云运维中心

产品介绍

文档版本 2.0

发布日期 2024-06-06

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

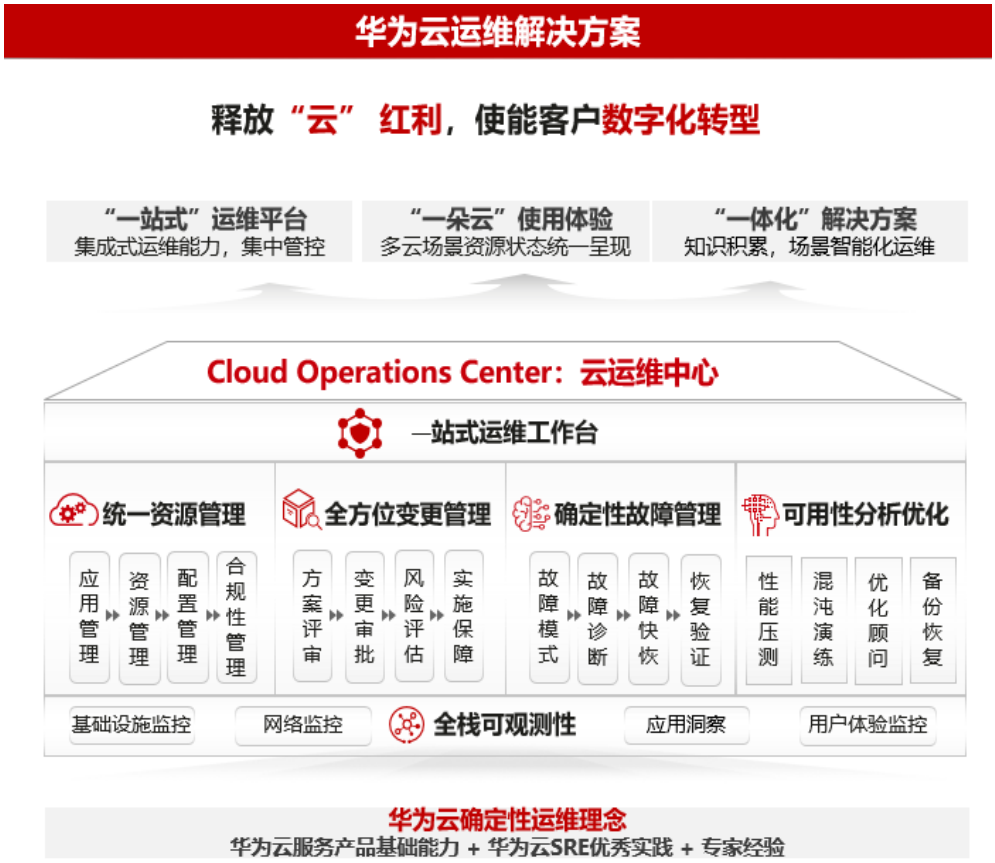
网址： https://www.huaweicloud.com/

目 录

1 什么是云运维中心

云运维中心（Cloud Operations Center，简称COC）为用户提供安全、高效的一站式智能运维平台，满足客户集中运维诉求。承载华为云确定性运维业务场景，提供变更管理、批量运维等核心特性，实现在安全合规的前提下，提升用户运维能力成熟度和云上运维效率。

图 1-1 COC 产品介绍



统一资源管理

- 应用管理：提供应用和资源关联关系建模能力，满足用户云上资源的集中式管理要求，降低管理成本。

- 资源管理：同步并纳管用户在云平台上使用的资源实例，构筑资源运维能力底座。
- 配置管理：提供应用和资源视角的管理能力，以及参数配置集中式看护、全生命周期管理的能力。
- 合规性管理：资源运维提供批量的补丁扫描修复能力，安全合规先行，兼顾高效。

全方位变更管理

- 方案评审：支持变更方案标准化（Standard Operating Procedure，简称SOP），将变更方案明确并电子化，经评审后归档。支持规则和流程解耦，保证变更执行过程不走样，同时将变更方案沉淀。
- 变更审批：按照预设审批流程审批变更单，保障变更方案可靠性、时间合理性、流程合规性。
- 风险评估：基于场景规则、流程规则、业务规则对变更进行管控，提前识别和拦截变更风险；通过变更日历实现变更冲突检测，降低服务间变更依赖导致的变更风险。
- 实施保障：按预定方案执行变更，变更步骤标准化、可观测，变更异常及时介入处理，实现变更实施全过程可控、可视、可管。

确定性故障管理

- 统一事件中心：提供事件发现、事件处理、恢复验证及持续改进的全流程标准化机制。
- 承载Warroom和故障回溯能力：现网事件智能启动Warroom，缩短故障处理非必要耗时，指挥中心实时观测故障处理进展。故障回溯实现问题总结和经验沉淀，客户问题不重犯，缩短故障恢复MTTR。
- 支持响应预案：支持客户对已知故障制定响应预案，通过预案自动化帮助客户处理确定性问题，实现已知问题快速恢复。
- 故障模式：融合专业风险分析方法和专家知识库，积累故障模式库，帮助客户分析云应用存在的潜在风险、传承运维经验。

韧性中心优化

- 全生命周期风险管理：覆盖部署态和运行态两部分的风险治理，贯穿应用和资源全生命周期，将华为云多年沉淀的动态清零风险管理经验使能用户。
- 使能主动运维：通过性能压测、应急演练/混沌工程、韧性评估等主动运维手段提升客户关键业务的质量和韧性。
- 丰富的故障演练武器：沉淀华为云实践经验，内置50个+演练攻击武器，赋能客户模拟复杂多样的业务受损场景并制定应对策略。
- 提升应用高可用能力：PRR（Production Readiness Review 生产就绪程度评审），承载华为云SRE对云应用上线评审的最佳实践，提供在线评审电子流和评审项，提升应用高可用能力。

访问方式

云服务平台提供了Web化的服务管理平台，即管理控制台和基于HTTPS请求的API（Application Programming Interface）管理方式。

- API方式

  如果用户需要将云服务平台上的云运维中心集成到第三方系统，用于二次开发，请使用API方式访问云运维中心，具体操作请参见**《云运维中心API参考》**。

- 控制台方式

  其他相关操作，请使用管理控制台方式访问云运维中心。

  如果用户已注册，可直接登录管理控制台，从主页选择“云运维中心”。如果未注册，请参见**注册华为账号并开通华为云**。

2 产品优势

一站式运维平台

- 提供集成式运维能力，支持集中管控和运维。
- ITSM、ITOM、专家服务相互协同，形成合力。
- 无需多平台间跳转，站内闭环，夯实一站式体验。

一体化解决方案

- 化零为整，原子化运维能力实现有机融合。
- 沉淀华为云运维专家经验，提供场景化运维解决方案。
- 安全生产、运维大脑、故障管理等优秀实践使能客户极简运维。

一朵云使用体验

- 构筑全场景资源管理驾驶舱，覆盖华为公有云、客户IDC等场景。
- 提供多视角数据呈现能力，挖掘数据价值，辅助整体运维决策。
- 云上运维能力延伸至客户IDC，淡化云边界，提升运维效率。

3 应用场景

运维态势感知 BI

面向不同角色运维人员的专属运维BI看板，辅助运维优化改进和洞察决策。

指标项丰富：预置接入30个+运维指标，构建7张运维态势感知大屏，从宏观到微观全面呈现运维全局态势，提供企业级运维沙盘。

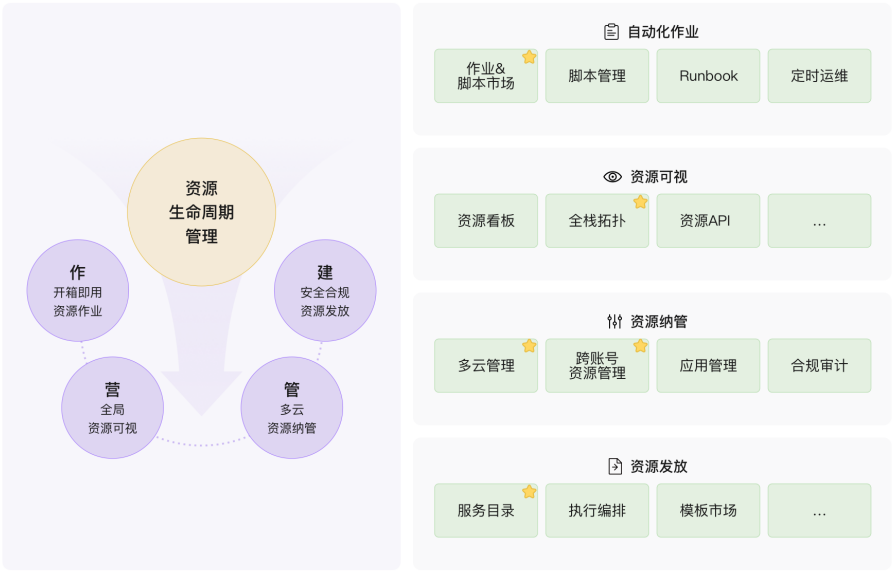
图 3-1 运维沙盘

资源全生命周期管理

提供资源定义、申请、发放、运维、变配&续期、回收等全生命周期管理，构筑统一资源管理驾驶舱。

- 全生命周期管理：打通用户资源管理全旅程断点，提升用户资源管理流畅度和运维效率。
- 资源管理驾驶舱：从全局视角实现用户资源可视化管理，支持多云和跨账号集中运维能力。

图 3-2 资源全生命周期管理

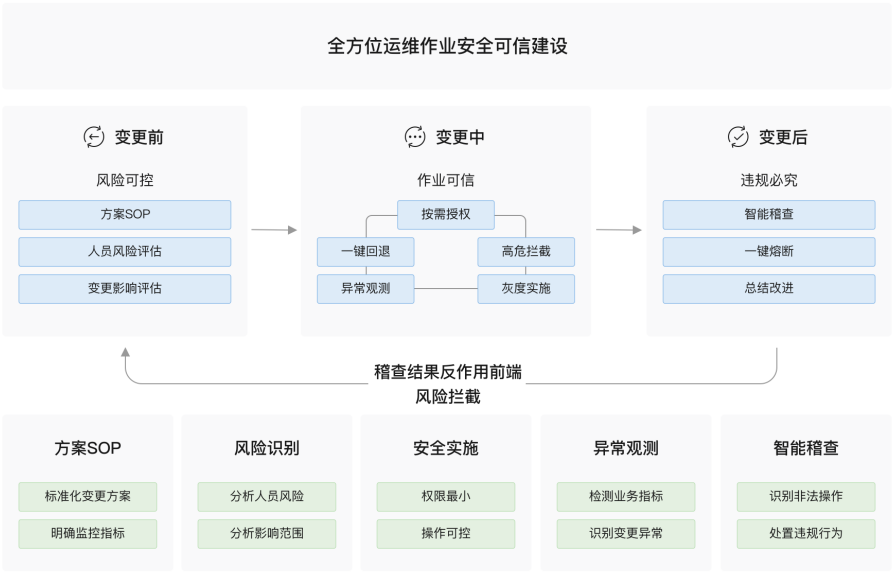


变更风控&作业可信

融合华为SRE安全生产最佳实践的管控模型，助力客户作业可信和稳定可靠。

- 全方位作业可信：构筑人员风险评估、高危命令拦截和自动化稽查能力，从事前、事中、事后逐层拦截变更风险，实现全方位运维作业可信。
- AI加持风险评估：通过高危命令智能拦截算法，AI加持消减作业风险。

图 3-3 变更风控&作业可信

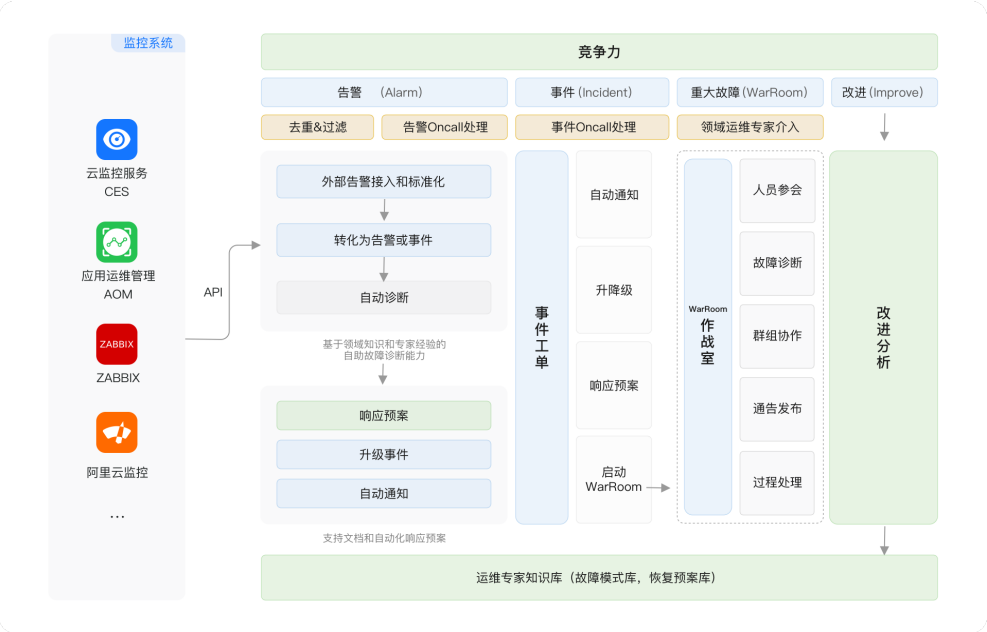


标准化故障管理

标准化故障管理流程，加持WarRoom驾驶舱，实现故障高效协同和快速恢复。

- 标准化流程：华为云标准故障处理流程服务化，通过WarRoom实现运维、研发等多兵种协同作战，响应预案提升故障处理效率。
- 运维知识库：基于历史故障和专家经验构筑运维知识库，实现已知故障快速恢复，未知故障沉淀经验。

图 3-4 标准化故障管理

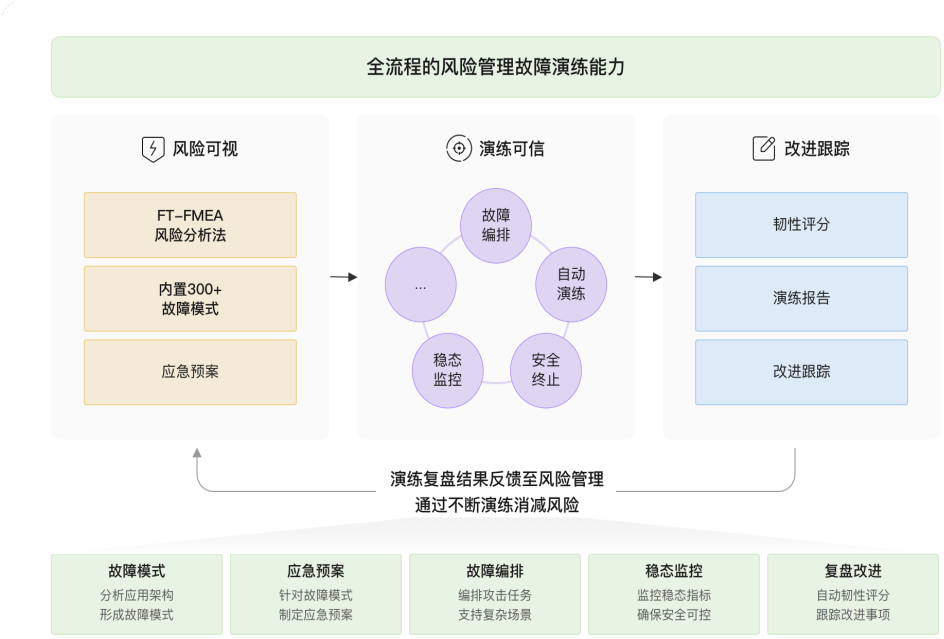


智能化混沌演练

全旅程混沌工程解决方案，快速评估应用潜在韧性风险，持续看护应用架构。

- 端到端混沌工程方案：从客户实际业务场景出发，按照风险分析、应急预案、演练执行、演练复盘4个维度，提供端到端混沌演练能力。
- 故障模式库：首创基于容错视角的故障场景分析方法，沉淀华为云SRE多年的故障模式库，用户开箱即用。

图 3-5 智能化混沌演练



4 产品功能

云运维中心COC提供的常用功能特性参见**表1 云运维中心COC功能概览**

表 4-1 云运维中心 COC 功能概览

功能名称	功能描述	发布区域
总览	COC全局总览页面，包含资源总览、资源监控、应用监控、安全概览、快捷入口等多个板块。用户可以在总览页面便捷查看、处理工作项，降低运维复杂度，改善运维体验。	Global
资源管理	COC提供以资源为基础的资源管理视图。面向各类资源提供纳管能力，可建立资源拓扑；按照资源类型汇聚，支持按照标签查询资源列表，并提供UniAgent安装能力。	Global
应用管理	COC提供以应用为中心的资源管理视图。提供应用和资源关联关系的建模能力。按照“应用 > 区域 > 分组 > 资源模型”进行管理，支持按照标签查询资源列表，并提供UniAgent安装能力。	Global
补丁管理	补丁管理提供了用户能够管理ECS实例上补丁的能力。通过补丁管理能力，用户能够实现OS补丁合规性扫描，OS补丁合规性修复功能。	Global
批量ECS操作	批量ECS操作为用户提供了管理ECS实例的能力，支持进行批量开机、关机、重启、切换操作系统、重装操作系统等操作。	Global
批量RDS操作	批量RDS操作为用户提供了管理RDS实例的能力，支持进行批量开启、停止、重启等操作。	Global
批量FlexusL操作	批量FlexusL操作为用户提供了管理云耀云服务器L实例的能力，支持进行批量开机、关机、重启、重装操作系统等操作。	Global
脚本管理	提供用户自定义脚本的创建、修改、删除以及在目标虚拟机上执行自定义脚本、公共脚本的能力。通过该功能，用户可以通过自定义脚本或公共脚本在目标实例（目前支持ECS）上执行操作。	Global
作业管理	提供用户自定义作业的创建、修改、删除以及在目标虚拟机上执行自定义作业的能力。通过该功能，用户可以通过自定义作业在目标实例（目前支持ECS）上执行操作。	Global

功能名称	功能描述	发布区域
定时运维	提供用户从脚本、作业等已有能力选择任务并且创建定时任务的能力。支持单次执行和周期执行两种执行方案，周期性包括Cron表达式和简单周期执行。	Global
参数中心	支持Region级参数全生命周期管理，持续看护参数正确性和一致性。支持作业编排等运维场景快速引用。	Global
事件中心	COC事件管理系统，可在事件大盘概览全部事件。提供手动处理事件和关联作业执行两种方式。支持手动事件升降级、转发责任人、查看处理记录、一键启动Warroom等能力。	Global
集成告警	COC集成告警中心，支持将原始告警通过流转规则清洗后，在COC中创建新的集成告警。告警分配到排班或个人，明确告警责任人。支持手动清除、转事件单、自动化处理等操作。	Global
WarRoom	提供人工以及自动两种拉起Warroom方式，基于起会规则快速拉起Warroom群组。提供Warroom作战平台、关键监控数据看板集成、关键变更操作集成、故障恢复操作平台。支持内外部Warroom联动，协助客户进行问题解决。	Global
流转规则	流转规则将所有接收的集成原始告警进行抑制、降噪、去重、路由分派操作，支持多监控源纵向抑制、横向收敛，进行多维降噪；支持每个流转规则配置事件时默认分配对象和通知策略，而实现更准确的通知。	Global
集成管理	集成配置支持简单、快速集成现有或第三方等监控系统；将业务下所有分散的监控系统告警进行统一收口及管理。不同的监控系统通过各自独立的集成接入密钥实现对接集成。	Global
变更管理	变更中心主要承载变更流程管理业务，以变更工单模式，从变更的申请、审批、执行三个大环节管控变更业务，为变更人员、变更管理人员提供统一管理平台。	Global
混沌演练	用户可配置演练模板、攻击模板，基于模板对物理机、虚拟机或CCE容器进行故障演练。支持故障模式管理功能。	Global
待办中心	待办任务大盘，可以查看待办任务处理情况、历史待办任务统计，以及全量待办任务概览。支持用户手动创建待办任务。	Global
执行记录	在执行记录中，可查询补丁、脚本、作业、ECS操作等任务的工单记录，支持查看工单详情。	Global
人员管理	人员管理为云运维中心提供了统一的人员数据管理。您可以在人员管理页面管理当前租户下的用户，人员管理中的用户从统一身份认证（IAM）同步，人员管理页面的数据作为云运维中心的用户基础数据，供创建待办、定时运维、通知管理、事件中心等多个基础功能模块使用。	Global
排班管理	排班管理为云运维中心提供了统一的、多维度、多形式、可自定义的人员管理模式。您可以在排班管理页面创建排班场景、排班角色，并将“人员管理”中的人员添加到“排班场景”、“排班角色”中完成排班的设置。	Global
通知管理	通知管理为用户创建通知实例，通知实例包含通知场景及匹配规则条件等，当出现一个事件单时，通知模块会启动场景匹配和规则匹配，解析出需要通知的人员、内容和发送通知的渠道，进行发送通知信息，实现了自动通知的功能。	Global
移动应用管理	用户可绑定或修改移动应用（当前仅支持企业微信）。	Global

功能名称	功能描述	发布区域
SLA管理	SLA为客户提供了工单时效管理，当工单触发某一个规则时，及时通知客户跟进和处理，并记录工单SLA触发详情。SLA管理中，支持使用公共SLA规则或自定义规则，并可以配置SLA打破、预警通知。	Global
帐号管理	提供弹性云服务器资源主机帐号纳管/托管能力，支持对主机帐号进行定期改密。	Global

5 权限管理

如果您需要对华为云上购买的资源，为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，可以帮助您安全的控制华为云资源的访问。如果华为号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用COC服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

通过IAM，您可以通过授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有COC的使用权限，但是不希望他们拥有删除COC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进行权限分配，通过授予用户仅能使用COC，但是不允许删除COC的权限策略，控制开发人员对COC资源的使用范围。

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。由于华为云各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。这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ECS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。

目前IAM支持两类授权模型，一类是经典授权（RBAC）模型，称为角色授权。

默认情况下，新建的主体没有任何权限，需要为主体授予系统角色、系统策略或自定义策略，并选择授权范围，才能使主体获得相应的权限。

另一类是基于ABAC的新模型，称为策略授权。管理员可根据业务需求定制不同的访问控制策略，将策略附加主体或为主体授予该策略即可获得相应权限，能够做到更细粒度更灵活的权限控制。授权后，主体就可以基于已有权限对云服务进行操作。

两者有如下的区别和关系：

表 5-1 角色授权与策略授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色授权	用户-角色-权限	• 系统角色 • 系统策略 • 自定义策略	为主体授予角色或策略	每个用户可以根据被分配的角色相对快速地被授予相关权限，但灵活性较差，难以满足细粒度精确权限控制需求，更适用于对维护角色和授权关系工作量较小的中小企业用户。
策略授权	用户-策略	• 系统策略 • 自定义策略	• 为主体授予策略 • 策略附加至主体	新增资源时，对比角色授权需要维护所有相关角色，基于策略的授权模型仅需要维护较少的资源，可扩展性更强，更方便。但相对应的，整体模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于策略授权的场景中，管理员仅需要创建一个自定义策略，在策略中通过条件键“g:RequestedRegion”的配置即可达到策略对于授权区域的控制。将策略附加主体或为主体授予该策略即可获得相应权限，权限配置方式更细粒度更灵活。

COC目前仅支持角色授权模型，该场景下支持的系统权限请参考**角色授权系统权限**。

关于IAM的详细介绍，请参见**IAM产品介绍**。

角色授权系统权限

COC服务支持基于角色授权的授权模型。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。

COC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COC时，不需要切换区域。

如**表5-2**所示，包括了COC的所有系统权限。基于角色授权场景的系统策略与基于策略授权场景的并不互通。

表 5-2 COC 系统权限

系统角色/策略名称	描述	类别	依赖关系
COC ReadOnlyAccess	云运维中心服务只读权限	系统策略	无

系统角色/策略名称	描述	类别	依赖关系
COC FullAccess	云运维中心服务管理员权限	系统策略	无

表3 常用操作与系统权限的关系列出了COC常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 5-3 常用操作与系统权限的关系

操作	COC ReadOnlyAccess	COC FullAccess
查看待办任务	√	√
创建及处理待办任务	x	√
查看资源列表	√	√
资源纳管	x	√
查看脚本列表	√	√
增删改及执行脚本	x	√
查看作业列表	√	√
增删改及执行作业	x	√
执行ECS操作	x	√
查看定时运维任务	√	√
增删改及执行定时运维任务	x	√
查看参数中心	√	√
增删改参数	x	√
查看事件单	√	√
创建及处理事件	x	√
查看告警记录	√	√
处理告警	x	√
查看混沌演练规划	√	√
执行演练任务	x	√
查看排班	√	√
创建排班	x	√
查看帐号基线	√	√

操作	COC ReadOnlyAccess	COC FullAccess
创建帐号基线	x	√

策略授权系统权限

COC服务支持基于策略授权的授权模型。如表4 COC系统策略所示，包括了COC基于策略授权中的所有系统策略。策略授权的系统策略与角色授权的系统策略并不互通。

表 5-4 COC 系统策略

系统策略名称	描述	策略类别
COCReadOnlyPolicy	云运维中心服务只读权限。	系统策略
COCFullAccessPolicy	云运维中心服务管理员权限。	系统策略

表5 常用操作与系统策略的关系列出了COC常用操作与系统策略的授权关系，您可以参照该表选择合适的系统策略。

表 5-5 常用操作与系统策略的关系

操作	COCReadOnlyPolicy	COCFullAccessPolicy
查看待办任务	√	√
创建及处理待办任务	x	√
查看资源列表	√	√
资源纳管	x	√
查看脚本列表	√	√
增删改及执行脚本	x	√
查看作业列表	√	√
增删改及执行作业	x	√
执行ECS操作	x	√
查看定时运维任务	√	√
增删改及执行定时作业任务	x	√
查看参数中心	√	√
增删改参数	x	√
查看事件单	√	√

操作	COCReadOnlyPolicy	COCFullAccessPolicy
创建及处理事件	x	√
查看告警记录	√	√
处理告警	x	√
查看混沌演练规划	√	√
执行演练任务	x	√
查看排班	√	√
创建排班	x	√
查看帐号基线	√	√
创建帐号基线	x	√

相关链接

- **IAM产品介绍**
- **通过角色/资源管理资源访问权限**

6 约束与限制

说明

云运维中心COC为全局服务，但在部分特殊区域（专属区域、HCSO等）暂不支持，如您有相关需求，请联系COC侧沟通处理。

在使用云运维中心COC时，您需注意以下使用限制，详见表6-1。

表 6-1 云运维中心使用限制

功能模块	对象	使用限制
公共	补丁/脚本/作业/ECS操作	单个操作任务最多支持选择200台实例。
	补丁/脚本/作业/ECS操作	执行工单时，超时时间小于等于86400秒（即24小时）。
资源管理	安装UniAgent支持操作系统	目前支持的Linux操作系统版本有： • EulerOS 2.2 64bit for Tenant 20210227 • EulerOS 2.3 64bit • EulerOS 2.5 64bit for Tenant 20210229 • CentOS 7.2 64bit • CentOS 7.3 64bit • CentOS 7.4 64bit • CentOS 7.5 64bit • CentOS 7.6 64bit for Tenant 20200925(制作资源镜像使用) • CentOS 7.6 64bit for Tenant 20210227 • CentOS 7.6 64bit for Tenant 20210525
	UniAgent客户端	当CPU使用率大于10%或者内存大于200M时，UniAgent客户端将自动重启。

功能模块	对象	使用限制
	UniAgent安装	单次最多可安装100台UniAgent主机。
应用管理	应用	租户创建的应用层级≤5层。
补丁管理	补丁基线	租户创建的补丁基线个数≤50个（不计入公共基线）。
脚本管理	脚本内容	自定义脚本内容≤4096字节。
作业管理	全局参数	单个自定义作业的全局参数≤30个。
Warroom	起会规则	租户创建的Warroom起会规则个数≤50个。
流转规则	流转规则	租户创建的流转规则个数≤50个。
集成管理	数据记录	COC保存集成数据源的最近10次数据记录。
人员管理	人员数量	租户创建的人员个数≤50个。
排班管理	排班角色	单个排班场景下的排班角色≤10个。
帐号管理	资源类型	目前支持纳管的资源类型： 弹性云服务器 ECS 目前支持托管（帐号导入）的资源类型： 弹性云服务器 ECS、分布式缓存服务 DCS、云数据库 RDS、分布式消息服务 DMS
	帐号基线	基线帐号数量≤30个，关联的组件数量≤100个。

7 计费说明

COC于2024年7月31日在中国站、国际站转商，转商后COC本身的基础功能免费，若后续部分高阶产品能力开始收费，提前30天通知。

云运维中心与其他云服务组合使用，例如为您提供发送通知等增值服务，这些增值服务可能产生额外费用，具体以对应云服务的收费为准，由提供该功能的服务结算。

8 与其他云服务的关联

云运维中心COC服务与其他服务的关系，如图1所示。

图 8-1 与其他服务的关系

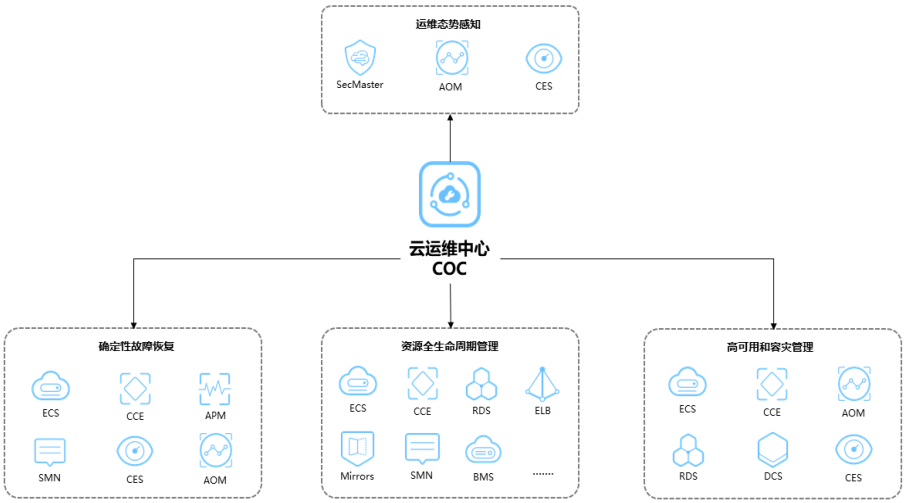


表 8-1 与其他服务的关系

服务名称	与其他服务的关系	主要交互功能
安全云脑	总览页面中提供用户查看到账号下的安全监控信息。从安全评分、安全监控、安全趋势三个维度呈现安全概览，并支持自定义看板。	查看安全概览
云监控	总览页面中支持资源监控总览，以及资源告警详情的查看。故障管理中，支持接入云监控服务产生的告警，并在云运维中心中进行流转处理。混沌演练中，支持在演练过程中查看云监控的指标数据。如需正常使用需先开通云监控服务。	资源监控 接入云监控告警 演练监控

服务名称	与其他服务的关系	主要交互功能
应用运维管理	总览页面中支持查看应用监控看板，在应用运维管理中已配置的仪表盘可以在云运维中心中进行展示。故障管理中，支持接入应用运维管理服务产生的告警，并在云运维中心中进行流转处理。混沌演练中，支持在演练过程中查看应用运维管理的指标数据。	应用监控 接入应用运维管理告警 演练监控
弹性云服务器	资源运维中，可以对弹性云服务器进行批量操作、脚本执行、作业执行、定时任务等运维操作。混沌演练中，支持对弹性云服务器进行演练任务执行。	资源运维 混沌演练
云容器引擎	混沌演练中，支持对云容器引擎进行演练任务执行。	混沌演练
应用性能管理	故障管理中，支持接入应用性能管理服务产生的告警，并在云运维中心中进行流转处理	接入应用性能管理告警
消息通知服务	云运维中心中的故障管理、资源运维等场景中，支持发送短信、邮件、语音、企业微信、钉钉等通知。如需使用需要先开通消息通知服务。	通知管理
云数据库	资源运维中，可以对云数据库进行批量操作。混沌演练中，支持对云数据库进行演练任务执行。	资源运维 混沌演练
裸金属服务器	资源运维中，可以对裸金属服务器进行批量操作、脚本执行、作业执行、定时任务等运维操作。	资源运维
对象存储服务	资源运维中，支持对弹性云服务器进行文件上传和分发，如需使用文件传输能力，需要在对象存储服务中购买存储桶。	执行公共脚本
数据加密服务	资源运维中，参数中心支持用户创建加密参数，需要在数据加密服务中购买密钥进行加密。帐号管理中，需要通过数据加密服务中的密钥保护帐号密码的安全。	加密参数 帐号管理

9 安全

9.1 责任共担

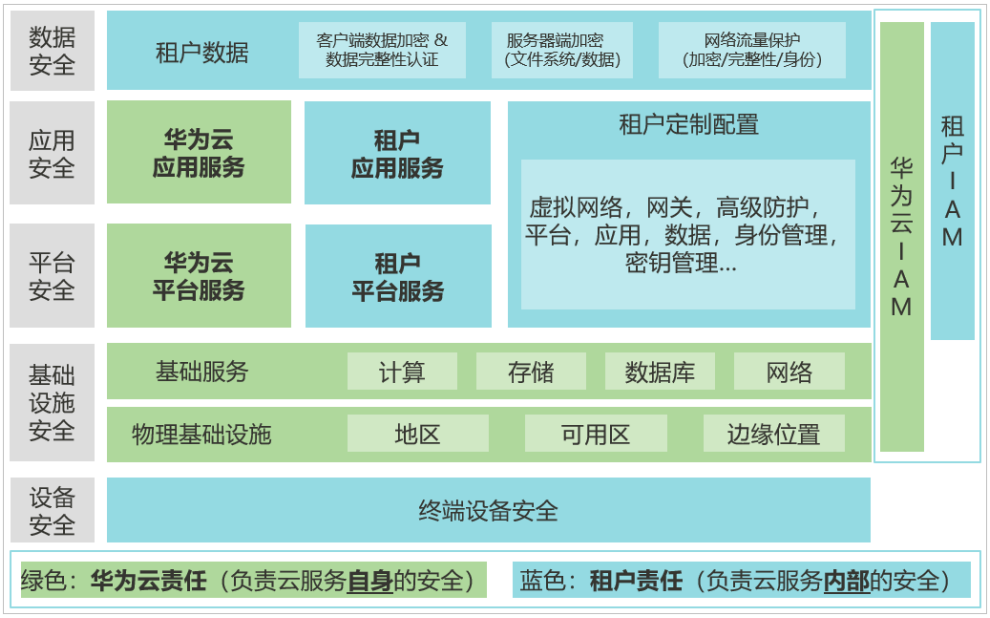
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图1**所示。

- 华为云：负责云服务自身的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- 租户：负责云服务内部的安全，安全地使用云。 华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 9-1 华为云安全责任共担模型



9.2 身份认证与访问控制

身份认证

用户访问COC的方式包括：COC控制台、API、SDK，无论哪种访问方式，其本质都是通过COC提供的REST风格的API接口进行请求。

COC的接口支持认证请求，经过认证的请求需要包含一个签名值，该签名值以请求者的访问密钥（AK/SK）作为加密因子，结合请求体携带的特定信息计算而成。通过访问密钥（AK/SK）认证方式进行认证鉴权，即使用Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。关于访问密钥的详细介绍及获取方式，请参见**访问密钥（AK/SK）**。

访问控制

COC支持通过IAM权限控制进行访问控制。关于IAM的详细介绍以及COC权限管理请参见**权限管理**。

9.3 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。

用户开通云审计服务并创建和配置追踪器后，CTS可记录COC的管理事件和数据事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

日志

用户开通云审计服务并创建和配置追踪器后，CTS可记录与云运维中心服务相关的操作事件。

详细的操作列表以及查看方法，请参见**查看审计日志**。

9.4 服务韧性

COC服务提供了3级可靠性架构，通过AZ内（Availability Zone，可用区）实例容灾、多AZ容灾、数据定期备份技术方案，保障服务的持久性和可靠性。

表 9-1 COC 服务可靠性架构

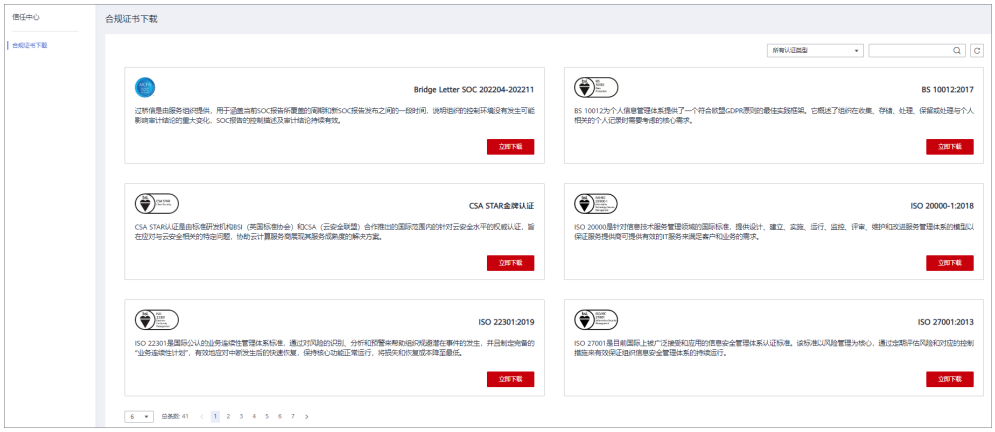
可靠性方案	简要说明
AZ内实例容灾	单AZ内，COC实例通过多实例方式实现实例容灾，快速剔除故障节点，保障COC实例持续提供服务。
多AZ容灾	COC支持跨AZ容灾，当一个AZ异常时，不影响COC实例持续提供服务。
数据容灾	通过数据定期备份方式实现数据容灾。

9.5 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 9-2 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 9-3 资源中心

销售许可证&软件著作权证书

另外，华为云还提供了以下销售许可证及软件著作权证书，供用户下载和参考。具体请查看**合规资质证书**。

图 9-4 销售许可证&软件著作权证书

10 修订记录

日期	修订记录
2023-11-30	第一次发布
2024-06-06	随服务版本刷新资料内容