

浅析天津电力云终端设计

介绍了天津电力云终端设计情况，通过对云终端底层硬件、网络规划、应用系统架构的阐述，展示天津电力云终端各个组成部分的设计思路及实现各部分功能的方法，对天津电力云终端投入使用后的预期效果进行展望。

于晓冬 赵迪 刘赫/国网天津电力公司信息通信公司

虚拟化技术，将所有办公计算机的运算合为一体，在服务器端进行集中处理，员工采用瘦终端设备，仅负责输入输出与界面显示，不参与任何计算和应用，具有高效、安全的特点。国网天津电力公司结合其他公司部署云终端的经验与自身特点，整理设计出天津电力公司云终端实施方案^[1]。

0 引言

随着国网公司SG186工程的建成投运和SG-ERP建设的启动，生产、经营和管理业务活动对信息系统愈加依赖，员工办公终端的规模随之不断扩大，在员工终端管理、运维成本、能耗以及信息安全等方面的问题明显增多，如何在满足办公需求的同时，落实公司“集约化”管理要求，提高对员工终端的管控手段，将是信息化工作面临的一个重要问题。

为提升终端管控水平，落实集约化的工作要求，国网公司开展了一系列云终端试点及推广建设工作。云终端采用“集中计算，分布显示”的架构，通过

1 终端设计

云终端系统采用虚拟化架构作为底层设计，它为云终端系统基础服务器层提供了一个高度可扩展、高度可靠且稳定的资源平台，它具有内置的业务连续性和灾难恢复功能，能够保护桌面数据和可用性。通过部署身份验证、桌面发布、桌面管控、应用发布、应用管控、审计应用、桌面数据库和审计数据库等基础服务器和组件，提供了云终端系统管理。云终端系统可以虚拟桌面交付给身处任何位置、使用任何类型设备的用户。终端用户通过瘦终端接入云终端系统。如图1所示。



于晓冬/助理工程师

关键词/Keywords

云终端 ·
硬件架构 ·
集约化 ·

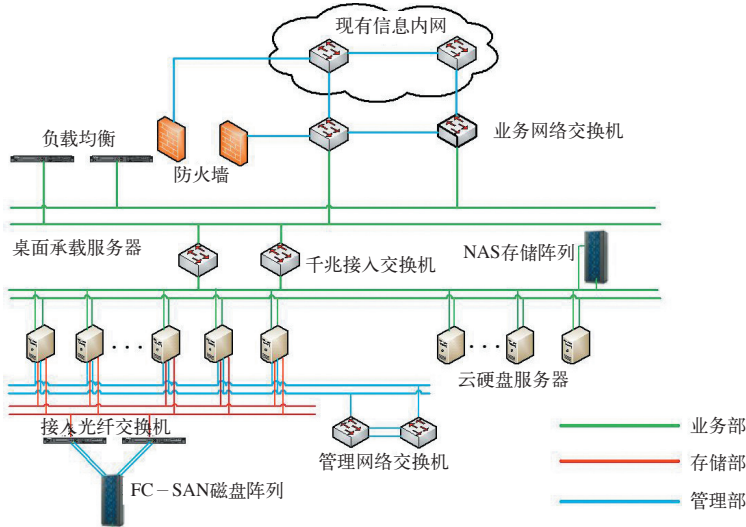


图1 云终端资源池部署情况

1.1 服务器硬件资源设计

1.1.1 云终端基础架构服务器设计

包括AD、桌面发布、桌面管控、审计应用、桌面数据库和审计数据库等关键组件。其中2台基础架构服务器会虚拟出包括域控服务器、DHCP服务器、数据库服务器、访问门户服务器、桌面控制服务器、云终端控制服务器、云安全设备管理服务器、行为审计控制服务器和行为审计应用服务器等用于对云终端系统提供服务的相应虚拟服务器，并根据情况提供适当的主备分担功能。

1.1.2 桌面承载服务器

目前设计公司云终端用户分别为资源型用户和标准型用户数，在对桌面承载服务器进行服务划分时，对不同用户分配资源略有不同。目前桌面承载服务器选用X86服务器系列。

1.1.3 云硬盘服务器

云硬盘服务器群集由元数据服务器、存储服务器和应用服务器构成，为所有云桌面用户提供数据存储服务。其中云硬盘元数据服务器采用分布式存储技术，可扩展的系统结构，利用多台存储服务器分担存储负荷，具有高可靠性和高可扩展性，能够提供海量的文件存储能力，这种技术同时提高了系统的可用性和存取效率。云硬盘存储服务器及云硬盘应用服务器主要负责对云终端系统账户资料等系统数据进行存储使用。

1.2 网络设计

1.2.1 基础架构和桌面承载资源池网络

云终端系统采用管理网、存储网和业务网三网隔离的设计原则，即管理网、业务网和存储网分离模式。

1) 管理网。对底层虚拟化服务器软件、物理服务器、存储和网络设备进行管理的网络，承载的流量包括存储、虚拟网卡的管理，虚拟机的迁移等。由于虚拟机迁移会占用大量带宽，因此管理网需要与业务网分开，以免影响业务的正常使用。

2) 业务网。业务系统使用的网络，承载的流量主要是云桌面虚拟机对外提供服务时产生的流量。业务网需要与客户方的网络互通，以实现桌面的接入及在桌面上操作具体业务。

3) 存储网。虚拟化服务器底层与磁盘阵列之间的存储网络，网络类型是光纤存储网络。

在运行的每台物理服务器都配置4个千兆以太网端口和2个8GbpsHBA端口。每2个以太网口做绑定，分别接入管理网络和业务网络。2个HBA卡做绑定，接入存储网络中。当相互绑定的其中一块网卡出现故障时，另外一块可保证通信正常。具体情况如下表及图2所示。

表 服务器端口绑定情况

网络名称	网络接口
管理网络	Bond0 + 2
业务网络	Bond1 + 3
存储网络	HBA0 + 1

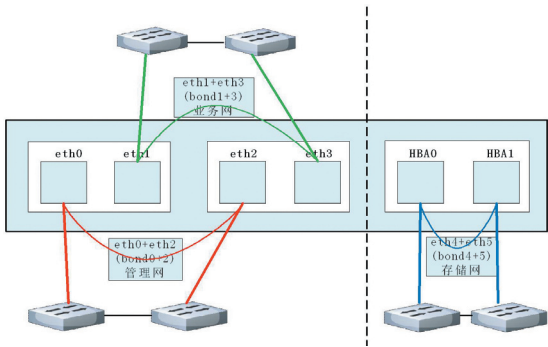


图2

1.2.2 云硬盘集群服务器网络

云硬盘集群服务器网络主要有介入层交换机及汇聚层交换机构成，每台服务器均部署2个网卡，分别上联至不同的介入交换机，每一个网卡为一个IP地址，如图3所示。接入层交换机和汇聚层交换机均具备IRF功能，可实现链路带宽增加和负载均衡^[2]。运用IRF技术，将多台交换机互联在一起，形成分布式交换架构，并作为一个逻辑交换实体运行。从管理和配置上，其为一台交换设备；从性能上，扩展了端口和带宽。其支持LACP协议，且支持跨设备的链路聚合，可以在设备之间进行链路的负载分担和互为备份。

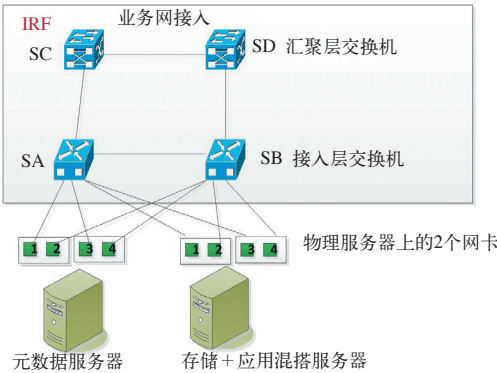


图3

1.3 存储设计

1.3.1 存储类型

在本方案中存储有共享和云硬盘两种存储架构，而共享存储又分为FC-SAN存储和NAS存储两种共享存储类型。

1) FC-SAN存储。保存操作系统镜像数据，包括桌面管理虚拟服务器操作系统镜像文件和虚拟桌面操作系统镜像文件。

2) NAS存储。保存用户桌面配置文件数据和文件夹重定向数据，以文件夹形式放在NAS存储设备中。

3) 云硬盘。保存用户个人办公文件，即所有用户的个人数据盘。

基础架构和桌面承载物理机底层虚拟化使用服务器本地磁盘；基础架构和桌面承载物理机虚拟化之后安装的虚拟机使用挂载的FC-SAN存储；虚拟机中用户的漫游配置文件和文件夹重定向数据使用挂载的NAS存储；云硬盘使用云硬盘物理服务器本地挂载的SATA磁盘。

1.3.2 存储网络

共享存储设备主要分为两种类型：基于块存储的FC SAN（光纤存储）和基于文件系统的NAS存储。

桌面虚拟化系统放置在FC类型的存储设备上，FC存储交换机与服务器采用交叉连接，形成冗余的存储链路网；NAS存储能提供大容量的存储空间，且存储成本较低，所以对于这种存储设备，主要用于存储用户的配置文件和用户数据文件，如图4所示。

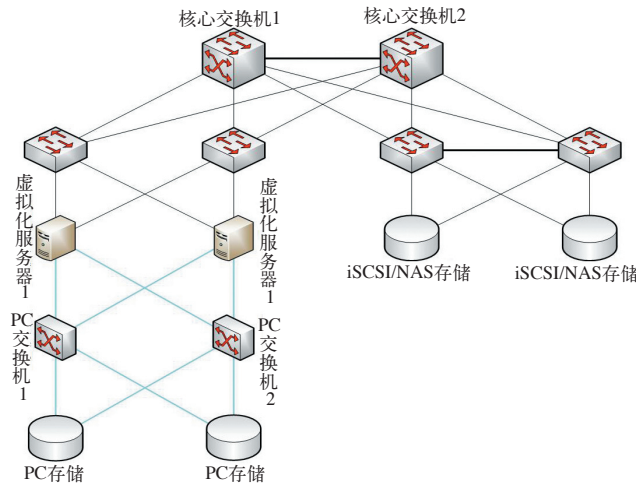


图4

1.4 云终端系统不同功能实现

1.4.1 活动目录

新建2台活动目录服务（身份验证）采用双机模式进行搭建，采用一主一辅的模式进行设计，保证活动目录服务的高可用。对于组策略设计是根据桌面安全管理等要求通过活动目录GPO组策略颗粒化配置OU下的云终端服务器及虚拟桌面、用户的Windows管理配置策略（包含云终端服务器策略、云终端用户策略）。

1.4.2 DHCP功能实现

在基础架构服务器上新建2台DHCP主备服务器，虚拟桌面虚拟机将使用DHCP动态分配IP。能够统一标准分配IP地址，集中管理地址池，以减轻部署运维的工作量。桌面创建时，不需要管理员再手工分配IP。

1.4.3 数据库部署

本次虚拟桌面项目采用SQL Server Mirror部署方式，MSSQL Mirror建立3台MSSQL虚拟机，分别为主镜像数据库服务器、备镜像数据库服务器及见证数据库服务器，项目中云终端控制器要配置主数据和备用数据库的IP地址，平常没有故障的情况下，SQL数据库的数据文件及日志文件在主、备数据库中相互镜像，保证数据的完整性，同时见证数据库服务器通过监听组件实时记录SQL Server的运行状态，保证数据库运行的稳定性、可靠性，一旦出现主数据库故障，见证服务器就主导备用数据成为主数据库。

1.4.4 许可服务

许可服务实现对云终端桌面控制器通信以管理每个用户会话的许可，与桌面控制服务器通信以分配许可证文件。必须至少创建一个许可证服务器来存储和管理许可证文件。

由于许可授权服务器存在30天宽限期，在宽限期内即使许可授权服务器因故障宕机也不影响用户使用，在30天内恢复即可。

1.4.5 云终端桌面控制

云终端桌面控制服务是多台控制器的组合集群，一同用于为最终用户提供虚拟化桌面。服务器集群作为单一管理实体运行，其中定义了资源类型，进行了分组并与用户相关联。

(下转第565页)

相当于在软件开发生命周期当中添加了新的敏捷性层。容器技术最大的突破就在于其一致性。基于Docker的应用程序能够在笔记本电脑与生产环境下获得同样的运行效果。由于Docker将与应用程序相关的所有状态都封闭了起来，因此不用担心底层操作系统的架构差异会给应用程序的运行依赖性带来影响或是产生新的漏洞。

4 结束语

Docker是容器技术中的佼佼者，其使用类似集装箱的思想将各种应用程序和他们所依赖的运行环境打包成标准的镜像，进而发布到不同的平台上运行，极大地方便了应用的开发及部署。同时，Docker作为一个容器级虚拟化的解决方案，其比传统虚拟化方式更加轻量，具有更高的性能、灵活性以及可扩展性。

未来云计算将逐步发展为Docker负责向上面向应用，平台负责向下面向硬件，Docker只专注于解决应用部署、扩容等问题，平台负责管理调度网络、存储等硬件资源。这种硬件、云平台和Docker容器的三层架构可以满足云信息化时代的所有应用场景。Docker正在迅速改变云计算领域

(上接第540页)

2 结束语

目前，天津电力云终端正处在部署阶段，相较于传统的人手一台PC机的老式办公手段，云终端具有以下优势：

- 1) 设计灵巧，云终端部署完成后，每个办公桌都将去掉传统的主机机箱，取而代之的是小小的云终端客户机，极大节约空间。
 - 2) 使用灵活，在每个部署有云终端的工位，登陆自己的账号后，都将展现自己设置的桌面，破除了空间的局限性。
 - 3) 节约能源，统一部署云终端后，每个云终端的功耗相比于传统PC主机有很大的低能耗优势。
 - 4) 维护方便，由于集中部署了云终端系统，方便了信息运维人员对于日常PC机的维护。
- 天津电力公司在云终端部署完成后，将大大

的运作规则，并彻底颠覆云技术的发展前景。

参考文献

[1] 戴王剑, 杨保华, 曹亚仑. Docker技术入门与实践[M]. 北京: 机械工业出版社, 2015.

[2] Docker介绍以及其相关术语、底层原理和技术[EB/OL]. <http://www.open-open.com/lib/view/open1413190983463.html>.

[3] Docker与虚拟机性能比较[EB/OL]. <http://blog.csdn.net/cbl709/article/details/43955687>.

[4] 容器不会取代OpenStack, 但二者如何深度整合?[EB/OL].<http://www.csdn.net/article/2015-05-20/2824734>.

[5] DockOne技术分享: OpenStack Magnum社区及项目介绍[EB/OL]. http://dockone.io/article/445utm_source=tuicool.

作者简介

沈雪晴（1990-），女，硕士，主要研究方向为IT运维、云计算和Web服务接纳控制研究。
(收稿日期：2015-12-10) **EA**
(编辑：崔文静)

提升信息化办公的效率，降低PC机损耗率，降低日常运维成本，落实公司“集约化”管理要求，提高对员工终端的管控力度。

参考文献

[1] 钟志琛, 邹海彬. 云终端提升电力企业桌面中断安全技术探讨[J]. 电力信息与通信技术, 2013(9).

[2] 韩向春, 潘勋, 陈晶, 等. 计算网格中动态负载均衡的分布调度模式[J]. 计算机工程与设计, 2007(12).

作者简介

于晓冬（1989-），男，本科，助理工程师，从事电网信息通信调度工作。
(收稿日期：2015-12-10) **EA**
(编辑：崔文静)