华为云 UCS

产品介绍

文档版本 01

发布日期 2025-08-28

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

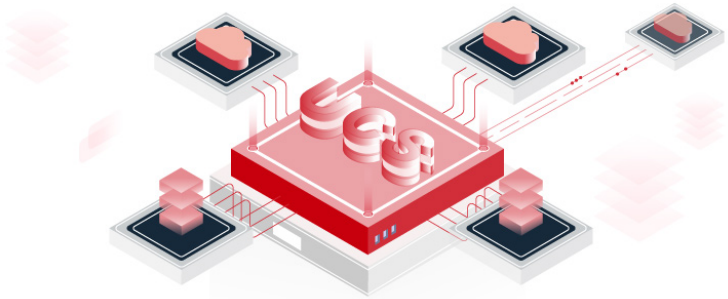
网址： https://www.huaweicloud.com/

目 录

1 图解华为云 UCS

初识华为云UCS

把云原生能力带到企业每一个业务场景



随着企业的容器化转型更加深入，

应用服务的云基础设施呈现多元化趋势。

公有云、私有云、边缘云等多云协同场景屡见不鲜，

这也从**算力、流量、数据、体验**等各方面产生了更多的需求。

什么是华为云UCS

分布式云原生（Ubiquitous Cloud Native Service, UCS），是一个分布式集群的统一管理平台，为企业提供了云原生业务部署、管理、应用生态的全域一致性体验，全面覆盖企业公有云、私有云、边缘云等场景，实现算力按需供给、流量智能调度、应用一键部署等诸多创新模式。

2 什么是华为云 UCS

华为云UCS（Ubiquitous Cloud Native Service）是业界首个专门针对集群跨云场景的分布式云原生产品，为企业提供云原生业务部署、管理、应用生态的全域一致性体验，让客户在使用云原生应用时，感受不到地域、跨云、流量的限制，把云原生的能力带入到企业的每一个业务场景，加速千行百业拥抱云原生。

华为云UCS是一个分布式集群的统一管理平台，在CNCF首个多云容器编排项目Karmada的基础上，实现了云原生应用跨云跨地域统一协同治理，支持华为云基础设施（CCE Standard集群、CCE Turbo集群）、伙伴云基础设施（CCE集群）、用户自有基础设施（自建Kubernetes集群等），以及第三方云服务设施（Kubernetes集群）的统一管理，全面覆盖中心区域、热点区域、客户机房、业务现场等多种使用场景。

华为云UCS具有以下创新模式：

- 应用与数据协同创新模式

  通过分布式数据管理，实现数据随应用一键迁移，全业务一体化迁移、弹性、容灾，让应用感受不到地域限制。
- 应用算力供给新模式

  通过分布式调度管理，实现百万级节点算力协同，随时、随地提供应用所需的算力资源，让应用感受不到跨云限制。
- 应用流量治理新模式

  通过分布式流量控制，实现智能流量分发调度，实时跨域、按需调配应用访问流量，让应用感受不到流量限制。

介绍视频

功能介绍

- **跨云、跨地域集群统一接入，统一管理**

  支持跨云、跨地域的集群统一接入、统一管理，支持接入华为云集群、本地集群、附着集群和伙伴云集群。
- **集群配置跨云、跨地域统一下发，管理更简单**

  支持多云多集群配置策略的统一管理，支持企业级项目租户的**权限管理**，可以通过统一的**策略管理中心**完成多云多集群的合规性审计。
- **可视化监控洞察，运维更简单**

支持立体化监控运维，并且兼容开源Prometheus和OpenTelemetry生态，拥有灵活的Dashboard，支持智能巡检、容器洞察、服务网格洞察。

- **算力统一调度，部署最优，运行最佳**

  基于Karmada内核，UCS可完成上千个分布式集群的统一接入，实现百万节点资源的协同调度，并拥有秒级响应速度。为用户提供了多种分布式部署策略，可以做到根据全局资源分布和业务特点，结合地理位置、网络QoS、资源均衡度等条件对应用进行最优化部署。

- **应用统一流量治理，提升业务体验**

  UCS可基于访问位置和业务策略对全域流量进行最优化调度，支持跨云多集群服务接入和流量管理，可实现基于权重、内容进行流量切分、灰度、故障倒换、熔断限流等功能。

- **应用数据协同，一键迁移**

  UCS实现了数据与业务一体化，围绕应用构建自动化的应用迁移、克隆能力，实现数据同步复制及跨云伸缩能力，支持存储层、容器层、中间件层等不同层次数据随应用场景实时联动，支撑应用容灾、扩容、迁移。

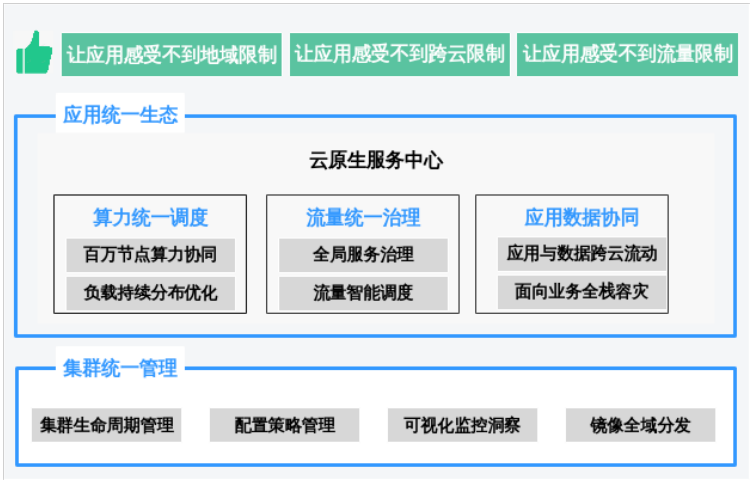
- **应用统一生态，全域可用**

  UCS拥有统一的服务规范，可真正实现应用开箱即用。通过自研部署引擎，统一服务生命周期管理，所有服务包统一管理、统一存储、全域分发，可实现跨云跨集群的一键部署。

产品架构

华为云UCS的产品架构如图2-1所示。UCS支持跨云、跨地域集群统一接入、统一管理，覆盖华为云集群（CCE Standard集群、CCE Turbo集群）、附着集群、伙伴云集群以及本地集群。通过多云多集群配置策略管理、可视化监控洞察、镜像全域分发，并结合三大创新模式，真正实现让应用感受不到地域、跨云、流量限制的目标。

图 2-1 UCS 产品架构



3 产品优势

华为云 UCS 的优势

随着云原生应用深入企业各个业务场景，跨云跨地域统一协同治理，保障一致应用体验等新的需求日渐突出，华为云UCS构建无处不在的云原生服务，加速各行各业云原生升级。

- **一站式多云统一体验**

  支持华为公有云（中心Region、IEC、CloudPond）、客户自建IDC以及第三方云场景的Kubernetes集群统一接入管理。同时基于多云多集群配置策略的统一管理，支持企业级项目租户的权限管理，可精细化管理子账号对接入Kubernetes资源的访问权限。以及通过统一的策略管理中心完成各个集群的安全策略和资源访问限制，便于多云多集群的合规性审计。UCS还提供按“应用->Region->集群->资源粒度”进行监控运维，以及灵活的Dashboard、智能巡检、容器洞察等多云运维监控能力。

- **百万级节点算力协同**

  华为云UCS基于华为云贡献至CNCF的多集群管理项目Karmada，通过多云管理平台能力，可支持上千个Kubernetes分布式集群的统一接入，同时最高可支持百万级节点资源协同调度，实现应用在分布式云场景下的跨云跨集群的弹性伸缩，应用故障时的跨云迁移，可根据全局资源分布和业务特点，结合地理位置、网络QoS、资源均衡度等条件下的应用最优化部署。让用户可以随时、随地提供应用所需算力资源。

- **智能流量分发调度**

  通过统一的容器网络编排和服务发现能力，实现跨云跨集群扁平化互通能力，达到业务体验一致和通讯安全可靠的目标。同时可支持用户接入流量就近分发至最合适的后端集群，缩短访问延时，同时支持流量基于访问者网段、地域、运营商等不同策略下的分发，通过UCS上的服务网格能力可以支持跨云跨集群的统一服务治理，实现基于网络QoS优先级调度、地理亲和等能力，同时借助网格能力可支持自动化灰度发布，服务拓扑可视化，服务调用链等能力，使得用户可以实现实时跨域、按需调配应用访问流量。

- **数据随应用一键迁移**

  UCS分别针对存储设施层、容器集群层、中间件数据层提供应对不同业务场景的数据复制能力。提供跨云迁移数据自动化同步能力，同时基于数据随应用的同步复制能力，可以实现在分布式基础设施上的弹性扩容。在扩容场景中，完成零人工干预的数据扫描和重建，完成以应用为中心，全业务一体化迁移、弹性、容灾。

华为云 UCS 对比传统云原生

表 3-1 UCS 与传统云原生对比

对比项	传统云原生	华为云UCS
体验性	各厂商对传统云原生都进行了一定程度上的定制，而在多元化场景下，为避免厂商绑定的情况发生，用户往往不会统一使用一个厂商的产品。因此用户在进行各区域集群管理时会有不一致的用户体验，这也会造成一定的学习成本。	**多云统一体验** 华为云UCS提供多云统一接入管理，弱化集群的厂牌限制，全面覆盖中心区域、热点区域、客户机房、业务现场等多个业务场景，为您提供统一的云原生体验。
可扩展性	传统云原生可以做到云上资源的弹性调度，但依然存在多云限制和地域限制，无法做到计算资源跨云调度。	**算力统一调度** 华为云UCS基于Karmada内核提供了多云资源的统一调度能力，支持将线下IDC的应用弹性至公有云。并提供了多种分布式部署策略，可以做到根据全局资源分布和业务特点，结合地理位置、网络QoS、资源均衡度等条件对应用进行最优化部署。
应用管理能力	传统云原生主要面对单一Region场景进行应用管理，对于应用迁移的需求较弱，应用管理能力的短缺并不是很突显。 而面对跨云的应用伸缩场景，传统云原生的应用数据克隆、迁移都需要运维人员手动执行，效率低，工作量大。	**应用一键迁移** 华为云UCS支持跨云场景的应用数据同步复制能力，可以实现在分布式基础设施上的弹性扩容，支撑应用容灾、扩容、迁移，大幅减少运维人员的工作复杂程度，提高生产效率。
流量治理能力	传统云原生的流量与业务分离，非按需分配，部分用户存在跨地域、跨运营商访问的情况，时延较高。	**统一流量治理** 以多云化为前提，华为云UCS支持将用户接入流量就近分发至最合适的后端集群，缩短访问延时，同时支持流量基于访问者的网段、地域、运营商等不同策略进行分发。
高效性	传统云原生在多云场景下的应用部署十分繁琐，需要在每个集群中进行手动部署，效率很低。	**服务开箱即用** 华为云UCS提供服务实例的边云协同一键分发功能，您无需在不同区域的每个集群中进行分别部署，大量减少重复工作量，提升工作效率。
运维能力	由于业务部署分散，往往中心Region、IDC、边缘节点等各个区域的资源需要单独进行监控，对于运维来说都要付出比较大的人力和精力。	**立体化监控运维** 华为云UCS支持立体化的监控运维，支持开源Prometheus和OpenTelemetry生态，可以统一监控所有区域的集群资源，大幅提升运维效率。

4 应用场景

4.1 电商直播场景

应用场景

电商直播客户在特定的直播时间段，或在促销、限时秒杀等活动期间，会遇到用户访问量激增的情况，导致服务器资源紧缺，业务时延增大。

为应对业务高峰期的流量冲击，UCS提供了智能的分布式流量治理和算力调度管理能力，灵活分配业务流量和边云资源，有效提升业务稳定性和用户体验。

优势

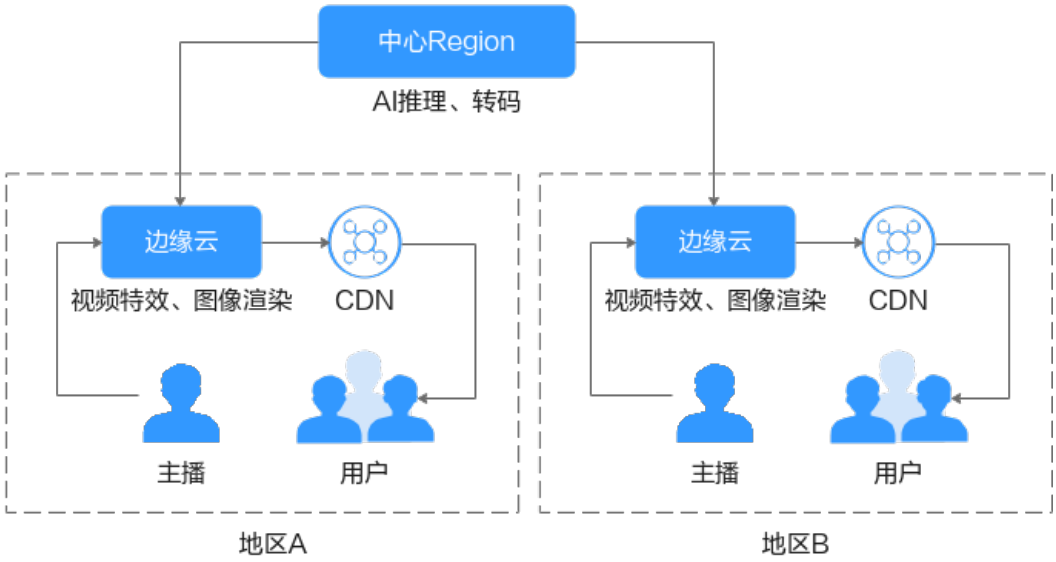
- **用户就近接入**

  根据用户所属区域，实现智能路由、就近接入，减少业务端到端时延。
- **统一算力供给**

  跨地域算力协同，根据直播人数和应用需要，灵活调度边端、云端资源，提升资源利用率。

建议方案

图 4-1 电商直播场景方案



4.2 金融行业场景

应用场景

对于金融行业用户，新兴互联网业务的快速发展和业务数据的高敏感性是一对既有的矛盾，而现有的混合云架构是解决这一矛盾的较优解决方案。而在实际落地场景中，这样的结构依旧存在一些痛点亟待解决。

- 痛点一：业务部署分散，无法极速扩容和大规模治理，难以有效应对高峰期的流量冲击。
- 痛点二：云端生态不统一，业务实例分发困难，缺少丰富的金融云原生SaaS。
- 痛点三：流量治理层面难以满足数据敏感业务和时延敏感业务的高性能要求。
- 痛点四：智能终端的快速发展带来运营监管的难度，无法集中管理海量终端，实施有效的监管和运营。
- 痛点五：缺少跨中心的业务监控与治理能力，业务实例无法实现跨云迁移。

优势

UCS提供了跨云跨数据中心的大规模治理能力，统一接管自建IDC、边缘云、中心云资源，一站式分发调度，助力加速金融行业的业务创新。

- **算力统一供给**

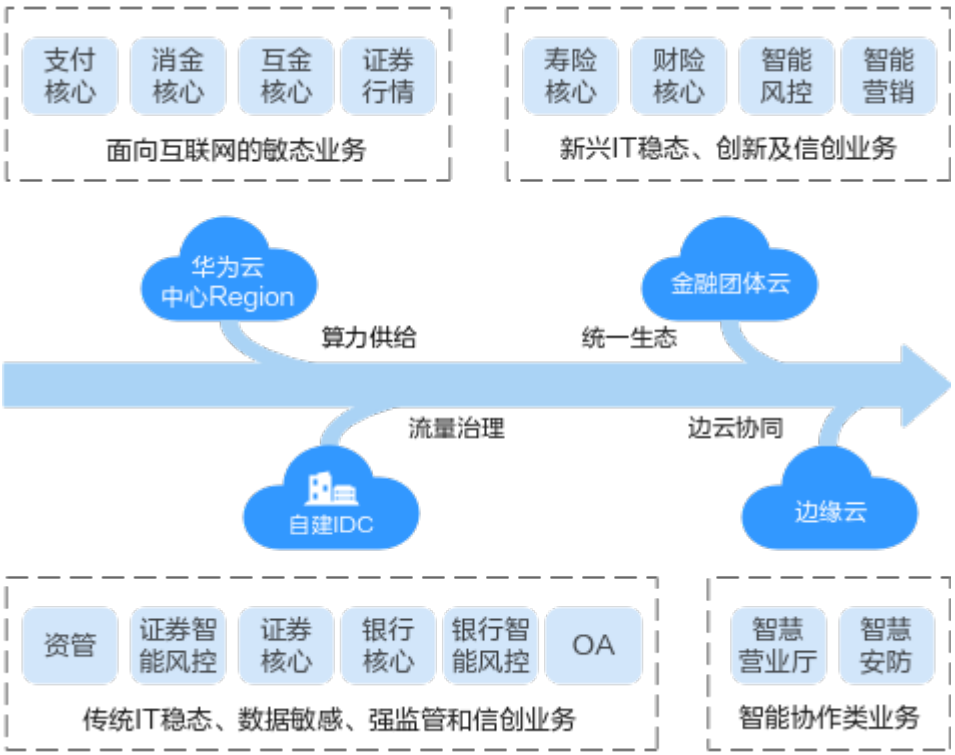
  面对金融行业新兴的互联网类业务，UCS支持极速扩容和大规模治理，提供实现本地、边缘、云资源统一调度，有效应对流量冲击。
- **统一生态建设**

  UCS构建了标准的金融应用生态，可以实现应用的跨地域跨云的统一分发和部署，支持业务实例跨云迁移。

- **云边统一协同**
  实现海量终端及边缘侧设备、应用的协同管理，加速金融行业智能安防、智慧网点的建设。
- **多云统一协同**
  构建多地多中心的金融数字化业务架构，实现跨云跨数据中心的统一治理。

建议方案

图 4-2 金融行业场景方案



4.3 汽车行业场景

应用场景

随着车联网等新业务场景的出现，汽车的数字化营销、智慧生产、智慧门店等新兴场景不断涌现，传统汽车行业的数字化转型成为产业发展趋势，但是与此同时也面临着多种挑战。

- 挑战一：传统稳态业务资源利用率不高，基础资源无法有效整合。
- 挑战二：弹性能力不足，无法满足大量在线用户并发接入，网络时延较高。
- 挑战三：涉及业务种类繁多，集群部署分散，运维管理困难。

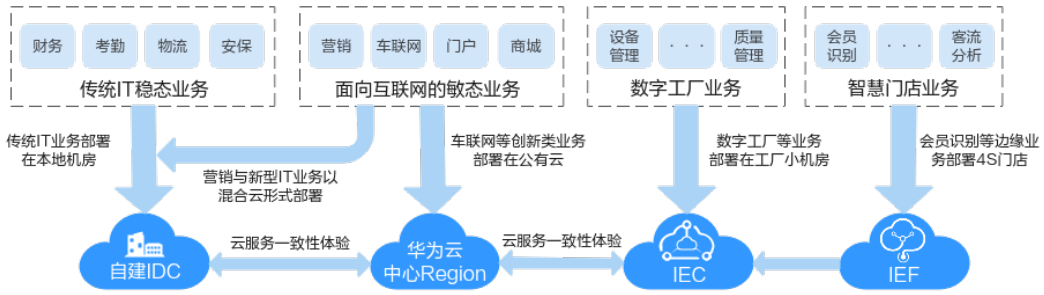
优势

UCS平台将边缘云、IDC、华为云资源有机整合，实现算力、流量、数据统一管理，加速汽车行业的数字化转型。

- **算力统一供给**
  打造敏态稳态业务共平台，整合所有基础资源，有效提升共享率和资源利用率。
- **流量统一治理**
  适配车联网、互联网创新的业务场景，实现根据业务特点灵活接入，降低用户使用时延。
- **统一管理平台**
  提供统一全网分布式应用的运维、运营入口，提升运营运维效率。

建议方案

图 4-3 汽车行业场景方案



5 计费说明

计费模式

华为云UCS提供包年/包月、按需计费两种计费模式，以满足不同场景下的用户需求。

- 包年/包月是一种预付费模式，即先付费再使用，按照订单的购买周期进行结算，因此在购买之前，您必须确保账户余额充足。
- 按需计费是一种后付费模式，即先使用再付费，按照实际使用时长计费。

在购买集群或集群内资源后，如果发现当前计费模式无法满足业务需求，您还可以变更计费模式。

计费项

华为云UCS的计费项由UCS管理服务费用组成，根据集群vCPU的数量按小时计费，如需查看每个用户集群的vCPU容量（计入UCS费用的部分），可运行以下命令：

kubectl get nodes -o jsonpath='{range .items[*]}{.metadata.name}{"\t"} {.status.conditions[?(@.type=="Ready")].status}{"\t"} {.status.capacity.cpu} {"\n"}' | grep True

6 安全

6.1 责任共担

华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图6-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 6-1 华为云安全责任共担模型

云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图6-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS服务）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好自身控制的中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

6.2 身份认证与访问

UCS支持IAM与Kubernetes的角色访问控制（RBAC）的精细的权限管理，实现UCS服务资源权限、集群中Kubernetes资源权限两种维度的权限控制，这两种权限针对的是不同类型的资源，在授权机制上也存在一些差异，具体如下：

- **UCS服务资源权限**：是基于IAM系统策略的授权。UCS服务资源包括容器舰队、集群、联邦实例等等，管理员可以针对用户的角色（如开发、运维）进行差异化授权，精细控制他们对UCS资源的使用范围。
- **集群中Kubernetes资源权限**：是基于Kubernetes RBAC能力的授权，可授予针对集群内Kubernetes资源对象的细化权限，通过权限设置可以让不同的用户有操作

不同Kubernetes资源对象的权限（如工作负载、任务、服务等Kubernetes原生资源）。

更多权限管理介绍，详见**权限管理章节**。

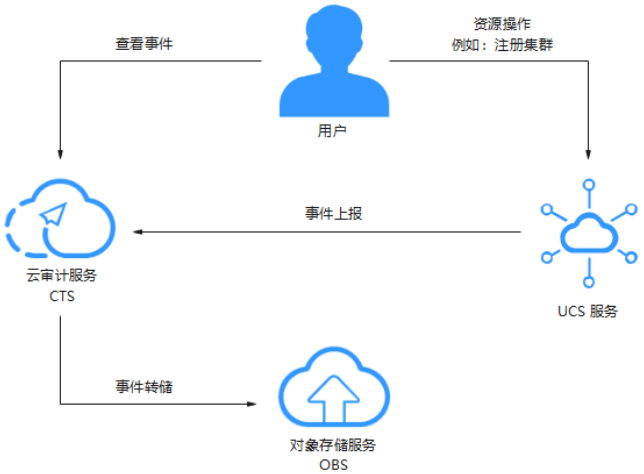
6.3 审计与日志

审计

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

图 6-2 云审计服务



日志

Kubernetes日志可以协助您排查和诊断问题。本节介绍UCS如何通过多种方式进行Kubernetes日志管理。

- 您可以方便地使用云原生日志采集插件采集应用日志并上报LTS，从而更好地利用LTS日志服务提供给您的各种日志统计分析等功能。具体操作，请参见**收集数据面日志**。
- 支持收集集群控制平面组件日志和Kubernetes审计日志，将日志从master节点采集到您账号的LTS日志服务的日志流中。具体操作，请参见**收集控制面组件日志**和**收集Kubernetes审计日志**。
- 支持收集集群Kubernetes事件，将Kubernetes事件从集群内采集到您账号的LTS日志服务的日志流中，以便对Kubernetes事件进行持久化存储和统计分析。具体操作，请参见**收集Kubernetes事件**。

关于UCS日志记录的详细介绍和配置方法，请参见**日志中心章节**。

6.4 监控风险安全

容器洞察提供基于Kubernetes原生类型的容器监控能力，全面监控集群的健康状态和负荷程度。

- 支持集群、节点、工作负载的资源全景。
- 支持节点的资源占用、工作负载的资源消耗。
- 展示近一小时的CPU/内存指标。

关于UCS监控风险安全的详细介绍，请参见**容器洞察章节**。

6.5 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 6-3 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 6-4 资源中心

网络安全专用产品安全检测证书&软件著作权证书

另外，华为云安全服务提供了网络安全专用产品安全检测证书、软件著作权等证书，供用户下载和参考。具体请查看**合规资质证书**。

图 6-5 网络安全专用产品安全检测证书&软件著作权证书

7 权限管理

如果您需要对购买的UCS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制资源的访问。

通过IAM，您可以在账号中给员工创建IAM用户，并授权控制他们对资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有UCS集群资源的使用权限，但是不希望他们拥有注销集群等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用集群，但是不允许注销集群的权限策略，控制他们对UCS资源的使用范围。

UCS 权限类型

UCS权限管理是在IAM与Kubernetes的角色访问控制（RBAC）的能力基础上，打造的细粒度权限管理功能。支持UCS服务资源权限、集群中Kubernetes资源权限两种维度的权限控制，这两种权限针对的是不同类型的资源，在授权机制上也存在一些差异，具体如下：

- **UCS服务资源权限**：是基于IAM系统策略的授权。UCS服务资源包括容器舰队、集群、联邦实例等等，管理员可以针对用户的角色（如开发、运维）进行差异化授权，精细控制他们对UCS资源的使用范围。
- **集群中Kubernetes资源权限**：是基于Kubernetes RBAC能力的授权，可授予针对集群内Kubernetes资源对象的细化权限，通过权限设置可以让不同的用户有操作不同Kubernetes资源对象的权限（如工作负载、任务、服务等Kubernetes原生资源）。

如果您的团队主要使用UCS服务资源，那么IAM系统策略能够满足您的诉求；如果还需要集群内各个Kubernetes资源对象的细化权限，则必须结合Kubernetes RBAC一起使用。

UCS 服务资源权限（IAM 授权）

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

UCS部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问UCS时，不需要切换区域。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各云服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对UCS服务，管理员能够控制IAM用户仅能对某一类舰队和集群资源进行指定的管理操作。

表7-1包括了UCS的所有系统权限。

表 7-1 UCS 系统权限

系统角色/策略名称	描述	类别
UCS FullAccess	UCS服务管理员权限，拥有该权限的用户拥有服务的所有权限（包含制定权限策略、安全策略等）。	系统策略
UCS CommonOperations	UCS服务基本操作权限，拥有该权限的用户可以执行创建工作负载、流量分发等操作。	系统策略
UCS CIAOperations	UCS服务容器智能分析管理员权限。	系统策略
UCS ReadOnlyAccess	UCS服务只读权限（除容器智能分析只读权限）。	系统策略

华为云各服务之间存在业务交互关系，UCS也依赖其他云服务实现一些功能（如镜像仓库、域名解析），因此，上述四种系统策略经常和其他云服务的角色或策略结合使用，以达到精细化授权的目的。管理员在为IAM用户授权时，应该遵循权限最小化的安全实践原则，表7-2列举了UCS各功能管理员、操作、只读权限所需要的最小权限。

表 7-2 UCS 功能所需的最小权限

功能	权限类型	权限范围	最小权限
容器舰队	管理员权限	• 创建、删除舰队 • 注册华为云集群（CCE Standard集群、CCE Turbo集群）、本地集群或附着集群 • 注销集群 • 将集群加入、移出舰队 • 为集群或舰队添加权限 • 开通集群联邦、联邦管理相关操作（如创建联邦工作负载、创建域名访问等）	UCS FullAccess
	只读权限	查询集群、舰队的列表或详情	UCS ReadOnlyAccess
华为云集群	管理员权限	对华为云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的读写权限。	UCS FullAccess + CCE Administrator
	操作权限	对华为云集群及集群下大多数Kubernetes资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限。	UCS CommonOperations + CCE Administrator
	只读权限	对华为云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的只读权限。	UCS ReadOnlyAccess + CCE Administrator
本地/附着/伙伴云集群	管理员权限	本地/附着/伙伴云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的读写权限。	UCS FullAccess
	操作权限	本地/附着/伙伴云集群及集群下大多数Kubernetes资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限。	UCS CommonOperations + UCS RBAC权限（需要包含namespaces资源对象的list权限）
	只读权限	本地/附着/伙伴云集群及集群下所有Kubernetes资源对象（包含节点、工作负载、任务、服务等）的只读权限。	UCS ReadOnlyAccess + UCS RBAC权限（需要包含namespaces资源对象的list权限）
镜像仓库	管理员权限	容器镜像服务的所有权限，包括创建组织、上传镜像、查看镜像列表或详情、下载镜像等操作。	SWR Administrator

功能	权限类型	权限范围	最小权限
权限管理	管理员权限	● 创建、删除权限 ● 查看权限列表或详情 **说明** 创建权限需要同时授予子用户IAM ReadOnlyAccess权限（IAM服务的只读权限），用于获取IAM用户列表。	UCS FullAccess + IAM ReadOnlyAccess
	只读权限	查看权限列表或详情	UCS ReadOnlyAccess + IAM ReadOnlyAccess
策略中心	管理员权限	● 启用策略中心 ● 创建、停用策略实例 ● 查看策略列表 ● 查看策略实施详情	UCS FullAccess
	只读权限	对于已启用策略中心的舰队和集群，拥有该权限的用户可以查看策略列表和查看策略实施详情。	UCS CommonOperations 或 UCS ReadOnlyAccess
服务网格	管理员权限	应用服务网格的所有权限，包括创建网格、添加集群、sidecar注入、查看网格列表或详情、卸载网格等。	UCS FullAccess + CCE Administrator
流量分发	管理员权限	创建流量策略、暂停调度策略、删除调度策略等操作。	（推荐）UCS CommonOperations + DNS Administrator 或 UCS FullAccess + DNS Administrator
	只读权限	查看流量策略列表或详情	UCS ReadOnlyAccess + DNS Administrator
容器智能分析	管理员权限	● 接入、取消接入集群 ● 查看基础设施、应用负载等多维度监控数据	UCS CIAOperations
云原生服务中心	管理员权限	云原生服务中心的所有权限，包括订阅服务、查看服务列表或详情、创建服务实例、查看实例列表或详情、删除服务实例、退订服务等操作。	UCS FullAccess
	只读权限	云原生服务中心的只读权限，包括查看服务列表或详情、查看实例列表或详情等操作。	UCS ReadOnlyAccess

集群中 Kubernetes 资源权限（Kubernetes RBAC 授权）

集群中Kubernetes资源权限是基于Kubernetes RBAC能力的授权，管理员可授予用户针对集群内特定Kubernetes资源对象的细化权限。这些资源包括集群级资源和命名空间级资源，细化的操作权限包括get、list、watch、create、update、patch，以及delete，权限最终作用在舰队或未加入舰队的集群的命名空间上。操作权限的说明如下：

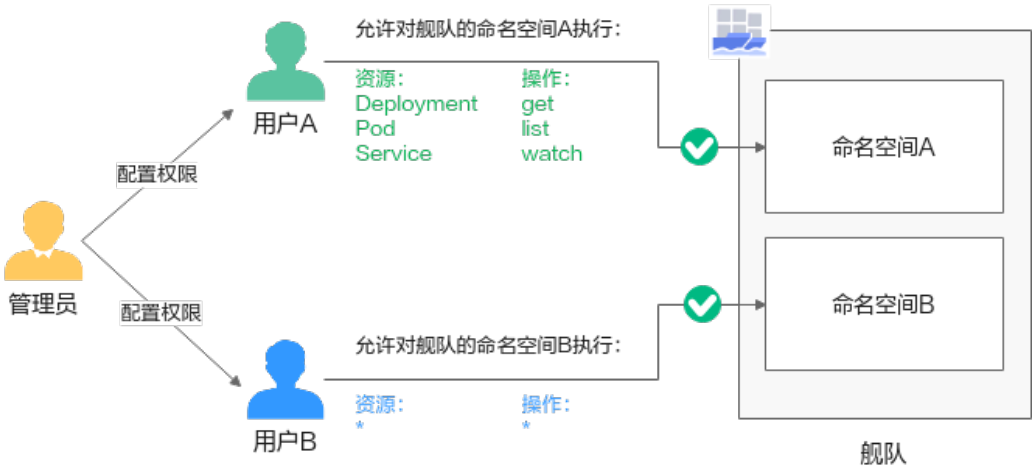
- get：按名称检索特定的资源对象。
- list：检索命名空间中特定类型的所有资源对象。
- watch：响应资源变化。
- create：创建资源。
- update：更新资源。
- patch：局部更新资源。
- delete：删除资源。

说明

关于集群级资源、命名空间级资源的解释，请参考**Kubernetes资源对象**。

例如，按照**图7-1**所示的方案配置权限后，用户A仅能对舰队的命名空间A中的Deployment、Pod、Service执行get、list、watch（只读操作）权限，而用户B可以对舰队的命名空间B中的全部资源执行全部操作。

图 7-1 Kubernetes 资源授权示意图



在UCS控制台中设置了五种权限类型：管理员权限、运维权限、开发权限、只读权限以及自定义权限，您可以直接使用这些权限类型为用户授权。当然，如果现有权限类型无法满足您的需求，也可以自定义权限，只需要指定操作类型和资源对象即可。

表 7-3 权限类型说明

权限类型	说明
管理员权限	对所有Kubernetes资源对象的读写权限

权限类型	说明
开发权限	对大多数Kubernetes资源对象的读写权限，对命名空间、资源配额等Kubernetes资源对象的只读权限
只读权限	对所有Kubernetes资源对象的只读权限

8 约束与限制

本小节主要为您介绍华为云UCS使用过程中的一些限制。

Kubernetes 版本约束

接入UCS服务的Kubernetes集群版本必须在1.19至1.32之间。

区域限制

集群通过私网接入UCS时，需要通过云专线（DC）或虚拟专用网络（VPN）服务将云下网络与云上虚拟私有云（VPC）连通，并利用VPC终端节点（VPCEP）通过内网与UCS服务建立连接。

该场景下，创建DC、VPN、VPC及VPCEP时仅支持选择“华北-北京四”区域。如不涉及集群私网接入场景，UCS无区域使用限制。

配额限制

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。UCS具有集群、舰队、权限、集群联邦，以及容器智能分析实例配额限制，如表8-1所示。若UCS提供的默认配额无法满足使用需要，您可以提交工单申请扩大配额。

- 集群配额：UCS支持接入的集群数量上限，华为云集群、本地集群、附着集群和伙伴云集群的数量均占用该配额值。
- 舰队配额：用户拥有的舰队数量上限。
- 权限配额：用户可以在“权限管理”页面创建的权限数量上限。
- 集群联邦配额：用户可以开通的集群联邦数量上限。不可申请扩大配额。
- 容器智能分析实例配额：用户可以创建的容器智能分析实例数量上限。不可申请扩大配额。

表 8-1 UCS 配额项

配额项	默认配额值
集群	50
舰队	50

配额项	默认配额值
权限	50
集群联邦	1
容器智能分析实例	1

用户在使用UCS时也会使用其他云服务，例如弹性云服务器、云硬盘、虚拟私有云、弹性负载均衡、容器镜像服务、云解析服务等。其他云服务配额与UCS配额相互独立，由各服务自行管理，详情请参见**关于配额**。

9 与其他云服务的关系

华为云UCS为用户提供一个统一的集群服务管理平台，与周边服务的依赖关系如图9-1所示。

图 9-1 UCS 与其他服务关系

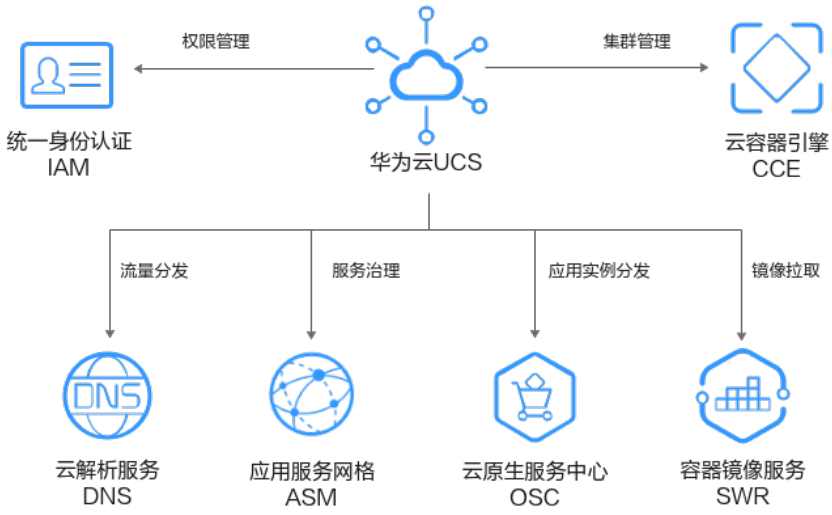


表 9-1 UCS 与其他服务的关系

服务名称	UCS与其他服务的关系	主要交互功能
云容器引擎 CCE	UCS支持接管云容器引擎中的CCE Standard集群、CCE Turbo集群，为集群提供应用分发、流量管理、集群监控、应用数据管理等多种功能。	注册华为云集群
统一身份认证 IAM	UCS在统一身份认证服务（IAM）能力基础上，为您提供细粒度的权限管理功能。	权限管理
云解析服务 DNS	UCS对接云解析服务，获取解析域名，提供大规模流量治理能力，实现流量的灵活接入。	流量分发

服务名称	UCS与其他服务的关系	主要交互功能
应用服务网格 ASM	UCS对接应用服务网格，为您的服务以无侵入的方式提供灵活的服务治理能力。	服务网格
云原生服务中心 OSC	UCS通过云原生服务中心构建统一的应用生态，支持云原生应用统一分发部署。	云原生服务中心
容器镜像服务 SWR	UCS集成容器镜像服务能力，可以通过容器镜像在UCS所管理的集群中创建工作负载。	镜像仓库