云数据中心自动化运维能力提升的方法研究

钱曼硕，曹圆圆，王雷
（中国电信股份有限公司上海分公司智能云网操作维护中心，上海 201315）

摘　要：根据对云数据中心十余年的运维经验，基于中国电信上海公司多年来在天翼网络云的规划、建设、验收、运维、交付等工作的积累。分别从数据中心架构、自动化运维手段建设等方面展开，从多方面共同实现云数据中心的高冗余，使用各种手段共同提升云数据中心的运维效能。助力企业云网融合发展，并给出了云数据中心自动化运维能力提升的手段建议。同时，此方法也可供业务平台参考，助力各业务系统从平台出发，提升业务平台的运维能力。

关键词：云网融合；云数据中心；云网运营；云资源；云监控；云运维
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000-0801.2025071

0　引言

为加快落实集团云改数转战略，助力企业高质量发展，全力推进云网运营条线的数字化转型，促进云网价值与运营效益提升，加快建成世界一流企业，中国电信集团公司（简称集团）在2023年初编制下发《中国电信云网运营自智工作实施指导意见》。2024年，集团进一步要求故障能够1分钟发现、5分钟定位、10分钟处置。面对维护SLA要求的不断提高，如何通过架构冗余实现业务的快速切换，如何通过自动化手段支撑运维人员及时地发现故障、定位故障、修复故障，成为运维部门亟须解决的问题。

通过对标《中国电信云网运营自智工作实施指导意见》的相关要求，利用资源池架构的各类冗余技术，在资源池内部建设、资源池出局资源建设等方面，从自身提升云数据中心的健壮性，形成高可用的云资源池，在出现故障时实现业务的自动切换。同时，利用各类成熟的运维软件，对症下药，从统一管理网络、统一监控、统一鉴权、统一审计、统一巡检等方面提升，形成一系列的云数据中心自动化运维手段，从而适应当前时代背景下的运维高要求。

1　云数据中心的冗余架构

云数据中心是一个虚拟化的基础设施，提供存储、计算和网络资源，利用云计算技术和网络，将物理服务器和存储设备整合到一个统一的平台上，使用户能够根据需要动态地获取和管理资源，具有高度的灵活性和可扩展性。

天翼网络云依托于中国电信强大的网络能力，承载其上的业务平台有丰富的网络出口，因此每个业务平台均根据不同的业务需求，存在多张相互隔离的网络，与大多数的私有云以及公有云对比，网络组网比较复杂。

云数据中心的高冗余性，决定了在发生故障

收稿日期：2024-11-26；修回日期：2025-03-09

时，依托于这一系列的冗余手段，能够实现计算、存储、网络的自动切换和自动执行，大大提升了业务的连续性。因此，云数据中心的冗余架构是云数据中心内一切自动化运维的基础，是最重要的手段。

同时，部分平台承载了企业内的核心业务，对于云资源池的冗余能力要求极高。云数据中心在做好自身冗余的同时，还要支撑业务实现双节点乃至多节点的部署，也需要配合业务平台完成节点级故障的及时切换。

云数据中心节点由计算、存储、网络、安全和管理5个子系统构成，其节点架构如图1所示。

（1）计算。该子系统由常见的物理服务器集群、虚拟服务器集群等构成，为了满足高性能的业务需求，也包含GPU云主机集群，以及智能网卡云主机集群。近些年来，云数据中心内部，信创服务器资源已成为主角，取代了原有x86计算资源为主的情况，主要提供虚拟化的计算资源，包括虚拟机和容器等。

（2）存储。该子系统与计算资源配合，为上层应用提供相关存储，计算资源与存储资源之间通过不同类型的网络进行连接，如FC网、以太网、IP网。近年来，通过IP网络连接的分布式存储已经成为主流，取代了原有以FC网连接的集中存储为主的情况。分布式存储中，也已经大量启用了信创的存储型服务器。同时，在算力资源池中，也存在部分通过RDMA网络实现互联的存储。

（3）网络。该子系统通常由接入层网络、核心网络和出口网络构成，接入网络直接与计算资源和存储资源连接，而核心网络则汇聚接入网络，与出口网络连接，出口网络与城域网各网络设备进行互联。

（4）安全。该子系统负责确保资源安全高效运营，是由基础设施安全、网络安全、软件安全、数据安全、管理安全等多层次的安全功能构成。近年来，随着自动化运维的高要求，安全子系统的要求也随之增加，相应的能力手段提升也更加明显。

（5）管理。该子系统负责对资源池的各类资源进行管理，然后通过其管理接口，与上层的统一资源管理平台接口连接，从而实现异构、跨节点资源的管理。安全子系统和自动化运维能力提

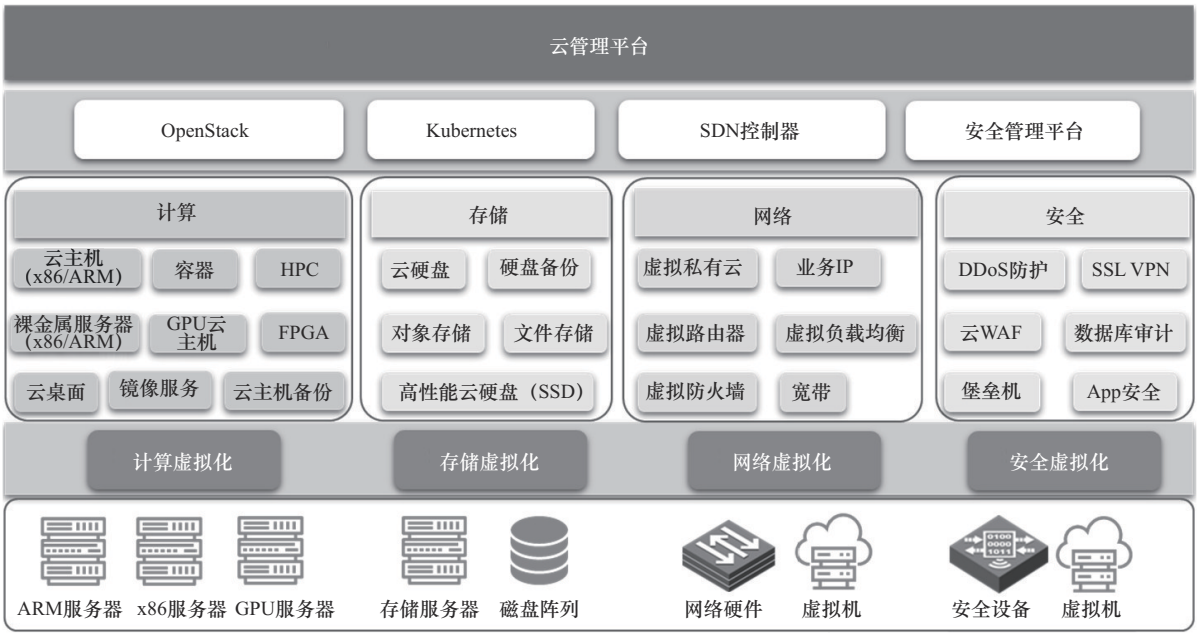

图1　云数据中心节点架构

升的基础，就是管理手段的提升，因此本系统是本文重点阐述的要点之一。

1.1 计算子系统的冗余实现

（1）硬件冗余

计算子系统的核心是物理服务器，无论是x86服务器或者是XC服务器，都需要利用硬件层面自身的冗余来实现业务的高可用性。

- 冗余的电源及风扇：电源以及风扇均需要冗余部署，且电源需要保持上联机架的两路电源，能够应对机房单路电中断的情况，此种冗余方式适用于所有的硬件设备，包含存储、网络设备，本文不再赘述。
- 冗余的网卡：虚拟化的网络，主要分为管理带内网络、业务网络、存储网络，在规划服务器时，需要注意配置多块网卡，且相同功能的网卡需要部署于不同的网卡上，如图2所示，从而实现在单网卡故障的情况下，业务不受影响。及时发现网卡的故障后，可以先对虚拟机进行热迁移，再进行停机维护，对于业务来说，几乎无感知。

（2）高可用集群

集群技术是保证业务连续性的关键技术，具体做法为将多台物理服务器配置为高可用性集群。其中，高可用性（HA）协议是一种通过自动故障转移来提供虚拟机高可用性的解决方案。它使用集群管理软件来监控虚拟机的运行状态，当检测到某个计算节点故障时，会自动在其他健康的物理主机上重新启动虚拟机，从而确保业务的连续性，如图3所示。

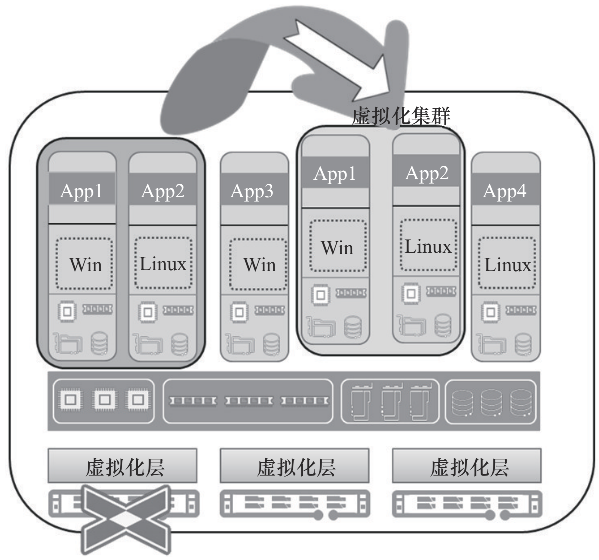

图3 主机发生故障后的虚拟机迁移

（3）数据冗余

定期对虚拟机的存储进行快照和备份，以便在数据损坏或丢失时快速恢复。

（4）业务异地部署

云数据中心按照双节点进行建设，其承载的重要业务部署在不同节点的云资源池内，设置自动故障转移机制，在一个数据中心发生故障时，自动切换到另一个数据中心，确保业务连续性。此方案最有效，但需要业务平台基于业务特性进行设计。

1.2 存储子系统的冗余实现

（1）集中式存储冗余情况

冗余主要包括控制器、风扇、电源、硬盘，控制器采用1+1双活冗余，也保证了服务器到存储的多路径冗余；电源模块形成1+1冗余，部分存储具备上下电源平面，形成2×（1+1）的冗余模式；风扇采用n+1主备冗余。大部分存储采用硬盘RAID 5\RAID 6技术对数据进行保护，个别

服务器					
	网卡1	网卡2	网卡3	FC卡1	FC卡2
0	1	3	5	F1	F2
	2	4	6		

	0.带外管理口	
IP光口	1.业务1	2.带内管理/vMotion1
	3.带内管理/vMotion2	4.iSCSl1
FC光口	5.iSCSl2	6.业务2
	F1.FC1	F2.FC2

图2 服务器网卡位置分布建议

业务需求要求采用 RAID 10 进行保护（如图 4 所示）。

（2）分布式存储冗余情况

- 多副本、纠删码（erasure code）等多种数据冗余策略。
- 故障域配置。同一个集群内（如图 5 所示）的多台存储服务器，需要分布于不同的机架上，从而将数据均匀分布在不同的故障域中，避免单机架掉电等情况造成的存储集群全阻。通过合理设置故障域和使用故障域感知的调度策略，可以有效地降低系统故障对业务的影响。
- 数据强一致性机制。确保写入数据的所有数据分片均一致之后才进行写入确认响应。

1.3　网络子系统的冗余实现

网络子系统包括接入层、核心层、出口层、防火墙、负载均衡等，为云数据中心节点提供网络资源。此外，近些年来 SDN 技术逐渐成熟，也成为了大型云数据中心的基本技术，提升了云数据中心网络的自动化运维能力。

（1）多路径网络连接

在网络设备之间部署多条物理链路，确保即使一条链路出现故障，数据流仍然可以通过其他链路进行传输。常用的技术是链路聚合（link aggregation），将多个网络接口聚合成一个逻辑连

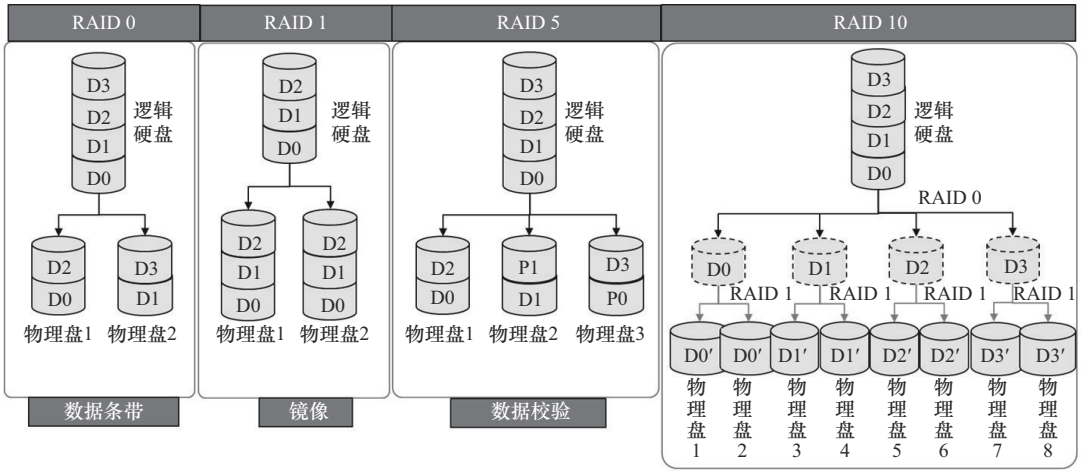

图4　常见RAID技术原理

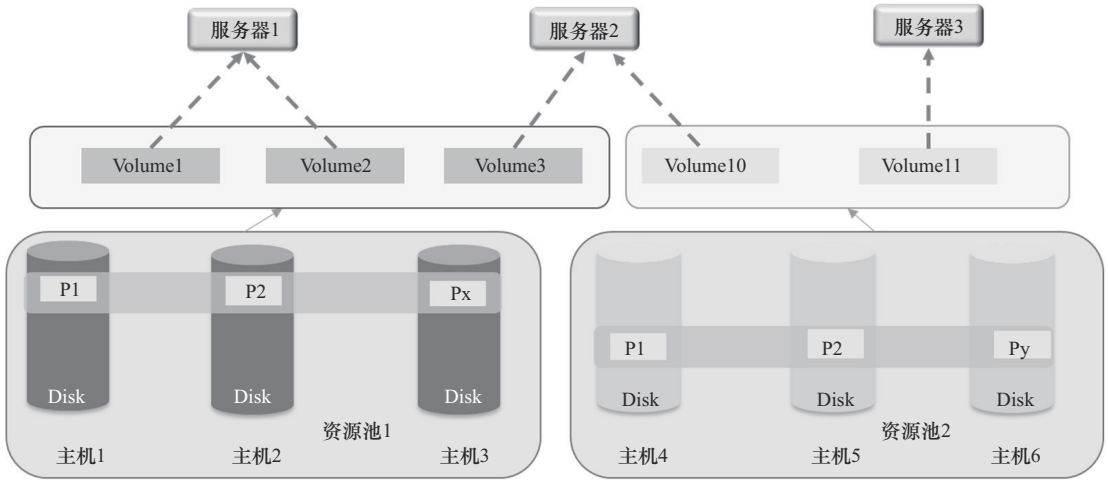

图5　分布式存储架构

接，提供更高的带宽和冗余能力，避免单点故障。

（2）路由保护

- 采用VLAN和虚拟路由技术，将不同业务或应用的流量隔离，降低故障传播风险，并增强安全性。
- 使用动态路由协议（如OSPF、ISIS、BGP等）实现自动路由选择和快速收敛，当网络拓扑变化时，能够迅速调整路由路径。

（3）冗余网络设备

- 高可用性（HA）协议。使用HSRP、VRRP（虚拟路由冗余协议）等协议，实现路由器和交换机的高可用性，确保网络的持续运行。
- 堆叠技术。允许多个网络交换机通过专用的堆叠端口连接在一起，形成一个逻辑单元。堆叠中的所有交换机共享管理和配置，能实现简化网络管理和故障恢复。但是堆叠技术没有通用标准，大多为厂商私有技术实现，出现BUG的概率较高，且在软件版本升级等维护操作中存在一定风险，现网中不建议使用。
- M-LAG技术。允许两个或多个物理交换机在逻辑上联合，作为单一的虚拟交换机进行链路聚合。M-LAG提供跨设备的冗余和负载均衡，确保即使其中一个交换机失效，流量仍然可以通过其他交换机转发。它还支持多条链路同时工作，提高了带宽和容错能力。相较于堆叠技术，M-LAG的故障隔离更为有效。由于多个交换机的存在，单个交换机的故障不会影响整个逻辑交换机的操作，而在堆叠技术中，某个交换机的故障可能会影响整个堆叠组的性能。因此在云数据中心内部的应用更为稳定。

（4）出局光路冗余

根据多年的维护经验，2根、4根等冗余的出局光路已经不能满足云数据中心的高SLA要求。在电信内部，对于重要核心链路制定了严格的SRLG要求，对于同一功能的一组链路，必须使用不同光缆、不同管道。不同管不同缆已经成为了资源池建设的基本要求，也成为了检验云数据中心业务连续性的重要指标之一。

1.4 安全子系统的系统化

安全子系统由基础设施安全、网络安全、软件安全、数据安全、管理安全等多层次的安全功能构成。各项安全均有相应的技术进行支撑，本文不再赘述。

面对日益强化的运维安全需求，通过技术手段提升基层员工的运维安全能力已经成为最为迫切的需要。本文也将着重展开运维安全手段的能力建设。

（1）统一认证能力：云数据中心的规模少则数百，多则数千数万，必须引入统一认证的能力，才能实现自动化的运维。

- TACACS+（terminal access controller access-control system plus）是一种通过集中的服务器为网络设备提供访问控制的协议。TACACS+提供了独立的认证、授权和记账服务。网络设备均支持TACACS+的认证。
- 轻量级目录访问协议（LDAP）是一种用于访问和管理目录服务的协议，主要用于存储用户、设备、权限等信息。它以树形结构组织数据，允许用户进行快速查询和修改。LDAP广泛应用于身份验证、授权管理和配置管理等领域，实现集中化的用户管理和安全控制。大部分服务器、存储设备均支持LDAP的认证登录。

（2）堡垒机能力：运维审计、运维合规是运

维安全的最重要组成部分，也是规避变更风险的最有效手段，运维留痕能力、提权电子化、双屏审核、配置金库等已经成为堡垒机不可或缺的功能。

1.5　管理子系统的系统化

如今，管理子系统已经不再局限于云管理平台等常规系统。随着自动化运维的需求日益旺盛，为了具备自动化运维能力，资源管理、告警管理、日志管理、端到端关联已经成为必须解决的问题。基础数据是一切自智能力的根本要素，没有基础数据，一切自智的规划均是空中楼阁。因此，近年来，基础数据能力的采集、规约，是天翼网络云运维工作中的重点，也是第2节着重展开的话题。

（1）资源管理能力。配置管理数据库（CMDB）在云资源池维护中，是一个用于存储和管理关于云基础设施及其配置的结构化信息的数据库。它包含资源信息、关系管理、变更记录、可视化与报表能力，为资源管理、故障排查、变更控制和合规性审计提供了基础支撑。

（2）监控、日志能力。目前成熟的开源软件Zabbix、普米、ELK、Grafna等已经成为了提升云数据中心运维能力的重要工具，结合运维团队少量的开发工作，可以大大提升云数据中心的运维效率和基础数据采集。

（3）云管理平台。云管理平台是一个系统化的平台，其将各类运维能力汇总，是与外部平台连接的统一接口，也是数据共享的接口。随着运维要求的进一步提升，云管理平台始终处于功能迭代及更新的状态，如图6所示。

2　云数据中心的运维手段探索

近10年来，中国电信上海公司从IT到CT云，到如今的CT边缘云，从2个节点、4个节点到如今近50个节点的规模。自动化运维已经成为了必须具备的要求，本节将根据几个典型的统一维护手段建设，以点见面，全面地阐述云数据中心的运维手段提升之路。

2.1　云数据中心验收标准

除了云数据中心设备的设备验收、冗余验收，这里着重讨论自动化运维能力提升所必须完成的基础建设工作，这是本节的关键，也是本节后续一切自动化手段能力建设的基础。在项目建设期间完成建设，是云数据中心实现有效管理的前提。

（1）统一管理网络。同一个运维团队，针对各节点的设备、资源，必须建立一张各业务独立、各物理节点统一的网络，这是后续管理手段集约的前提。必须有一张规划好的管理网络，在电信内部，可以借助大网强大的城域网能力，新建一个云管理VPN群组来实现。

（2）逃生管理网络。为了避免数据中心内部的IP网络故障，必须完成串口交换机的建设，通过console口实现网络设备的管理，同时，为了在城域网故障的时候对资源池进行远程维护，需要建设一个基于传输（如OTN等）搭建而成的云管理逃生网络。

（3）统一的NTP服务。时间同步，是资源池启用时必须要具备的条件。可通过以下方式实现：核心云池部署主备两台NTP服务器，与外部时钟源进行同步；各物理节点分别部署NTP次级代理节点，与核心云池的NTP服务器进行同步；同一个云数据中心内的设备完成与本节点NTP服务器的时间同步。统一的时间，是后续实现端到端维护时对各项数据进行匹配的重要判断依据。

（4）SNMP、Syslog预配置及监控纳管。对于全量设备完成SNMP采集账号、trap目标服务器、trap范围等配置，完成Syslog范围、目标服务器等配置。为了保证监控数据不因为远距离传输而丢失，建议各项采集均在本物理节点内完成，采用Server+Proxy的架构，节点内部署采集探针和Syslog服务器，完成本物理节点的全量设

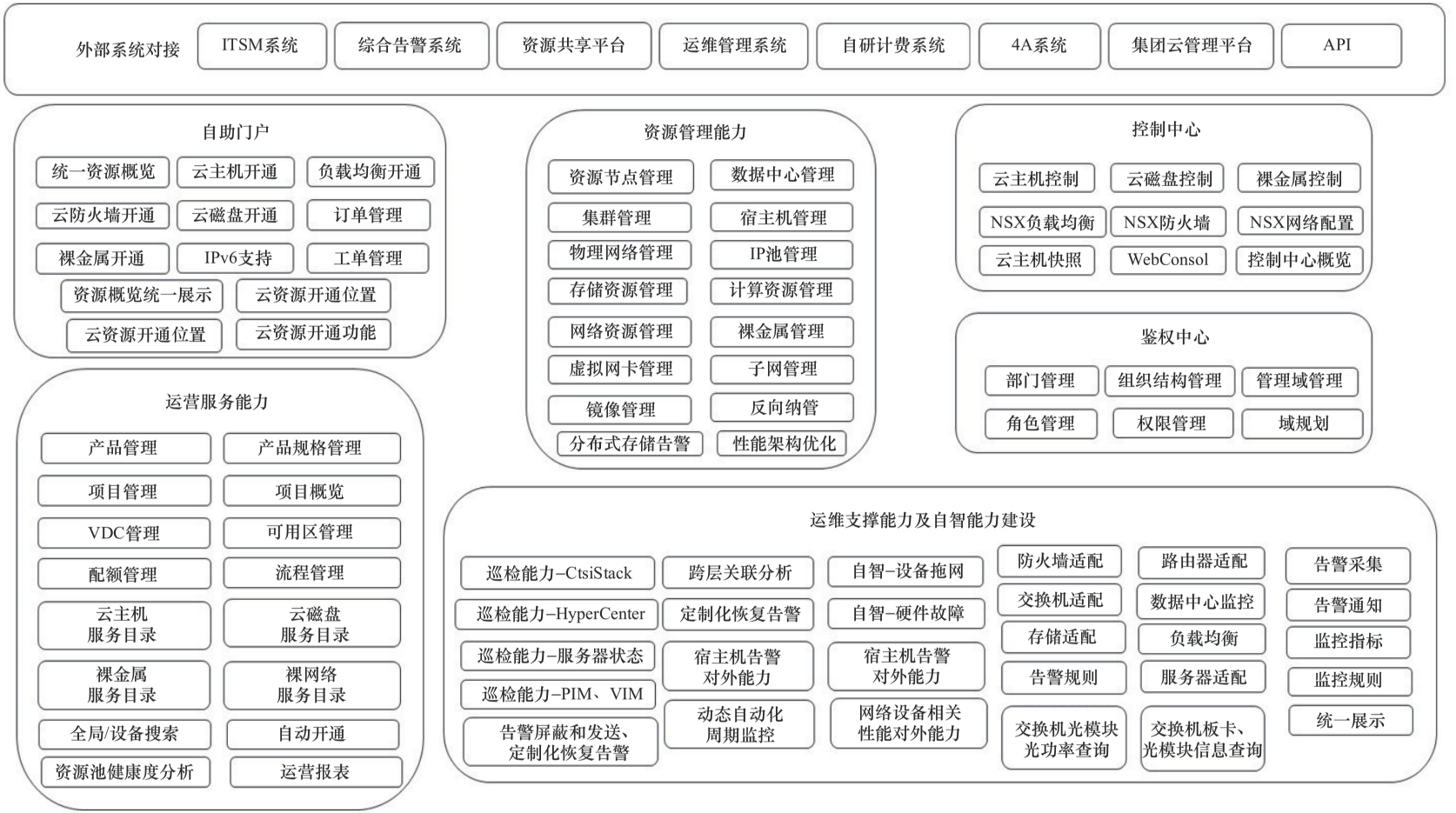

图6　云管理平台功能架构

备告警采集、性能采集、日志采集工作。此项工作是后续自动化运维的基础数据，是自动化运维执行的重要依据。

（5）Tacacs+、LDAP 预配置及账号鉴权纳管：对于全量网络设备完成 Tacacs+预配置，并完成只读权限和管理员权限的预配置，其中，由于各网络设备厂商的权限设置不同，对于只读权限的设置，注意要完成定制化配置。服务器、存储以及各类管理平台一般都具备 LDAP 账号能力，可以在开局时完成全量设备的 LDAP 账号认证预配置。此项工作是后续完成各类自动巡检和安全运维的前提。

2.2　云数据中心资源管理能力建设

资源数据是开展一切云运维工作的基础，需要考虑储存哪些数据，如何储存这些数据，数据之间的关系是什么，这些数据哪里可以使用，怎样保证数据的准确性，如何稽核这些数据，怎样保证数据的安全。结合这些疑问，需要从以下几方面考虑 CMDB 的建设。

（1）资源池及位置信息。资源池信息包含各类属性的私有/公有云池；位置信息包含园区信息、机楼信息、机房信息、机架信息以及 U 位信息。

（2）物理设备信息。物理设备信息包含云数据中心内部各类型物理设备的基本信息。从设备功能上分，包含服务器、交换机、路由器、存储、防火墙等。基于每一种功能的物理设备，相应的属性标签各有差异，随着各条线的精细化管理，动态增加属性字段。

（3）非物理设备信息。包含虚拟化集群信息，也包含不含物理位置属性的各类主机信息。此类设备的特征主要是和物理设备存在从属关系，需要做好匹配。

（4）连接信息。需要包含设备与设备之间的物理连线关系。

（5）其他信息。此部分包含处于云数据中心外围但影响资源池维护工作的信息，如出局链路信息、维保厂商信息、设备资产信息等。需要包含出局链路的保护组关系、资产和资源的匹配关系等。

CMDB 各类信息的录入必须严格执行专人维护，做好数据稽核后再进行录入，其余成员仅能通过订阅相应数据进行查看，不可编辑。

同时，CMDB 的录入嵌入验收流程中，从管理流程上提升数据的完整性。

CMDB 的引入，首先可以直观地展示出云数据中心内的各类资源情况，其次，CMDB 需要兼顾 API 能力，和各类系统做好对接并提供基础数据，如和堡垒机系统做好对接完成全量设备维护管理纳管、和监控系统对接完成全量资源完成监控覆盖、和端到端系统对接完成资源关联等。

2.3　云数据中心监控能力

对于云数据中心的监控，主流的开源软件有 Zabbix、Prometheus，针对日志级监控，使用 ELK。其中，Zabbix 对于物理设备的监控，适配度更高。本文重点基于 Zabbix 在云资源池监控的应用进行阐述。

Zabbix 采用一个主节点、多个代理节点的部署模式，各节点间借助城域网 B 平面，通过统一云管网络实现节点间的互通，所有性能的采集在节点内部完成，由代理节点将采集数据和告警数据上报至主节点，由主节点进行统一展示和应用。具体逻辑部署拓扑如图 7 所示，保证各个节点和 Server 节点网络互通，时延在 30 ms 以下。容器化部署 Zabbix Server、Zabbix Proxy、keepalived、nginx、mysql 等各类组件，其中 keepalived 用作高可用，nginx 用作反向代理。

通过部署监控系统，可以实现以下能力。

（1）性能采集能力

- 包含网络设备的 CPU、内存使用情况、端口状态、端口流量、端口误码情况，以及电源、风扇、温度、功耗情况等指标，并能够通过性能数据形成自定义时间区间的曲线图。

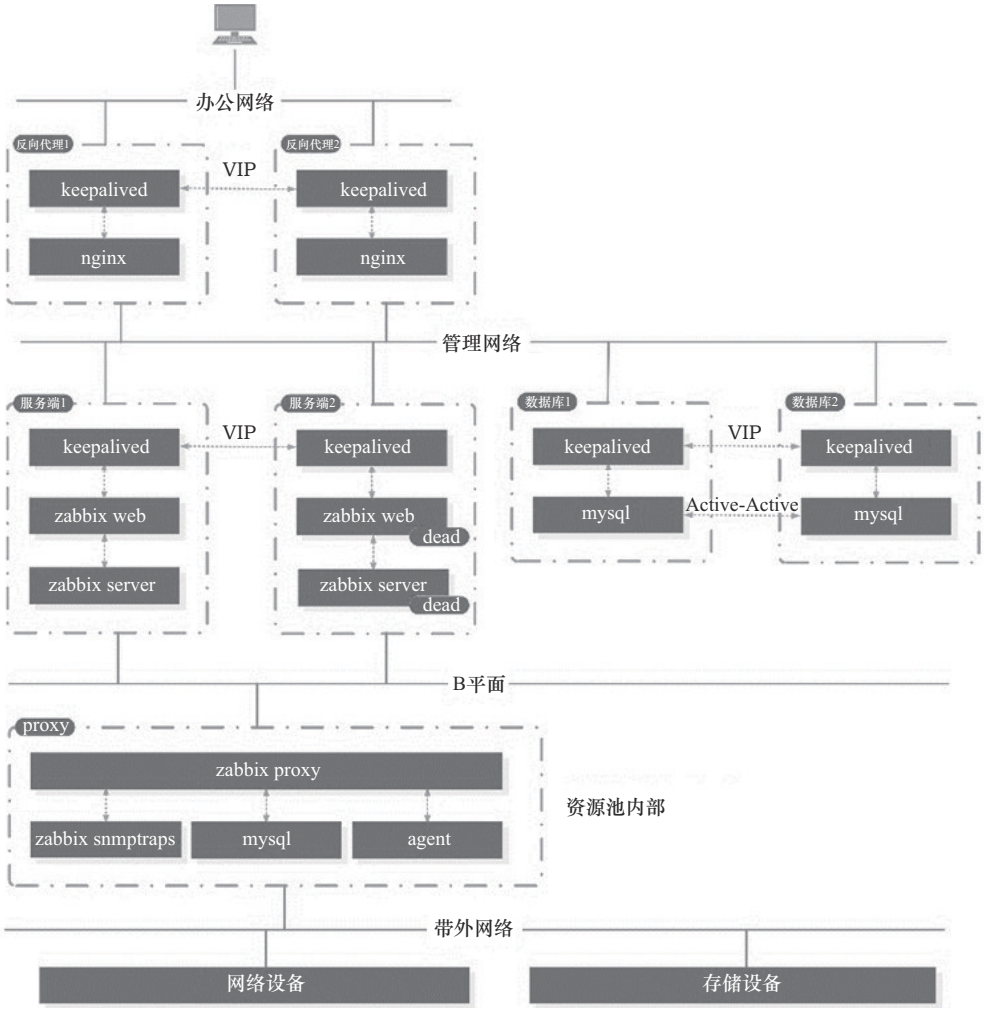

图7　Zabbix监控逻辑拓扑

- 包含存储设备的硬盘状态，以及控制器状态，电源、风扇、温度、功耗情况等指标，并能够通过性能数据形成自定义时间区间的曲线图。
- 包含服务器设备的CPU、内存使用情况，以及电源、风扇、温度、功耗情况等指标。
- 能够采集监控系统自身的性能数据指标。
- 具备自动发现、自动识别新增的端口、硬盘、电源等设备变动情况并执行性能采集的能力。
- 具备将采集到的数据进行能力开放的能力，如下文谈到的端到端监控能力调用。

（2）告警能力

- 设备通过SNMP Trap自动上报设备产生的告警，并由告警平台触发规则，将告警通过邮件、企微、短信等发送给维护负责人。
- 通过采集到的性能数据，自定义告警触发规则，并产生告警，发送给维护责任人。
- 根据维护操作或者工程情况，屏蔽相关设备告警上报的能力。
- 对系统本身的告警实现采集并上报。
- 具备将告警上报能力进行开放的功能，

例如，和综合告警系统实现对接，形成告警实时派单等。

2.4　应用——安全运维能力形成

安全运维能力的建立，需要将统一认证、堡垒机、云网资源以及CMDB组合为一个整体，辅以运维管理规范及流程。接下来着重分析各系统可以提供哪些能力、各能力可以被谁调用。

（1）CMDB：CMDB包含了全量的设备信息以及资源信息，因此堡垒机中纳管的设备清单，需要从CMDB提供的接口自动获取，从而实现设备纳管率100%。

（2）统一认证系统：主要包含LDAP和TACACS+，TACACS+用于网络设备统一认证，以及LDAP实现服务器、存储和CMDB、堡垒机等各类管理平台的统一认证。

（3）堡垒机：堡垒机作为安全运维的重要载体，是运维人员直接交互的系统，高阶功能均需要依赖堡垒机自身的能力，如金库模式、双屏审核、操作审计、录屏以及账号提权等。

2.5　应用——端到端的监控能力形成

端到端的监控能力形成依靠各项基础数据的采集。主要包含以下几点基础能力：CMDB能力、端到端拓扑能力、性能采集能力、告警采集能力、智能分析能力（调用电信启明网络大模型）。通过将基础能力组合，形成端到端告警监控的高阶应用。

资源数据采集中，如何动态地采集到所有资源的关系数据，而不是导入一份静态数据，从而实现根据拓扑的变更实时更新，是最大的挑战，需要通过以下两点实现。

（1）连接关系的采集

- 对于使用光纤端口的网络设备，均支持LLDP，可以通过SNMP，对于网络设备的LLDP信息进行采集，从而可以完成一份以网络设备连接信息为底的基础数据。
- 对于FC存储和FC交换机设备，可以使用SNMP采集光纤交换机以及FC存储，服务器的WWN信息，以WWN信息来组合形成FC连接信息。
- 对于部分服务器，通过在操作系统内部安装LLDP进程，完成连接信息采集，可以实现服务器与网络设备之间的连接关系采集。
- 对于部分不支持LLDP采集的设备，通过采集IP地址的MAC信息，以及网络设备上的ARP信息、MAC表信息，基于MAC地址的对应关系，完成连接关系自动采集的补全。

（2）从属关系的采集

此处主要涉及虚拟机和服务器之间的对应关系，此部分通过虚拟化管理软件提供的API，实时采集虚拟机所在的宿主机状态信息，宿主机通过和服务器硬件的对应关系，实现虚拟机和服务器硬件告警的关联。

基于基础数据的采集，关系图谱可以展现出以下3种关系。

（1）设备与设备之间的连线关系。

（2）设备与资源之间的从属关系。

（3）设备、连线与告警、性能的对应关系。

3　结束语

现有的运维手段，距离电信云网自智L4的目标仍有很多可以提升的方面，如自动巡检、自动故障定位等，仍须做好相应的技术选型和部署覆盖。本文结合自动化运维手段落地实践和基础数据在实践中的重要性给出了明确的阐述。从资源规划、资源建设阶段，即完成相应基础数据的采集，成为建立自动化运维手段的关键要素，也为后续提升自动化运维能力指出一条清晰的路径。

参考文献：

[1] 钱曼硕, 腾贞琪, 刘溪云, 等. 云网资源图谱实现资源可视的方法研究[J]. 电信科学, 2022, 38(Z2): 24-34.

[作者简介]

钱曼硕（1985−），男，中国电信股份有限公司上海分公司智能云网操作维护中心工程师、云计算运营支撑中心副主任，主要从事云资源池架构规划，建设和运维的工作。

曹圆圆（1995−），男，中国电信股份有限公司上海分公司智能云网操作维护中心工程师，主要研究方向为云计算、自动化开发。

王雷（1975−），男，中国电信股份有限公司上海分公司智能云网操作维护中心高级工程师，主要从事云资源池建设和运维的工作。