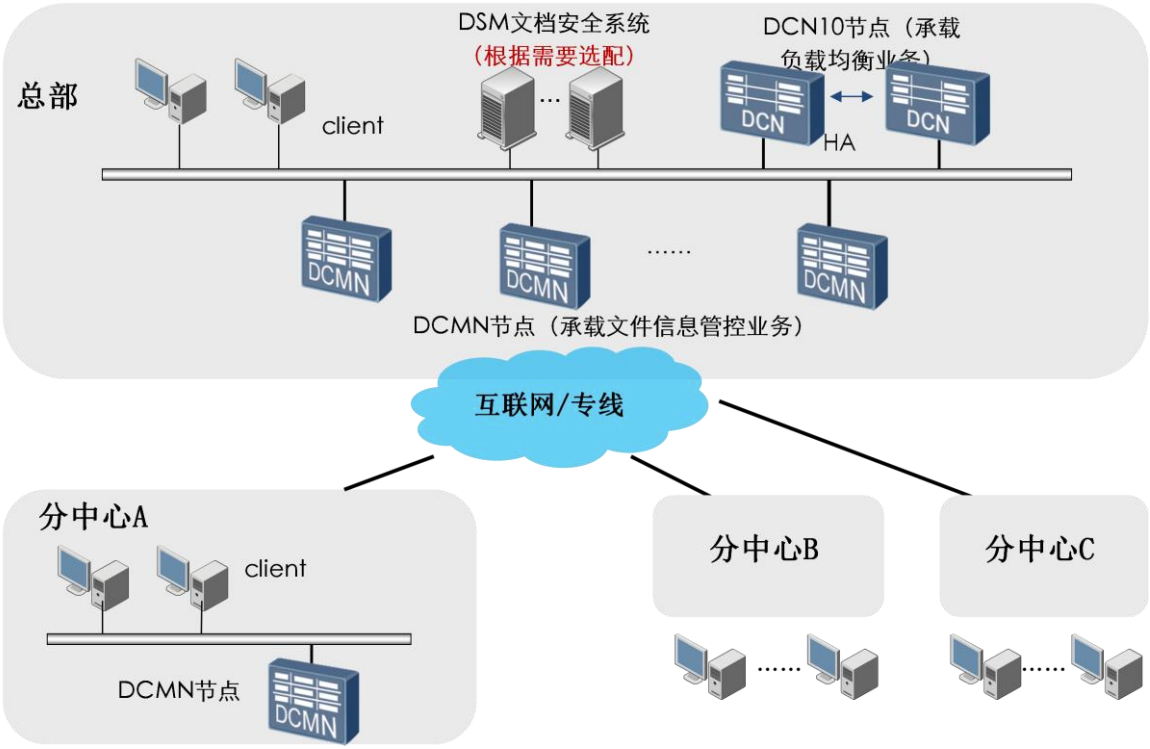
本次建设方案中配置XX台DCMN节点，每台DCMN节点部署OIC文件信息管控业务，多台DCMN节点之间的存储数据共享，每台设备都提供外部访问接口以提升IO吞吐率。系统集中部署在数据中心，存储所有非结构化数据信息，并面向用户提供网络空间业务、内部团队/部门的文档集中管理共享业务、海量文档全文检索服务。

支持跨地域分布式部署，在分中心部署DCMN节点，直接对本地产生和处理的信息进行本地化存储管理，就近存储、就近访问；总部和分中心OIC文件管控业务需要路由可达，并进行业务交互，形成为相互关联的一套系统，数据统一组织统一展现，可集中检索、调度、管理。

需要涉密文档自动强制集中加密功能，则需单独部署DSM文件安全管理系统。

9.2.1 方案组网

图表 106 OIC方案组网



9.2.2 配置建议

单台文件信息管控节点DCMN支持100用户并发，根据WEB文件管控类业务模型计算，可支持1000在线用户。建议配置N台DCMN节点，N=在线用户数/1000，DCMN节点根据用户数扩容。

DCMN数量在4台以下（包括4台）时，无需另行配置DCN10节点，可由DCMN节点自身提供SEM管理服务和负载均衡服务；当DCMN节点数量大于4台时，需加配2台DCN10节点，独立提供SEM管理服务和负载均衡服务，并以HA方式避免单点故障。

单台文件信息管控服务DCMN500/1000节点分别支持5TB/10TB有效存储，RAID6+1热备盘保障数据可靠性。文件信息管控服务节点可根据项目的需要平滑升级扩容，在增加计算性能的同时，提高存储空间。

多中心部署时，由于需要链路通信和统一调度，总部和分支机构之间带宽不应<30Mbps。

9.2.3 高可用设计

配置3台以上的DCMN节点，这些DCMN节点中有3台需要安装数据库并做负载均衡、互为主备，保障数据库数据可靠性。

提供运行管理服务的DCMN或DCN节点中需要部署SEM管理服务和负载均衡服务，以HA方式避免单点故障。

所有DCMN节点采用服务器间负载方式保障业务可靠性，任一台节点A发生故障后，用户可自动负载至其他节点B为用户提供服务。

9.3 方案特点

9.3.1 业务特点

来源多样：手工上传、FTP/CIFS标准协议传输、开放接口等方式可集中各业务系统、个人PC等多来源信息数据，提供海量存储空间集中管理共享。

查阅管控：自动转换文档为flash方式在线查阅，防止用户复制网页；可控下载,包括仅在线查看不可下载、可下载为pdf格式等管控手段。

集中加密：联动DSM文档安全管理系统实现文档自动加密和实时权限控制，机密信息仅被获权用户下载，传播后也仅能被具备权限的指定员工阅读。加密触发方式支持灵活定义，提供包括文件存储目录、文件密级等组合方式。

增值服务：面向个人和团队分别提供存储空间，支持全格式文件在线编辑、多种多媒体在线播放、信息在线分享、全文检索等多种增值服务能力

9.3.2 技术特点

- **全文搜索**

OIC采用了业界主流的倒排索引技术构建全文检索引擎，可广泛兼容doc/pdf/txt/html/xml/ppt/xls等文件类型，基于海量文件基数快速建立索引。同时针对信息管理所特有的历史海量小文件累积，存储、管理困难的业务场景，优化了搜索模块的设计，综合采用了数据库分表和数据缓存等多种技术，大大提升了在面向海量文件并发用户检索时的性能。

支持安全搜索，文档检索功能和权限设置严谨挂钩，检索结果和用户权限匹配，对没有阅读权限的文档不可浏览。

- **自动精简配置**

虚拟网盘技术一般预分配存储空间的管理方法是：业务管理人员为每个用户分配一个固定空间，比如20GB，不管此用户个实际使用空间的大小，它都占用分配给它的物理空间，带来极大的存储空间浪费。

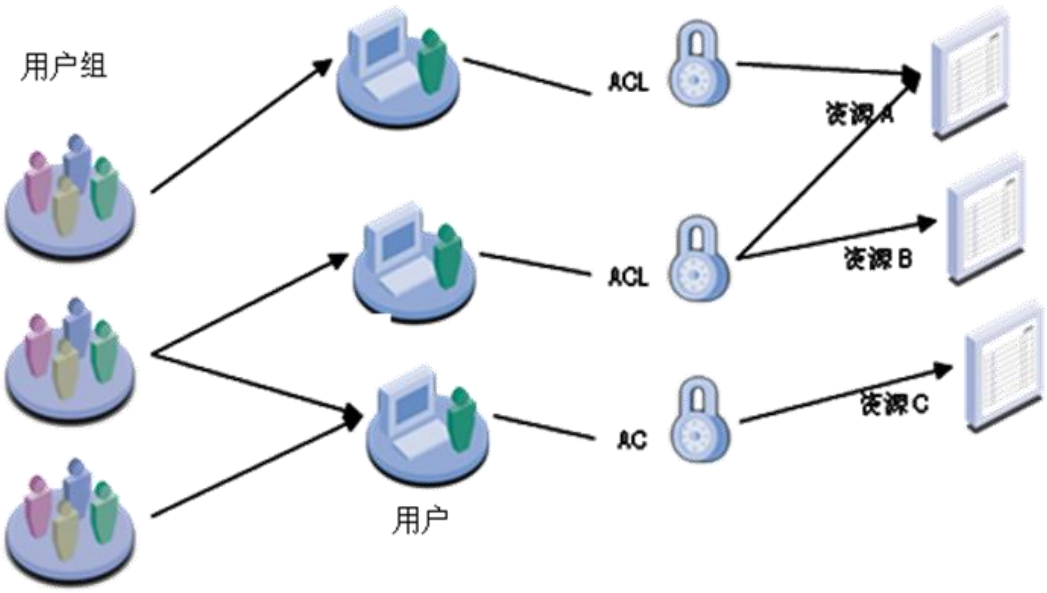
OIC在提供应用层自动精简分配能力，例如初始默认为每个用户分配20GB的逻辑空间，但在后台该用户只是占用了实际使用大小的物理存储空间，当用户往个人空间上传文档时，系统会自动计算判断，如果在指定限额内则可顺利上传，否则提示用户超额上传失败，可通过申请分配更多空间解决。从而支持存储空间的共享和调剂，提高存储空间的利用率。

- **ACL 权限管理和日志审计**

OIC采用用户、用户组管理机制，一个用户组可以同时拥有多个用户。在系统中用户是作为系

统内部权限管理的基本单位。系统中授权机制是通过ACL（访问控制列表）来实现，每个资源及功能均可以有一个用于控制该资源或功能访问权限的ACL。支持用户、组和角色的完整权限控制体系，严格遵循只有合适的人才能看到合适的内容的要求。

图表 107 OIC用户权限管理



9.4 配置清单

图表 108 OIC配置清单

设备名称	型号	数量	描述
分布式内容管理节点	DCMN1000 DCMN500		部署文件信息管控业务 部署SEM管理系统
文件信息管控用户数license	用户license		根据项目需要配置，单DCMN最大支持1000用户数
分布式计算节点	DCN10		选配 DCMN数量大于4台时必配
HA软件	HA软件		选配 2台DCN10做双机时，配置1套
DSM文档加密软件	软件license		选配 用户license根据实际情况配置
DMS 文档加密服务器（含数据库和操作系统）	PC Server		选配 部署DSM文档加密软件

9.5 方案组件规格

图表 109 OIC组件规格

	文件信息管控服务节点		运行管理节点
型号	DCMN1000①	DCMN500	DCN10
系统硬盘	2*2TB SATA （RAID1）	2*1TB SATA （RAID1）	2*300GB SAS（RAID1）
存储空间	8*2TB SATA	8*1TB SATA	—
单机性能	上行：320Mbps 下行：400Mbps 并发用户数≤100		管理节点数≤100
兼容格式	文档转换：doc、docx、xls、xlsx、ppt、pptx、rtf、pdf、wps、et、dps、odt、ods、odp 全文搜索：doc, docx ,xls, xlsx, ppt, pptx, pdf, txt, html, xml 集中加密：Microsoft Office Word、Excel、PowerPoint 2003/2007/2010中英文版本、Adobe Reader 7.0/8.0/9.0中英文版		—

10 合作伙伴统一运维审计方案

部署统一运维审计（统一运维审计系统）后系统将断开操作用户与目标服务器之间的直接连接。用户对服务器的远程操作全部集中登录到统一运维审计上，通过二次跳转系统将用户直接连接到指定服务器，实现用户对服务器资源操作管理的集中人证、集中控制、集中审计。

部署方式：物理旁路，逻辑网关,采用双机热备部署;

部署条件：运维审计系统的 IP 地址与被测试的设备之间 IP 可达，协议可访问。

登录过程：集中管理的标志就是入口唯一，统一运维审计（统一运维审计系统）是用户操作的唯一入口。用户通过唯一的自然人 ID 登录到运维审计系统上，然后运维审计系统会根据授权关系表，提示用户选择可以访问的目标设备和相应系统登录账户，用户选择完成后会自动登录到目标设备，实现单点登录。

10.1 需求分析

10.1.1 所存在的问题

- ✓ 用户身份不唯一，用户登录后台设备时，仍然可以使用共享账号（root、administrator 等）访问，从而无法准确识别用户的身份；

- ✓ 缺乏严格的访问控制，任何人登录到后台其中一台设备后，就可以访问到后台各种设备；
- ✓ 重复枯燥的密码管理工作，大大降低了工作效率的同时，人员的流动还会导致密码存在外泄的风险；
- ✓ 难于限制用户登录到后台设备后的操作权限；
- ✓ 无法知道当前的运维状况，也不知道哪些操作是违规的或者有风险的；
- ✓ 缺乏有效的技术手段来监管代维人员的操作；
- ✓ 操作无审计，因操作引起设备故障的时候无法快速定位故障的原因和责任人；

10.1.2 问题分析

出现以上问题的主要原因在于：

- ✓ 运维操作不规范；
- ✓ 运维操作不透明；
- ✓ 运维操作风险不可控；

10.1.3 带来的后果

- ✓ 违规操作可能会导致设备/服务异常或者宕机；
- ✓ 恶意操作可能会导致系统上敏感数据/信息被篡改、被破坏；
- ✓ 当发生故障的时候，无法快速定位故障原因或者责任人；

10.1.4 解决之道

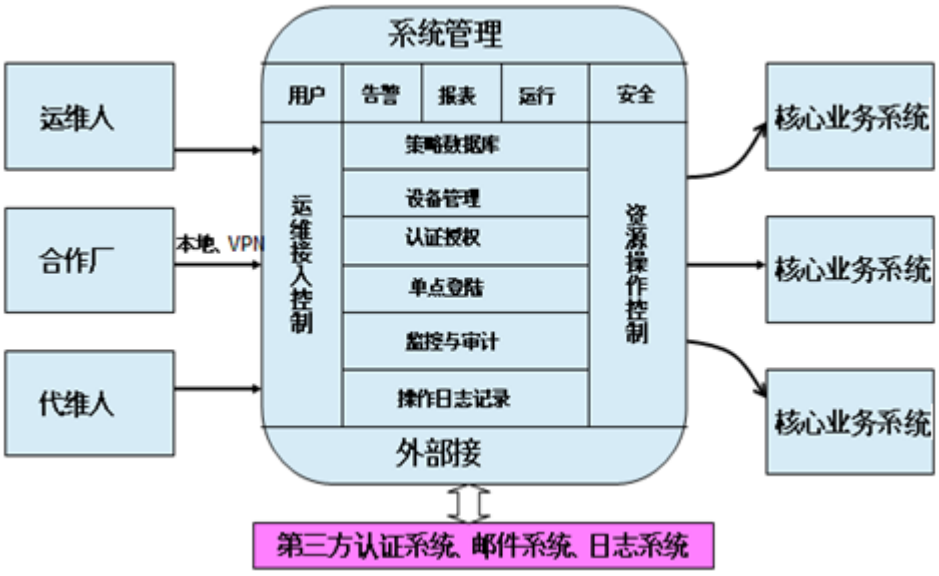
根据客户的现状及问题，可通过部署齐治科技的IT运维操作监控系统（简称：Shterm），实现以下效果：

- ✓ 实现维护接入的集中化管理。对运行维护进行统一管理，包括设备账号管理、运维人员身份管理、第三方客户端操作工具的统一管理；
- ✓ 能够有效的整合用户现有的运维管理手段及第三方认证系统；
- ✓ 能够制定灵活的运维策略和权限管理，实现运维人员统一权限管理，解决操作者合法访问操作资源的问题，避免可能存在的越权访问，建立有效的访问控制；
- ✓ 实现运维日志记录，记录运维操作的日志信息，包括对被管理资源的详细操作行为；
- ✓ 实现运维操作审计，对运维人员的操作进行全程监控和记录，实现运维操作的安全审计，满足信息安全审计要求；
- ✓ 能够有效的检索运维操作细节；
- ✓ 能够对于高危及敏感的操作进行实时告警；
- ✓ 能够提供灵活的报表及统计分析；
- ✓ 实现运维操作的合规性要求、遵从现有的法律法规；

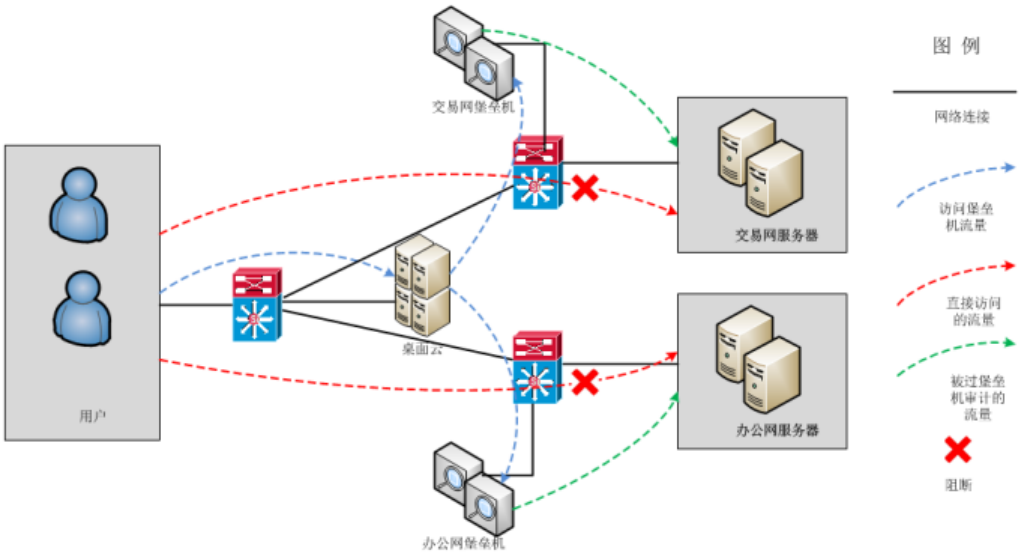
10.2 方案概述

统一运维审计系统平台功能设计如下图所示，主要考虑3方面的问题：用户接口、平台管理、资源控制等。在功能设计时，采用了模块化和组件化的设计思想，将整个运维平台分为5个功能子系统，结合用户接口、系统接口来完成图示的所有功能。

图表 110 统一运维审计功能图



图表 111 统一运维审计逻辑组网图



1） 操作网关方式部署

集中管理是实现运维操作安全管理的首要前提。

针对当前核心设备分散管理的现状，集中管理倡导的是一种统一管理的理念。集中管理是未来运维操作安全管理的必然趋势。

实现集中管理，关键点在于对用户原有的运维环境不造成任何影响。综合各种部署方案，我们采用了旁路“操作网关”的部署方式。

2） 用好共享账号

在当前的运维环境中，普遍存在操作者身份无法识别的安全隐患。这主要是由操作者共享使用核心设备上的系统账号造成的。

设备数量达到一定规模，必然会使用到共享账号。共享账号就是多人共同使用同一个存在于设备上的系统账号，使用共享账号会让整体账号的数量减少。但是仅仅依赖系统上的单一系统账号，无法既能区分用户身份，又能完成工作角色的定位。

如何准确的区分用户身份和工作角色，进而实现操作者和具体的操作过程一一对应？

Shterm将用户身份认证和系统工作角色功能分离，在Shterm上增加了用户账号，完成用户的身份确认。原来系统上的账号依然存在，但是作用只是完成工作角色授权的工作账号。

用户登录Shterm是采用唯一的用户账号，然后根据工作角色的需要，转换成系统账号登录到被管理设备上。这样既能够保证整体账号数量最少，管理方便；同时又能够实现对用户、工作角色的双重定位。

当用户加入、离职或岗位变动，当代维人员和原厂商进行维护的时候，只需要在Shterm上变更该用户账号即可，对系统上的系统账号没有任何影响。

代维人员维护系统并不需要知道用户系统的最高权限的系统帐号密码，这样大大降低了管理风险。

原厂商进行临时维护的时候只需要临时分配一个用户账号，当使用结束后该账号会自动回收，减少了账号管理的成本。

3） 访问控制规则

目前，用户只要知道用户名和密码就可以任意访问任意设备,这种现状必然会带来“未授权访问的安全风险”。

部署了Shterm后，情况就发生了变化。Shterm逻辑上成为了用户登录的唯一入口，因为入口唯一，访问控制很容易配置了。

相同工作任务的集合可以放置在一个访问规则组里，当用户岗位、职责改变时，对用户相关联的组、系统权限、可访问设备通过Web的勾选，很容易调整。

根据工作内容的需要，可以配置不同的许可或禁止的登录策略。既可以设定固定日期的登录策略，也可以设定固定时间间隔的策略，还可以设定一天中指定时间段的策略，并且能够针对具体的地址段进行控制。

Shterm的访问控制列表可以让用户一目了然的知道某台设备上允许哪些用户登录。某台设备上的系统账号有多少个用户可以使用。

另一方面，从安全运维的角度分析，权限控制策略是从操作的层面上，降低高危操作所带来的安全风险：

对于使用Telnet/SSH等协议进行远程管理的设备（各种网络设备和Unix服务器），操作权限的多少取决于用户可以执行的命令。所以，针对操作指令的控制才是核心。

对于服务器设备操作，Shterm可以对服务器的超级用户root操作权限进行控制，即使是root用户，权限也是受限制的，可以限制root用户只能执行某些操作（白名单）和无法执行某些操作（黑名单）。

当多人同时使用一个root账号时，Shterm可以对同一个系统账号进行操作权限再分配，保证使用同一个root账号的不同用户拥有不同的操作指令权限，彻底解决了共享root账号权限一致的情况，真正实现细粒度的操作权限控制。

对于网络设备操作，Shterm可以保证即使多个用户在进入enable状态的时候，提供高于网络设备系统更好级别的控制力度，保证每一个用户的操作指令都能严格受到控制。

对于操作权限的控制意味着我们从被动接受用户输入到了主动控制。

对于用户的操作可以有3种执行状态：允许执行，拒绝执行，禁止执行。

对于高危命令（删除，重起，关机等）可以实时告警，一旦高危操作触发，会立即给相关人员发送告警邮件，保证用户在第一时间内知道高危操作是否对系统造成了影响。

4） 完整操作审计

运维操作审计是整个Shterm解决方案的重要组成部分。管理员确定了以操作网关方式来部署，解决了之前共享账号的问题，配置了访问规则，明确了操作权限，那么最后也是最重要的就是操作和操作审计。

Shterm支持的运维操作方式和相应的操作审计基本涵盖了目前企业日常运维所涉及到的绝大

部分操作模式，包括字符会话、图形会话、Web Client会话、文件传输、Oracle数据库操作审计等等。

对不同会话采用不同的审计方式针对字符会话，Shterm的审计功能会完全记录所有会话内的输入输出，并可以使用模式方式对这些输入输出进行查询以定位操作时间节点和操作内容。对于图形会话要采用全程的录像和键盘鼠标操作的记录，并在图形会话回放的过程中同步的显示出来。对于Web Client方式的操作会话，也是目前非常主流的一种操作模式，Shterm可以利用对于图形会话的审计方式来审计Web Client方式的会话，即，既包括了图形录像也包括了键盘鼠标记录，并且可以如图形会话一样，键盘输入信息可以进行完全的检索以便快速定位一个较长的审计录像。针对文件传输，FTP、SFTP之类的上传下载，Shterm支持全部的信息记录，包含时间，人员，IP等等信息。对于Oracle数据库的操作审计，采用跳板机和应用发布的方式，能够把图形方式操作中的数据库语句全部完成的审计到Shterm平台内。

此外，Shterm对审计人员本身也有严格要求，一方面，对审计人员的审计操作，Shterm有严格的记录，审计管理员何时查阅了某个会话操作都要有明确记录。另一方面，Shterm支持非全局性的操作审计，即，审计人员也没有权利审计所有的会话信息，因为会话中可能包含了非常敏感甚至机密的企业信息。

5） 运维自动化

日常运维中经常需要对一些操作进行重复性动作，例如每天去执行一些脚本、检测一些状态等，重复繁琐的工作容易令人出现操作的失误。如果能通过一些技术手段，替代用户的重复操作，使用户从重复繁琐的工作中释放出来，可以让用户有更多的时间去专注于更多技术领域。

操作自动化是运维操作管理的终极目标，通过Shterm的自动脚本功能，可让Shterm自动帮助运维人员执行各种常规操作（如自动巡检、自动备份配置等），从而达到降低运维复杂度、提高运维效率的目的。

根据客户的现状及问题，可通过部署齐治科技的运维操作管理系统（Shterm，简称运维统一运维审计），实现以下效果：

- 实现维护接入的集中化管理。对运行维护进行统一管理，包括设备账号管理、运维人员身份管理、第三方客户端操作工具的统一管理；
- 通过主从帐号管理，使用户认证与系统授权分开，从而有效解决系统帐号共享使用而带来的身份不唯一的问题；并实现与现有的第三方认证系统（LDAP、Radius、AD 域、TOTP 等）整合；
- 能够制定灵活的运维策略和权限管理，实现运维人员统一权限管理，解决操作者合法访问操作资源的问题，避免可能存在的越权访问，建立有效的访问控制；
- 实现对核心设备操作的双人授权访问与双人操作复核，有效降低运维操作风险；
- 密码托管和自动改密，使得密码管理规范能有效落地，避免了因人员的流动还会导致设备密码存在外泄的风险；
- 能完整记录运维人员的操作过程，当系统因人为操作导致故障的时候，能够快速定位故障原因和责任人，满足信息安全审计要求；
- 能够有效的检索运维操作细节；
- 能够对于高危及敏感的操作进行实时告警；
- 能够提供灵活的报表及统计分析；
- 实现运维操作的合规性要求、遵从现有的法律法规

10.3 子方案亮点

10.3.1 成熟稳定

齐治公司从2005年成立，自主研发的统一运维审计系统。自2005年被阿里巴巴选中后，为其旗下的25000余台服务器提供着运维操作安全服务，其服务器数量、在线维护人员数量等硬指标在全国首屈一指，是完全可以信赖的优秀产品。

至今，在国内，齐治公司是：

- 唯一专注于运维操作管理领域的厂商
- 在运营商、金融、互联网、电力、政府、烟草和海关等多个高端行业得到大规模使用
- 唯一在单个用户超过 2,300 个并发用户环境成功部署
- 唯一在单个用户超过 10,000 台服务器环境成功部署
- 唯一在单个用户超过 2,000 台网络设备环境成功部署

10.3.2 安全可靠

Shterm是以安全性为基础构建坚实的运维堡垒，是业内唯一不存在中高级安全漏洞、对外不开放非安全端口的产品。

- 只开放 3 个端口（22、443 和 5899），彻底杜绝 telnet、ftp、rdp 等非安全服务端口开放
- 使用 SSL、SSH 封装传输过程；
- 唯一同时拥有国家保密局和中国国家信息安全产品认证的；

10.3.3 技术先进

品质的保障在于点滴细节，奇智统一运维审计系统在核心功能上面拥有独家的技术，可以最大程度降低运维操作风险，以确保后台设备系统的稳健运行。其领先性主要体现在以下几点：

- 唯一在运维审计域获得国家发明专利及香港发明专利的产品；
- 唯一实现图形会话关键字（键盘输入、剪贴板、模糊识别）检索的产品；
- 唯一实现类 citrix 方式的应用发布的产品；
- 唯一真正实现统一运维审计方式的数据库审计（100%记录所有 sql 语句，并实现 sql 与图形审计关联）的产品；

10.4 配置清单

图表 112统一运维审计配置清单

型号	数量	配置
齐治运维审计系统 Shterm-H5（2U）	4	硬盘≥2×1TB，支持Raid1，支持存储
		内存≥4G
		CPU 1×4 核
		图型操作并发数≥200

		字符操作并发数≥1，000

11 典型案例

11.1 深圳证券交易所

• 客户需求：

- 办公内网数据可外移，网络跨接问题不能完全禁止，存在安全隐患
- 终端多场景复用，硬件资产管理弱，且接入终端数量、类型多
- 运维，业务操作，文档使用等行为无法审计
- 文档、策略未统一管理，维护难度大

• 桌面云及统一运维审计子方案：

- 在办公内网DMZ区，部署接入网关，提供移动办层公安全接入
- 在办公内网隔离层部署1200用户规模桌面虚拟化及200用户规模应用虚拟化系统提供负载均衡，安全认证功能
- 办公内网服务器前部署统一运维审计，进行运维管控和审计

• 客户价值：

- 数据上云，本地不保存业务数据，核心资产信息零丢失
- 多种准入认证方式满足客户多场景办公安全需求，支撑客户业务高效开展

11.2 中国工商银行

• 客户需求：

- 工行重要敏感的信息大量采用工行专有公文编辑器和OFFICE/PDF为载体，目前这些文档信息几乎任何工行用户都可以不受限制的进行阅读，使得自身宝贵的信息资产面临威胁。

• 文档安全管理子方案：

- 全行上线DSM，几十万用户使用
- 对OFFICE/PDF文档进行加密和权限管理
- 对接档案管理，notes等OA系统
- 移动介质管控，离线使用限制

• 客户价值：

- 文档加密及权限管理保护敏感信息，扩散范围可控，减少无意识泄密

- 结合OA系统，用户体验好，公文高效流转

11.3 兴业银行

•客户需求：

- 网络环境日趋复杂，重要机密信息保护、终端系统安全访问控制和安装防病毒系统、人员活动跟踪和审计记录等急需进一步加强，需要以技术手段预防和消除有可能出现的信息安全风险。

•PolicyCenter子方案：

- PolicyCenter以接入控制技术为核心，策略强制为纽带，通过网络和系统两个层面来搭建PolicyCenter平台。
- 将现有终端的补丁管理、软件分发、防病毒、资产管理、信息安全、权限控制等相关技术进行整合，避免非法、不安全的终端接入或把终端的安全问题带给其它终端、业务系统
- 采用分布式部署方案，全国35个地市和地区，共4100个终端

•客户价值：

- 用户免受病毒、黑客等的攻击和干扰。有力保障了文档资料的安全，从而为银行系统正常的业务开展提供了内网安全平台
- 提供信息安全管理经验，从技术和管理两个方面为数据安全保驾护航

11.4 中国建设银行

•客户需求：

- 影响：建行员工工作需要上网，近6个月30多台终端感染木马被通报
- 政策：监管部门发文要求加强信息安全管控
- 要求：各分行办公网和互联网必须隔离

•安全沙箱子方案：

- 沙盒网关：安全桌面和真实桌面完全隔离
- 普通PC：真实桌面办公，安全桌面上网
- 网吧机：启动后只能进入安全桌面
- 特殊终端：白名单放行

•客户价值：

- 实现了终端的安全性检查，防止了信息的泄漏，规范了员工的上网行为，统一了管理和维护的界面，终端的感染数量降到了0，满足了安全需要
- 内外网隔离：数据出不去，病毒木马进不来，提高办公效率20%
- 高回报：极大节省建行对于内网信息安全防控的投资

12 缩略语

重要名词解释、所有术语定义、首字母缩写和缩略语：

缩略语	英语全称	中文名称
A		
ACL	Access Control List	访问控制列表
AD	Active Directory	活动目录
AG	Access Gateway	接入网关
API	Application Programming Interface	应用程序接口
B		
BIOS	Basic Input/Output System	基本输入/输出系统
BMS	Business Management System	经营管理系统
BOSS	Business and Operation Support System	业务运营支撑系统
C		
C/S	Client/Server	客户端/服务器模式
CAPEX	Capital Expenditure	总投入成本
CNA	Computing Node Agent	计算节点代理
CPU	Center Process Unit	中央处理器
CRM	Computing Resource Manager	计算资源管理器
CTI	Computer Telephony Integration	计算机与电话集成
D		
DB	Database	数据库
DC	Data Center	数据中心
DDC	Desktop Delivery Controller	即桌面传输控制器
DDOS	Distributed Denial Of Service	分布式拒绝服务
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DMZ	Demilitarized Zone	隔离区
DNS	Domain Name Sever	域名服务器
DRS	Dynamic Resource Scheduling	动态资源调度
DS	Data Store	数据存储服务器
DSC	Desktop Session Controller	桌面会话控制器
DSG	Desktop Session Gateway	桌面会话网关
DSM	Document Security Management	文档安全管理

E		
ECC	Error Checking and Correcting	差错校验纠正
ERP	Enterprise Resource Planning	金融机构资源计划
ESC	Elastic Service Controller	弹性服务控制器
F		
FC	Fibre Channel	光纤通道
FE	Fast Ethernet	快速以太网
FS	File Sever	文件服务器
FTP	File Transfer Protocol	文件传输协议
FusionAccess	FusionAccess	华为桌面管理平台，也称vDesktop
FusionManager	FusionManager	华为云管理平台
FusionSphere	FusionSphere	华为云平台
FusionCompute	FusionCompute	华为虚拟化基础引擎
G		
GE	Gigabit Ethernet	千兆以太网
GSLB	Global Server Load Balancing	全局服务器负载均衡
GUI	Graphic User Interface	图形用户界面
GW	GateWay	网关
H		
HA	High Availability	高可用性
HTTP	Hyper Text Transport Protocol	超级文本传送协议
I		
ICA	Independent Computing Architecture	独立计算架构
IDC	Internet Data Center	Internet数据中心
IMG	Image Server	镜像服务器
IP	Internet Protocal	因特网协议
IPSec	IP Security	因特网协议安全协议
iSCSI	Internet SCSI	网络SCSI接口
ISM	Integrated Storage Management	云存储的管理维护软件
IT	Information Technology	信息技术
ITA	IT Adapter	IT适配器
L		
LAN	Local Area Network	局域网

LB	Load Balance	负载均衡
LCM	Life Cycle Manager	生命周期管理
LS	License Server	桌面许可服务器
M		
MN	Management Node	管理节点
N		
NAS	Network-Attached Storage	网络附加存储
NC	Network Computer	网络计算机
NEBS	Network Equipment Building System	网络设备制造系统
NFS	Network File System	网络文件系统
NRM	Network Resource Manager	网络资源管理器
O		
OA	Office Automation	办公自动化
OBS	Object Based Storage	对象存储
OMM	Operations and Maintenance Management	操作和维护
OMS	operational management system	运营管理系统
OPEX	Operating Expense	维护成本
OS	Operate System	操作系统
OSC	Object based Storage Controller	对象存储控制器
OSP	Object based Storage Provider	对象存储提供者
OVF	Open Virtualization Format	开放虚拟化格式
P		
PC	Personal Computer	个人计算机
POE	Provisioning Orchestration Engine	业务发放引擎
PQ	Priority Queuing	优先级队列调度
Q		
QoS	Quality of Service	服务质量
R		
RAID	Redundant Array of Independent Disks	独立磁盘冗余阵列
RDP	Remote Desktop Protocol	远端桌面协议
REST	Representational State Transfer	表述性状态转移

S		
SAN	Storage Area Network	存储区域网络
SB	Service Block	服务块
SBC	Server-Based Computing	基于服务器计算
SC	Soft-Client	软客户端
SCSI	Small Computer System Interface	小型计算机系统接口
SLA	Service-Level Agreement	服务等级协议
SOAP	Simple Object Access Protocol	简单对象访问协议
SOX		
SQL	Structured Query Language	结构化查询语言
SSL	Secure Sockets Layer	安全套接层
T		
TC	Thin Client	瘦客户机
TCM	Thin Client Management	TC管理软件
TCO	Total Cost of Ownership	总体拥有成本
TCP	Transfer Control Protocol	传输控制协议
TSM	Terminal Security Management	即PolicyCenter前身，终端安全管理
U		
UAP	Universal Access Platform	通用接入平台
UDP	User Datagram Protocol	用户数据报（文）协议
UPF	User Profile Function	用户签约描述功能
UVP	Unified Virtualization Platform	统一虚拟化平台
V		
vCPU	virtual CPU	虚拟CPU
vDesktop	virtual Desktop	虚拟桌面管理平台，也称FutionAccess
VDI	Virtual Desktop Infrastructure	虚拟桌面构架
VLAN	Virtual LAN	虚拟局域网
VM	Virtual Machine	虚拟服务器
VOIP	Voice Over IP	IP承载语音
VPC	Virtual Private Cloud	虚拟私有云
VPN	Virtual Private Network	虚拟专用网

W		
WI	Web Interface Web	接入辅助部件
WIA	Web Interface Adapter	WI适配器