解决方案实践

华为云 Landing Zone 解决方案实践

文档版本 1.0

发布日期 2024-05-11

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

版权所有 © 华为技术有限公司

目 录

1 方案概述 1
2 资源与成本规划 7
3 实施步骤 9
3.1 企业 IT 治理架构 9
3.2 Landing Zone 总体设计原则 12
3.3 Landing Zone 网络规划 13
3.3.1 账号网络架构 15
3.3.2 网络互联方案 16
3.3.3 网络安全 19
3.3.4 混合 DNS 19
3.4 身份和权限管理 20
3.5 资源治理 30
3.6 安全合规 39
3.6.1 企业上云面临的安全风险 39
3.6.2 云上安全设计原则 40
3.6.3 安全责任边界 42
3.6.4 整体安全架构 44
3.6.5 安全配置基线 46
3.6.6 合规审计 48
3.7 运维监控 49
3.7.1 运维监控原则 49
3.7.2 统一资源监控 51
3.7.3 统一日志存储 52
3.8 财务管理 57
4 自动化部署步骤 62
5 附录 63
6 修订记录 66

版权所有 © 华为技术有限公司

1 方案概述

应用场景

随着很多企业逐渐将越来越多的业务系统往云上迁移，企业客户需要将IT治理模式延伸或迁移到公有云上。公有云在安全稳定、服务质量、执行效率、成本效益等方面的优势逐渐被企业接受和认可，越来越多的企业也优先采用云原生的方式开发面向未来的新应用系统。企业全面云化的时代已经来临，为了避免大规模上云带来的管理失控、安全失控、成本失控等系列问题，企业开始逐渐重视云上IT治理，但在具体实践中经常会遇到以下各种挑战。

- 如何做好业务单元（如事业部、产品线、部门、项目组等）的安全和故障隔离，确保业务单元之间的云资源、应用和数据的隔离?
- 如何避免单点故障带来雪崩效应、减少单点故障的爆炸半径?
- 企业组织架构和业务架构经常调整，云上资源如何灵活应对?
- 如何设计跨多个业务单元的网络架构、建立受控的网络连接通道?
- 如何统一管控多个业务单元的边界网络出入口?
- 如何规划生产、开发和测试环境?
- 公共资源如何在多个业务单元之间共享?
- 如何统一监控、运维和管控多个业务单元的云资源?
- 如何统一管控各业务单元的预算和成本？如何优化云成本?
- 如何避免各业务单元过度使用云资源?
- 如何划分用户组？应该为用户组设置哪些权限?
- 云资源、数据和应用如何满足国家、行业和企业自身的安全合规标准?
- 在尽量保留原有IT治理模式的前提下，如何将其迁移到公有云上?

要应对上述挑战，需要设计一套全面的云上IT治理方案和最佳实践，对业务单元、人员、权限、云资源、数据、应用、成本、安全等要素进行全面有效管理。华为云通过Landing Zone解决方案来全面应对云上IT治理的挑战。Landing Zone本身是一个航空术语，指直升飞机等飞行器可以安全着陆的区域。目前国内外多家云厂商都借用了这个航空术语，将企业业务系统安全平稳迁移到公有云的解决方案命名为Landing Zone，目的是系统性解决企业大规模使用云服务所带来的IT治理和安全合规的挑战。

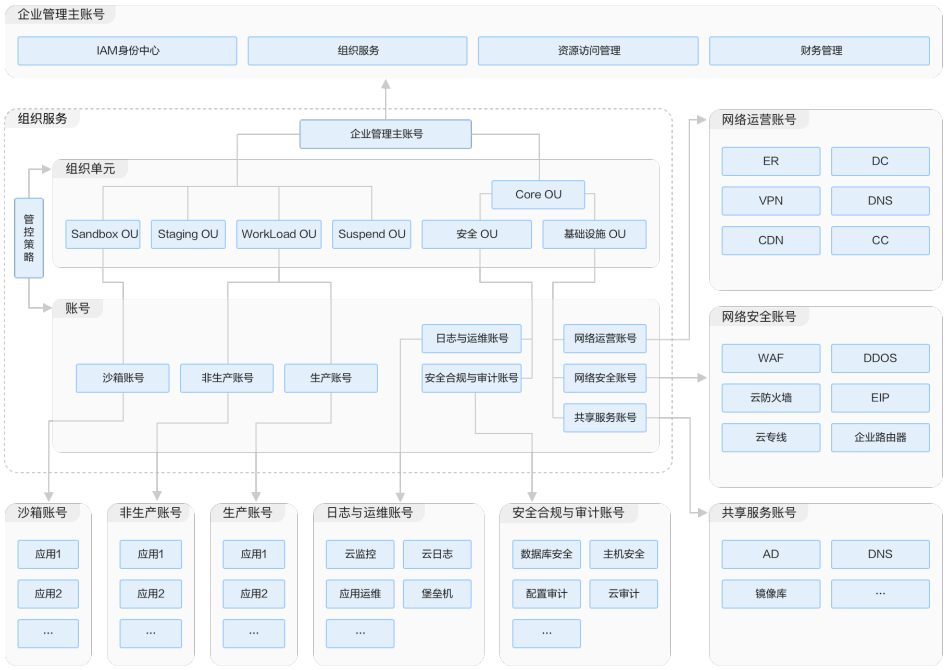
方案架构

Landing Zone解决方案的目标是在云上构建安全合规、可扩展的多账号运行环境，首先要规划组织和账号架构。按照康威定律，企业在华为云上的组织和账号结构要与企

版权所有 © 华为技术有限公司

业的组织和业务架构总体保持一致，但也不要完全照搬复制。华为云提供以下参考架构，建议按照业务架构、地理架构、IT职能等维度设计组织层级和账号。

图 1-1 华为云 Landing Zone 参考架构



1. 按照业务架构在华为云上划分不同的组织层级和OU，每个业务OU下面可以按照业务系统创建独立的子账号。规模较大的业务系统或安全隔离要求严格（如需要遵守PCI-DSS、HIPPA等合规标准）的业务系统对应一个独立的子账号，安全隔离要求不高的多个小型业务系统可以共享一个子账号。以销售部为例，可以为销售管理系统、数字化营销系统等较大的业务系统创建独立的子账号；以研发部为例，可以将围绕单个产品的设计、研发等系统部署在一个子账号中。
2. 按照地理架构在华为云上划分不同的组织层级和OU，每个地理区域OU下面可以按照国家或地区创建独立的子账号，在上面可部署本地的客户关系管理系统、客户服务系统等。上述参考架构把中国区等区域组织映射为华为云的OU，为其下属的北京、上海等分公司创建独立的子账号以承载本地化的应用系统。
3. 针对企业的中心IT部门，在华为云上创建对应的组织单元，并按照IT职能创建以下子账号，一方面实现IT管理领域的职责和权限隔离，另一方面对企业内多个子账号进行统一的IT管理。

版权所有 © 华为技术有限公司

表 1-1 IT 职能账号

账号名称	账号履行的IT职能	责任团队	资源或云服务
网络运营账号	集中部署和管理企业的网络资源，包括网络边界安全防护资源，实现多账号环境下的统一网络资源管理和多账号下VPCDMA网络络的互通，尤其需要集中管理面向互联网的出入口和面向线下IDC机房的网络出入口	网络管理团队,安全管理团队	NATG, EIP, VPC, 专线, 云连接, VPN, CFW，WAF, Anti-DDoS
公共服务账号	集中部署和管理企业的公共资源、服务和应用系统，并共享给其他所有子账号使用	公共服务管理团队	NTP服务器、AD服务器、自建DNS服务器、OBS桶、容器镜像库、协作办公系统等
安全运营账号	作为企业安全运营中心，统一管控整个企业的安全策略、安全规则和安全资源，为其他账号设置安全配置基线，对整个企业的信息安全负责	安全管理团队	统一部署具备跨账号安全管控的服务，如DEW、SCM、VSS等
运维监控账号	统一监控和运维各个子账号下的资源和应用，及时发现预警	运维团队	云堡垒机、Grafana, Prometheus或第三方运维监控系统
日志账号	集中存储其他账号的运行日志、审计日志	日志分析团队,合规审计团队	日志服务LTS、OBS桶、SIEM系统
数据平台账号	集中部署企业的大数据平台，将其他账号的业务数据统一采集到数据平台进行存储、处理和分析	数据处理团队,业务分析团队	数据湖、大数据分析平台、数据接入服务、数据治理平台
DevOps账号	统一管理整个企业的CI/CD流水线，并进行跨账号部署	软件研发团队	DevCloud，或自建DevOps流水线
沙箱账号	用于进行各种云服务的功能测试、安全策略的测试等	测试团队	按需部署各种需要测试验证的资源和服务

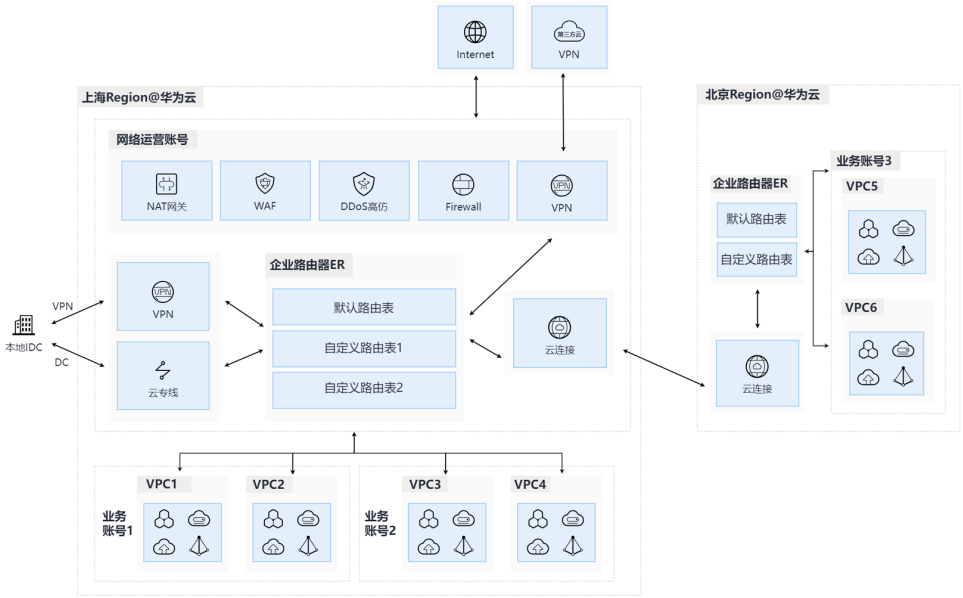
4. 除了上述子账号之外，中心IT部门可以根据自己的职责和权限隔离需求创建更多的子账号。比如独立的应用集成账号、协同办公账号等。
5. 需要注意的是在组织的根下面会默认关联一个主账号，主账号下不建议部署任何云资源，主要是做好以下管理工作：
   - **统一组织和账号管理**：创建和管理组织结构和组织单元，为组织单元创建子账号，或者邀请已有账号作为组织单元的子账号。

版权所有 © 华为技术有限公司

- **统一财务管理**：针对整个企业在华为云上的成本进行分析和统计；统一在华为云上充值、申请信用额度和激活代金券，再划拨给各个子账号，定期审视子账号的资金、信用额度和代金券的使用情况，及时进行回收。
- **统一组织策略管理**：为各个组织单元和子账号设置组织策略，强制限定子账号下用户（包括账号管理员）的权限上限，避免用户权限过大带来安全风险，创建组织策略时可以将其应用到某一个组织单元，该组织策略可以继承到关联的子账号和下层组织单元。

6. 在每个子账号下面还可以通过企业项目（Enterprise Project, EP）对资源进行细粒度的逻辑分组，比如将一个应用系统的子系统、一个产品的子产品映射为华为云上的一个企业项目，用户还可以按照EP进行成本分摊和细粒度授权。

图 1-2 网络运营账号



7. 在上述多账号架构下，网络运营账号作为Landing Zone的网络枢纽，该账号集中管理多账号的边界网络出入口，并打通多账号下VPC之间的网络。在网络运营账号下集中部署企业路由器（Enterprise Router, ER），通过ER联通各账号下的VPCDMA网络络，从而实现多账号共享使用VPN和云专线与线下IDC互通，也能实现多账号共享使用公网NAT网关与互联网通信，还能共享使用云连接与其他Region进行互通。在该账号下统一管理网络资源，一方面可以减少管理工作量，另外也有利于制定和实施统一的网络安全策略，例如统一部署面向互联网连接的DDoS高仿、云防火墙CFW、WAF等安全资源并统一配置具体的安全防护策略

图 1-3 多账号资源共享和统一管控

8. 在多账号网络互通的基础上，可以进一步实现多账号的资源共享和统一管控。资源共享主要是针对公共资源的共享，比如NTP服务器、AD服务器、自建DNS服务

版权所有 © 华为技术有限公司

器、OBS桶、容器镜像库等，也可以是DevCloud等PaaS服务，在一个或多个独立的子账号中集中部署和维护这些公共资源，并共享给其他账号使用，没有必要在每一个子账号中单独部署和维护。统一管控主要针对的是管理类系统，如监控运维、资源治理、安全防护、财务管理等，集中管理多账号环境下的监控、运维、资源、安全、财务等，避免在每个子账号中分散式管理带来的管理成本高、标准不统一的问题。统一管控可以有效制定和实施企业范围内的IT治理策略。

方案优势

1. 为了实现业务单元的安全和故障隔离，华为云的推荐做法是将不同业务单元的应用系统分别部署在不同的账号中。华为云账号具备以下三个属性。
   - 华为云账号是一个资源容器，用户可以在其中部署任意云资源和上层业务应用系统，不同的账号相当于不同的资源容器，账号之间是完全隔离的。因此在一个账号中的故障和安全风险不会影响和传播到其他账号。
   - 华为云账号也是安全管理边界，每个账号都有独立的身份和权限管理系统，一个账号内的用户只能访问和管理本账号的资源，未经允许，一个账号内的用户不能访问其他账号的资源、数据和应用。
   - 华为云账号还可以作为独立的账单实体，每个账号可以单独在华为云上充值、购买云资源、结算和开票。
2. 因此华为云账号可以针对业务单元进行有效的故障和安全隔离，还可以进一步进行管理和财务隔离。
3. 另外，为了避免单点故障带来雪崩效应、减少单点故障的爆炸半径，核心办法就是不要把所用业务系统及其云资源部署在单一账号，也就是不要“把鸡蛋放在一个篮子里”。单一账号存在两个严重的问题：其一是单一账号的爆炸半径太大，如果该账号发生崩溃将导致企业所有业务系统不可用；其二是云平台上账号的资源配额是有上限的，不能在一个账号内无限扩容云资源。
4. 因此当企业全面上云时通常需要采用多账号架构。按照康威定律，企业的多账号架构通常会与其组织架构或业务架构保持一致，即按照业务单元、地理单元、职能单元等维度划分账号。采用多账号架构后可以实现职责分离，不同的账号负责不同的事情、承载不同的业务，每个账号的管理员可以对本账号内的资源进行自治管理，但同时从IT治理角度肯定要求一定程度的统一管控，比如多账号的统一运维管理、安全管控、资源管理、网络管理、财务管理等。针对这些核心诉求，华为云提出了Landing Zone解决方案来**帮助企业在云上构建安全合规、可扩展的多账号运行环境，实现多账号的资源共享和“人财物权法”的统一管控。**
   - **人的管理**：多账号环境下对业务单元、账号、用户、用户组、角色等进行统一管理；
   - **财的管理**：多账号环境下对资金、预算、成本、发票、折扣等进行统一管理；
   - **物的管理**：多账号环境下对计算、存储、网络、数据、应用等云资源进行统一运维、监控和管理；
   - **权的管理**：多账号环境下对云资源的访问权限进行统一管理，确保访问权限符合最小授权原则；
   - **法的管理**：多账号环境下对安全合规进行统一管理，确保符合国家、行业和企业自身的安全合规要求。
5. 企业成功实施了Landing Zone解决方案之后，可以有效规避大规模上云之后的管理失控、安全失控、成本失控的风险，全面应对各种IT治理挑战，帮助企业建立分统结合的IT治理体系和完善的安全合规体系。
   - 分统结合的IT治理体系：即在分权分域分级管理的基础上进行一定程度的统一管控，如统一运维、统一安全等；

版权所有 © 华为技术有限公司

- 完善的安全合规体系：云上运行环境（包括云资源、数据、应用等）满足国家、行业和企业自身的安全合规标准。

版权所有 © 华为技术有限公司

2 资源与成本规划

本方案的云资源清单受企业规模、组织层级、业务架构等因素影响较大，具体资源清单及价格请以实际调研后提供为准。Landing zone解决方案提供专业服务能力，匹配8大领域，推荐专业服务如下。

图 2-1 Landing Zone 设计与实施服务

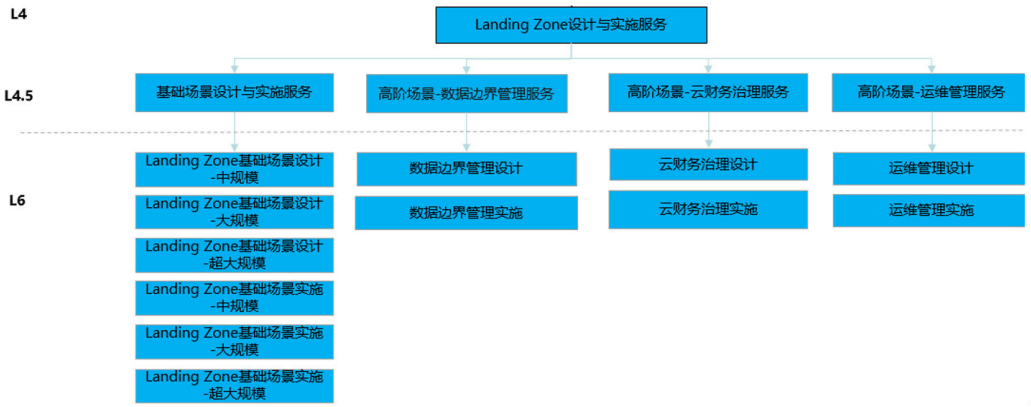


表 2-1 资源与成本规划

offering八大场景	基础场景设计与实施服务	高阶场景-数据边界管理服务	高阶场景-云财务治理服务	高阶场景-运维管理服务
资源组织与账号管理	√	√	“/”	“/”
身份权限管理	√	√	“/”	“/”
集中网络管理	√	√	“/”	“/”
安全管理	√	√	“/”	“/”
合规审计	√	√	“/”	“/”
共享服务管理（数据边界）	“/”	可选	“/”	“/”

版权所有 © 华为技术有限公司

offering八大场景	基础场景设计与实施服务	高阶场景-数据边界管理服务	高阶场景-云财务治理服务	高阶场景-运维管理服务
财务管理	“/”	“/”	**可选**	“/”
运维管理	“/”	“/”	“/”	**可选**

1. **以安全合规、权限管理、网络划分角度**：客户在使用云的过程中，必须要遵从全球法律法规要求、身份权限的设计和相关网络的划分。推荐使用“基础场景设计与实施服务”。
2. **以数据边界角度：**基于“基础场景设计与实施服务”之上，客户业务上对跨账号、跨网络和环境内部资源之间的访问有相关需求，推荐使用“**高阶场景-数据边界管理服务**”。
3. **以降本增效角度：**客户对明确云资源使用情况以及费用情况，优化云资源成本，降低不必要的 支出，更快地识别成本差异和异常情况的需求，推荐使用“**高阶场景-云财务治理服务**”。
4. **以运维治理角度：**客户对所有成员账号的资源管理、事件管理、变更单进行统一查看、操作和日志监控有相关需求，推荐使用“**高阶场景-运维管理服务**”

版权所有 © 华为技术有限公司

3 实施步骤

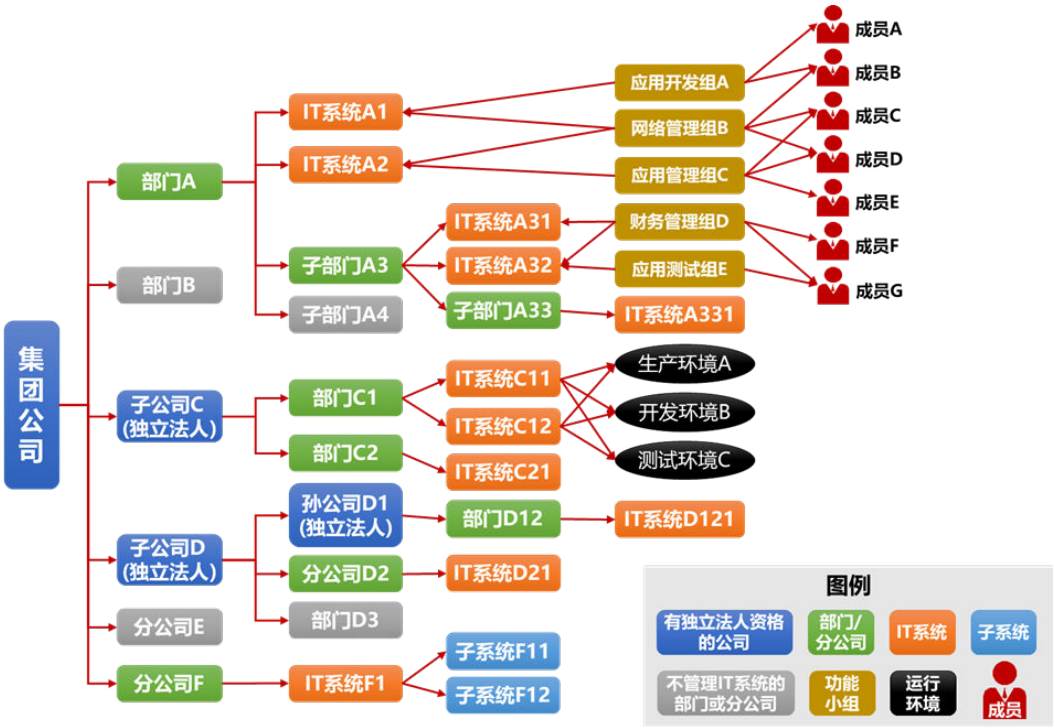
3.1 企业IT治理架构
3.2 Landing Zone总体设计原则
3.3 Landing Zone网络规划
3.4 身份和权限管理
3.5 资源治理
3.6 安全合规
3.7 运维监控
3.8 财务管理

3.1 企业 IT 治理架构

大企业的业务覆盖范围很广泛，分布在不同的子行业和地理区域，为支持整个公司的长期稳定运行和有效管理，通常采用集团化和等级式管理模式。随着经营范围和规模的不断扩大，需要不断建立子公司、分公司，子公司再建立孙公司，大部门也逐步拆分成多个小部门，组织结构的层级也就越来越多。大企业的IT治理架构也会受到组织结构的影响，以下是一个典型的大企业IT治理架构示意图，由于图片空间有限，该示意图中没有穷举全部的层级和图元。本文所描述的Landing Zone最佳实践以下图的IT治理架构为基础，将其映射到华为云上有效运转起来。

版权所有 © 华为技术有限公司

图 3-1 大企业 IT 治理架构



在上述大企业IT治理架构中，各个层级的具体含义如下：

- **集团公司：**是指以资本为主要联结纽带,以母子公司为主体，以集团章程为共同行为规范的，由母公司、子公司及其他成员共同组成的企业法人联合体。
- **子公司：**其50%以上有投票表决权的股份或资本被另一企业（母公司）所拥有的企业，母公司对子公司的一切重大事项拥有实际上的决定权。子公司具有独立法人资格，在法律上是完全独立的公司，是独立的核算主体和纳税主体。子公司可以根据经营管理需求再成立自己的子公司或分公司。
- **分公司：**分公司是母公司管辖的分支机构，是指母公司在其住所以外设立的以自己的名义从事活动的机构，如在各个省市成立的销售分公司。分公司不具有企业法人资格，其民事责任由母公司承担。
- **独立法人：**独立法人是指依法在工商部门登记的拥有企业独立法人营业执照的经济组织，具备独立的民事行为能力，能够独立承担民事责任。
- **部门：**母公司、子公司和分公司都可以基于自己的经营管理需求设立部门，如软件企业可以按照不同的软件产品线设立不同的部门，工业制造企业可以按照业务流程设立研发部、制造部、采购部、销售部、服务部等。大部门还可以再进一步拆分成小部门。
- **IT系统：**企业按照业务需求和IT管理需求建设的IT系统，包括业务支撑类应用系统（如ERP、CRM、营销管理系统等）和IT管理类应用系统（如SOC、运维监控系统等），IT系统的开发、测试、实施和运行需要消耗一定的计算、存储、网络、安全、数据库、中间件、大数据、AI服务等资源。
- **子系统：**IT系统通常包含多个相互解耦且相互关联的子系统、功能模块或微服务，这些子系统相互协作，共同实现IT系统的功能。
- **功能小组：**参与IT系统建设和管理的成员按照职责划分为不同的功能小组，如基础设施组、网络组、安全组、应用开发组等。
- **成员：**一个成员代表一个参与IT系统建设和管理的人，可加入到同一部门下不同的IT系统和功能小组，但一般不参见其他部门的IT系统。

版权所有 © 华为技术有限公司

- **运行环境：**IT系统通常要部署到不同的运行环境：互联网环境、生产环境、开发环境和测试环境。

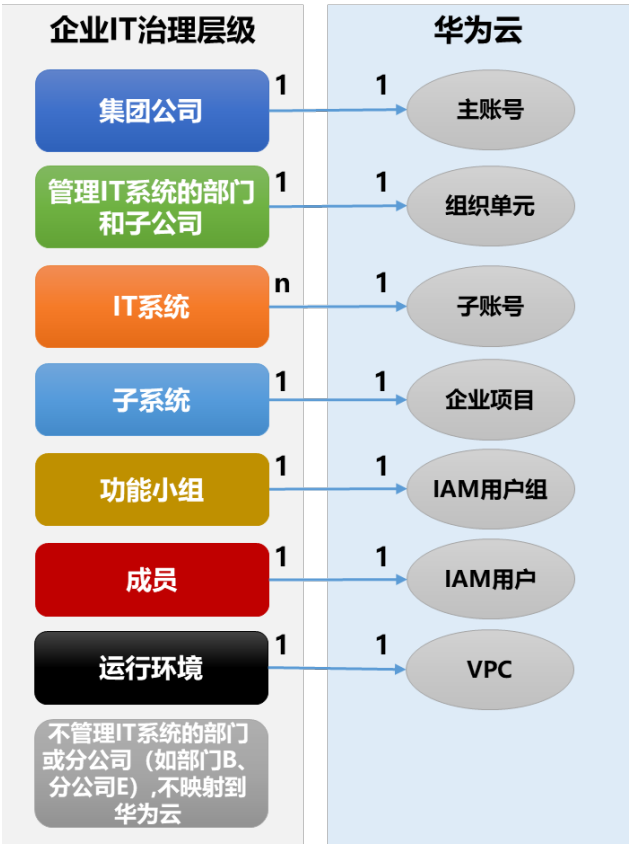
图 3-2 大企业 IT 治理架构的层级关系

层级关系	关系描述
公司(独立法人) 1 n 部门/分公司	1个集团公司或者1个独立法人的子/孙公司包括多个部门和多个分公司(不具备法人资格，类似部门)
部门/分公司 1 n 子部门	1个部门或者1个分公司可以管理多个子部门
集团公司 1 n 子公司(独立法人)	1个集团公司可以控股多个子公司（子公司是独立的法人，拥有自己独立的公司名称、章程和组织结构）
部门/分公司 1 n IT系统	1个部门可以管理多个IT系统
IT系统 1 n 子系统	1个IT系统可以包含多个子系统、功能模块或微服务
IT系统 m n 功能小组	1个IT系统可以由多个功能小组（如开发组、测试组等）共同完成，1个功能小组（如统一运维组、财务组等）也可以参与到多个IT系统
功能小组 m n 成员	1个功能小组可以由多个成员组成，1个成员可以同时加入多个功能小组
部门/分公司 1 n 成员	1个部门包含了多个成员，成员一般不允许加入到多个部门。
IT系统 m n 运行环境	1个IT系统需要多个运行环境（如生产环境、开发环境、测试环境），1个运行环境也可以承载多个IT系统。

上述IT治理架构中的各个层级需要逐一映射到华为云上，在华为云上创建相应的对象，推荐的映射关系如下图所示。集团公司映射为华为云的主账号，下面的子公司、分公司和部门都可以映射为华为云的组织单元（Organization Unit, OU）。IT系统映射为子账号，子系统则可以映射为企业项目。功能小组映射为华为云IAM的用户组，成员则可以对应到华为云IAM的用户。生产、开发和测试等运行环境可以划分到不同的VPC。

版权所有 © 华为技术有限公司

图 3-3 企业 IT 治理架构到华为云的映射



3.2 Landing Zone 总体设计原则

1. 不需要把企业内部的完整组织结构映射到华为云上，只把那些负责管理IT系统的组织单元（如部门、分公司）和使用IT资源的用户映射到华为云上。如行政部门不管理、不查看、不操作任何云上IT资源，就不需要在华为云上创建一个对应行政部门的组织；如财务小张不负责IT系统的成本核算、分析和预算管理，就无需为小张在华为云上创建一个拥有财务管理权限的用户。
2. 如果企业内部的IT组织结构（直接管理IT系统）层级很深，建议只把最上面两层IT组织单元映射到华为云上的组织单元，其他下面层级的IT组织单元不建议映射到华为云上，避免避免IT治理的碎片化。
3. 针对业务部门，可以按照业务支撑系统创建对应的子账号，如果业务系统的规模比较大，或者需要遵守严格的安全合规标准（如PCI-DSS、HIPPA等），将其映射为一个独立的子账号；如果几个小型业务系统不要求严格的安全隔离，那就可以将这几个小型业务系统部署到一个子账号中。
4. 针对IT部门，可以按照IT职责划分不同的IT管理类子账号，如安全运营、运维监控、网络运营、DevOps等子账号。
5. 主账号的密码建议由企业的CTO或CIO保管，子账号的密码建议由所属组织单元的负责人保管。主账号和子账号的权限很大，企业需要制定符合自身安全管控要求的账号管理和使用策略。

版权所有 © 华为技术有限公司

3.3 Landing Zone 网络规划

网络架构设计原则

华为云基于大量成功交付的项目，总结提炼了以下用户和权限管理原则：

1. **业务隔离原则**

   不相关的业务进行流量隔离。按照生产环境、开发环境、测试环境分别划分独立的VPC；在每个VPC中按照接入层、应用层和数据层来分别划分子网。在互联网入口侧部署DMZ VPC，用于WAF等互联网安全的配置。

2. **整体划分原则**
   - **VPC的网络容量：**每个VPC可使用IP地址建议不超5000个
   - **VPC间是隔离性大于连通性：**VPC间默认隔离，可通过对等连接实现点对点互通；账户
   - **子网间是连通性大于隔离性：**子网间默认互通，但建议通过ACL访问控制按需隔离；

3. **VPC划分原则**
   - 业务账号可根据生产、开发、测试环境划分VPC，之间的网络建议不打通，确保生产、开发、测试环境的隔离。
   - 网络运营账号创建一个集中的DMZ VPC，用于集中部署面向互联网连接的NAT网关，集中管理互联网的出入口，这样方便集中实施边界安全防护策略。
   - Landing Zone架构下多个账号之间需要经常互访，需要打通VPC之间的东西向网络访问通道，所以需要统一规划Landing Zone的VPCDMA网络络的IP地址，避免地址重叠导致无法实现网络互通。

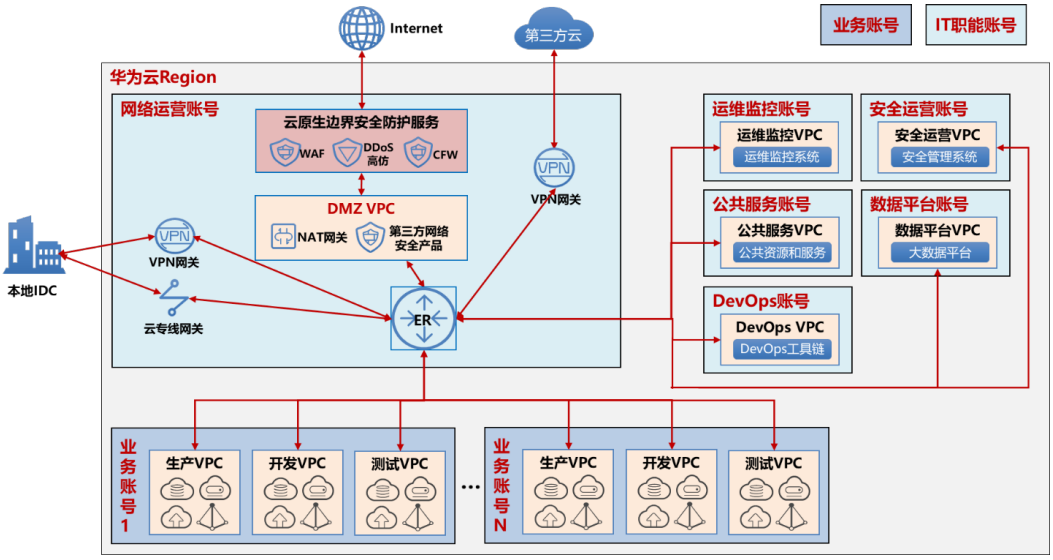
4. **子网划分原则**
   - 同VPC内子网不可重叠，需要互通的VPC间子网不能重叠。
   - 业务账号下，可以按照业务系统的应用层和数据层划分不同的子网。之间采用ACL进行网络访问控制。默认只有应用子网对公网提供服务，数据子网只可被应用子网访问。
   - 建议不同业务系统使用不同子网，可使用子网ACL控制按需访问。

整体网络架构设计

Landing Zone的整体网络架构设计如下图所示：kin'g'zukingzu

版权所有 © 华为技术有限公司

图 3-4 网络架构设计



上述网络架构的核心是网络运营账号，作为连接其他账号的网络枢纽，其他账号之间的通信必须通过该账号的ER进行。ER可以通过设置路由规则决定哪些VPC之间的网络可以连通，华为云基于以下假设并根据各个账号的职责梳理各个账号下VPC之间的连通性矩阵，据此则可以在ER上设置对应的路由规则。

- 运维监控账号需要运维第三方云和本地DC中的资源；
- 安全运营账号需要到公网获取系统补丁包；
- 数据平台需要获取第三方云和本地DC的数据；
- DevOps账号需要从Github上下载代码，需要将软件制品部署到各个业务账号；
- 公共服务账号需要与本地IDC互联；
- 生产、开发、测试环境要求网络隔离。

图 3-5 各账号 VPCDMA 网络络的连通性矩阵

账号名称	网络运营账号互联网连接	网络运营账号本地IDC连接	网络运营账号第三方云连接	公共服务账号VPC	安全运营账号VPC	运维监控账号VPC	数据平台账号VPC	DevOps账号VPC	业务类账号生产VPC	业务类账号开发VPC	业务类账号测试VPC
网络运营账号互联网连接	N/A	X	X	X	✔	X	X	✔	按需	按需	按需
网络运营账号本地IDC连接		N/A	X	✔	X	✔	✔	X	按需	按需	按需
网络运营账号第三方云连接			N/A	X	X	✔	✔	X	按需	按需	按需
公共服务账号VPC				N/A	✔	✔	✔	✔	✔	✔	✔
安全运营账号VPC					N/A	✔	✔	✔	✔	✔	✔
运维监控账号VPC						N/A	✔	✔	✔	✔	✔
数据平台账号VPC							N/A	X	✔	✔	✔
DevOps账号VPC								N/A	✔	✔	✔
业务类账号生产VPC									X	X	X
业务类账号开发VPC										X	X
业务类账号测试VPC											X

日志账号是集中存放审计日志和运行日志的地方，主要使用了华为云的LTS服务和OBS服务，该两个服务没有租户面IP地址，所以不需要考虑与其他账号的VPC进行互通。沙

版权所有 © 华为技术有限公司

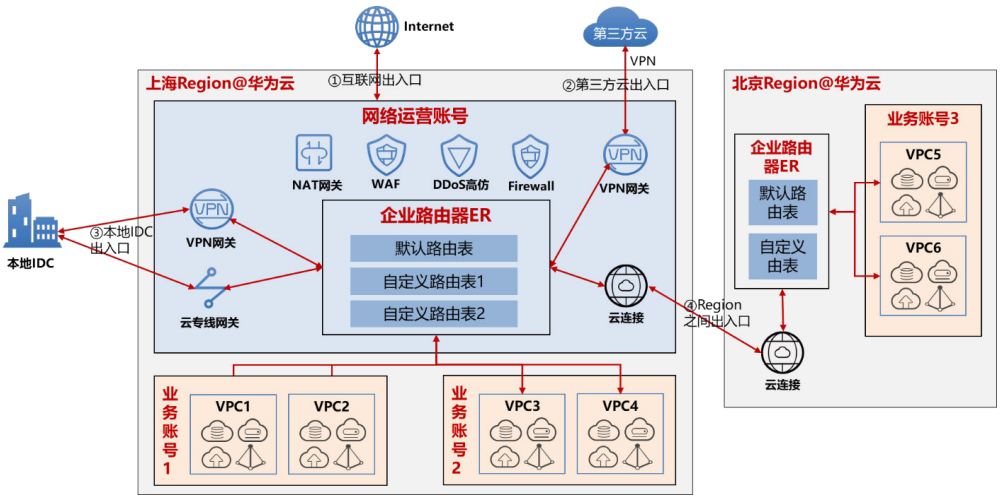
箱账号是一个允许客户任意测试华为云上资源的地方，包括VPC的功能测试以及与其他账号之间连通性测试，所以也不需要预先在ER中配置与其他账号的连通性。

3.3.1 账号网络架构

公共网络账号的网络架构

1. 在该账号中集中部署网络资源（ER、VPN、DC、CC、公网NAT网关）和网络边界安全防护（WAF、CFW、Anti-DDoS）。集中控制和管理四个网络出入口：互联网出入口、本地IDC出入口、第三方云出入口、其他Region出入口。
2. 在互联网出入流量的访问策略中，建议不允许从公共IP地址访问所有端口。只开放必要的Internet IP地址和端口。阻止对所有其他端口的访问。Internet请求首先到达WAF，WAF转发到NAT网关特定的弹性IP和端口。

图 3-6 公共网络账号的网络架构设计



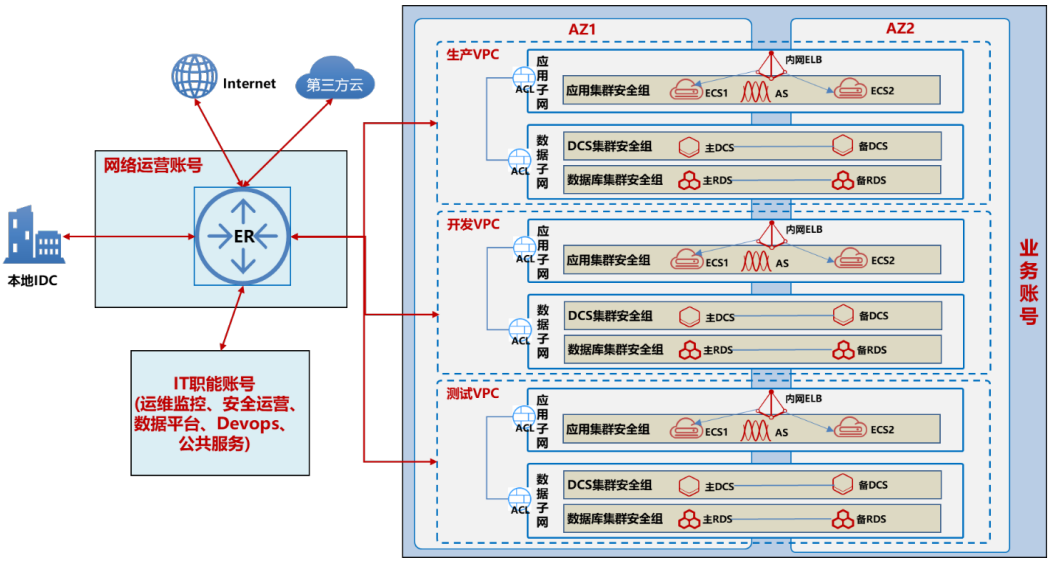
3. 当VPC挂载到ER时，ER自动学习VPC路由。设置手动路由策略，禁用不同环境VPC之间的路由。
4. VPC之间的云防火墙访问控制策略如下：
   - 默认规则：允许所有业务账号访问网络运营账号的VPN网关、云专线网关、NAT网关，并使用访问控制策略。
   - 当ER允许两个VPC连接时应该创建一个策略来允许来自可信来源的流量，然后创建另一个策略来拒绝来自所有其他来源的流量。确保允许策略的优先级高于拒绝策略。

业务账号的网络构架

针对大的业务系统，一般是对应一个独立的子账号，在该账号中建议为每个业务系统创建三个独立的VPC：生产VPC、开发VPC、测试VPC，VPC之间彼此隔离。每个VPC至少部署二个子网：应用子网和数据子网，分别对应业务系统的应用层和数据层。子网之间使用网络ACL进行访问控制，还可以将云主机、RDS等资源放入到安全组，通过安全组规则进行实例级别的访问控制。业务系统的应用主机集群可以跨可用区部署，实现应用层的高可用；再使用华为云跨可用区的主备数据库集群和缓存集群实现数据层的高可用。如下图所示：

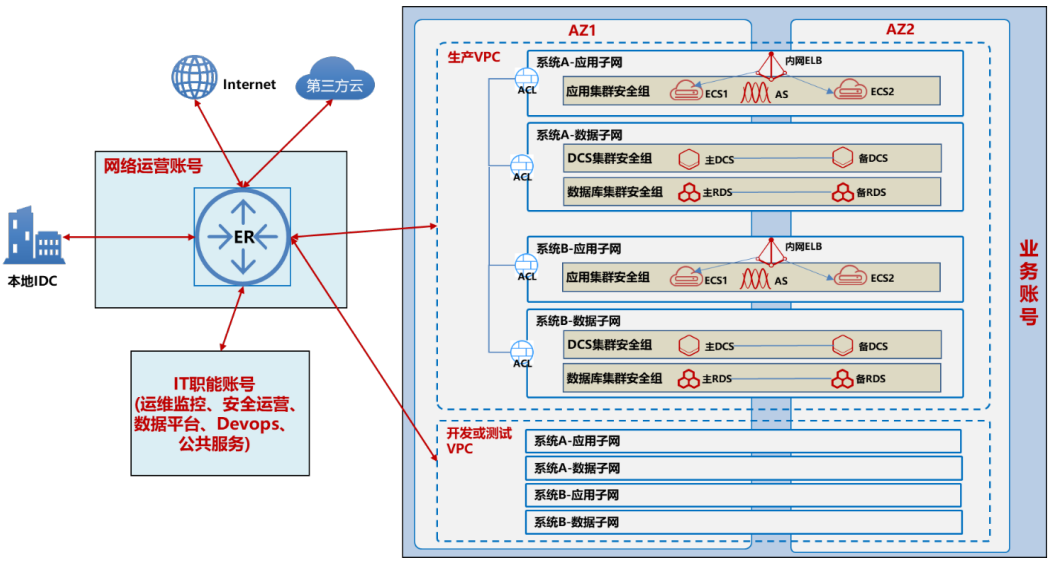
版权所有 © 华为技术有限公司

图 3-7 一个大型业务系统对应一个独立子账号



针对多个没有严格安全隔离需求的小型业务系统，可以共用一个子账号，在该账号中同样建议创建三个独立的VPC：生产VPC、开发VPC、测试VPC，VPC之间彼此隔离。这些小型业务系统共同部署在这几个VPC中，不同的业务系统通过子网隔离，每个业务系统也都有独立的应用子网和数据子网，为这些子网创建ACL，以控制不同子网之间的内部网络流量。如下图所示：

图 3-8 多个小型业务系统共用一个子账号



3.3.2 网络互联方案

VPC 之间的互联

1. 企业路由器（ER）是云上大规格，高带宽，高性能的集中路由器，支持路由学习、动态选路以及链路切换，减少路由条目配置及维护工作量。将同Region的多个VPC接入ER中，就可以实现同区域多个VPC互通。

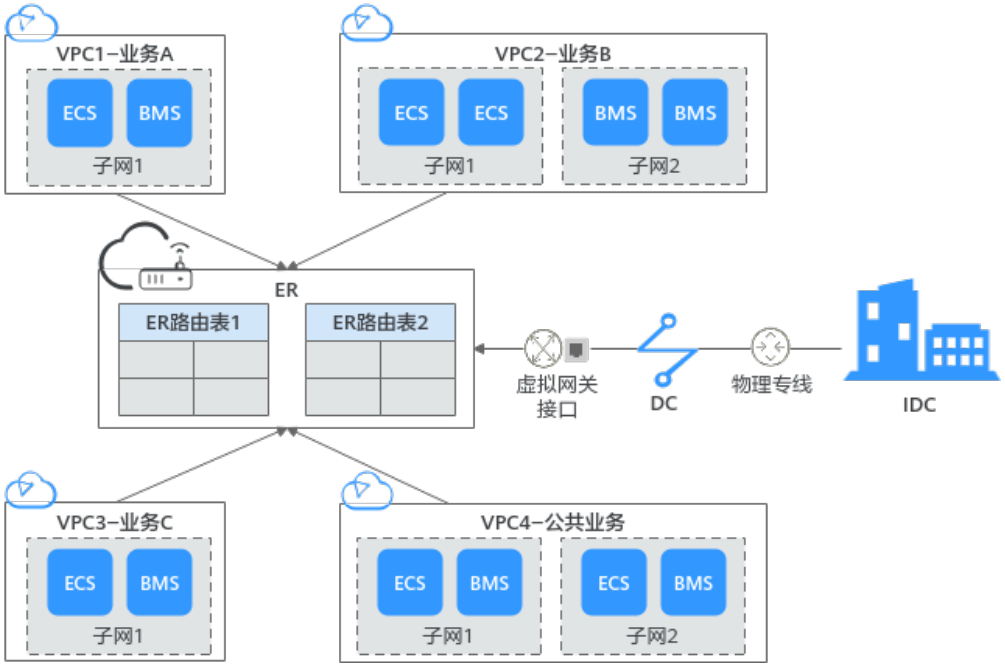
版权所有 © 华为技术有限公司

2. 不同应用账号的VPC可以通过ER路由规则隔离。VPC之间支持灵活互通和隔离。
3. VPC间访问策略
   - DMZ VPC所有子网默认对内只能访问维护子网和公共服务子网的服务端口.
   - DMZ VPC建议不同业务用不同子网，默认隔离，按需放通
   - DMZ VPC业务系统建议分应用子网和数据子网，默认只有应用子网对公网提供服务，数据子网只可被应用子网访问
   - 公共运维VPC对线下网络放通公共服务子网访问权限，按需放通维护子网访问权限；
   - 生产VPC按照业务划分不同子网，业务内可划分应用子网和数据子网，默认数据子网只可被应用子网访问，应用子网按需对其他子网放通。生产VPC各子网放通维护子网的访问。
   - 开发测试VPC按照业务划分不同子网，业务内可划分应用子网和数据子网，默认数据子网只可被应用子网访问，应用子网按需对其他子网放通。开发测试VPC各子网放通维护子网的访问。
   - 生产VPC和开发测试VPC默认不互通，不建立对等连接，数据传输建议通过OBS存储传输。

云上云下互联

1. **单条专线场景**

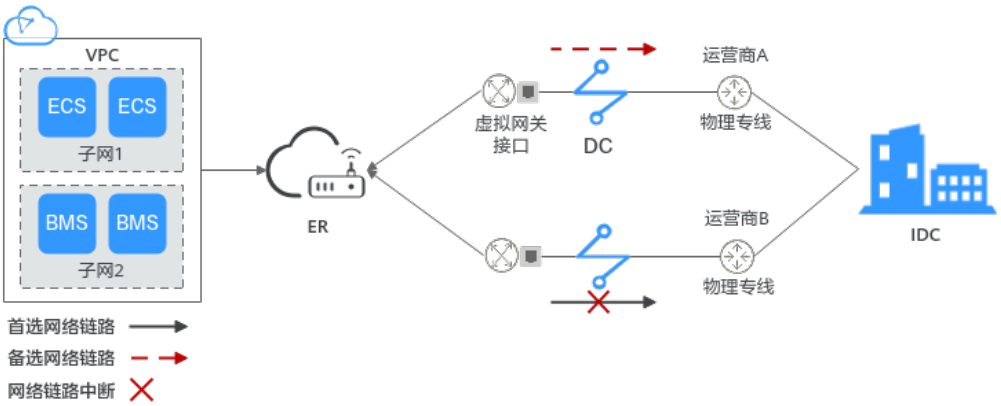
图 3-9 单条专线场景



   - 通过将专线接入ER，实现线下IDC和云上多个VPC互通。避免了需要为每个和IDC互通的VPC建立专线。多个VPC可以共享专线访问线下IDC，免去多条专线配置，降低成本。
   - 通过将VPC关联至ER中不同的路由表，灵活实现VPC之间的互通和隔离，网络拓扑简洁，配置简单易管理。
2. **多条专线场景**

版权所有 © 华为技术有限公司

图 3-10 多条专线场景

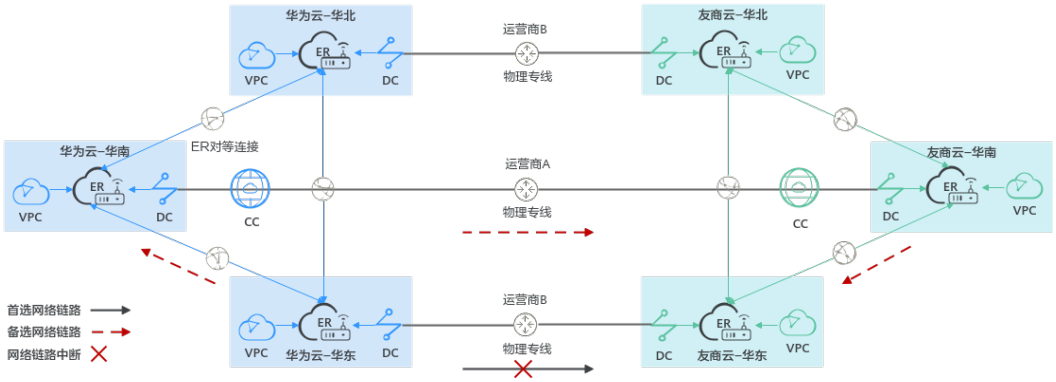


- 云上业务访问线下IDC要求高带宽、高可靠时，通常部署两条或更多的专线链路，专线链路之间相互独立。
- 专线接入ER后，可以实现专线的动态选路和切换。多个链路之间进行负载分担实现高带宽，同时保证可靠性；多个链路之间互为主备，单链路故障秒级切换，避免了单点故障带来的业务中断。

Region 之间的互联

跨Region互联，采用每个Region部署一台ER。只需要将每个Region的ER接入云连接（Cloud Connect），构成ER对等连接，实现云上跨Region网络互通。这样的好处是无需在CC中接入所有网络实例，简化网络拓扑；支持路由学习，无需手工配置路由，快速构建组网。

图 3-11 Region 之间的互联



云间互联（华为云与其他云的互联）

1. 客户业务部署在多朵云上，避免被厂商绑定，降低风险；同时部署在多个region，实现就近接入。客户没有自建骨干网，使用云平台的骨干网实现多云多region网络互通。
2. 示意图参考以上图3，不同公有云之间通过DC专线链路（不同运营商）互通，同云之间互通走云厂商骨干网。ER可以实现专线和云连接之间的链路联动，用作负载分担或者主备。

版权所有 © 华为技术有限公司

3.3.3 网络安全

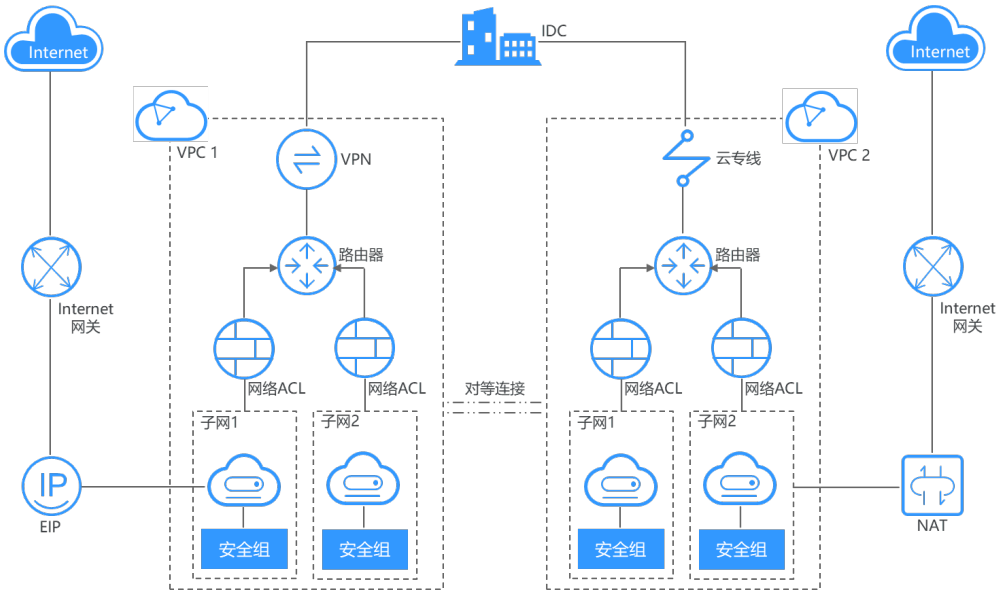
边界安全

1. 包括互联网边界、云上云下的边界、Region之间的边界、云间的边界，安全防护策略包括南北向防火墙、Anti-DDoS、WAF、IDS/IPS等。
2. 当互联网用户使用https协议访问应用程序时，经过WAF和云防火墙，潜在的恶意流量将被过滤。
3. 云上云下边界打通一般通过VPN或者云专线DC。VPN使用IPSe技术在公网中加密，保证安全便捷。云专线使用私有通道打通站点，私密性极高，时延稳定，抖动小，性能强。

内网安全

1. VPC的子网之间主要通过安全组和网络ACL作为访问控制手段。

图 3-12 内网安全



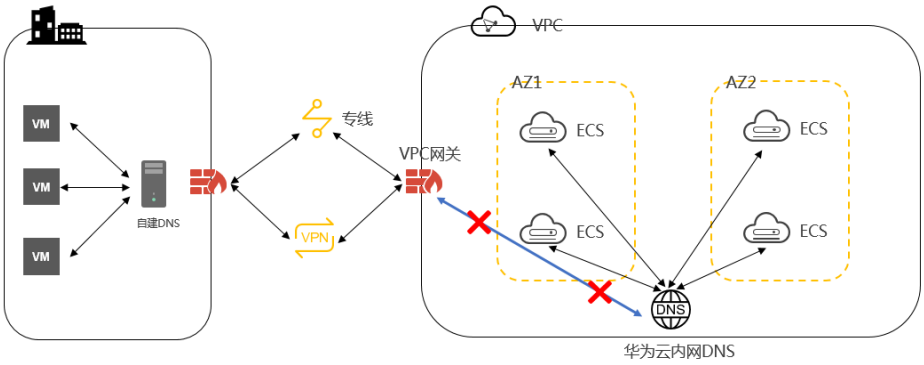
2. 安全组与网络ACL（Access Control List）用于保障虚拟私有云VPC内部署的云资源的安全。安全组类似于虚拟防火墙，为同一个VPC内具有相同安全保护需求并相互信任的云资源提供访问策略；您可以为具有相同网络流量控制的子网关联同一个网络 ACL，通过设置出方向和入方向规则，对进出子网的流量进行精确控制。

3.3.4 混合 DNS

1. 通过专线把本地数据中心和华为云服务器打通，本地服务器和华为云服务器就可以直接通信，但是基于安全因素考虑，华为云的DNS服务器只能华为云的服务器使用，本地DNS服务器和华为云的DNS服务器之间网络是不能通信的，本地数据中心DNS服务器有自己业务域名，华为云服务器DNS有华为云服务域名，这样问题就出现了：
   - 本地数据中心服务器用的自己的DNS服务器，可以解析本地域名，但是无法解析华为云服务域名，比如OBS，SFS等
   - 华为云服务器使用华为云的DNS，可以解析华为云服务域名，但是无法解析本地数据中心的域名

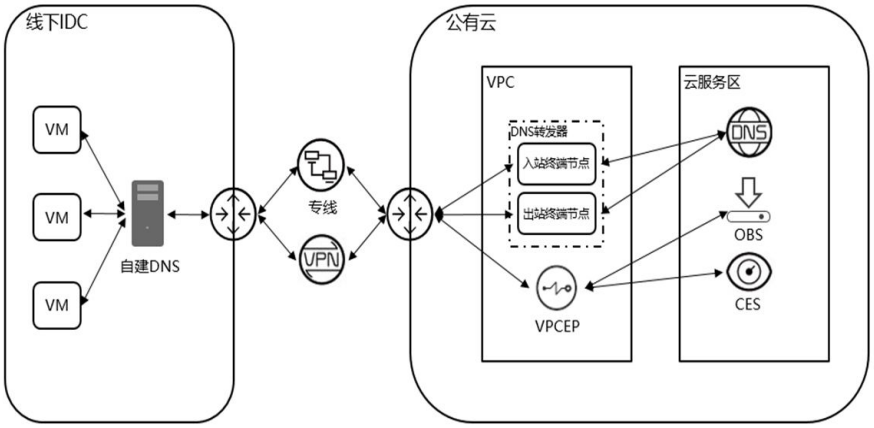
版权所有 © 华为技术有限公司

图 3-13 混合 DNS 1



2. 解决方案：华为云提供混合DNS解决方案DNSEP，通过dnsep 把公有云dns地址下沉到客户自己vpc内，可以实现线下dns和公有云dns互相forward。步骤如下：
   - 线下自建DNS把要解析的云服务域名(*.myhuaweicloud.com)转发给入站终端节点到达云上dns；
   - 云上dns会根据出站终端节点配置的域名转发规则把相应域名解析转发到指定的线下DNS解析。

图 3-14 线下 DNS 解析



3.4 身份和权限管理

用户和权限管理原则

华为云基于大量成功交付的项目，总结提炼了以下用户和权限管理原则：

1. 建议使用企业自己的身份管理系统（如Azure AD等）与华为云IAM进行联邦身份认证，前者的用户通过SSO（Single Sign-on）登录到华为云控制台进行操作。企业自己的身份管理系统能更好更及时地匹配员工的入职、转岗和离职流程，避免转岗和离职人员继续拥有访问华为云的访问权限。
2. 不要把华为云IAM作为企业自己的用户管理系统，无需与华为云发生交互的企业员工，就不用在华为云IAM上创建相应的用户或用户组。
3. 不要将用户的密码共享给其他人，而是为每个管理或使用华为云资源的人创建一个单独的用户并分配相应的权限，这样每个自然人在华为云的操作都能被追踪审计。

版权所有 © 华为技术有限公司

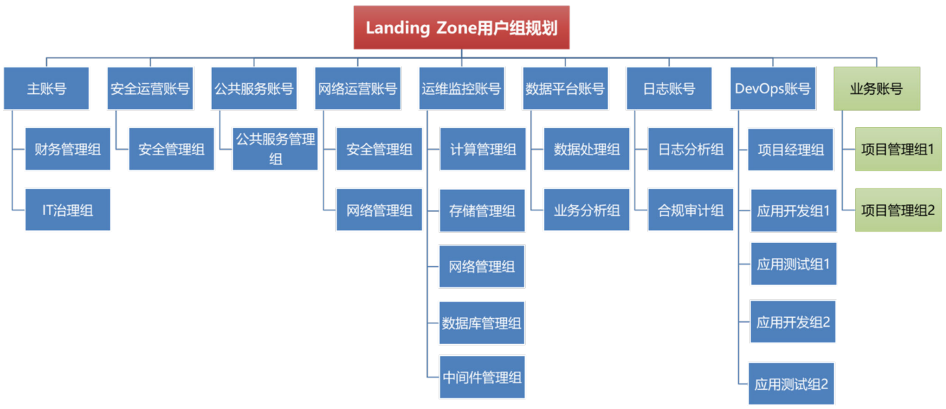
4. 建议按照IT职能来划分用户组，将对应的员工加入与其职责匹配的用户组，以下为推荐的用户组划分方式：
   - 从资源运维和管理角度，需要遵守统一管理和运维的原则以提升效率。在运维监控账号内按照运维职责创建统一管理的用户组，包括计算管理组、存储管理组、网络管理组、数据库管理组等，这些用户组负责运维和管理所有账号的云资源，支撑上层应用系统的安全稳定运行。这些用户组可以通过跨账号委托（请参考跨账号委托授权章节）的方式去运维和管理其他账号下的资源，所以在业务账号下一般不用再创建资源运维和管理的用户组。
   - 从安全防护角度，需要遵守统一安全管控的原则。在安全运营账号下创建安全管理组，一方面管理和维护安全运营账号内的安全云服务，另一方面通过跨账号委托去管理和维护部署在其他账号内的安全云服务。
   - 从应用开发角度，在DevOps账号中按照不同的应用系统创建独立的应用开发组或应用测试组，这些用户组可以通过跨账号委托访问业务账号下的开发环境或测试环境的云资源。
   - 从项目管理角度，每个企业项目都应该在华为云上创建一个项目管理组，其成员是项目经理、系统管理员，可以管理该企业项目内的所有资源，包括生产环境、开发环境和测试环境的全部资源。
   - 从财务管控角度，需要遵守统一财务管控原则，在主账号中设置一个财务管理组，负责统一管控该账号下所有组织层级和企业项目在华为云上的消费，并进行成本分析和成本优化。
   - 从全局IT治理角度，需要在主账号中设置一个IT治理组，用于创建和管理组织单元和子账号，并为其创建和管理组织策略，限定子账号的权限上限。
   - 从合规审计角度，需要遵从统一的企业合规要求，在日志账号下创建设置一个合规审计组，负责监控该账号下的资源、用户、权限和操作等是否满足企业的安全合规要求，并设计优化措施。
   - 建议为外来访客或只希望查看云资源的用户设置一个只读用户组。
5. 遵守最小授权原则，只授予用户组完成职责所需的最小权限，如果用户组的职责产生变化，应该及时调整用户组的权限。按照最小授权原则，优先在企业项目中对用户组进行授权，如果确实需要针对账号内所有区域或特定区域的所有资源进行统一授权，则可以使用IAM项目进行授权，避免在各个企业项目中逐一授权，简化授权操作。
6. 在企业项目中授权时，建议按照用户组而不是用户进行授权，简化授权操作。
7. IAM账号管理员（与IAM账号同名）的权限很大，建议不要直接使用IAM账号管理员访问华为云，而是创建一个IAM用户，并按照最小授权原则授予相应的权限，以使用该IAM用户代替IAM账号管理员进行日常管理工作，保护IAM账号的安全。

用户组规划

1. 基于上述原则，针对Landing Zone的各类账号规划以下用户组，按照最小授权原则在华为云上为这些用户组配置对应的云服务访问权限。企业自己的身份管理系统的用户组逐一映射到华为云上的这些用户组，即可拥有对应的云服务访问权限。

版权所有 © 华为技术有限公司

图 3-15 Landing Zone 用户组规划



2. 上述各个用户组的职责范围和权限配置建议如下表所示：

表 3-1 IT 职能账号的用户组划分

用户组	账号	职责和资源管理范围	推荐的权限
admin	每个账号	该用户组是默认生成的，拥有所有操作权限。该用户组不需要创建，也不能被删除。通常将账号所关联的组织单元的负责人加入到该组	该用户组默认具备了所有操作权限，无需手动设置该用户组的权限
计算管理组	运维监控账号	该组成员负责统一管理和运维所有的计算资源，包括云主机、物理机、K8S容器引擎、虚拟机镜像、函数工作流等，可以设置自动弹性伸缩策略	ECS FullAccess BMS FullAccess AutoScaling FullAccess IMS FullAccess CCE FullAccess CCI FullAccess FunctionGraph Administrator Agent Operator Ticket Administrator
存储管理组	运维监控账号	该组成员负责统一管理和运维所有的存储资源，包括云硬盘、对象存储、弹性文件系统等；同时负责管理备份容灾资源，如云备份、存储容灾服务等	EVS FullAccess OBS Administrator SFS FullAccess SDRS Administrator CBR FullAccess DSS FullAccess Agent Operator Ticket Administrator

版权所有 © 华为技术有限公司

用户组	账号	职责和资源管理范围	推荐的权限
网络管理组	网络运维账号， 运维监控账号	该组成员负责统一管理和运维所有的网络资源，包括ER、VPC、弹性负载均衡、VPN、云专线、DNS、NAT等	VPC FullAccess ELB FullAccess NAT FullAccess VPN Administrator DNS FullAccess VPCEndpoint Administrator Direct Connect Administrator CDN Administrator Agent Operator Ticket Administrator
安全管理组	安全管理账号， 运维监控账号	负责统一管理和运维所有安全云服务和资源，如应用防火墙、DDoS高仿、主机安全、数据库安全、数据加密、容器安全、云审计等	Anti-DDoS Administrator CAD Administrator VSS Administrator HSS FullAccess DBSS Security Administrator KMS Administrator WAF FullAccess SCM FullAccess CGS FullAccess SA FullAccess CBH FullAccess Agent Operator Ticket Administrator
数据库管理组	运维监控账号	该组成员负责统一管理和运维所有的数据库相关的云资源和服务，包括RDS、文档数据库、数据复制服务、数据管理服务、分布式数据库中间件等	RDS FullAccess DDS FullAccess DRS Administrator DAS Administrator DDM FullAccess Agent Operator Ticket Administrator

版权所有 © 华为技术有限公司

用户组	账号	职责和资源管理范围	推荐的权限
中间件管理组	运维监控账号	该组成员负责统一管理和运维所有的中间件相关的云资源和服务，包括微服务引擎、分布式缓存、分布式消息、API网关、ServiceStage、区块链等	ServiceStage FullAccess CSE FullAccess DCS FullAccess DMS Administrator SMN Administrator APIG FullAccess BCS Administrator Agent Operator Ticket Administrator
数据处理组	数据平台账号	该组成员负责统一管理和运维所有的大数据及AI云资源及服务，包括MapReduce、数据仓库、数据湖、实时流计算、图引擎、推荐系统、ElasticSearch、表格存储等	ModelArts FullAccess MRS FullAccess DWS FullAccess DLI Service Admin DGC Administrator GES FullAccess Elasticsearch Administrator DIS Administrator CS FullAccess CloudTable Administrator DLF FullAccess RES FullAccess Ticket Administrator
合规审计组	日志账号	该组成员负责云审计日志的管理、资源合规信息的管理以及所有云服务的安全配置信息的查阅等	CTS Administrator LTS FullAccess RMS FullAccess Agent Operator Ticket Administrator
日志分析组	日志账号	该组成员负责统一搜索、查看和分析各种日志数据	LTS FullAccess OBS Administrator Ticket Administrator
财务管理组	主账号	该组成员负责账号内的统一财务管理，包括管理发票、管理订单、管理合同、管理续费、查看账单等权限。不能购买和操作云资源。	BSS Finance Ticket Administrator

版权所有 © 华为技术有限公司

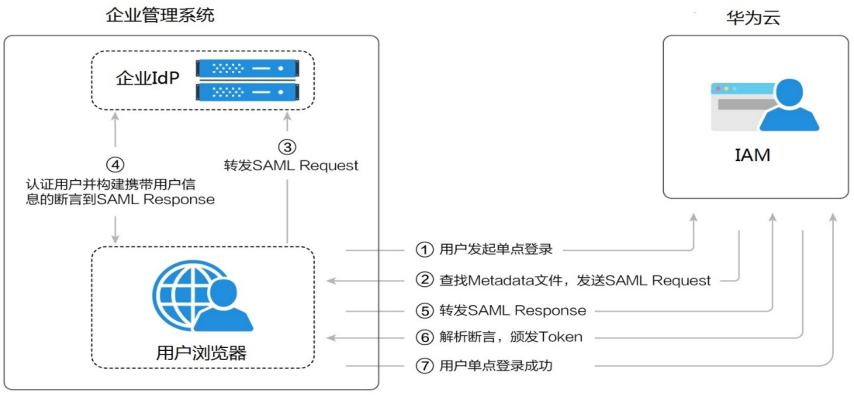
用户组	账号	职责和资源管理范围	推荐的权限
IT治理组	主账号	该组成员负责统一创建和管理组织单元和子账号，并为其创建和管理组织策略	BSS Administrator Ticket Administrator
只读用户组	每个账号	该组成员只能访问指定的单个或多个企业项目的资源，如外来访客或者外部审计人员可以加入到该组	Tenant Guest IAMReadOnlyAccess
公共服务管理组	公共服务账号	该组成员负责管理所有的公共服务和资源	部署了哪些公共服务，就授予对应云服务的FullAccess权限。
项目管理组	业务账号	该组成员全权管理项目下的所有资源，包括对企业项目本身进行管理	建议设置所参与企业项目内所有云服务的FullAccess权限
应用开发组	DevOps账号	该组成员负责管理所参与开发的应用系统在开发环境的云资源	建议设置所参与应用系统在开发环境的所有云服务的FullAccess权限
应用测试组	DevOps账号	该组成员负责管理所参与测试的应用系统在测试环境的云资源	建议设置所参与应用系统在测试环境的所有云服务的FullAccess权限

联邦认证

1. 华为云建议使用企业自己的身份管理系统（如Azure AD等）作为IdP（Identity Provider）与华为云IAM进行联邦身份认证，前者的用户通过SSO（Single Sign-on）登录到华为云控制台进行操作。联邦认证的最佳实践如下：
   - 所有需要进行日常云上运维操作的用户均建议通过集中的联邦认证系统认证后，方允许访问云控制台。
   - 每个用户的密码必须受到强有力的安全措施的充分保护，建议在联邦认证系统上实施包括密码长度、密码复杂度、密码重置策略和增强的身份验证方法（多因素身份验证），访问IP白名单等安全策略。
   - 用户在云上的操作权限通过云用户组进行定义，并通过身份转换规则映射到联邦认证系统上的用户相关属性（例如组、角色或职责等）。
   - 建议使用用户在联邦认证系统中唯一且不变的属性作为映射字段，避免变更后对云上资源使用和审计的影响。
2. 华为云IAM服务的“身份提供商”提供对SAMLv2协议（包括IDP-initial和SP-initial两种模式）的支持，且采用一种称为“虚拟用户SSO”的实现机制：
   - 将经过联邦认证系统认证后的用户映射到华为云的一个虚拟用户上，该虚拟用户仅在本次登录会话中按需创建，会话退出后即被销毁。
   - IAM提供身份转换规则机制，由客户的安全管理员编写规则，将每个联邦用户的属性映射到虚拟用户会话中的显示用户名和IAM用户组。
   - IAM基于虚拟用户会话的显示用户名+租户ID来生成唯一的user id，用于支持用户审计。

版权所有 © 华为技术有限公司

图 3-16 联邦认证流程



3. 身份转换规则的典型例子：
   - 在IdP侧和华为云侧分别创建同名的用户组，在IdP侧将用户归集到对应的用户组，在华为云IAM为用户组设置相应的权限。
   - 使用联邦用户的First Name和Last Name属性值作为虚拟用户的显示用户名，且格式为{LastName} {FirstName}。
   - 使用联邦用户的Group属性值映射到IAM的已创建的同名用户组，例如果Group属性值为admin，则该联邦用户访问云控制台后，即对应华为云IAM的admin用户组的权限。

版权所有 © 华为技术有限公司

图 3-17 身份转换规则的典型例子

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0} {1}"
                    }
                },
                {
                    "group": {
                        "name": "{2}"
                    }
                }
            ],
            "remote": [
                {
                    "type": "FirstName"
                },
                {
                    "type": "LastName"
                },
                {
                    "type": "Group"
                }
            ]
        }
]
```

4. 关于如何使用Azure AD建立与华为云的联邦认证，请参考 **https://bbs.huaweicloud.com/blogs/212731**

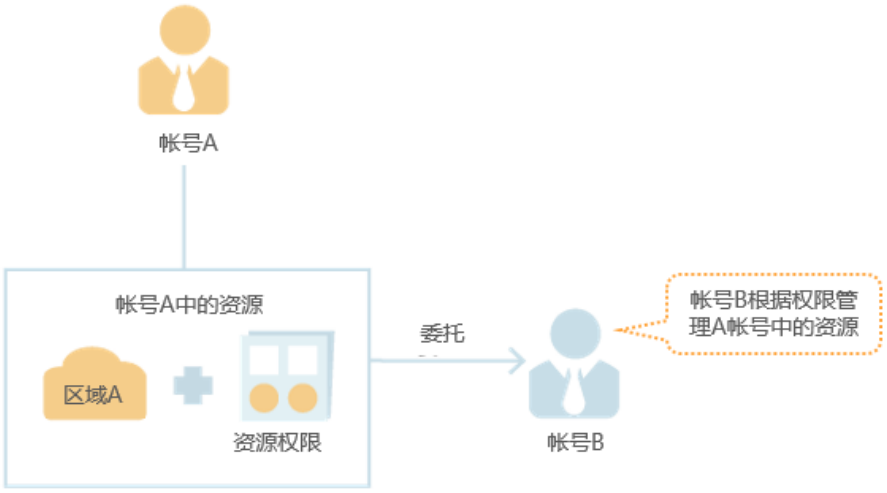
跨账号委托授权

在Landing Zone的多账号运行环境中，通常会涉及不同账号间的资源互访诉求，特别是针对安全运营、运维监控等账号下的用户需要跨账号访问其他子账号下的资源。在华为云上使用跨账号委托的机制来满足该诉求。委托时的最佳实践如下：

- 委托是基于账号间的信任。被委托方建议通过权限管控，授权云用户去使用委托，而不是允许所有云用户都可以使用委托方创建的委托。
- 建议对委托实施最小授权原则。
- 委托的配置过程如下：
  a. 账号 A 在其IAM中创建一个委托将资源访问权限委托给账号B

版权所有 © 华为技术有限公司

图 3-18 委托的配置 1



b. 账号B再将被委托的资源访问权限授予本账号的IAM用户，由后者管理账号A中的资源。

图 3-19 委托的配置 2

图 3-20 权限授予的例子如下

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Action": [
                                "iam:agencies:assume"
                        ],
                        "Resource": {
                                "uri": [
                                        "/iam/agencies/b36b1258b5dc41a4aa8255508xxx..."
                                ]
                        },
                        "Effect": "Allow"
                }
        ]
}
```

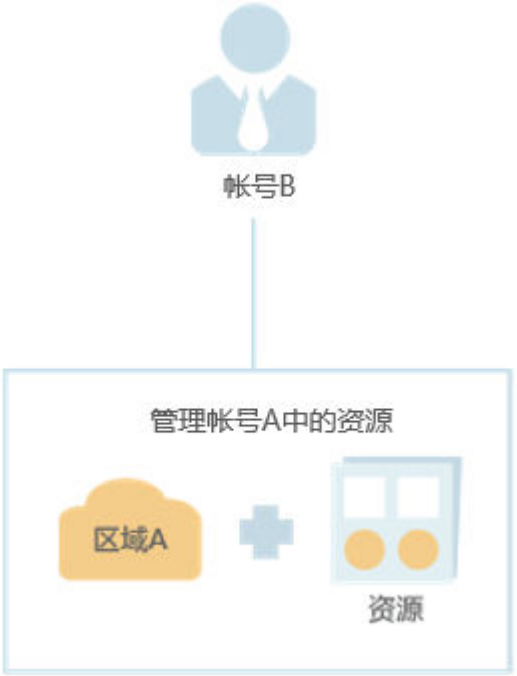
注意

用你获得的委托IP替代上面的字符串“b36b1258b5dc41a4aa8255508xxx...”，其他的地方不要修改。

c. 账号 B 或者被授权的用户切换角色到账号A，即可访问和管理账号A的资源。

版权所有 © 华为技术有限公司

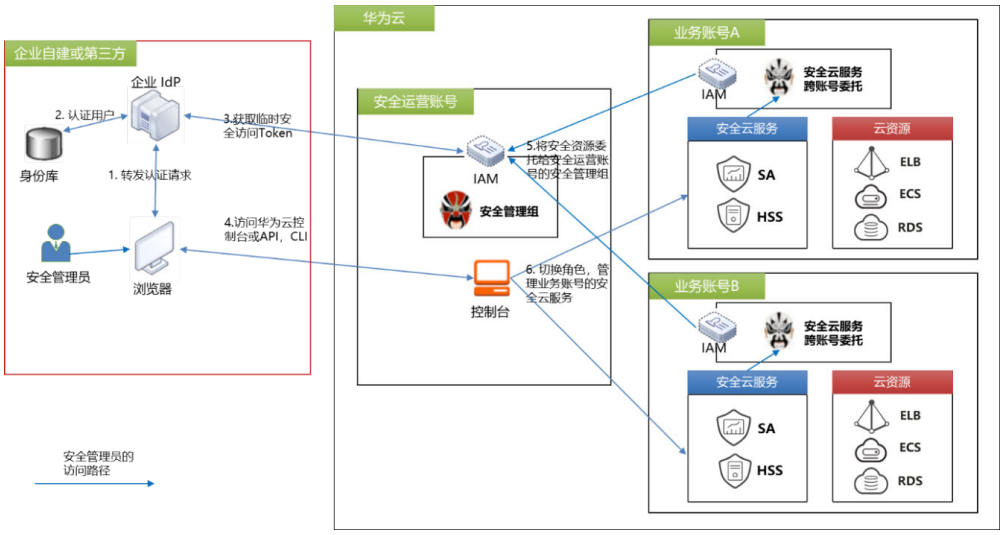
图 3-21 委托的配置 4



典型场景

1. 在Landing Zone参考架构中，专门设计了一个安全运营账号，用于统一管理企业范围内多个账号的安全资源和服务，这就需要跨账号访问部署在其他业务账号下的安全服务，比如SA、HSS等，通过以下联邦认证和跨账号委托的方式可以实现该目标。首先安全管理员通过SSO登录到安全运营账号的控制台，再通过切换角色到业务账号，然后访问和管理业务账号的安全云服务。

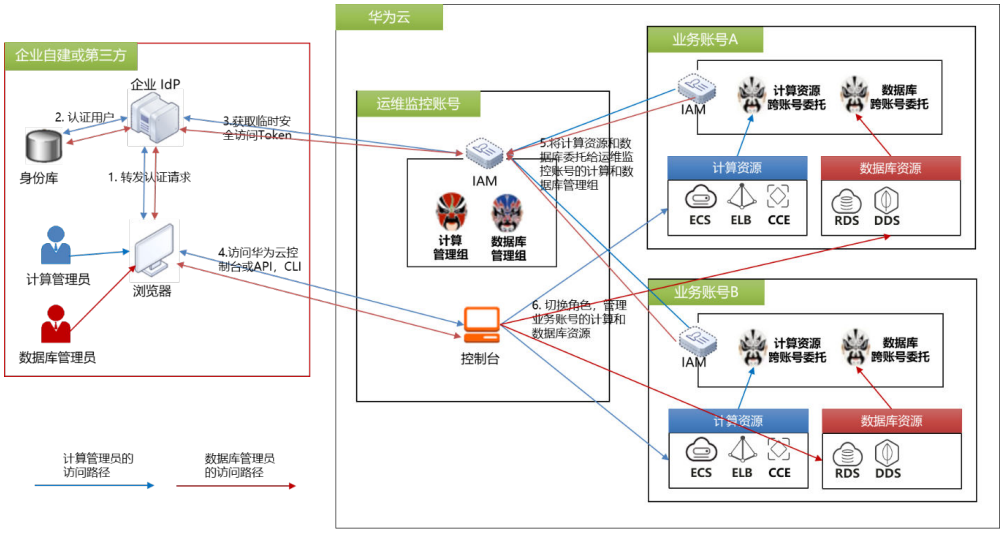
   图 3-22 安全运营账号统一管理多个业务账号的安全云服务



2. 另一个类似的场景是运维监控账号需要统一监控和运维企业范围内多个账号的资源，这也要求运维监控账号能够跨账号其他访问账号下的资源，通过以下联邦认证和跨账号委托的方式可以实现该目标。

版权所有 © 华为技术有限公司

图 3-23 运维监控账号统一管理各业务账号的云资源



3.5 资源治理

根据Landing Zone的参考架构，设计多账号下的资源治理方案，包含资源共享、资源标签、资源命名规范、资源管理、配额管理、镜像管理等。

资源治理原则

华为云基于大量成功交付的项目，总结提炼了以下资源治理原则：

1. 使用企业项目而不是IAM项目进行资源的分组和管理，企业项目可以跨区域管理资源，支持资源的迁入迁出、资源的成本核算及分析，比IAM项目更灵活，更能满足企业的项目管理需求。
2. 针对每个企业项目，按照职责分别创建不同的用户组，如应用开发组、应用测试组和应用管理组、项目管理组等，并授予相应的权限；为每个项目成员在华为云上创建一个用户，并加入到对应的用户组。
3. 每个账号下创建一个公共项目，或者使用默认企业项目default，用于包含以下公共资源，供其他企业项目共享使用：
   - 成本很难分摊到其他企业项目的公共云资源，如共享带宽、云连接等
   - 账号范围内应该统一管理的云资源，如云备份、VPC等
   - 大量购买时更加优惠的资源套餐包，建议在账号范围内统一订购，而不是为每个企业项目单独订购
4. 部门（对应到华为云上的组织单元和子账号）作为独立核算的单元，不建议部门之间共享使用任何云资源，即使这两个部门是父子关系；但一个部门内的多个IT项目可以共享使用云资源，如共享带宽、云连接等。
5. 针对每个账号提供多种运行环境：生产环境、开发环境、测试环境，各个环境之间需要有一定的安全隔离措施，可以通过VPC建立隔离的运行环境。多个小应用系统可共享一个VPC，大型应用系统可以独占一个VPC。

版权所有 © 华为技术有限公司

表 3-2 运行环境

运行环境名称	运行环境描述
生产环境	部署核心生产系统，如ERP、PLM、SCM等，以及数据仓库及大数据系统，大的应用系统（如大型ERP系统）可以独占一个生产环境。核心生产环境的重要性高，可用性和数据安全要求高，需要建立严格的容灾备份机制和数据安全保护体系。
开发环境	部署开发系统，如Devops流水线、源代码管理系统等，开发环境的可靠性要求不高，对网络安全和数据安全要求也不高，酌情提供一定的数据备份和数据安全保护措施。在中小企业，开发环境可与测试环境合并。
测试环境	部署测试系统和准生产系统，测试人员在该环境完成系统上线之前的功能测试、性能测试、安全测试和集成测试等测试工作。测试环境的可靠性要求不高，对网络安全和数据安全要求也不高，酌情提供一定的数据备份和数据安全保护措施。在中小企业，开发环境可与测试环境合并。

6. 规划VPCDMA网络段的时候，需要考虑VPC之间的通信交互，如果两个VPC之间需要进行通信，这两个VPC的网段就不要互相冲突；有频繁交互关系的VPC尽量创建在同一个区域内，否则跨区域的VPC通信需要额外购买带宽包。
7. 定期（月度、季度、年度）统计分析各个组织单元、企业项目的资源利用率，及时发现资源空转、资源利用率低的情况，并及时删除空转资源、进行资源整合。
8. 为防止资源滥用，要限定账号（主账号和各个子账号）在华为云上各服务资源的配额，对该账号下用户所能申请的资源数量和容量做限制。

资源共享

基于公共服务账号，梳理可以共享给其他账号的公共资源，比如NTP服务器、AD服务器、自建DNS服务器、OBS桶、IMS私有镜像、SWR容器镜像库、协作办公系统等。

资源管理

在安全审计账号中，可以对整个组织的合规遵从进行统一管理，包括将多账号的资源配置快照归档到统一的桶中，管理员统一配置组织下各子账号的合规规则。

1. **统一合规策略配置**
   - RMS服务提供资源合规特性，帮助您快速创建一组合规规则，用于评估您的资源是否满足合规要求。
   - 在组织多账号场景下，当需要配置多个组织账号下的合规规则时，可以将多个子账号的合规规则设置API的访问权限委托给根账号。
   - 通过调用API的方式，使用根账号获取IAM token后，逐个调用子账号的API配置合规规则。
2. 多**账号的资源配置快照统一存储**
   - RMS服务支持每个账号在开启资源记录器并成功配置对象存储桶（OBS）后，RMS会定期（24小时）对您的资源进行快照并存储。
   - 在组织多账号场景下，当需要获取多个组织账号下的资源配置快照数据时，可先针对每个账号开启资源记录器，配置自己的对象存储桶（OBS）。再对每个桶配置根账号只读权限。

版权所有 © 华为技术有限公司

- 通过调用API的方式，使用根账号获取IAM token后，逐个访问子账号的OBS桶获取资源快照文件

资源标签

华为云的标签是由用户定义的键和值组成，标签可以更灵活地帮助用户管理资源，包括识别、搜索筛选等。

1. 在为华为云资源创建标记策略时，华为云有以下建议：
   - 请勿在标签中存储个人身份信息或其他机密或敏感信息
   - 对标签使用标准化的区分大小写格式，并跨所有资源类型一致地应用该格式
   - 虽然标签有长度规格上限，尽量不要每个标签都达到标签规格上限，标签长度能标明含义即可
   - 需要提前考虑规划好支持多种用途的标签准则，如管理资源访问控制、成本跟踪、自动化和组织
2. 标签命名限制和要求
   - 每个资源最多可以有 20 个用户创建的标签。注意：以 _sys_开头的系统创建标签将保留供华为云系统使用，并且不计入此限制
   - 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值
   - 标签键必须包含 1 到 128 个 Unicode 字符，并且以 UTF-8 格式表示
   - 标签值必须包含 0 到 255 个 Unicode 字符，并且以 UTF-8 格式表示
   - 标签键和值区分大小写。最佳实践是，决定利用标签的策略并在所有资源类型中一致地实施该策略。例如，决定是使用 HuaweiCloud、huaweicloud 还是 Huaweicloud，应保持相同的规则。避免含义模糊的标签出现
3. 常见标签策略
   - **资源治理标签**：用户可以配置标签来与资源一起显示，并且可以按标签进行搜索和筛选。使用TMS服务，用户可以按资源类型，标签范围过滤资源，给多个资源批量标记标签
   - **成本标签**：华为云的费用中心->成本中心可让用户在使用标签标识和管理资源的同时，还可以将标签激活为成本标签来归集成本。成本标签可以应用在成本分析和预算管理中
   - **自动化标签**：资源或特定于服务的标签通常用于在自动化任务时做资源过滤筛选。自动化标签用于选择加入或退出自动化任务，或识别要存档、更新或删除的资源的特定版本。例如，用户可以运行自动化脚本，这些脚本可在非工作时间内关闭开发环境以降低成本。在这种场景，可以通过给ECS服务的虚拟机资源标记标签标明是否需要被关闭虚拟机
4. 通过标签分析成本
   - 登录“成本中心”。
   - 选择“成本标签”。
   - 选中标签，进行激活或取消激活操作。

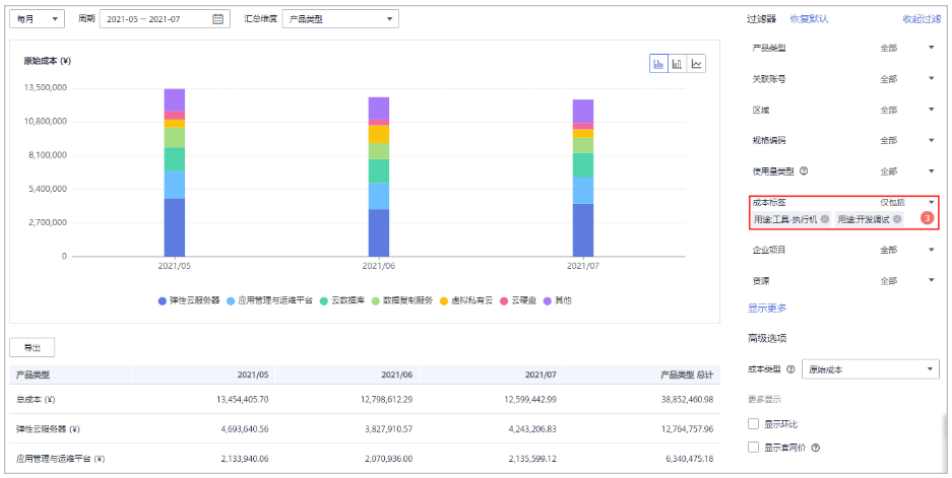
版权所有 © 华为技术有限公司

图 3-24 标签分析成本

- 登录华为云控制台，进入成本中心。
- 选择“成本分析”。
- 通过成本标签进行成本数据筛选。

图 3-25 通过成本标签维度进行成本数据汇总

图 3-26 通过成本标签进行成本数据过滤



镜像管理

1. 虚拟机镜像管理

   企业可以通过镜像导入或者公共镜像创建自己的私有镜像，然后将私有镜像共享给其他应用账号使用。

版权所有 © 华为技术有限公司

2. 公共镜像

企业可以通过公共镜像作为应用的基础镜像。通过公共镜像在创建出虚拟机后，用户可以根据安全和业务要求，在镜像里进行基础的业务配置或者安全配置。配置完成后，可以通过虚拟机创建私有镜像。

- 华为云公共镜像中提供了多种类型开源版公共镜像：

表 3-3 多种类型开源版公共镜像

CentOS	64bit：CentOS 6：6.10/6.9/6.8/6.5/
	64bit：CentOS 7：7.9/7.8/7.7/7.6/7.4/7.3/7.2
	64bit：CentOS 8：8.2/8.1/8.0
Ubuntu	64bit：Ubuntu 20.04/18.04/16.04
Debian	64bit：Debian 8：8.8.0
	64bit：Debian 9：9.0.0
	64bit：Debian 10：10.0.0
	64bit：openSUSE Leap 15： 15.0
CoreOS	64bit：CoreOS 2079.4.0
FreeBSD	64bit：FreeBSD 11.0
openEuler	64bit：openEuler 20.03

- 在市场镜像中，可以选择商用版linux和windows镜像：

表 3-4 商用版 linux 和 windows 镜像

windows	Windows Server 2012 Standard/Datacenter
	Windows Server 2012 R2 Standard/Datacenter
	Windows Server 2016 Standard/Datacenter
	Windows Server 2019 Standard/Datacenter
suse	64bit：SLES 12：12 SP5
	64bit：SLES 15：15 SP1

3. 镜像导入

如果客户使用的镜像超出华为公共镜像范围，可以使用IMS服务，进行镜像导入，目前IMS支持系统盘、数据盘和ISO镜像导入能力；支持vhd、zvhd、vmdk、qcow2、raw、zvhd2、vhdx、qcow、vdi或qed格式镜像文件创建私有镜像

版权所有 © 华为技术有限公司

图 3-27 镜像导入

4. 镜像创建
   - 可以通过IMS服务创建系统盘、数据盘、整机镜像，创建完成后，镜像可用于复制、共享可以直接登录IMS Console操作。
   - 为便于用户定制化操作，可以Packer创建私有镜像：

     图 3-28 Packer 创建私有镜像

   - 使用Packer创建镜像，需要一个json格式的模板文件。在模板文件中，您需要指定构建器、配置器，还可以指定后处理器。在配置器中，您可以指定对源镜像的任何操作，可以指定安装软件也可以对相关配置做修改。

```
{
"builders": [{
"type": "openstack",
"identity_endpoint": "https://iam.xxx.com/v3",
"tenant_name": "xxx",
"domain_name": "domain_name",
"username": "username",
"password": "password",
"ssh_username": "root",
"region": "xxx",
"image_name": "Ubuntu-image-updating-powered-by-Packer",
"instance_name": "Ubuntu-image-updating-powered-by-Packer",
"source_image": "f1dd2272-7041-479e-9663-646632b6ac00",
"availability_zone": "xxx",
"flavor": "s3.medium.2",
"use_blockstorage_volume": true,
"networks": ["11d661c4-e41f-487f-a6f6-9b88d623dd5d"],
"floating_ip": "8f686f9a-3408-4fdd-be75-ea768065800c"
}],
"provisioners": [{
"inline": [
"apt-get update -y"
],
"inline_shebang": "/bin/sh -x",
"type": "shell",
"skip_clean": true
}],
"post-processors": [{
"strip_path": true,
"output": "packer-template-ubuntu-updating-result.log",
"type": "manifest"
}]
}
```


版权所有 © 华为技术有限公司

- 其中：tenant_name、region、availability_zone、flavor、networks、floating_ip均为创建私有镜像时使用的云服务器的属性信息

5. 镜像共享

用户A获取用户B的项目ID之后，可以将指定的私有镜像共享给用户B。共享镜像可以分为批量镜像共享和单个镜像共享两种方式，用户可以按照需要进行选择。注意：共享镜像前，请确认私有镜像已清除敏感数据和文件。

图 3-29 共享镜像

资源命名规范

本章节提供了关于云上资源统一命名的参考。命名约定的使用，对客户在高效管理云上资源上非常重要。制定标准和一致的命名规范，能使客户在云上资源的成本分析、自动化、安全控制等方面的管理更加清晰和便捷。

1. **命名原则：**
   - 命名规则是可扩展的
   - 确保在一定范围内的命名是唯一的
   - 通过资源命名便于分类，譬如为监控、安全控制等提供可见性

表 3-5 计算资源命名规范

华为云资源	资源名规范	Example	Comment
ECS	ecs-{appname}-{apptype}-{env}	ecs-adv-app-dev ecs-adv-cache-prod	名称的长度为1～64位字符；支持中文字符、英文字母、数字及“_”、“-”、“.”。

版权所有 © 华为技术有限公司

华为云资源	资源名规范	Example	Comment
Image	Img-{appname}-{apptype}-{env}	ims-adv-app-dev	名称的长度为1～128位字符；支持中文字符，英文字母，数字，特殊字符包含“_”、“-”、“.”、空格。名称的首尾字母不能为空格。
EVS	disk-{appname}-{env}	ims-adv-dev	名称的长度为1～255位字符；支持中文字符，英文字母，数字，特殊字符包含“_”、“-”、“.”、空格。
Snapshot	ss-{appname}-{env}-{datagenerated}	ss-adv-dev-20220101	名称的长度为1～255位字符；支持中文字符，英文字母，数字，特殊字符包含“_”、“-”、“.”、空格。
AutoScaling	as-{appname}-{env}	as-adv-dev	名称的长度为1～64位字符，只能包含中文、字母、数字、“_”、“-”。

表 3-6 网络资源命名规范

华为云资源	资源名规范	Example	Comment
VPC	vpc-{appname}-{env}	vpc-adv-dev	名称的长度为1～64位字符，只能包含中文、字母、数字、“_”、“-”、“.”。

版权所有 © 华为技术有限公司

华为云资源	资源名规范	Example	Comment
Subnet	sn-{appname}-{env}-{SubnetType}	sn-adv-dev–db	● 1、子网类型：、app、elb、db、cache、web ● 2、名称的长度为1～64位字符，只能包含中文、字母、数字、“ ”、“_”、“-”、“.”。
ELB	elb-{appname}-{env}	elb-adv-dev	名称的长度为1～255位字符，只能包含中文、字母、数字、“ ”、“_”、“-”、“.”。
EIP	eip-{appname}-{env}	eip-adv-dev	名称的长度为1～64位字符，只能包含中文、字母、数字、“ ”、“_”、“-”、“.”。
NAT	nat-{appname}-{env}	nat-adv-dev	名称的长度为1～64位字符，只能包含中文、字母、数字、“ ”、“_”、“-”、“.”。

版权所有 © 华为技术有限公司

表 3-7 存储资源命名规范

华为云资源	资源名规范	Example	Comment
OBS	obs-{ appname}-{env}	obs-logs-dev	1、名称的长度为1～64位字符，只能包含中文、小写字母、数字、“-”、“.” 2、禁止两个英文句号（.）相邻，禁止英文句号（.）和中划线（-）相邻，禁止以英文句号（.）和中划线（-）开头或结尾 3、禁止使用IP地址 4、如果名称中包含英文句号（.），使用虚拟主机方式HTTPS访问OBS，会导致证书校验失败

3.6 安全合规

3.6.1 企业上云面临的安全风险

1. 企业上云的安全风险是被提及最多，也是顾虑最多的点。自有IT产业以来，如下风险就被广泛讨论：
   - **挑战1：如何满足内外部监管机构的合规要求**

     随着网络数字空间的逐步发展，各区域、国家、行业的法律法规如GDPR、网络安全法逐步明确，无意识的违规轻则引起整改问责、重则涉及高额罚款。均会对企业业务开展带来较高风险。
   - **挑战2：如何构建一套全方位、全体现的安全运营系统，保障业务的SLA达成**

     网络攻击行为在过去数年发生了巨大的改变，传统以破坏系统为主的网络攻击行为，发展到现阶段将DDoS攻击、加密、撞库/搬库的技术用于勒索和灰色产业对抗的经济目的，更要求企业构建一套健全的安全运营系统，以保证系统的网络运营正常和业务安全。
   - **挑战3：如何兼顾安全和业务的效率**

     传统IT建设过程中，企业往往将安全作为独立的体系构建。安全、合规部门通过规范流程、部署安全防护设备等方法对业务进行保护。在此过程中，安全、合规部门对业务的理解有一定的局限性，导致安全容易被视为是业务快速发展的瓶颈。
2. 同时应该意识到，随着云时代的到来，计算、存储、网络、大数据技术的云化方案成熟，企业又面临了新的安全挑战。

版权所有 © 华为技术有限公司

- **云上挑战1：安全技术如何快速适配业务的弹性扩缩**

  在过去，企业进行IT建设时，往往按照业务最大值计算服务器的建设规模。而云技术的到来，让企业完全可以以最小成本开通业务，弹性伸缩的特征让企业无需过度担心业务高峰期到来时的资源瓶颈。那么在这种情况下，用传统的安全软件，很难同步匹配业务的快速扩缩容

- **云上挑战2：如何确保云服务、云资源的配置、策略安全**

  根据国内外调查，云上Top安全威胁中包括不安全的配置。因为云资源具备快速开通的特点，而且大多数云上应用采用DevOps开发，开发周期大量缩短。如果使用不安全的镜像、或云资源默认配置的访问权限过大都将产生严重后果。

- **云上挑战3：如何让安全能力在多团队共享和共建**

  传统企业安全部门和业务部门在技术上存在较厚的技术墙，双方在业务流上互相守护自己的业务范围，并不需要过多的共享。但是在公有云场景下，同一企业内不同系统的业务架构具备一定的相似性，甚至风险和消除风险的手段和云平台的方式都是类似的。那么这些技术是否可以共享?

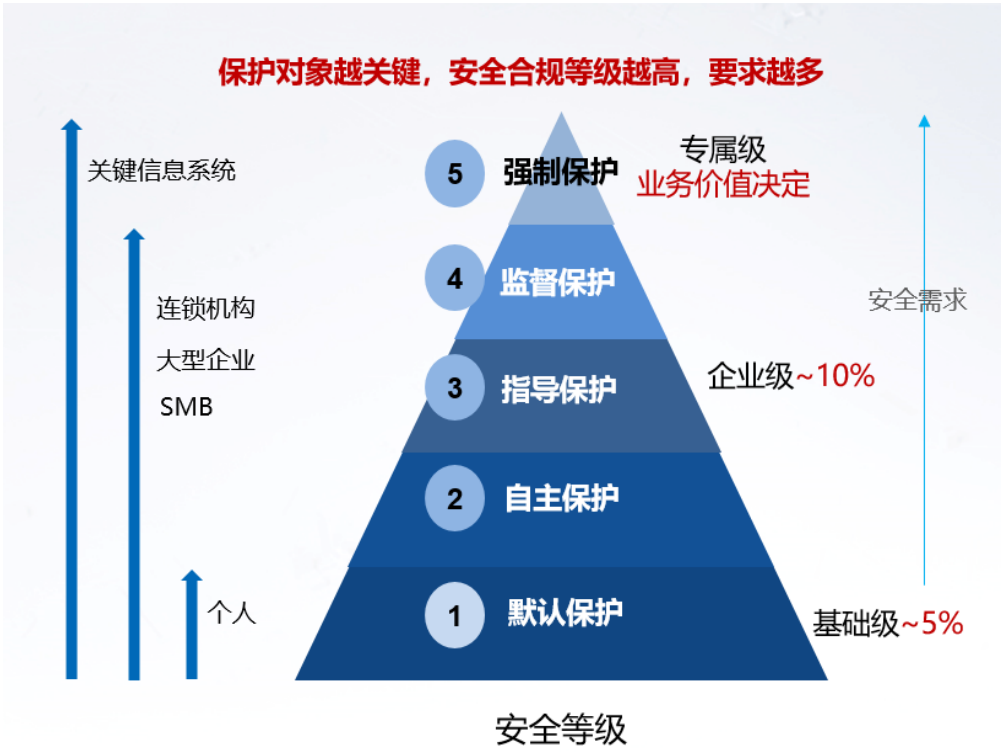
3.6.2 云上安全设计原则

原则 1：基于业务价值制定安全目标

1. 安全是一项系统工程，从建设成本和方案上看有较大的弹性空间。那么如何衡量安全、合规的投资预算呢?
   - 识别合规要求：华为云建议客户优先分析业务的合规要求，比如可以根据等级保护的规则匹配业务系统的安全等级，或和业务团队共同识别业务的行业要求（如支付行业需要满足PCI DSS的要求）。当明确了合规目标并根据合规目标实施的安全方案，可以初步的安全也业务价值相匹配。
   - 评估安全风险：在完成合规评估后，应从攻击者视角出发评估业务系统的安全性。在安全评估中，通过威胁分析来识别风险，并评估风险等级并制定消减措施。需要注意的是，在做风险接受是，应考虑当前的防御方案是否会让攻击者发起攻击的成本超过其获得的利益。如果上述假设不成立，则应该配置足够的安全服务产品，以提升攻击成功难度，降低系统被攻击的可能。
2. 华为云提供MDR（管理检测与响应）服务，MDR服务的安全评估服务可以帮助客户进行云上系统的安全风险评估，而MDR服务中的等保助手、密评助手等专项能力也可以帮助客户对业务系统进行安全方案的设计和改造。
3. 华为云建议客户在进行IT系统建设时，预留预算用于安全、合规方案的建设。一般性系统预留5%、面向互联网提供服务、易受攻击的系统，预算建议上升至15%。

版权所有 © 华为技术有限公司

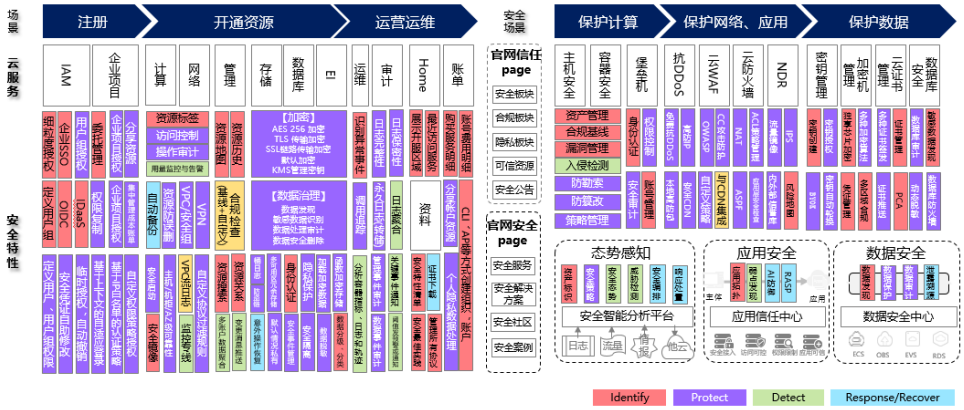
图 3-30 安全等级



原则 2：主动安全、默认安全

1. 安全是设计出来的。因此在业务安全设计时，华为云建议客户参考IPDRR模型（识别 Identity，防护Protect，检测 Detect，响应React，恢复Restore）来进行安全方案的设计。华为云各个云服务已实现超过387条安全特性，这些特性组合系统可以帮助客户在云上构建一整套安全架构。其中大多数安全特性是作为云服务的基础能力向客户提供的。

图 3-31 华为云服务安全特性清单



2. 通过分析云上安全事件，华为云发现大量的安全事件是由于不完善的资源配置导致的入侵和可靠性问题。因此在开通云服务、云资源时，应结合上图确认安全特性是否打开，如虚拟机镜像应完成安全加固并配置主机安全类服务产品，存储资源的ACL访问策略默认最小集合，数据资源使用KMS管理密钥、运维通道使用云堡垒机等。并定期使用安全服务对资源、账号进行扫描，利用安全基线进行比对以发现分析和不安全的配置。

版权所有 © 华为技术有限公司

3. 华为云态势感知服务SA、漏洞扫描服务VSS、管理检测与响应服务MDR均可提供自动化或人工的基线检查能力。

原则 3：最小化授权

1. 将企业内部组织、资源进行分组管理，并利用细粒度授权功能，对企业账号、资源、操作进行精细授权，尽量避免提供多个对象共享同一资源的场景，对资源访问的共享数量和使用尽可能最小化。
2. 企业云上基于企业项目的授权管理原则包括：
   - 企业客户在云上按自身组织或项目管理模式对云服务进行资源的分组和管理；针对公共资源管理，可以创建公共项目或者使用默认Default企业项目；
   - 针对每个企业项目，按照职责分别创建不同的用户组，并授予相应的权限；
   - 不建议直接使用IAM账号访问云，而是创建IAM用户，并授予用户管理权限，使用该IAM用户代替IAM账号进行日常管理工作，保护IAM账号的安全；
   - 遵守最小授权原则，只授予用户组完成职责所需的最小权限，如果用户组的职责产生变化，应该及时调整用户组的权限；

原则 4：云原生安全

1. 使用云服务场景多且复杂，与传统的企业IT和安全所要求的技能有很大的差别，如果不能掌握足够的技能，即使云服务供应商提供了全面的安全能力和服务，如果不能正确的配置使用或防护不全面，依然会让企业云上环境面临巨大的安全风险。
2. 云服务提供商通常都会提供面向IaaS资源和PaaS资源的安全类服务，比如Anti DDoS、WAF、主机防护、密钥管理等。这些服务展现出智能化、规程化、自动化、无码化的特征。在性能、弹性、兼容性上有较好的表现。同时，云服务提供商的安全运营经验也在持续的推动云原生安全服务的能力有针对性的增强，因此，对于基础安全方案，如保护业务系统的计算安全、存储安全、网络安全、数据安全、安全合规等应优先选择云原生安全服务

原则 5：持续合规、安全可视

1. 相对比传统IT系统的举证合规方案，云技术让持续合规、安全可视变为了可能。
2. 云上高性价比的存储方案，全方位的审计服务和AI的行为分析能大量的节约合规成本，合规报告自动生成，再也不用空出数月来完成大量的文档写作了。而标准化的日志结构、报表呈现，将AI技术应用到日志分析，能迅速发现并纠正违规行为，可显著提升企业的合规遵从度
3. 华为云安全治理云图Compass服务是一个自动化合规评估和安全治理平台，将华为积累的全球安全合规经验服务化，帮助客户快速实现云上业务的安全遵从，提升用户获得法规及行业标准的认证效率，实现持续合规

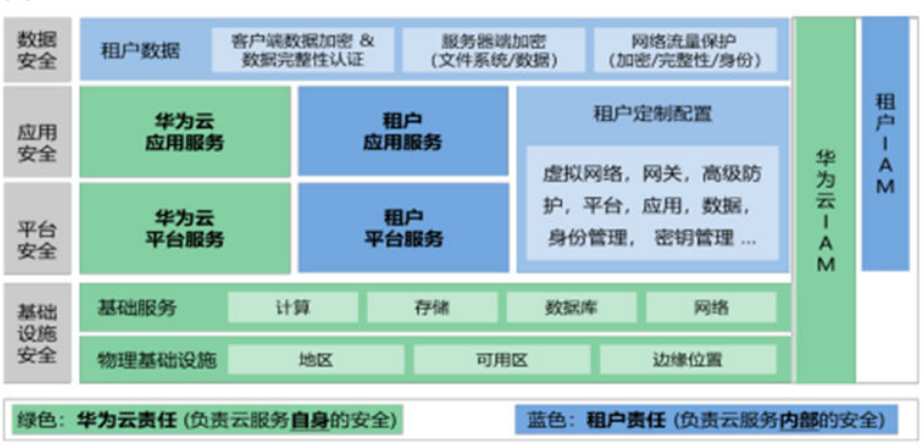
3.6.3 安全责任边界

1. 过去，企业在内部IT基础设施建设时，安全性问题需要企业自己负责。而当迁移到云端，云服务提供商和云消费者在安全性问题上发生了变化——云提供商和云消费者对云系统中的计算资源有不同程度的控制。与传统IT系统（一个组织控制整个计算资源堆栈和系统的整个生命周期）相比，云提供商和云消费者协作设计、构建、部署和操作基于云的系统。
2. 华为云作为国内进步最快的云厂商，在责任共担模型上也参考了业界最佳实践，并提出了自己的一些理解。如图所示，绿色部分由云厂商负责，蓝色部分由租户

版权所有 © 华为技术有限公司

负责。云提供商负责服务自身的安全，**提供安全的云**；租户负责云服务内部的安全，也就是**安全的使用云**。

图 3-32 华为云安全责任共担模型 来源：《华为云安全白皮》



3. 华为云作为云供应商，主要依据同客户签订的服务水平协议（Service Level Agreement，简称SLA）承担数据保护责任，负责协议中基础设施、平台或软件的安全。并且凭借自身的技术优势，为客户提供了一系列与数据保护相关产品及服务。
4. 华为云服务等级协议官网入口：**https://www.huaweicloud.com/declaration/sla.html**
5. 中国用户考虑使用责任共担模型时，在国内仍然普遍存在的监管要求的大环境下，首先应当考虑合规要求与责任共担模型的结合。
6. 最常见的情况是，企业安全主管必须考虑云计算环境下如何根据等级保护条例2.0进行定级。一般需要遵循如下的原则：
   - **将云平台作为基础设施，云租户企业业务系统作为信息系统分别定级**。即云平台由云服务提供商申请进行等级保护定级，云平台上的租户业务系统单独申报定级。例如业务系统备案后确认为三级系统，则租户侧的安全责任需要按照三级的要求来设计实施。
   - **云平台不承载高于其安全保护等级的业务应用系统。**公有云提供商一般有多个Region提供给租户，但是基本上普通的Region最高可以达到等保3级水平。假如某金融支付类业务系统，按照监管部门要求需要达到4级水平，则不能在普通的Region上面部署，必须在达到4级等保水平的特殊Region部署使用。云平台和租户参考责任共担模型分别履行4级等保水平的安全防护责任。
7. 根据公安部《信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求》，按照IaaS，PaaS，SaaS三个层次，管理要求和技术要求两个分类，等保标准就云服务商和云租户的责任进行了更为细致的梳理（见下表）：

版权所有 © 华为技术有限公司

图 3-33 基于等级保护三级的责任共担模型

安全要求	IaaS	PaaS	SaaS
第一部分 管理要求			
系统安全运维管理	双方共担	云服务商承担	云服务商承担
系统安全建设管理	双方共担	双方共担	双方共担
安全管理机构和人员	云服务商承担	云服务商承担	云服务商承担
第二部分 技术要求			
应用和数据安全	双方共担	双方共担	双方共担
设备和计算安全	双方共担	云服务商承担	云服务商承担
网络和通信安全	双方共担	云服务商承担	云服务商承担
物理和环境安全	云服务商承担	云服务商承担	云服务商承担

8. 云提供商的责任，可能由云自有团队提供技术、人员等手段满足，也可能委托授权给第三方安全运营，但责任仍然归属于云提供商。
9. 租户（云消费者）的责任，在大企业中，由于组织分工的不同，可能进一步细分为基础设施团队、应用团队、安全团队等来承担，但责任仍然归属于云消费者。

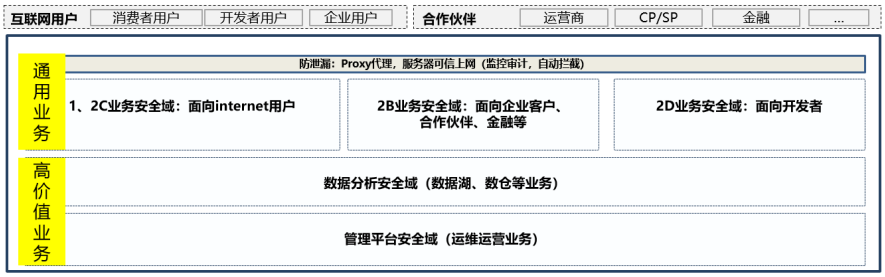
3.6.4 整体安全架构

1. **传统数据中心网络安全防护往往会面临如下困境：**
   - 1、业务场景复杂，受攻击面大
   - 2、过渡依赖网络边界防护，加密让入侵检测失效
   - 3、安全工程能力不足，应用安全先天不足
   - 4、漏洞层出不穷，无法及时修复
   - 5、内网一马平川，无险可守
2. **IT安全团队面临的挑战：**
   - 网络肯定会被攻破，一旦网络边界防护被突破，黑客在内网将畅通无阻，难以保障关键信息资产的安全和业务系统的稳定运行。
   - 传统IT安全严重依赖网络边界安全防护，想要完全据敌于国境之外是不太现实的。因此在安全设计上，要考虑局部业务被入侵后，不要造成全局性的安全影响。同时基于规则的静态防护措施，在面对动态的攻击时，迟早会被绕过。
3. **因此安全设计上建议如下：**
   - 建立纵深的防御体系，避免单层防线失效后攻击者畅通无阻，增加攻击者的成本，给安全监控响应团队赢得更多的响应时间；
   - 要加强安全态势感知能力，及时发现入侵风险，及时响应处置；
   - 建立分层分级的安全防护，识别核心数据、核心业务，针对性加强安全防护；
   - 假设内网是不安全的，对业务实施网络微分段隔离，当网络边界防护被突破时，可以有效将入侵的影响控制在局部，控制爆炸半径；
   - 对重要业务系统、核心数据要做好容灾备份，在遭受极端情况时，能够快速恢复业务；

版权所有 © 华为技术有限公司

- 在所有的安全防护措施中，网络的隔离和访问控制是最基础最有效的，建议业务上云过程中，利用云上虚拟网络技术，进行合理的网络安全域划分，对业务实施网络微分段隔离。
- 下面以两个具体的例子，介绍业务上云后网络安全域的规划设计，供参考。

图 3-34 XX 客户业务上云网络安全架构设计



安全设计目标

1. 防入侵：业务间隔离，防横向移动，防风险扩散
2. 防泄密：降低内部人员网络泄密风险，数据泄密可审计可追溯
3. 安全设计原则：
   - 区域治理：隔离不同业务属性的环境(如消费者、企业、开发者等)，支撑数据转移控制
   - 服务隔离：最小化攻击面，限制黑客横向移动范围，在最小范围遏制攻击者
   - 安全集成：互相隔离的服务间通过API、消息方式安全集成
   - 隐私遵从：云服务作为数据处理者和云服务作为数据控制者遵从隐私合规要求
   - 数据保护：降低内部人员泄密风险
4. **高价值服务区：**资产价值大（账号类、支付类、密钥类、批量用户数据存储）、或具备获取批量数据能力高权限（运营、运维）的服务，需要被重点保护。
5. **通用服务区：**对外部用户或者内部其他服务提供服务、且不涉及存储批量用户数据、资金处理、账号数据管理、密钥管理等的服务。

表 3-8 安全设计目标

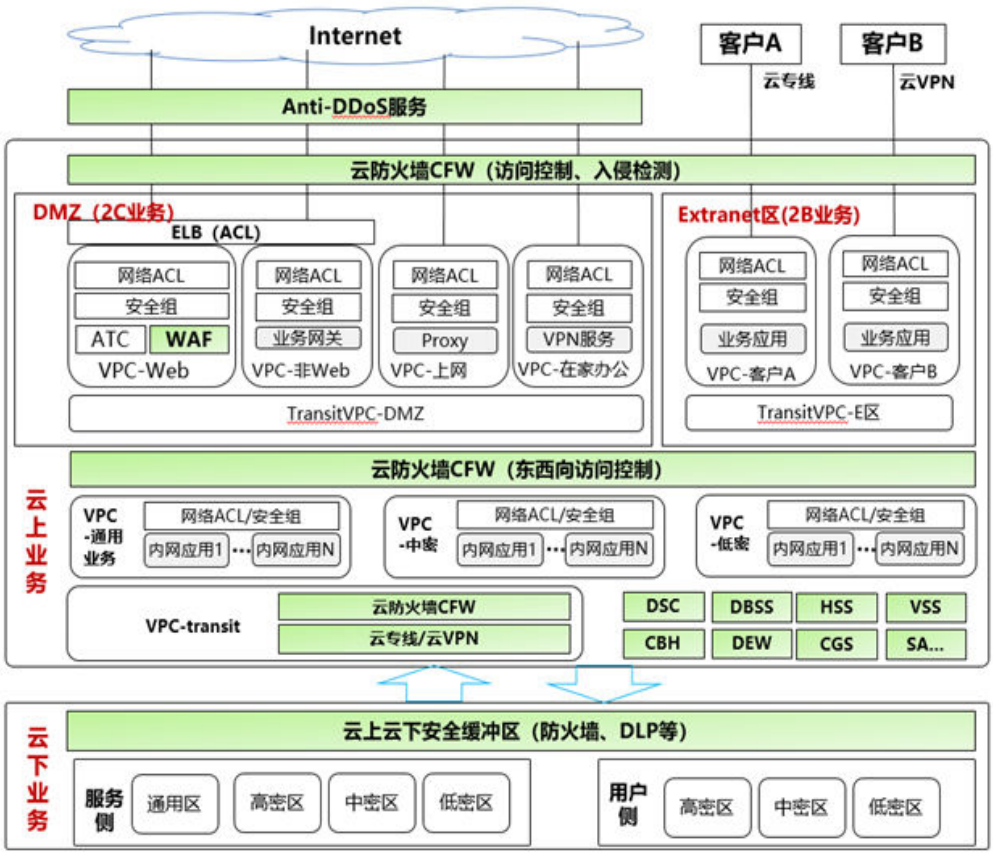
安全域	定义
2C业务安全域	面向internet用户提供服务，与2C、2D业务安全域默认网络隔离，可以从互联网访问
2B业务安全域	与合作伙伴、企业客户集成，与2C、2D业务安全域默认网络隔离，与伙伴、企业客户间通过专线、VPN等建立点对点的集成关系
2D业务安全域	为开发者提供服务，与2C、2B业务安全域网络隔离，可以从互联网访问
数据分析安全域	部署数据湖、数仓、大数据分析平台等业务，是数据的聚集地，与其它各安全域默认内网隔离，只能从企业内网访问

版权所有 © 华为技术有限公司

安全域	定义
管理平台安全域	为各安全域提供运维、运营平台，供研发、运营、运维人员开展运营运维活动的服务，只能从企业内网访问。

网络安全架构设计

图 3-35 网络安全架构设计



3.6.5 安全配置基线

1. 华为云安全提供态势感知服务来保护客户业务的安全合规，态势感知服务支持资源管理、威胁告警、漏洞管理、基线检查等多种功能。
2. 在安全运营账号中，业务账号的委托的态势感知将用于提供合规风险检查：
   - 基线检查：支持检测云服务关键配置项，通过执行扫描任务，检查云服务基线配置风险状态，分类呈现云服务配置检测结果，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。
   - 针对华为云服务关键配置项，您可以从“安全上云合规检查”、“等保2.0通用要求”、“护网检查”、“等保2.0扩展要求”四大风险类别，了解云服务风险配置的所在范围和风险配置数目。
   - 基线检查包括安全合规性检查、系统配置检查、账户检查和弱密码检查等规则。

版权所有 © 华为技术有限公司

表 3-9 服务器基线检查

检查项	说明
经典弱密码检测	通过与弱密码库对比，检测账号密码是否属于常用的弱密码。支持MySQL、FTP及系统账号的弱密码检测。
密码复杂度策略检测	检测系统账号的密码复杂度策略。
配置检测	根据CIS标准并结合华为多年最佳安全实践进行检测。目前支持的配置检测类型有：Tomcat、SSH、Nginx、Redis、Apache2、MySQL5。

表 3-10 态势感知服务基线检查支持的检查项目，具体基线分类如下：

基线检查项目		
检查规范	**检查类别**	**包含的检查项数量**
安全上云合规检查	**身份与访问管理**	12
	检测	7
	基础设施防护	25
	数据防护	22
	事件响应	13
护网检查	**安全套件覆盖**	8
	账号加固	2
	主机加固	2
	Sudo漏洞	1
	访问控制	1
	敏感信息排查	2
等保2.0通用要求	**安全通信网络**	8
	安全区域边界	20
	安全计算环境	34
	安全管理中心	12
等保2.0扩展要求	**安全通信网络**	5
	安全区域边界	8
	安全计算环境	19
	安全管理中心	4

版权所有 © 华为技术有限公司

基线检查项目		
	安全建设管理	8
	安全运维管理	1

3. 在设置和应用程序启动期间，初始化配置步骤为：

步骤1 将态势感知启用到专业版

步骤2 勾选基线检查项目

步骤3 设置基线检查计划

步骤4 执行基线检查计划

步骤5 查看和处理基线检查结果

步骤6 修复所有漏洞。解决基线检查中所有不通过的项

步骤7 再次执行检查并查看态势感知上的结果，确保所有相关事件都得到正确处理。

----结束

3.6.6 合规审计

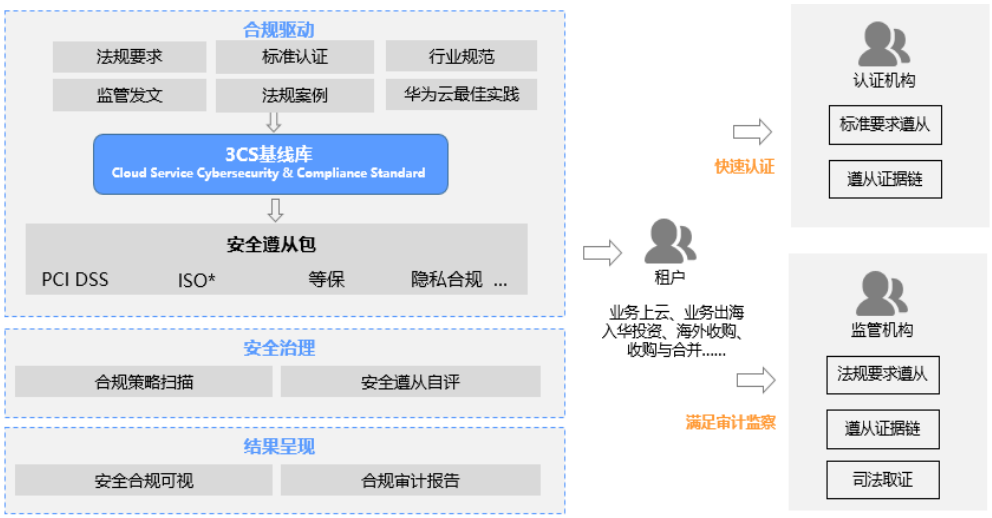
Compass 合规检查

安全治理云图（Compliance Compass，简称 Compass）为客户提供自动化合规评估和安全治理的平台，将华为积累的全球安全合规经验服务化，帮助用户快速实现云上业务的安全遵从，提升用户获得法规及行业标准认证的效率。Compass服务提供安全遵从包，合规策略扫描，安全遵从自评，合规总览等功能。

- **安全遵从包：**华为开放的安全治理模板，包含法规标准条款原文、合规策略、自评估检查项以及华为专家的改进建议，覆盖等保三级、等保四级、PCI DSS、ISO27701、ISO27001、隐私等法规标准。租户可以订阅/取消订阅安全遵从包，查看合规评估与治理结果。
- **合规策略扫描：**Policy as Code，将法规标准条款代码化，周期性、自动化扫描云上资产合规情况。
- **安全遵从自评：**将无法代码化的法规标准条款转化成检查项，租户可完成自身业务的自评，进行证据链管理。
- **安全合规总览：**可视化呈现合规评估结果与安全治理情况

版权所有 © 华为技术有限公司

图 3-36 安全合规总览



- **合规治理经验服务化：**Compass以华为内部“云服务网络安全与合规标准”3CS为基座，将华为积累的全球安全合规经验服务化，开放华为云安全治理模板，将法规条款、标准要求转化为业务语言、IT语言，帮助客户识别自身合规状态。
- **提升获得标准认证的效率：**Compass开放多种安全治理模板，内含合规策略和自评估检查项；合规策略将自动化扫描租户云上资产的合规状态，自评估检查项将帮助租户快速梳理业务情况；支持一键导出报表，提升租户获得法规及行业标准认证的效率。
- **高效实施安全治理动作：**Compass通过数据看板将所有的合规情况集中展示，向租户显示当前的安全性与合规性状态。租户可以轻松发现识别潜在问题，并根据华为专家建议采取必要的安全治理动作

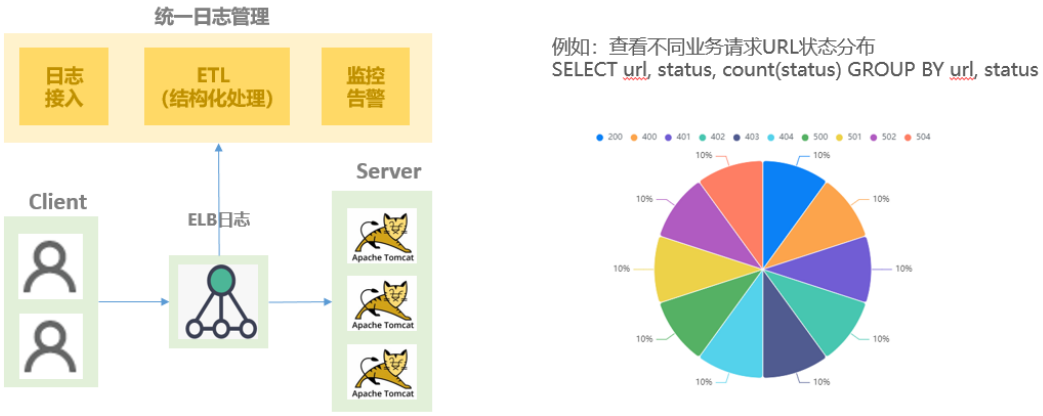
3.7 运维监控

3.7.1 运维监控原则

1. 当应用部署在公有云上，云平台需提供已开通资源的监控能力，包括计算、存储、网络、数据库等云服务资源。资源监控指标反馈资源的运行状态、资源消耗和性能参数等，运维人员可根据不同参数配置相应的阈值告警，当资源异常时通过短信或邮件等方式通知。除了开箱即用的指标数据以外，部分云服务提供完整的日志采集、上报和存储能力，如负载均衡、VPC、WAF等服务日志，应用日志通过安装代理采集并集中管理。通过日志洞察完成日志聚合查询，可视化分析和实时告警。
2. 业务监控指标，如业务登录成功率等。可通过ELB（弹性负载均衡）日志洞察分析，日志系统对该日志ETL后，提取业务URL请求，状态码、访问IP、时延等关键数据，通过SQL聚合可得到不同时间段内业务的运行状态，配置SQL阈值规则可实现业务的实时监控，如下图所示。

版权所有 © 华为技术有限公司

图 3-37 业务监控指标



3. 运维人员可根据资源和应用维度选择监控服务，满足多层次运维要求。下表列出各云服务提供的监控能力。

表 3-11 云服务提供的监控能力

分类	云服务	数据	数据描述
资源监控	CES	指标	提供云资源，如虚机/网络/存储等100+云服务开箱即用指标监控。
指标告警	CES	告警	自定义指标阈值规则，如CPU超过90%。
告警通知	SMN	告警	统一通知服务，支持短信/邮箱/钉钉/微信/webhook等方式。
事件告警	CES	事件	支持事件类型告警，如EIP带宽超限事件告警。
资源分组	CES	指标	将云资源按照项目或应用维度划分资源组，满足企业权限控制。
日志监控	LTS	日志	提供应用/云资源/移动端等日志采集，满足运维日志集中管理能力。
日志告警	LTS	告警	支持关键词和SQL告警规则，提供日志实时监控能力。
日志报表	LTS	日志	提供日志可视化能力，包括图表、柱状图、饼图，同时支持仪表盘和模板能力。
日志备份	LTS	日志	将日志转储OBS，提供冷备份，支持跨账号转储。
日志订阅	LTS	日志	将日志转储至kafka，实时消费日志，支持跨账号转储。
业务监控	LTS	日志	LTS收集业务日志并对其结构化处理，提供可视化分析。或直接将ELB日志提取成业务指标。

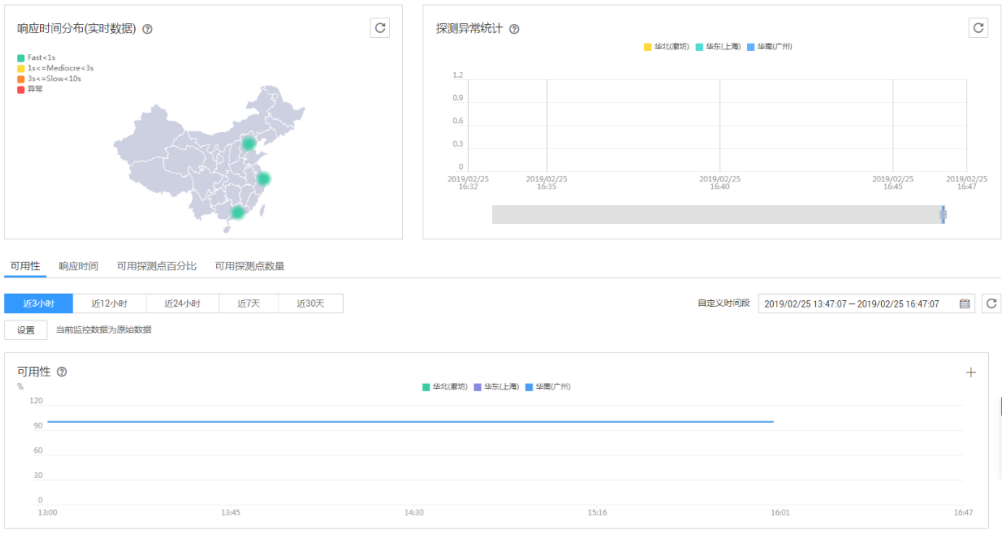
版权所有 © 华为技术有限公司

分类	云服务	数据	数据描述
容器监控	AOM	监控	当使用CCE容器引擎，AOM将提供一站式容器应用的监控、告警和日志分析；
性能监控	APM	性能	提供应用性能分析，包括应用拓扑、分布式链路追踪等能力。

3.7.2 统一资源监控

1. CES服务是面向租户资源的统一监控平台，采用Region级部署方式，对不同Region，不同账号的云资源进行监控及告警。每个账号下都有独立的监控大屏，告警通知、资源分组等功能。能够全方位、立体化的监控租户资源的使用情况，出现问题会触发告警，并通知租户。
2. 站点监控用于模拟真实用户对远端服务器的访问，从而探测远端服务器的可用性、连通性等问题。提供简单的添加配置，不再浪费资源和精力配置复杂的开源产品。支持站点异常告警，不用担心网站出问题而无人知晓。

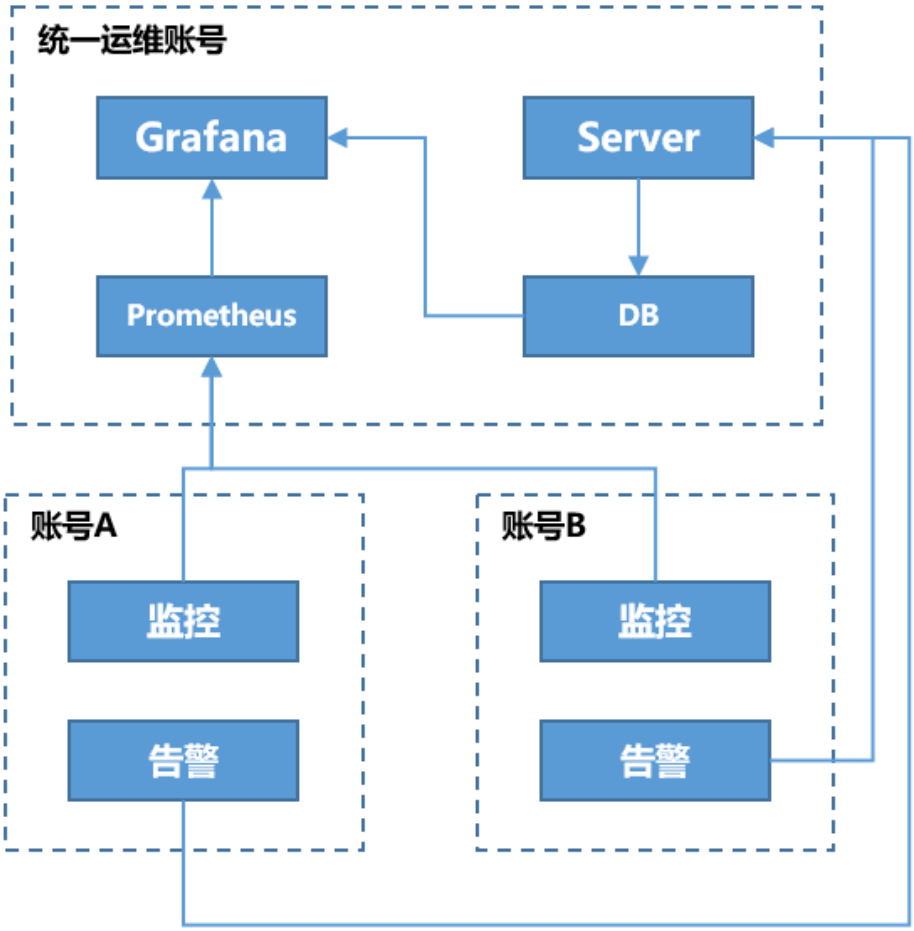
图 3-38 统一资源监控



3. 针对Landing Zone解决方案中需要在多个账号下对所有资源进行监控的诉求，可以通过CES的exporter及开放接口，将不同账号的监控数据和告警数据接入到第三方的平台进行展示。告警配置可以通过华为云提供的默认模板，根据客户自身需求进行修改，修改后的最终模板可以应用在不同账号下的资源；通过该功能可以简化客户告警配置的复杂度，提升告警配置效率。如下图所示：

版权所有 © 华为技术有限公司

图 3-39 统一运维账号



- 账号A、账号B的监控数据通过CES提供的exporter能力在客户侧Prometheus进行任务配置，将数据接入。
- 客户的第三方监控平台提供一个定时任务（建议1分钟粒度），调用CES的告警历史接口，将告警写入数据库中。
- 通过配置客户侧Grafana的数据源（Prometheus，数据库），最终将监控及告警数据集中呈现。

  exporter使用手册：https://github.com/huaweicloud/cloudeye-exporter

3.7.3 统一日志存储

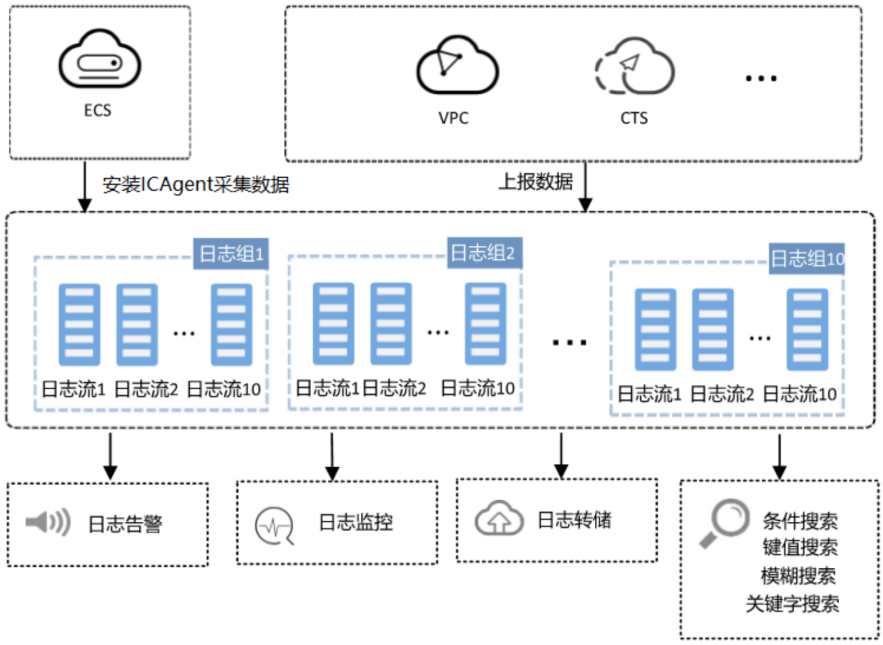
华为云日志服务提供安全可靠的多账号运行环境，可以将不同账号下的云服务日志、用户应用程序日志统一收集到日志账号中。

统一日志收集

1. 下面的架构图描述了云日志服务（Log Tank Service，简称LTS）的主要功能，云日志服务用于实时收集来自主机、云服务、容器、移动终端、开源软件、用户后台应用和WEB端的日志数据。对采集的日志数据，可以通过关键字搜索查询、SQL可视化图表分析、监控和告警、转储到对象存储或KAFKA。

版权所有 © 华为技术有限公司

图 3-40 统一日志收集



2. 华为云将提供并实施集中式日志服务（即每个应用账号将收集自己账号下应用程序和云服务的日志，并将所有日志接入到日志账号），建议在每个应用账号内收集以下主要类型的日志：
   - CTS审计日志（用户操作日志）
   - 系统日志（ECS日志）
   - 安全中心+WAF+云防火墙日志（安全相关日志）
   - SQL审计日志（数据库审计日志）
   - ELB日志（弹性负载均衡第7层网络日志）
   - 堡垒主机操作日志

表 3-12 将创建以下日志流来收集上述类型的日志

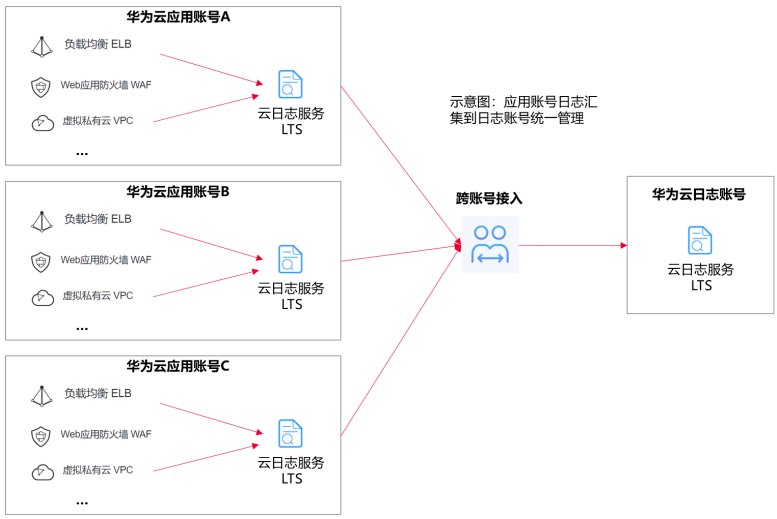
日志类型	日志组	日志流	存储周期（天）	转储到对象存储
CTS审计日志	actiontrail-<account name>	Automatically generated: actiontrail_actiontrail-<account name>	180	是
Syslog	syslog-<accountname>	syslog-<accountname>	180	是
Security Centre + WAF + 云防火墙日志	security-<accountname>	security-<accountname>	180	是

版权所有 © 华为技术有限公司

日志类型	日志组	日志流	存储周期（天）	转储到对象存储
RDS Audit Log(MySQL)	rdsaudit-<accountname>	rdsaudit-<accountname>	180	是
VPC流日志	vpc-<acountname>	vpc-<acountname>	180	是
ELB7层访问日志	slb-<accountname>	slb-<accountname>	180	是
CCE容器集群日志	k8s-<accountname>	k8s-<clusterid>	180	是
ER日志	er-<accountname>	er-<accountname>	180	是

3. 应用账号中的日志存储时间将设置为180天，同时日志数据将转储到对象存储服务（OBS）。这样符合中国的分类保护标准(等保) 2.0合规性。使用格式“%Y/%m/%d/%H/%m”来定义目录层次结构，其中正斜杠（/）表示OBS目录的级别，这样可以利用OBS生命周期配置进行长期日志存储，以节省成本并进行归档。
4. 在应用账号中收集日志后，需要将应用账号中的日志集中到日志账号。为了实现这一点需要在应用账号的统一身份认证服务中创建委托，被委托方是日志账号，并授予日志账号” LTS FullAccess”权限。创建委托后，在日志账号中就可以配置跨账号接入，将应用账号中的日志流接入到日志账号中集中存储。

图 3-41 应用账号日志汇集到日志账号统一管理



版权所有 © 华为技术有限公司

表 3-13 对于未来的需求，需要收集以下日志类型

分类	云服务	日志类型	日志内容
基础服务	容器类服务（CCE/CCI/IEF/AOS）	应用	容器应用的运行日志
基础服务	虚拟私有云 VPC	网络	网络日志
基础服务	弹性负载均衡 ELB	网络	业务请求日志
基础服务	内容分发网络 CDN	网络	域名访问日志
基础服务	弹性公网IP日志	网络	高精度秒级监控功能，以日志形式将高精度网络带宽监控数据推送到日志服务，帮助您实时监控互联网业务流量变化，及时调整弹性公网IP的带宽峰值
基础服务	弹性文件服务NAS	存储	将NAS数据导入LTS
基础服务	OBS	存储	将OBS数据导入LTS
基础服务	SMN	消息	短信等通知内容分析
PAAS服务	应用管理与运维平台 ServiceStage	应用	应用运行日志
PAAS服务	软件开发平台 DevCloud	应用	应用运行日志
PAAS服务	区块链 BCS	应用	应用运行日志
PAAS服务	函数服务 FunctionGraph	应用	函数日志
PAAS服务	应用运维管理 AOM	应用	应用运行日志
PAAS服务	API网关APIG	应用	API调用日志
PAAS服务	云审计 CTS	审计	云审计日志
PAAS服务	应用与数据集成平台 ROMA Connect	应用	API调用日志
PAAS服务	DCS	审计	redis_audit_log Logstore用于存放Redis审计日志。 redis_slow_run_log Logstore用于存放Redis慢日志和运行日志
安全	Web应用防火墙 WAF	安全	攻击、请求和访问防火墙日志
安全	态势感知 SA	安全	HSS、ANTIDDOS等安全风险日志

版权所有 © 华为技术有限公司

分类	云服务	日志类型	日志内容
安全	云堡垒机 CBH	安全	堡垒机系统的操作日志
安全	DDoS高防日志	安全	展示被DDoS高防保护的网站总体访问状况，包括PV、UV、流入流量、网络in带宽峰值、网络out带宽峰值、访问趋势、来源分布等数据
数据库	RDS操作审计日志	数据库	RDS SQL审计日志记录了对数据库执行的所有操作
数据库	ManagoDB日志	数据库	审计日志、慢日志和运行日志
EI	图引擎服务（GES）	大数据	操作审计日志
EI	AI开发平台ModelArts	大数据	大数据任务的运行日志（由于是内置租户，仅在ModelArts上查看）
EI	MapReduce服务MRS	大数据	大数据任务的运行日志（由于是内置租户，仅在ModelArts上查看）
联接与协同	设备接入服务IoTDA	应用	MQTT设备的业务运行日志
联接与协同	IoT边缘 IoTEdge	应用	边缘设备的日志

应用日志收集

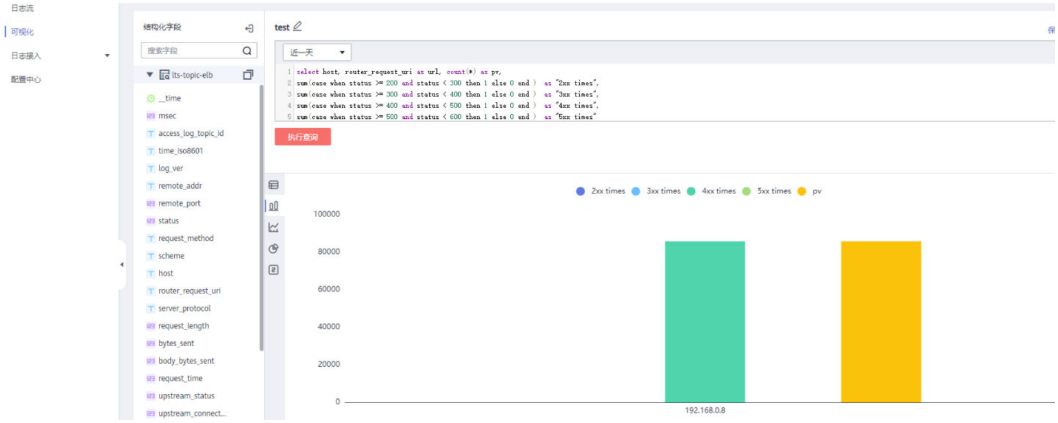
1. 对于应用日志，华为云建议使用ICAgent收集，应用日志一般包括应用程序日志、客户自建网关日志、操作系统日志、容器日志等，这些日志会写入本地系统磁盘，ICAgent通过实时监听本地文件的变化来采集日志，ICAgent与您的程序解耦，您不需要更改代码，它可以将这些日志从所在主机发送到华为云日志服务。
2. 对于华为云上的CCE容器应用，您在控制台上打开日志采集开关即可收集日志到日志服务。对于用户自建的K8S集群，您可以使用日志服务提供的CRD方式采集原生K8S容器日志。（https://support.huaweicloud.com/usermanual-lts/lts_04_1110.html）

日志分析

一旦日志收集到日志服务，日志分析团队就可以使用关键词来搜索过滤感兴趣的日志，可以使用SQL语法来分析日志，并生成可视化图表（表格、柱状图、饼图、折线图等）。日志分析团队可以将图表组合到仪表盘中，为业务提供运营分析，支持提取仪表盘为模板，为不同的日志流提供开箱即用的分析能力。日志分析团队可以基于关键词或者是SQL语句创建告警规则，用来监控系统的运行情况，告警可以通过短信、邮件、企业微信、钉钉等多种方式发送。

版权所有 © 华为技术有限公司

图 3-42 日志分析



日志与第三方系统集成

用户的SIEM（安全信息和事件管理，例如Splunk）位于内部部署环境中，而不是云上。出于安全考虑，云上服务无法直接从外部环境访问任何SIEM端口。华为云日志服务LTS提供API，让任何外部应用程序和平台都可以使用这些API来检索LTS中存储的日志。同时LTS可以实时转储日志到DMS（KAFKA），外部应用程序可以实时消费DMS（KAFKA），接入到用户自己SIEM系统中。因此建议企业将日志账号中的日志流实时转储到DMS（KAFKA），企业的SIEM系统可以实时消费KAFKA接入日志数据。

图 3-43 云日志服务数据对接客户的 SIEM

3.8 财务管理

财务管理原则

华为云基于大量成功交付的项目，总结提炼了以下财务管理原则：

1. 为实现统一财务管控，主账号为组织单元添加子账号时开启以下权限：
   - 请求查看子账号财务信息
   - 请求查看子账号消费消息
   - 禁止子账号自行开票
   - 允许代子账号开票
   - 允许子账号继承主账号商务折扣
2. 在主账号下要设置一个财务管理员，拥有主账号财务管理的所有权限，定期核算整个企业在华为云的消费情况，进行成本控制，定期（每月、每季、每年）统计华为云消费并计入企业财务报表。每个子账号（对应一个组织单元）也建议设置财务管理员，在本账号下核算华为云消费情况、进行成本控制、成本分析。

版权所有 © 华为技术有限公司

3. 主账号的财务管理员统一在华为云上充值、申请信用额度和激活代金券，再划拨给各个子账号，定期审视子账号的资金、信用额度和代金券的使用情况，及时进行回收。为确保资金安全，建议开启资金安全二次验证功能。
4. 主账号和各子账号的财务管理员要协同项目经理，根据资金使用成本和项目需求确定各类云资源的计费模式，是按需计费，还是包月、包季、包年等；定期按照企业项目、产品类型等维度进行成本统计和分析，结合资源利用率分析结果设计成本优化方案，如按需计费改为包周期、资源整合、订购套餐包等，并制定下一周期的成本预算；持续监控资源到期情况，及时对快到期的资源进行续费。
5. 为防止子账号过度消费资源，主账号可以统一分配可用资金给各个子账号，同时开启余额预警；为防止项目成员过度订购云服务，还可以限定单个企业项目在华为云上订购云服务的资金配额限制，同时开启余额预警。

多账号财务管理

同一个企业下存在多个华为云账号时，可以建立企业主子账号关联关系，企业主账号您可以根据自己的企业结构创建多层组织、新建子账号或关联子账号，并使其从属于主账号创建的组织部门，从而对这些子账号的财务进行管理。

1. **主子账号关联**

   主账号可以通过创建一个华为云账号并与之关联，或者邀请一个华为云账号与之关联。同时主账号可以根据公司业务在企业中心创建组织部门信息，子账号可以从属与某个组织部门。

2. **主子账号资金管理**

   主账号充值后，可以划拨现金、代金券给子账号用于资源的开通。子账号也可以通过自主充值后，进行资源的开通。

3. **主子账号商务继承**

   主账号可以将其商务继承给子账号，继承后子账号的消费可以使用主账号的商务。避免同一家企业针对其不同账号需要签署多个商务的麻烦，增加了便利性。

4. **主子账单查询**

   主子账号消费后，可分别登录华为云查看自己的消费数据。主账号可以申请查看子账号消费数据，申请成功后即可查看子账号的消费数据。

5. **主子发票**

   主子账号消费后，各自独立向华为云申请开发票。主账号也可以代子账号开票。

成本计划

1. **估算和预测成本**
   - 云支出的可变性，导致云支出是很难预测的。
   - 对于新产品发布或区域扩张，客户可使用**华为云价格计算器**在线自助估算各种产品，不同区域、不同规格、不同购买选项的成本。
   - 对于已使用产品，客户也可以使用**华为云成本中心的成本分析**来预测每日（最多未来90天）或每月（最多未来12个月）的云成本。该预测，主要基于客户历史成本和历史用量情况，应用机器算法进行估算。
2. **创建预算以跟踪成本**
   - 跟踪成本计划的有效工具是预算。
   - 一旦完成成本的估算与预测，客户可以在华为云成本中心的**预算管理**创建精细粒度的预算来管理成本，并可以创建预算提醒，在实际或预测超过预算阈值时，自动通知利益相关人支出异常。

版权所有 © 华为技术有限公司

- 客户还可以创建**预算报告**，每天/每周/每月，定期将指定预算进展通知给利益相关人。

成本分配

准确有效的成本分配，有利于企业内部的成本透明与问责。而透明的成本责任制是企业财务管理的基础。

1. **确定成本组织方式**
   - 企业进行财务管理之前，需要先确认云支出的组织方式，确保将企业在华为云上的支出能分摊到企业内部的组织层级结构上。
   - 对于使用多账号的企业组织来说，可以使用关联账号来天然分摊企业在华为云的支出。同时，企业还可以使用标签将组织信息标记在资源上，资源标签会随资源使用添加到客户的成本数据上。客户可以使用标签识别不同环境（比如生产、测试）的成本、或使用标签识别不同的组织、产品、负责人。
   - 华为云成本中心为客户提供**成本标签**功能，企业各子账号（含主账号）在成本中心将资源标签激活为成本标签后，各账号就可以在成本中心基于成本标签进行成本分析、预算跟踪。成本标签只能影响激活后新产生的成本数据，因此建议客户尽早进行成本标签的规划和激活。
   - 对于不能通过标签归集的成本（比如企业内部共用资源产生的成本，未及时标记标签产生的成本，或暂不支持标签管理的产品成本），建议客户在企业内部约定分配规则，将这类共同成本分配到企业内部。分配规则可以是平均分配、自定义比例，或者按照可归集成本的比例进行二次分配。
2. **采用应计视角的摊销成本**

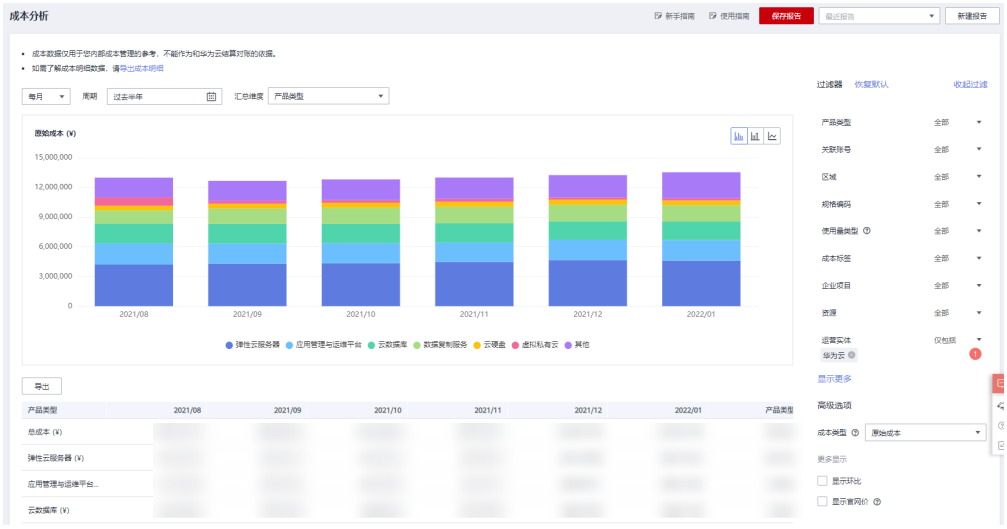
   华为云成本中心为客户提供了不同的成本类型：
   - **原始成本**：反映了客户的原始使用和购买情况。该成本是基于云服务官网价，应用了商务折扣、促销折扣等优惠之后的金额。
   - **摊销成本**：反映了包年/包月产品的预付金额在订单有效期间内按日分摊后的有效成本。比如客户购买了有效期为一年的云服务共365元，则每天的摊销成本为1元。
   - 从财务视角来看，摊销成本为应计成本，是按照权责发生制计算的成本，因此更建议客户使用摊销成本在企业内部分摊成本。
   - 详细的成本摊销规则可参见：**https://support.huaweicloud.com/usermanual-cost/costcenter_000002_01.html**

成本分析

1. 了解组织内的成本趋势和成本驱动因素，是企业进一步有效管理成本、控制和优化成本的关键。

版权所有 © 华为技术有限公司

图 3-44 分析成本及用量的趋势及分布



2. 华为云成本中心的**成本分析**支持使用汇总和过滤机制可视化您最多18个月的原始成本或摊销成本，从而通过各种角度、粒度、范围深度分析成本和用量的趋势及驱动因素。企业主账号可以同时分析名下各子账号的成本和用量情况。
3. 客户可以使用成本中心提供的**预置分析报告**对常见场景快速分析，预置报告包括：

报告名称	说明
按产品类型汇总的月度成本	了解过去6个月原始成本较高的产品类型。
按关联账号汇总的月度成本	了解过去6个月原始成本较高的关联账号。
每日成本	了解过去3个月的每日原始成本趋势，以及未来1个月的成本预测。
月度摊销成本	了解过去6个月摊销成本的月度趋势。
ECS的月度按需成本和使用量	了解过去6个月云主机每月按需原始成本和按需使用量情况。

4. 如果预置报告不能满足客户诉求，客户还可以**自定义分析**，通过调整时间粒度、周期、汇总条件、过滤条件以及成本类型，来洞察成本和用量的情况。对于客户经常关注的自定义分析，建议保存为**自定义报告**，便于再次查看相同条件下的分析数据。
5. 无论是预置报告还是自定义分析报告，**报告分析结果均支持导出**CSV文件。同时，华为云成本中心还支持导出**携带标签和关联账号的月度摊销成本明细**，便于客户深入分析

成本优化

云支出的主要影响因素，是费率和用量。因此企业在华为云上的成本优化也主要从这两方面着手考虑。

1. **降低费率**

版权所有 © 华为技术有限公司

- 对于长期使用的按需产品，建议客户优先采用包年包月或资源包。
- 客户可使用华为云成本中心的**按需转包年包月优化评估**发现节省成本的机会。该评估基于客户ECS、EVS、RDS历史按需资源的使用情况进行分析，为客户提供按需转包年包月的可优化资源清单和优化前后的成本对比。
- 如果客户已购买资源包，客户还可以使用华为云成本中心的**资源包使用率/覆盖率分析**，分析已购买资源包的使用情况。对于使用率过低的资源包，判断是否购买过量；对于覆盖率过低的资源包，判断是否购买不足。客户根据分析结果优化下一周期的资源包购买。

2. **减少用量**
   - 客户可通过监控云服务的利用率，来识别空闲资源或利用率较低的资源。释放空闲资源或降配利用率低的资源，可以减少不必要的付费用量。需要注意的是，无论是释放资源还是降配资源，都需要和业务部门确认，以确保不影响业务使用。
   - 客户可以基于业务技术方案的优化，比如存算分离、分时复用将资源充分利用起来，或使用性价比高的实例，来减少付费用量。

版权所有 © 华为技术有限公司

4 自动化部署步骤

1. Landing Zone解决方案的实施需要进行大量的手工配置，比如新增一个子账号就需要为该账号创建对应的VPC、子网、ACL、安全组，开通CTS，创建各种必要的云资源，配置安全基线等。所以需要自动化Landing Zone的配置工作，华为云推荐使用业界主流的资源编排工具Terraform执行自动化部署和配置Landing Zone。
2. Terraform是一个开源的IT基础设施编排管理工具，Terraform支持使用配置文件描述Landing Zone解决方案。通过Terraform可以轻松创建、管理、删除华为云资源，并对其进行版本控制。

图 4-1 Terraform 自动化部署和配置华为云资源

3. 关于如何使用Terraform部署华为云的资源，请参考 **https://support.huaweicloud.com/qs-terraform/index.html** ，Terraform支持编排的华为云资源请参考 **https://registry.terraform.io/providers/huaweicloud/huaweicloud/latest/docs**。后续华为云会提供基于Terraform的部署模板用于自动化部署和配置Landing Zone。

版权所有 © 华为技术有限公司

5 附录

背景信息

表 5-1 华为云 Landing Zone 工具集

工具	所属云服务	具体描述
账号	IAM	账号（Account）是云上资源归属和使用计费的主体，对其所拥有的资源具有完全控制权限，可以创建和管理用户、用户组，并对用户组进行授权。账号统一接收用户进行资源操作时产生的费用账单。不同账号间有严格的物理隔离，网络互不相通，跨账号的资源互访需要使用特定的工具解决。
组织	企业中心	华为云提供的组织管理功能，允许企业在华为云上创建匹配自身组织结构的组织单元（Organization Unit, OU），并可以通过创建账号或邀请其他账号的方式为组织单元添加账号，实现对多个账号的统一资金管理和消费汇总。创建组织结构的账号为主账号，添加到组织单元的账号为子账号，主子账号通过组织结构构成了一种层级关系。主账号可以将自己的账号余额、信用额度、代金券划拨给子账号，主账号也可以查看子账号在华为云上的财务信息和消费信息，子账号可以继承主账号的商务折扣。需要指出的是，主账号和子账号间依然有严格的物理隔离，网络互不相通。
企业项目	EPS	企业项目（Enterprise Project, EP）是云资源的逻辑集合，其中的资源可以迁入迁出，方便租户按照自身的项目管理模式在华为云上进行资源的分组管理、成本核算和权限控制。一个企业项目可以包含多个区域的资源，可以授权给一个或者多个用户组进行管理。企业项目的灵活性较好，推荐用作企业的IT项目管理。
IAM项目	IAM	IAM项目针对同一个区域（Region）内的资源进行分组和物理隔离，在IAM项目中的资源不能转移到另一个IAM项目，只能删除后重建，灵活性不高。

版权所有 © 华为技术有限公司

工具	所属云服务	具体描述
用户	IAM	用户由华为云账号在IAM中创建，是云服务的使用人员，具有独立的身份凭证（密码和访问密钥），根据账号授予的权限使用资源，账号可以随时修改或者撤销IAM用户的使用权限。用户不进行独立的计费，由所属账号统一付费。
用户组	IAM	用户组是用户的集合，华为云通过用户组功能实现用户的授权。用户需要加入特定用户组后，才具备对应的权限。当某个用户加入多个用户组时，此用户同时拥多个用户组的权限，即多个用户组权限的全集。
策略	IAM	IAM提供的一种细粒度授权机制，可以精确到具体服务的操作、资源以及请求条件等，使用基于策略的授权是一种更加灵活地授权方式，能够满足企业对权限最小化的安全管控要求。策略根据创建的对象，分为系统策略和自定义策略。
授权	IAM	华为云通过给用户组授予策略或角色，用户组中的用户就能获得了相应的权限，这一过程称为授权。用户获得具体云服务的权限后，可以对云服务进行操作。有两种授权范围，一个是IAM项目，另一个是企业项目，IAM项目的授权范围是账号内特定区域，企业项目的授权范围仅限于特定企业项目。按照最小授权原则，推荐在企业项目中进行授权。
服务配额	公共服务	华为云平台上单个账号内各服务资源的配额，对用户所能申请的资源数量和容量做了限制，但企业如果确实会使用超过配额的云服务资源，可以提工单申请扩大配额。
资金配额	CBC	为防止用户过度订购云服务，限定账号和企业项目在华为云上订购云服务的资金上限。
成本中心	CBC	成本中心是华为云免费向客户提供的一项成本管理服务，可帮助客户收集华为云成本和使用量的相关信息、探索和分析华为云成本使用情况、监控和跟踪华为云成本。主要功能包括成本分析、预算管理、成本监控、成本优化建议和成本标签等。
安全合规	Compass	Compass是一个自动化合规评估和安全治理的平台，以华为内部云服务网络安全与合规标准为基座，将华为积累的全球安全合规经验服务化，开放PCI DSS、ISO27701、ISO27001等安全治理模板，将合规语言IT化实现自动化扫描，可视化呈现合规状态，一键生成合规遵从性报告，帮助租户快速实现云上业务的安全遵从，提升租户获得法规及行业标准认证的效率。

版权所有 © 华为技术有限公司

工具	所属云服务	具体描述
态势感知	SA	SA（Situation Awareness，态势感知）是华为云安全管理与态势分析平台。能够检测出超过20大类的云上安全风险，包括DDoS攻击、暴力破解、Web攻击、后门木马、僵尸主机、异常行为、漏洞攻击、命令与控制等。利用大数据分析技术，态势感知可以对攻击事件、威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。
资源合规	RMS	通过设置合规规则对特定云资源进行合规检查，如检查某个区域内所有已挂载的云硬盘是否加密。
云审计	CTS	是一种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。
标签管理	TMS	标签用于标识云资源，当您拥有相同类型的许多云资源时，可以使用标签按各种维度（例如用途、所有者或环境）对云资源进行分类管理。
企业路由器	ER	企业路由器（Enterprise Router, ER）可以连接VPC或本地网络来构建Region级别的中心辐射型网络，是云上大规格，高带宽，高性能的集中路由器。企业路由器使用边界网关协议，支持路由学习、动态选路以及链路切换。企业路由器能够打通多个账号内VPC之间的网络，可以通过VPN、专线与本地网络三层互通，通过云连接与用户在其他Region的VPC互通，通过路由配置，实现灵活的隔离和互通。
VPC	VPC	为云服务器、云容器、云数据库等资源构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云上资源的安全性，简化用户的网络部署。
子网	VPC	提供一个网段，用来管理云资源网络平面，可以提供IP地址管理、DNS服务。默认情况下，同一个VPC的所有子网内的云服务器均可以进行通信，但可以通过设置网络ACL或安全组进行子网间的安全访问控制，不同VPC之间默认不能通信。

版权所有 © 华为技术有限公司

6 修订记录

表 6-1 修订记录

发布日期	修订记录
2024-05-11	第一次正式发布。

版权所有 © 华为技术有限公司