IT 融合云资源池跨平台版本升级改造实践

张志良，魏富生，李海俊
（中国联通内蒙古分公司 云网运营中心，内蒙古 呼和浩特 010050）

摘要：根据公司全面推进数字化转型的总体战略要求，统筹推进内蒙古联通数据中心、云计算与网络的深度融合，建设智能化综合性数字信息基础设施。通过对 IT 融合云资源池互联网域跨平台版本升级改造中的现状情况、目标架构、部署方案、技术实现方式进行详细分析和架构设计，实现敏捷高效响应业务需求、集约共享提升云资源效能的目标。有效支撑了核心生产系统持续服务，提升了 IaaS 层资源保障能力，积累了丰富的升级改造技术实践经验。

关键词：IT 融合云资源；IaaS ；核心域；互联网域
中图分类号：TN929.5　　**文献标识码：**A　　**文章编号：**2096-9759(2023)06-0165-04

0 引言

随着内蒙古联通全面深入落实联通集团公司数字化转型的总体战略，落实中国联通战略规划纲要“大联接、大计算、大数据、大应用、大安全”战略布局，云网运营中心积极推进建设云网融合、智能敏捷、绿色低碳、安全可控的智能化综合性数字信息基础设施，以实现IT融合云资源的统一规划布局、统一投资建设、统一资源调度和统一维护的目标 。作为公司集约化统一的内部资源池，已实现集团规划指导省分收敛集约为1个目标云池：IT 融合云资源池。实现公司内部资源池统筹管理，统一支撑公司B、D、M、O、E域系统应用部署需求，为各IT单元提供因地制宜的云化演进策略。

集约化的云资源统一运营服务工作，提升了云资源的服务支撑能力，提高了资源需求响应部署能力，实现了资源共享资源统筹能力，提供了新型基础设施助力公司的数字化转型发展。

为了不断提升 IT 融合云资源 IaaS 基础设施层的服务能力、支撑架构的完善性，满足公司五大中台、省分触点、前端业务、数据交互、CT+IT 融合业务应用的各类持续服务，进行资源池互联网域的迭代升级改造。

1 IT 融合云资源互联网域架构面临的问题

内蒙古联通 IT 融合云资源池统一支撑公司 B、D、M、O、E 域系统业务应用的资源需求、安全管控需求。随着公司的互联网化转型、业务发展模式的变革，各类应用业务逐步由传统的内部系统服务、用户到店办理业务、员工通过内部网络进行办公管理和生产运营的模式，转型为用户通过互联网服务应用自助办理业务、应用触点上门办理、公网系统服务数据交互、物联网应用管理、员工远程办公管理和生产运营的新型模式。公司的业务发展和运营管理对互联网应用的需求逐步增多，应用安全的保障要求也逐步提高。IT 融合云资源池互联网域架构体系的完善性受到极大挑战，面临以下问题。

1.1 资源池架构不新

IT融合云资源互联网域建设于2016年，采用出口防火墙+资源池平台+对内网防火墙方式，WAF 串接方式接入，安全控制是硬件设备配置管理、策略控制方式。在应对互联网时代大安全、大应用、业务隔离需求，整体架构明显滞后。

1.2 资源池版本较底

目前IT融合云资源互联网域的云操作系统是华为FusionSphere虚拟化（XEN），此版本于 2022 年 6 月起全面停止了技术支持。此版本在资源隔离、资源超分、资源管理、自动化部署、业务面和管理面分离控制、设备带外管理等方面功能不足。

1.3 资源池性能不足

IT 融合云资源互联网域的核心交换机 HW6855、管理交换机 HW5320 运行性能使用率在 60%以上，计算资源的服务器CPU 频率低、内存 128G\160G、存储资源 75TB，单台宿主机在分配虚拟机、业务存储资源需求上能力不足。

1.4 资源池安全控制方式有限

IT 融合云资源互联网域在东西向、南北向数据流安全控制、应用的安全防护上，安全控制方式较少，安全保障能力不足。

2 IT 融合云资源互联网域架构升级部署与实践

2.1 云资源现状分析

（1）服务器

IT 融合云资源池互联网域现有服务器配置：

表 1 服务器设备现状表

序号	型号	功能	数量	CPU	内存（G）
1	HP DL360 G9	管理节点	2	E5-2640 v3 @ 2.60 GHz 2*8 核	128
2	HW RH2288H V3	计算节点	6	E5-2650 v3 @ 2.30 GHz 2*10 核	256
3	HW RH2288H V3	计算节点	11	E5-2630 v4 @ 2.20 GHz 2*10 核	160
4	HW RH5885 V3	计算节点	11	E7-4809 v3 @ 2.00 GHz 4*8 核	256
5	HW RH5885 V3	计算节点	9	E7-4809 v3 @ 2.00 GHz 4*8 核	128
合计			39	980 核:管理 32 核 计算资源 948 核	7520

存在的问题：

①CPU 类型不统一。计算节点服务器有 4 种不同类型的CPU，主频不一致。

②系统资源安全保障能力不足。华为 FusionSphere 虚拟化（XEN）管理平台在虚拟机 HA 功能实现中，当物理服务器发生故障、虚拟机 VM 手工迁移的场景中，虚拟机 VM 不能够

收稿日期：2023-03-18
作者简介：张志良（1976-），男，内蒙古乌海人，大学本科，高级工程师，主要研究方向：云资源运营管理、云计算安全、IT 架构规划；魏富生（1999-），女，内蒙古巴彦淖尔人，大学本科，主要研究方向：云计算平台、网络安全运维；李海俊（1973-），男，内蒙古呼和浩特人，大学本科，高级工程师。主要研究方向：网络安全、短彩信的管理、业务支撑。

迁移到不同主频的 CPU 物理服务器上，只能动态迁移到同主频的CPU物理服务器上，资源池总的计算资源虽然较多，但是分类到同型号CPU主频的服务器中，资源明显有限，并在日常维护、发放虚拟机 VM 中，都需人为考虑资源的使用率、应用业务系统的异常情况支撑保障等问题。

（2）网络和安全

IT 融合云资源池互联网域现有网络和安全设备配置：

表 2 网络和安全设备现状表

设备名称	设备型号	设备接口
核心交换机	HW 6855	48 口万兆
管理交换机	HW 5320	48 口千兆
防火墙	DP F1000	万兆、千兆接口
深信服 WAF	AF-1820	千兆接口

存在的问题：交换机性能使用率在 60%以上，WAF 设备串联在防火墙和核心交换机之间，带宽利用率在 85%以上，随着业务增长，WAF 设备串接方式明显影响业务的访问流量。

（3）存储设备

HW 6800 V3 可用空间 75TB，使用率在 90%。在应用不断增长的需求下，仅能分配给业务最小资源空间，并及时回收下线系统资源，对业务发展存在滞后。

（4）资源池管理平台

互联网域资源池管理平台在 2016 年上线使用，部署华为 FusionSphere 虚拟化（XEN）软件 FusionComputeV100R006C10SPC101（zen）版本，此版本于 2022 年 6 月起全面停止技术支持。此版本在资源隔离、资源超分、资源管理、自动化部署、业务面和管理面分离控制、设备带外管理等方面功能不足。

（5）承载业务

部署公司触点受理、前端业务、数据交互、CT+IT 融合业务应用 138 台虚拟机 VM 共 37 套系统。

云资源池互联网域的服务器计算资源不统一、网络和安全设备性能不足、存储空间不足、资源池平台管理软件功能不足等问题，对于运营生产安全、应用业务的发展支撑存在诸多亟待解决的重要问题。

2.2 云资源升级改造架构分析与实践

（1）升级扩容资源池可用设备条件

2021 年 IT 融合云资源内网核心域升级改造工程完成，核心域重点部署公司 B、D、M、O、E 域关键业务系统，设备性能要求较高，互联网域作为业务的前端延伸服务功能区，对设备性能要求相对低一些。梳理核心域项目替换下线的资源设备，分析设备性能部分设备可以利旧在互联网域升级改造中使用，提高资产利用率，降低 CAPEX 投资。资源可利用情况如下：

10 台浪潮 NF5280M5 Gold 5120 CPU @ 2.20GHz *2 颗 14 核 384G 内存 2*1.6T SATA 盘。

2 台 HW S9312 交换机，4 块 24 口 万兆板、2 块 48 口千兆板；

2 台 HW 6300 48 口万兆；

4 台 HW 5300 48 口千兆；

1 台 HW 6800 V3 存储 96TB 可以空间；

2 台 DP F1000 防火墙 具备万兆、千兆接口；

1 套 FusionCloud6.5.1 版本 100 CPU lisense 使用许可。

（2）架构升级改造分析

华为 FusionCloud6.5.1 云平台管理节点部署需要 3 台服务器。配置基本要求：HW RH2288H V5，CPU 主频 2.20GHz 以上，内存 384G 以上，系统盘 2 块 960G SSD，利旧服务器配置不能满足管理平台搭建需求；

网络设备 2 台 HW S9312 作为核心交换机、2 台 HW 6300 作为管理交换机、2 台 HW 6300 作为 EOR 扩展交换机、2 台 HW 5300 作为带外管理交换机可以满足扩容需求；

服务器 10 台浪潮 NF5280M5 设备，总的计算资源不能满足现网 138 台虚拟机 VM 资源需求；

存储 HW 6800 V3 设备空间可以满足应用资源迁移需求；

防火墙 2 台 DP F1000 可以满足拓展资源池东西向业务域的安全隔离需求；

无可利旧万兆 WAF 设备，不能解决南北向带宽流量瓶颈问题；

综合以上可利旧使用的设备资源，云平台管理服务器、WAF、计算资源服务器不能满足整体架构改造需求，结合现网资源情况、业务特性，经过分析资源池架构升级改造思路，建议采用以下方式进行：

①梳理资源池在网运行设备，可以将核心域资源池计算节点 3 台 HW RH2288H V5（5120 CPU @ 2.20GHz *2 颗 14 核 384G 内存 2*960G SSD 盘）宿主机业务在线迁移到其他宿主机上，服务器从计算节点管理池中下线，使用利旧设备中的 3 台浪潮服务器 NF5280M5（Gold 5120 CPU @ 2.20GHz *2 颗 14 核 384G 内存 2*1.6T SATA 盘）并入核心域资源池计算节点，补回原有资源池计算能力。以此方式可以满足互联网域资源池管理节点的部署服务器设备需求；

②WAF 的网络接入由“透明模式”即串接方式变更为“旁路模式”旁挂方式，仅引流监测需要防护的业务数据流；

③资源池防火墙和核心交换机采用万兆口直连，原南北向 GE 带宽提升为 10GE 带宽；

④搭建新版本云资源管理平台，将 7 台浪潮 NF5280M5 设备纳入计算节点，逐步迁移原有平台业务系统，将腾退后原平台计算节点服务器分批并入新平台计算节点，解决计算资源不足问题；

⑤利旧 2 台 DP F1000 防火墙，用于资源池东西向业务隔离与互访控制；

⑥新资源池平台搭建，需要保障应用业务服务期间不中断，原有网络设备需要共用。

（3）改造升级实施方式

通过对扩容资源设备可用条件以及架构升级改造可行性分析，采用以下方式进行实施：

首先：进行网络升级改造。

规划新资源池平台网络业务 Vlan:

表 3 资源出 VLAN 规划表

分类	VLAN 号
安全区业务:	1000~1399
安全区互联:	1500~1899
资源池业务	2000~2599
资源池互联	2600~2999
资源池管理	3100~3199
心跳专用	3500~3699

安全区业务：VLAN1001:云安全平台 172.168.1.0/24
VLAN1002:4A 管理平台 172.168.2.0/24
VLAN1003:安全狩猎平台 172.168.3.0/24
.....
资源池业务：VLAN2001:微信公众号 172.169.1.0/24
VLAN2003:沃受理 172.169.2.0/24
.....
资源池管理: VLAN3106: external-api 1.0.1.0/24
规划新资源池平台管理网络 Vlan:

表 4 资源池管理网络规划表

网络平面	VLAN ID	VNI ID	子网	网关	用途	备注
external-api	3106	N/A	1.0.1.0/24	1.0.1.254	OpenStack 管理平面	VNC 登录虚拟机、登录 Portal，与 FusionCompute 管理平面互通
external-om	3107	N/A	1.0.2.0/24	1.0.2.254	OpenStack 管理平面	FusionCompute 管理平面互通，供告警、性能等数据上报
internal-base	3108	N/A	1.28.0.0/24	N/A	OpenStack 管理平面	默认为 1.28.0.0/20，如重新规划，修改 sys.ini 文件；OpenStack 内部管理网络，物理组网时，需要在交换机上为其设置 VLAN
Public_Service	3111	N/A	1.0.3.0/24	1.0.3.254	ManagerOne 云服务平面	公共服务平面
DMZ_Service	3112	N/A	1.0.4.0/24	1.0.4.254		
DMZ_Tenant	3113	N/A	1.0.5.0/24	1.0.5.254		
Heart_Beat	3114	N/A	1.0.6.0/24	1.0.6.254		

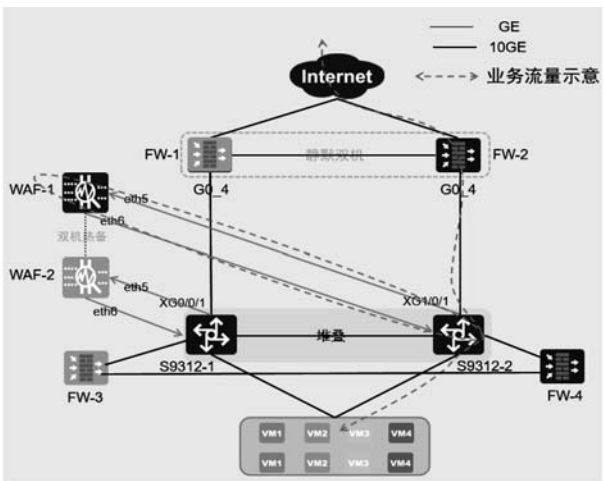

图 1 IT 融合云资源池互联网域网络升级改造拓扑图

升级核心网络交换机CE6855为S9312，保持原有系统VLAN、网关地址、上下级设备互连IP不变，配置在S9312上进行设置，CE6855作为二层接入交换机，仅透传业务VLAN、原有网关等配置信息清除。

WAF 设备接入由“透明模式”即串接方式变更为“旁路模式”旁挂方式，仅引流监测需要防护的业务数据流。

新增资源池东西向防火墙（FW-3、FW-4），用于资源池东西向业务隔离与互访控制；

升级改造中，需要保障应用业务服务期间不中断，原有网络防火墙、互联网出口设备需要共用。

核心交换机 9312 划分业务区、Security 区、4A 区，同步实现资源池各类物理设备的带外管理，新增防火墙（FW-3、FW-4）用于资源池东西向业务隔离与互访控制。

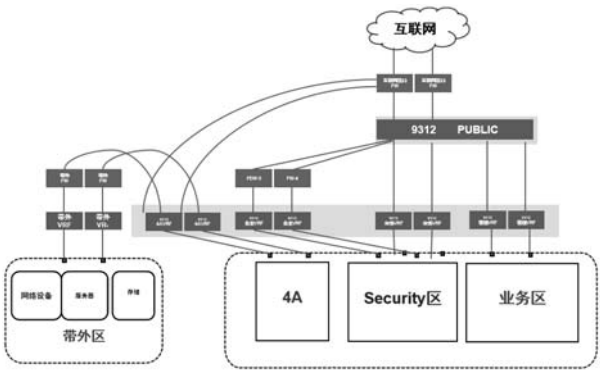

图 2 IT 融合云资源池互联网域网络安全控制拓扑图

其次：进行平台搭建和业务迁移

第 1 步：用 3 台利旧浪潮服务器替换核心域 3 台符合配置要求的华为服务器。互联网域新增 3 台华为服务器作为管理节点，利旧 7 台浪潮服务器搭建新互联网域资源池计算节点；

第 2 步：原互联网资源池业务通过使用迁移工具和重新部署系统两种方式改造迁移至新建互联网资源池；

第 3 步：逐步回收原互联网资源 31 台服务器，并入新建资源池；回收利旧原资源池存储 1 套到新资源池。

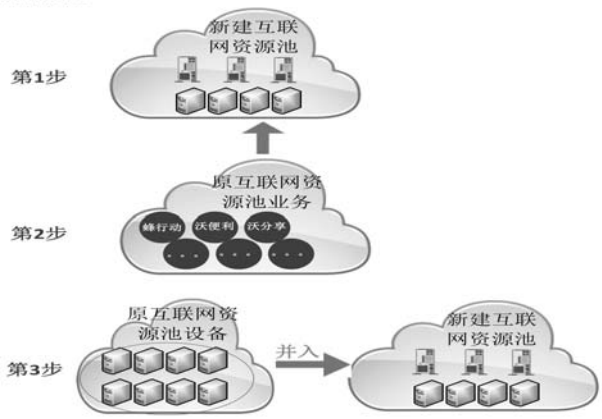

图 3 IT 融合云资源池互联网域迁移改造示意图

（4）资源池升级改造成效

通过对网络架构、管理节点和计算资源的升级改造，IT 融合云资源池安全管控能力、计算资源能力得到了较大的提升，提高了应用业务系统的支撑能力，能够快速响应新增应用资源需求和部署交付。

云资源池互联网域升级后服务器配置：（下转第 171 页）

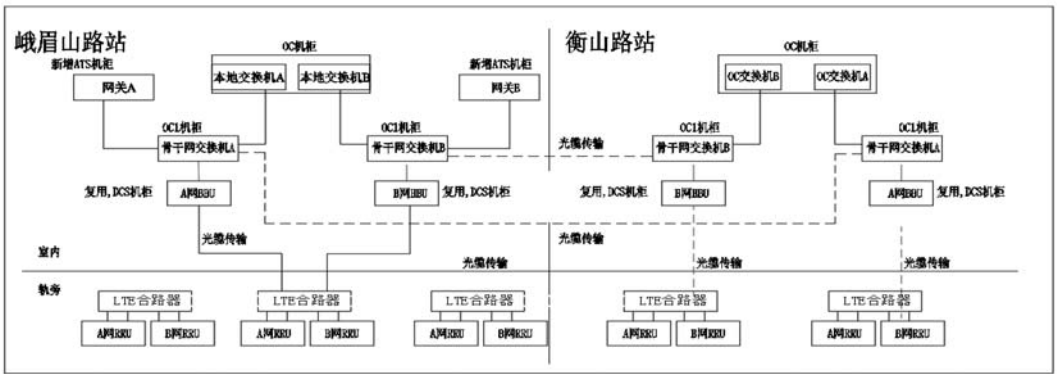

图 7 TACS 网络通信系统配置

5 结语

通过改造方案实施后，TACS 系统在 1 号线上验证了与外部轨旁设备、与车辆接口、通信质量等直接相关功能，还完成了在实验室无条件、现场有条件的功能，以及与外部系统联调的场景。通过实际验证得出，采用 TACS 系统将列车控制方式从联锁和 ZC 结合转移到车载信号子系统，实现了从“车-地-车”转变为“车-车”的通信方式，这一功能的提升减少了轨旁室内外设备的数量，减少了传输距离，在折返线时可以用比 CBTC 系统更少的时间完成折返功能，从而降低了运营和维护成本。同时，减少了对控制中心的依赖，使得发生故障的概率降低，提高了运营效率。此外，TACS 系统采用的车车通信方式，不依懒于轨旁设备，使得线路间的互联互通变得较为容易，是将来信号系统列车运行控制系统的主要方向。

参考文献：

[1] 杜建新, 左旭涛. 列车自主运行系统在城市轨道交通网络化建设和运营中的适用性分析[J].城市轨道交通研究,2020(10).
[2] 倪尉.TACS 系统在城市轨道交通信号系统更新改造工程中的应用研究[J].铁道通信信号,2022 年第 58 卷第 8 期.
[3] 朱莉.城市轨道交通信号系统改造方案研究[J].城市轨道交通研究,2021(4):118-121.
[4] 陈绍文.列车自主运行系统下城市轨道交通线路配线需求研究[J].城市轨道交通研究,2022,25(11).
[5] 罗情平,吴昊,陈丽君.基于车车通信的列车自主运行系统（TACS）的探讨与研究[J].城市轨道交通研究,2018,21(07).

（上接第 167 页）

表 5 服务器升级整合表

序号	型号	功能	数量	CPU	内存(G)
1	HW RH2288H V5	管理节点	3	Gold 5120 CPU @ 2.20GHz 2*14 核	384
2	浪潮 NF5280M5	计算节点	7	Gold 5120 CPU @ 2.20GHz 2*14 核	384
3	HW RH2288H V3	计算节点	11	E5-2630 v4 @ 2.20GHz 2*10 核	160
4	HW RH5885 V3	计算节点	20	E7-4809 v3 @ 2.00GHz 4*8 核	256
合计			41	1140 核:管理 84 核计算资源 1056 核	12160

云资源池互联网域升级后能力提升对比：

表 6 资源池升级改造前后性能对比表

	计算资源 CPU 核	CPU 分配率	计算资源内存 G	内存分配率	存储 TB	存储分配率
升级前	948	85%	7264	79%	75	90%
升级后	1056	38%	11008	52%	171	39%

升级后华为 FusionCloud6.5.1 具有 CPU 超分管理功能（原资源池版本不具有此功能），结合业务重要性，设置超分值 2；计算节点服务器 CPU 为双线程，总的能力为 4224 vCPU 。升级后，资源池 CPU、内存、存储的使用分配率明显较低，资源池平台安全性得到了有效保障，提高了应用业务系统需求资源部署的支撑算力。

核心交换机运行性能使用率由 60%以上降低到 25%左右，有效保障了业务数据的交换能力，提升了业务处理效率。

安全功能提升：

①新增防火墙（FW-3、FW-4），实现了资源池东西向业务隔离与互访明细策略控制。

②新增带外监控管理，统一监控管理资源池互联网域服务器、网络设备、安全设备，提升了平台监控管理、远程维护、应急响应能力。

③云安全管理平台部署：实现主机微隔离、主机防病毒、主机防 Webshell 扫描、主机防暴力破解、主机入侵防御等能力，提升了应用业务系统的安全管控能力。

3 结语

IT 融合云资源池互联网域在升级改造后具备更完善的网络安全体系，与资源池核心域形成统一的技术栈，实现了公司统一规划布局、统一投资建设、统一资源调度和统一维护的目标。通过流程贯通、统一服务标准实现全网资源一点看全、开通能力一点调用、智能应用一点部署、网络数据一点汇集、通信能力一点集成，以准确的数据支撑公司管理者规划与决策云资源的统一规划布局、统一资源调度和统一维护，实现敏捷高效响应业务需求、提升资源效能的目标。在数字化转型的战略背景下，打造云资源集约化的 IaaS 层数字化基座，提供了宝贵的网络安全架构升级、各类平台集约化改造、资产设备利旧的实践经验。

参考文献：

[1] 顾炯炯.云计算架构技术与实践[M]. 北京:清华大学出版社,2018:51-64.
[2] 阿里云智能全球技术服务部著.企业迁云实战[M].北京:机械工业出版社,2019.
[3] [美]Thomas ERL.云计算 概念、技术与架构[M]. 北京:机械工业出版社,2017:40-44 .
[4] 刘鹏.云计算(第三版)[M].北京:电子工业出版社,2018:32-39.
[5] 王思轩.数字化转型架构:方法论与云原生实践[M].电子工业出版社,2021:33-46.