企业管理

最佳实践

文档版本 01

发布日期 2024-07-10

华为技术有限公司

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

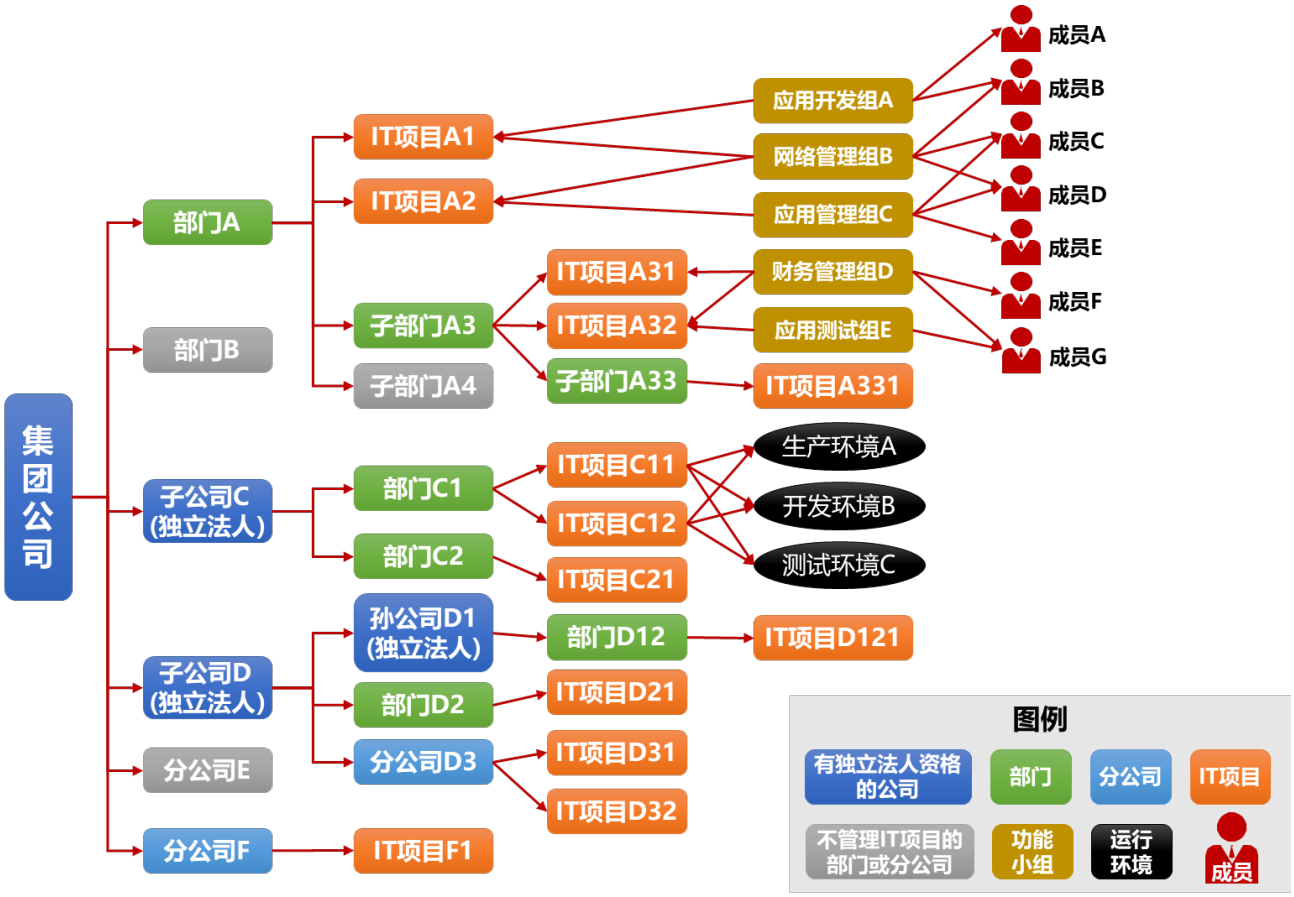
目 录

1 大企业 IT 治理最佳实践

1.1 大企业 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，由于图片空间有限，该架构图中没有列出全部的层级，如IT项目A331的功能小组、成员和运行环境没有呈现出来。本章所描述的大企业IT治理最佳实践以下图的IT治理架构为基础，将其映射到华为云上有效运转起来。

图 1-1 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：

1. **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。
2. **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。
3. **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。分公司不具有企业法人资格，其民事责任由母公司承担。
4. **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。
5. **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。
6. **IT项目：**企业按照自己的项目管理模式设置的信息化、数字化或软件开发项目，IT项目中应用系统的开发、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。
7. **功能小组：**参与IT项目的成员按照职责不同可以划分为不同的功能小组，如一个ERP项目可以划分为计算组、存储组、网络组、安全组、数据组、应用组、财务组、系统管理员组等。

8. **成员：**一个成员代表一个参与IT项目的人，可加入到同一部门下不同的IT项目和功能小组，但一般不参加其他部门的IT项目。
9. **运行环境：**IT项目中的应用系统（如ERP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。多个IT项目可以共享一套运行环境，大型IT项目（如大型电商、大型ERP系统）也可以独占一套运行环境。

上述大企业IT治理架构中各个层级之间的关系如下图所示：

图 1-2 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 1 — n IT项目	1个部门可以管理多个IT项目，独立法人不建议直接管理IT项目，由下面的部门或者分公司直接管理
分公司 1 — n IT项目	1个分公司可以管理多个IT项目
IT项目 m — n 功能小组	1个IT项目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项目
功能小组 m — n 成员	1个功能小组可以由多个成员组成，1个成员可以同时属于不同项目下的类似功能小组(如运维工程师A可以同时加入项目1和项目2的运维组)，也可以同时参加同一项目的不同功能小组
IT项目 m — n 运行环境	1个IT项目中的应用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项目的应用系统。

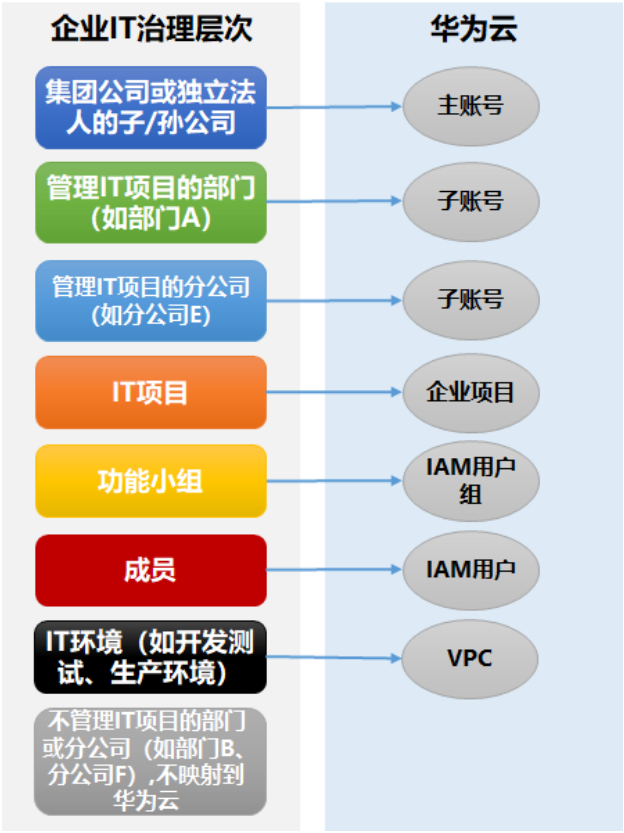
1.2 云上 IT 治理最佳实践

1.2.1 总览

映射关系

大企业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：

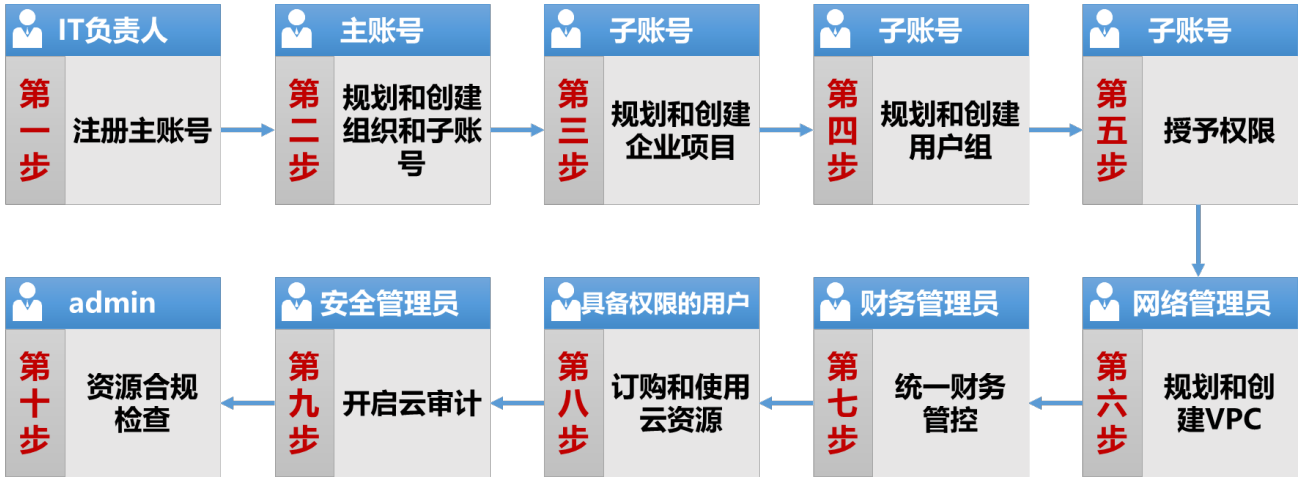
图 1-3 大企业 IT 治理架构到华为云的映射



操作步骤

基于上述映射关系，按照以下步骤完成设置和操作：

图 1-4 大企业 IT 治理最佳实践的十大步骤



1.2.2 步骤一：注册主账号（操作主体：IT 负责人）

有独立法人资格的集团公司、子公司（如子公司C、子公司D）、孙公司（如孙公司D1），分别由各自指定的IT负责人在华为云上分别注册自己的主账号，独立制定华为

云的预算并充值，并在华为云上建立独立的组织结构（参照步骤二）。不要把子公司的账号关联为集团公司的子账号。

涉及到的操作如下：

1. **注册华为账号并开通华为云业务**：注册华为账号并开通华为云业务后，基本信息、订单信息、费用信息等都和该账号相关联。
2. **开通企业中心功能**：开通后该账号即成为企业主账号，可以执行关联子账号等操作。
3. **进入企业中心页面**：提供多入口，方便您进入企业中心。

1.2.3 步骤二：规划和创建组织和子账号（操作主体：主账号）

以集团公司为例，使用上面创建的主账号登录华为云，进入企业中心页面，针对集团公司下面每一个管理IT项目的部门（部门A、部门A3）和分公司（分公司F），在华为云上分别创建对应层级的组织单元，如**图1-5**所示。并给每个组织单元添加一个子账号，该子账号代表该组织单元在华为云上行使管理职能。

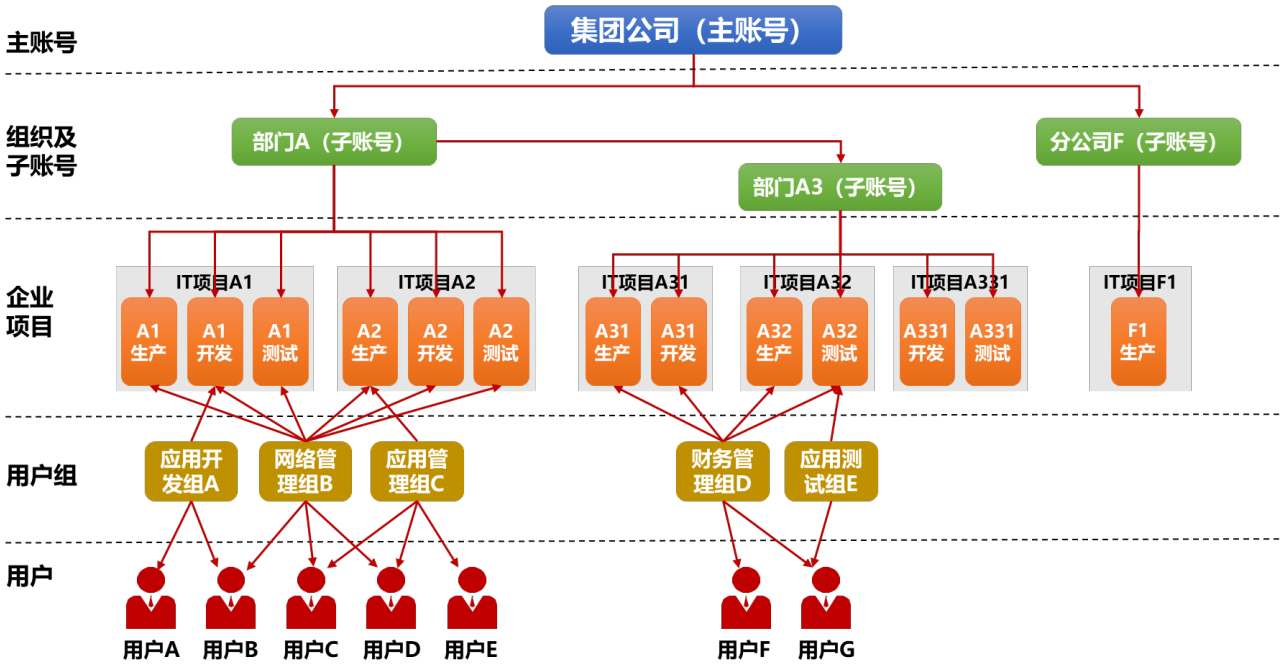
创建子账号时，可以设置以下权限：查看子账号财务信息、查看子账号消费消息、禁止子账号自行开票、允许代子账号开票、允许子账号继承主账号商务折扣。

子部门A33虽然也管理IT项目，但属于三级部门，层级较深的部门不建议在华为云上创建对应的组织单元，而是将其管理的IT项目A331挂到上级部门A3下面，如**图1-5**所示。不管理IT项目的部门（部门B、子部门A4）和分公司（分公司E），与华为云不产生交互关系，所以无需为此在华为云上创建对应的组织单元。

涉及到的操作如下：

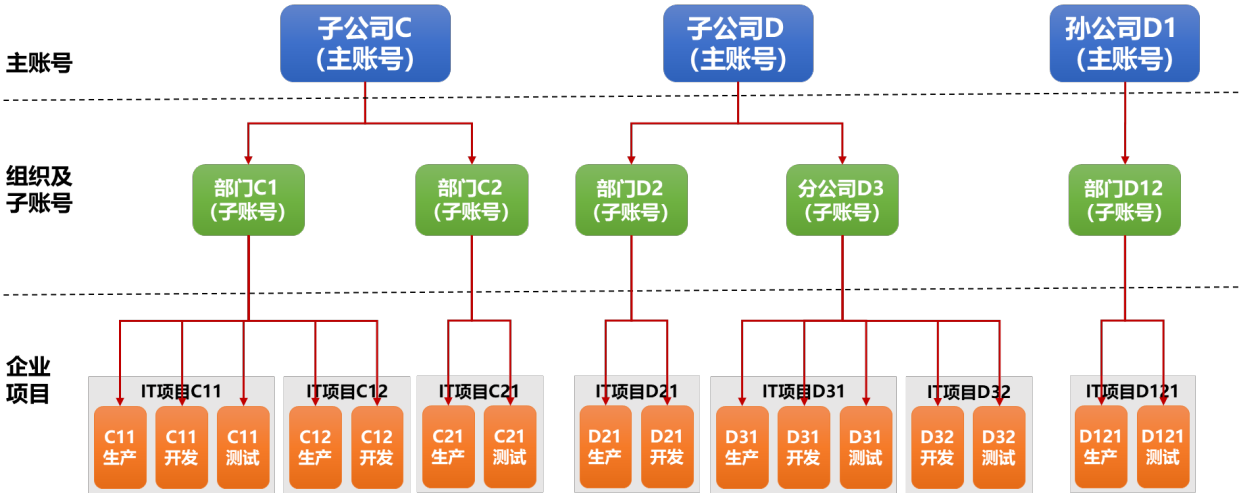
1. **新建组织**：企业主账号可以创建组织，用于将关联的子账号挂载在组织单元上，挂载后可以按组织统计资金的消费情况。
2. **管理组织策略**：您可以通过设置组织策略决定子账号的云服务访问权限。
3. 关联子账号：企业主账号通过创建子账号或邀请子账号的方式，建立企业主子关联关系。您可以通过两种方式关联子账号，即**新建子账号**和**邀请子账号**。
4. 给子账号授权：企业主账号可以在关联子账号时，完成主账号对子账号的授权，也可以在关联后**变更子账号权限**。您还可以查看**权限说明**，具体了解主账号与子账号组成的多种权限策略。

图 1-5 集团公司映射到华为云



其他子公司和孙公司下面的组织按照同样的方式创建，如下图所示。

图 1-6 子公司和孙公司映射到华为云



1.2.4 步骤三：规划和创建企业项目（操作主体：子账号）

如果1个IT项目中的应用系统需要部署到多个运行环境（生产环境、开发环境和测试环境），为了做好项目成员的权限控制，应该按照这个应用系统所需的运行环境在华为云上创建不同的企业项目。也就是说1个IT项目可以映射到华为云上的多个企业项目，如图1-5和图1-6所示。

以集团公司的部门A为例，该部门在上云前管理两个IT项目A1和A2，这两个IT项目的应用系统都需要部署在生产环境、开发环境和测试环境。接下来就用部门A的子账号登录华为云，进入项目管理控制台为IT项目A1创建3个企业项目：A1生产、A1开发、A1测试，再为IT项目A2创建3个企业项目：A2生产、A2开发、A2测试。通过这种方式划分

企业项目，再结合后面的用户组划分和权限设置，可以确保开发组成员只能看到开发环境的云资源，测试组成员只能看到测试环境的云资源。

以子部门A3为例，该部门在上云前直接管理2个IT项目A31、A32，以及下属部门A33（该部门没有映射到华为云）管理的IT项目A331。A31只需要生产和开发环境，A32只需要生产和测试环境，A331只需要开发和测试环境，接下来就用部门A3的子账号登录华为云，进入项目管理控制台为IT项目A31创建2个企业项目：A31生产、A31开发，为IT项目A32创建2个企业项目：A32生产、A32测试，为IT项目A331创建2个企业项目：A331开发、A331测试，如**图1-5**所示。

分公司F下的IT项目F1 只需要生产环境，那么就用分公司F的子账号登录华为云为IT项目F1创建1个企业项目：F1生产。子公司C、子公司D、孙公司D1下面的IT项目到企业项目的映射就不赘述了，如**图1-6**所示。

涉及到的操作如下：

1. **企业项目的应用场景**：在规划企业项目之前，您可以先了解企业项目的应用场景。
2. **如何开通企业项目**：企业账号可申请开通企业项目。如果您的账号未进行实名认证，请先进行**企业实名认证**。如果企业账号注册成为华为云合作伙伴，将无法进入企业项目管理页面。如果您的账号已进行个人实名认证，则需将账号升级为企业账号，才可以申请开通企业项目，具体请参见**如何变更为企业账号**。
3. **如何进入项目管理页面**：若您的企业账号已进行实名认证并已申请开通企业项目，可按此步骤进入项目管理页面。
4. **创建企业项目**：您可以根据部门或者业务，创建对应的企业项目。创建企业项目的用户必须是管理员，或在IAM侧已关联EPS FullAccess策略的用户。每个主账号默认可以创建100个企业项目。

说明

- 集团公司或大的子公司不推荐直接管理IT项目，而是由下面的部门或分公司（对应华为云上的子账号）管理IT项目。
- 每个主账号或子账号下面有一个默认企业项目default，该项目由系统自动生成，未选择企业项目的云资源会被放到default项目内。

1.2.5 步骤四：规划和创建用户组（操作主体：子账号）

以集团公司的部门A为例，使用部门A的子账号登录华为云，进入IAM控制台，针对IT项目A1、A2下面的三个功能小组：应用开发组A、网络管理组B、应用管理组C，在华为云上创建与之对应的3个用户组，并创建用户A、B、C、D、E，加入到对应的用户组，如**图1-5**所示。

以子部门A3为例，使用子部门A3的子账号登录华为云，针对IT项目A31下面的功能小组：财务管理组D、应用测试组E，在华为云上创建与之对应的2个用户组，并创建用户F、G加入到对应的用户组。用户组、用户和企业项目的关系如**表1-1**所示。

表 1-1 用户组及其参与的企业项目

华为云用户组	华为云用户	参与的企业项目
应用开发组A	用户A、用户B	A1开发
网络管理组B	用户B、用户C、用户D	A1生产、A1开发、A1测试、A2生产、A2开发、A2测试

华为云用户组	华为云用户	参与的企业项目
应用管理组C	用户C、用户D、用户E	A2生产
财务管理组D	用户F、用户G	A31生产、A31开发、A32生产、A33测试
应用测试组E	用户G	A32测试

上面的用户组划分并不全面，只是为了演示用户组和各个层级的关系，具体实践时的用户组划分更加复杂。下面着重考虑到大企业在统一运维管控和统一财务管控的诉求，为大企业在华为云上的一个子账号推荐用户组的具体划分方式，以及各个用户组的职责和应该具备的权限，如表1-2所示。权限级别为账号的用户组，如admin组、计算管理组、存储管理组、网络管理组等，在整个账号层面对资源进行统一管控。权限级别为企业项目的用户组，如应用开发组、应用测试组、应用管理组和项目管理组，仅管理所参与的1到多个企业项目的云资源。应用开发组成员只能访问和管理开发环境的云资源，应用测试组成员只能访问和管理测试环境的云资源。

表 1-2 用户组划分及权限设置

用户组	权限级别	职责	推荐的权限
admin	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全局管理组	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	账号	该组成员负责统一管理和运维账号下所有的计算资源，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
存储管理组	账号	该组成员负责统一管理和运维账号下所有的存储资源，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

用户组	权限级别	职责	推荐的权限
网络管理组	账号	该组成员负责统一管理和运维账号下所有的网络资源，包括VPC、弹性负载均衡、VPN、云专线、DNS、NAT、CDN等	VPC FullAccess ELB FullAccess NAT FullAccess VPN Administrator DNS FullAccess VPCEndpoint Administrator Direct Connect Administrator CDN Administrator
安全管理组	账号	该组成员负责统一管理账号下的身份认证服务，包括用户、用户组、权限、委托等；同时管理账号下的所有安全云服务，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	Security Administrator Anti-DDoS Administrator CAD Administrator VSS Administrator HSS FullAccess DBSS Security Administrator KMS Administrator WAF FullAccess SCM FullAccess CGS FullAccess SA FullAccess CBH FullAccess CTS Administrator
数据库管理组	账号	该组成员负责统一管理和运维账号下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

用户组	权限级别	职责	推荐的权限
大数据及AI管理组	账号	该组成员负责统一管理和运维账号下所有的大数据及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 HiLens FullAccess
中间件管理组	账号	该组成员负责统一管理和运维账号下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、容器镜像、ServiceStage、区块链等	ServiceStage FullAccess CSE FullAccess DCS FullAccess DMS Administrator SMN Administrator APIG FullAccess BCS Administrator SWR Admin
财务管理组	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 Administrator
统一运维组	账号	该组成员负责统一监控和运维账号内的所有云资源，但不负责具体的资源订购和资源操作。	建议设置各个云服务的ReadOnlyAccess权限，以及下面的权限： AOM FullAccess CES FullAccess APM FullAccess TMS Administrator

用户组	权限级别	职责	推荐的权限
项目管理组	企业项目	需要为每一个企业项目创建一个项目管理组，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，设置default项目中共享给其他项目使用的云资源的ReadOnly权限，以及以下项目管理权限： EPS FullAccess EnterpriseProject BSS FullAccess
应用开发组	企业项目	该组成员仅负责管理所参与的1到多个企业项目在开发环境的云资源	建议设置所参与企业项目在开发环境的所有云服务的FullAccess权限，同时设置default项目中共享给其他项目使用的云资源的ReadOnly权限
应用测试组	企业项目	该组成员仅负责管理所参与的1到多个企业项目在测试环境的云资源	建议设置所参与企业项目在测试环境的所有云服务的FullAccess权限，同时设置default项目中共享给其他项目使用的云资源的ReadOnly权限
应用管理组	企业项目	该组成员仅负责运维所参与的1到多个企业项目内的应用系统，主要管理企业项目在生产环境的云资源，也可以管理开发环境和测试环境的云资源。应用管理组也需要对资源进行操作。	建议设置生产环境下所有相关云服务的CommonOperations、Operator权限以及下面的权限： AOM FullAccess CES FullAccess APM FullAccess TMS Administrator

说明

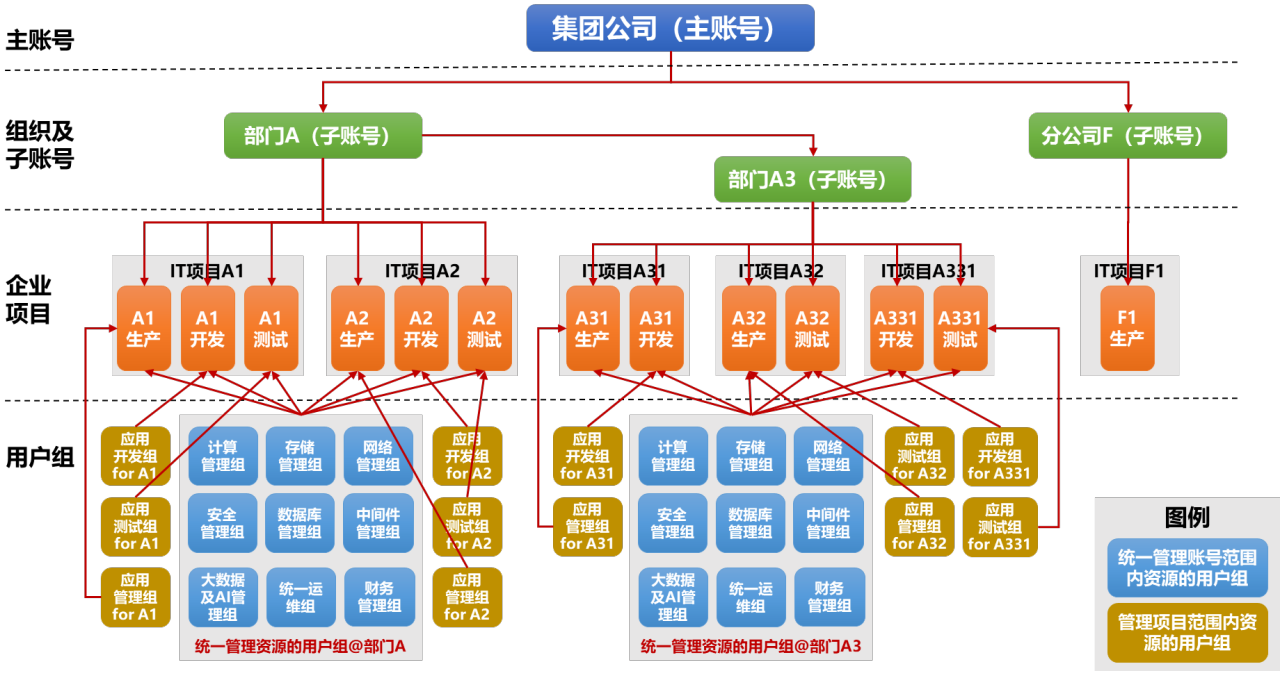
上述为用户组推荐的权限没有列举所有必要的权限，也有可能配置了过多和过大的权限，实际应用过程中可根据申请的云资源类型，并按照最小授权原则为用户组授予必要的权限。例如，在华为云上不需要启用WAF（Web应用防火墙），就无需为安全管理组添加WAF FullAccess权限。

基于上述用户组的具体划分方式，集团公司的部门A和子部门A3的用户组规划如图1-7所示，尽管这两个部门是父子关系，但在华为云是两个不同的账号，需要给每个账号都分别创建统一管控账号范围内资源的用户组。由于图片空间有限，并没有把项目管理组呈现出来，每一个企业项目都应该设置独立的项目管理组。

需要注意的是，这种方式将统一管控的范围限制在了部门级（对应子账号），无法做到公司级（对应主账号）的统一管控，对大企业比较合适，中小企业则应该在公司级（主账号）下创建统一管控资源的用户组。

除了在每一个部门（子账号）创建一个财务管理组之外，也需要在公司层面（主账号）下创建一个财务管理组，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，定期核算企业在华为云的消费情况。

图 1-7 部门 A 和子部门 A3 的用户组规划



涉及到的操作如下：

1. **创建用户组**：您可以通过统一身份认证服务（IAM）来创建用户组。

1.2.6 步骤五：授予权限（操作主体：子账号）

表1-2中的用户组有不同的权限级别，权限级别为账号的用户组，如计算管理组、存储管理组、网络管理组等，其权限在IAM中授予。权限级别为企业项目的用户组，如应用开发组、应用测试组、应用管理组和项目管理组，其权限在企业项目中授予。

以集团公司的部门A为例，使用部门A的子账号登录华为云，进入IAM控制台，为计算管理组、存储管理组、网络管理组、安全管理组、数据库管理组、中间件管理组、大数据及AI管理组、财务管理组、统一运维组授予表1-2所推荐的权限。在IAM控制台进行授权时需要选择合适的作用范围：全局服务或者区域级项目，前者适用于全局级云服务，如OBS、TMS、CDN、SCM等云服务，后者适用于按区域部署的云服务，如ECS、RDS等。例如，为安全管理组授予SCM FullAccess权限时需要将作用范围选为全局服务；为数据库管理组授予RDS FullAccess权限时需要将作用范围选为区域级项目并选择具体的区域，按照最小授权原则，尽量不要选择“所有项目”，而是选择要管理的RDS资源所在的区域项目。

说明

上述区域级项目是指IAM项目，默认情况下一个区域对应一个IAM项目。

然后进入企业项目控制台，为企业项目“A1生产”添加用户组“应用管理组for A1”并授予相应权限；为企业项目“A1开发”添加用户组“应用开发组 for A1”并授予相应权限。通过这种权限设置方式，用户组“应用管理组for A1”的成员（该成员没有加入其他用户组）只能访问企业项目“A1生产”内的云资源，同理，用户组“应用开

发组 for A1”的成员（该成员没有加入其他用户组）只能访问企业项目“A1开发”内的云资源。部门A下面其他企业项目的用户组授权以此类推。

应用开发组、应用测试组和项目管理组的成员在为企业项目创建云资源时，可能会用到放置到default项目的共享云资源，例如创建一个ECS云主机时会用到default项目中的VPC、共享带宽等。因此需要在default项目中为这些用户组授予共享云资源的ReadOnly权限。

说明

admin用户组是系统默认生成的，拥有账号下的所有操作权限，无需手动设置该用户组的权限。

图1-7所示的用户组划分方式将统一管控的范围限制在了部门级（对应子账号），无法做到公司级（对应主账号）的统一管控。如果大公司仍然希望在公司级进行统一资源管控，也可以考虑在公司级（主账号）下创建统一管控资源的用户组，然后在各个子账号下分别创建“普通账号”的委托类型，将子账号下面的资源管理权限委托给主账号，主账号再将这些委托权限分配给统一管控资源的用户组。

涉及到的操作如下：

1. **创建用户组并授权**：您可以通过统一身份认证服务（IAM）来创建用户组并授权。管理员可以创建用户组，并给用户组授予策略或角色，然后将用户加入用户组，使得用户组中的用户获得相应的权限。
2. **为企业项目关联用户组并授权**：将用户组与企业项目关联，并为其设置一定的权限策略，该用户组中的用户即可拥有策略定义的对该企业项目中资源的使用权限。
3. **为企业项目关联用户并授权**：将用户与企业项目关联，并为其设置一定的权限策略，该用户即可拥有策略定义的对该企业项目中资源的使用权限。

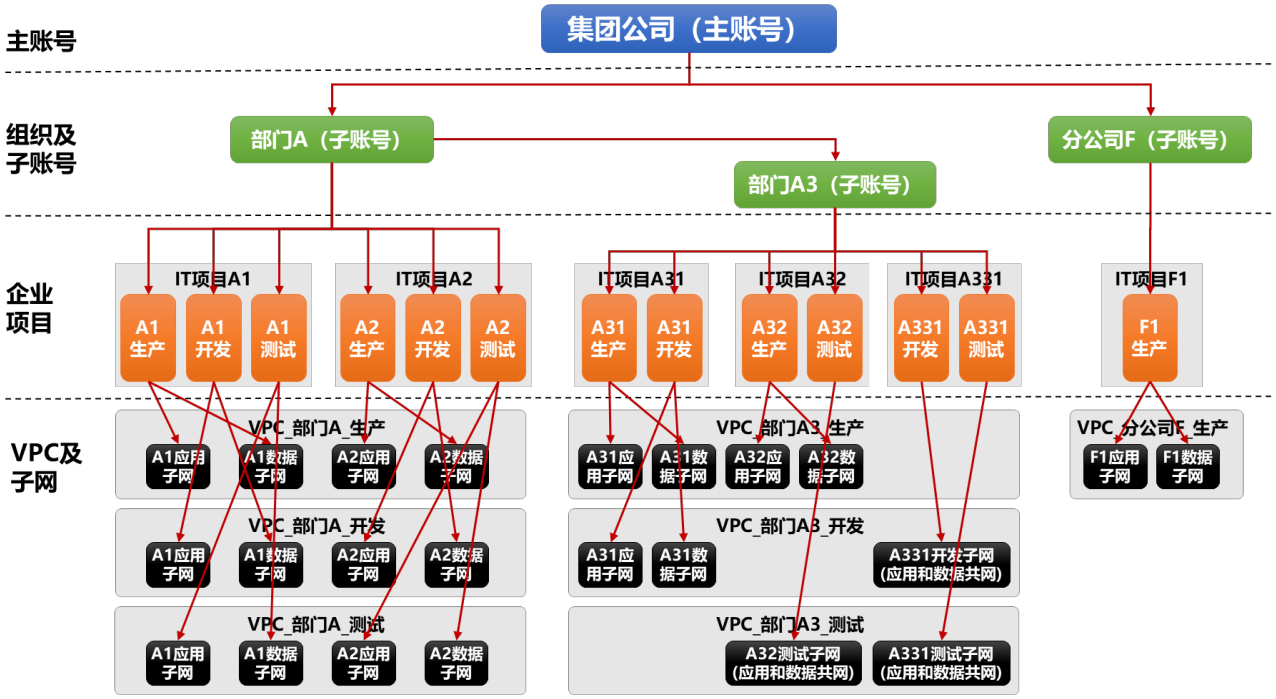
1.2.7 步骤六：规划和创建 VPC（操作主体：网络管理组成员）

以上面集团公司为例，需要针对每个子账号（部门A、部门A3、分公司F）提供多种运行环境：生产环境、开发环境、测试环境，各个运行环境之间需要有一定的安全隔离措施。VPC之间的网络默认不通，具备很好的隔离性，所以推荐在大企业中采用VPC来创建隔离的运行环境，通常一个VPC对应一个隔离的运行环境，推荐的VPC规划如图1-8所示，具体考量因素如下：

- 一个VPC不能跨子账号，所以不能让不同子账号下面的企业项目共享一个VPC，每个子账号都有自己独立的生产、开发和测试VPC。
- 在生产环境内，由于安全隔离要求较高，将各个企业项目的应用系统和数据库系统放在不同的子网，通过网络ACL或安全组对子网间通信进行安全访问控制。
- 在开发和测试环境内，企业项目A1开发、A1测试、A2开发、A2测试、A31开发对安全隔离要求较高，在开发、测试环境中也要求将应用系统和数据库系统部署在不同的子网；而企业项目A32测试、A331开发、A331测试对安全隔离要求较低，在开发、测试环境中将应用系统和数据库系统部署在同一个子网。
- 同一个企业项目在同一运行环境的应用子网和数据子网建议尽量放在同一个可用区内，应用系统和数据库系统之间进行跨可用区通信会引入1-2毫秒的网络时延。例如，企业项目“A1生产”对应的两个子网“A1应用子网”和“A1数据子网”应该设置为在同一个可用区。
- 需要考虑不同子账号下的应用系统之间的交互关系，如果位于不同子账号下的应用系统需要互通，这对应的VPC的网段就不要产生冲突。例如，如果部门A下面的A1生产系统需要与部门A3下面的A31生产系统进行交互，则对应的两个VPC“VPC_部门A_生产”和“VPC_部门A3_生产”的网段不能冲突。

- 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。

图 1-8 集团公司的 VPC 规划



规划完VPC之后需要在华为云上将其创建出来，以集团公司的部门A为例，使用一个网络管理组的成员登录华为云，进入VPC控制台，按照图1-8的VPC规划为部门A创建生产、开发、测试VPC，并为每个企业项目创建相应的应用子网和数据子网。由于这几个VPC内的网络由多个企业项目共享使用，所以创建这些VPC的时候，可以选择归属到default企业项目。

涉及到的操作如下：

1. **网络规划**：在创建VPC之前，您需要根据具体的业务需求规划VPC的数量、子网的数量、IP网段划分和互连互通方式等。
2. **创建虚拟私有云和子网**：当创建新账户或账户余额不足时，主账号可以对现金账户进行充值操作。

1.2.8 步骤七：统一财务管控（操作主体：财务管理组成员）

使用主账号的财务管理组成员登录华为云，进入费用中心，为主账号进行充值、汇款认领、激活代金券、设置余额预警、开票、合同管理。

涉及到的操作如下：

1. **账户充值**：当创建新账户或账户余额不足时，主账号可以对现金账户进行充值操作。
2. **汇款认领**：主账号线下使用通用充值账号汇款到华为云时，需要进行汇款认领，认领成功后的金额会充值到客户的华为云账户中。
3. **激活代金券**：主账号可以使用线下获取的16位激活码，激活生成代金券。
4. **设置余额预警**：开通余额预警后，当可用额度、通用代金券和现金券的总金额低于预警阈值时，系统会自动给联系人发送短信和邮件提醒。

5. **开具华为云发票**：主账号想要对华为云消费的金额进行报销等操作时，可以申请开具发票。
6. **合同管理**：主账号可以根据需求申请线上/纸质合同等。

进入企业中心的“资金拨款与开票”页面，将主账号账户余额、信用额度和代金券划拨给各个子账号。为确保资金安全，需要在企业中心开启资金安全设置，当执行拨款、回收等敏感操作时需要输入验证码。

涉及到的操作如下：

1. **划拨账户余额/信用余额/代金券**：企业主账号可以将自己的账户余额/信用额度/代金券划拨给子账号。
2. **回收账户余额/信用余额/代金券**：企业主账号可以将自己划拨的账户余额/信用额度/代金券进行回收。
3. **设置资金安全**：开启资金安全二次验证功能，可确保资金安全。

主账号财务管理员需要定期审视子账号的资金、信用额度和代金券的使用情况，及时回收各个子账号未使用的资金。也需要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）统计华为云消费汇总并计入企业财务报表。

主账号和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，以降低云资源租用成本。

各子账号财务管理员需要到费用中心持续监控资源到期情况，及时对快到期的资源进行续费。也需要持续监控子账号的账户余额，如果发现账户余额不足够续费时，及时联系主账号的财务管理员进行资金划拨。为防止项目成员过度订购云服务，建议限定各个企业项目在华为云上订购云服务的资金配额限制和余额预警。

各子账号的财务管理员也要定期到费用中心的费用分析页面，按照企业项目、产品类型、区域、计费模式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。

进行成本统计时，可以建立企业项目群将逻辑上相关的几个企业项目放在一起。以集团公司的部门A为例，进入“企业项目群管理”界面，创建两个企业项目群：项目群A1、项目群A2，将三个逻辑相关的企业项目“A1生产”、“A1开发”、“A1测试”放到项目群A1，将另外三个逻辑相关的企业项目“A2生产”、“A2开发”、“A2测试”放到项目群A2，然后就可以按照项目群A1、A2进行成本统计了。

涉及到的操作如下：

1. **创建企业项目群**：开通了企业项目的用户可以将其账号下的企业项目进行分类，同一类型的企业项目加入到同一企业项目群中，方便用户按企业项目群对企业项目进行财务管理。
2. **查看企业项目群的消费统计**：可查看近12个月的月度消费金额和消费信息等。

1.2.9 步骤八：订购和使用云资源（操作主体：具备权限的用户）

创建好VPC和子网后，就可以为各个企业项目订购云资源了。首次在华为云上订购云资源时，往往会一次性订购大量的云资源，涉及的资源类型也很多，包括计算、存储、网络、数据库、安全、大数据等云资源，如果使用不同权限的用户组分别订购的话，来回切换用户组不是很方便，所以建议首次订购时直接使用admin组下的用户完成所有初始资源的订购。后面再由其他具备权限的用户组成员针对某类资源执行扩容、修改、启停等操作，如由计算管理组成员对云主机进行弹性伸缩设置、创建镜像、开关机等操作。

订购云资源时，需要选择将资源放入对应的VPC和子网。以企业项目“A1生产”为例，申购的ECS云主机时将其VPC设置为“VPC_部门A_生产”，如果该云主机用于部署应用软件，则将其子网设置为“A1应用子网”，如果该云主机用于部署数据库软件，则将其子网设置为“A1数据子网”。后续由安全管理员为“A1应用子网”和“A1数据子网”设置网络ACL进行安全访问控制。

订购云资源的时候要指定一个企业项目，这些订购的云资源被创建出来后将归属到该企业项目进行成本核算和权限控制，用户还可以在资源管理控制台、云服务器控制台等地方按照企业项目筛选查看资源。每个账号下面有一个default企业项目，可用于包含统一管理、统一订购的云资源，供其他企业项目共享使用，针对大型企业的特点，推荐但不局限于将以下云资源放到default项目进行共享：

表 1-3 多个企业共享使用的云资源

资源分类	推荐放入default企业项目供其他企业项目共享使用的云资源
计算	镜像服务IMS等
存储	云备份CBR（含云服务器备份、云硬盘备份和混合云备份）、对象存储OBS、CDN等
网络	虚拟私有云VPC、共享带宽、云连接DC、域名解析DNS等
安全	DDoS高防等
应用中间件	应用与数据集成平台ROMA、API网关等
大数据及AI	智能数据湖运营平台DAYU、云数据迁移CDM等

说明

华为云上各个云服务在持续对接企业项目的过程中，目前阶段并不是所有的云服务都支持放置到企业项目，随着对接过程的完成，未来会更新上表中的内容。

订购云资源时或者在创建完资源后可以给这些资源打标签（需要具备TMS管理员权限），打完标签后，可以在资源管理控制台、云服务器控制台按照标签筛选查看资源，也可以在创建资源合规检查的时候按照标签筛选要检查的目标资源。

1.2.10 步骤九：开启云审计（操作主体：安全管理组成员）

使用一个安全管理组的成员登录华为云，进入云审计服务的控制台，**开通云审计服务**，将会生成一个名为“system”的管理事件追踪器，开通云审计后系统将自动跟踪当前租户在当前区域（Region）内所有云资源的操作记录。云服务审计仅保存近7天的操作记录，如果需要保存更长时间的操作记录，需要开通**OBS**（对象存储服务）转储，将操作记录长期保存到OBS中。开通云审计服务可以满足企业的安全审计和合规要求。

接下来创建关键操作通知，在发生特定操作（如创建或删除资源）时，使用SMN（消息通知服务）主题，向用户手机、邮箱发送消息，也可直接发送http/https消息。可用于实时感知高危操作、触发特定操作或对接租户自有审计分析系统。

说明

CTS（云审计服务）的作用范围是区域级，如果租户同时在多个区域订购了资源，需要分别在这几个区域开通云审计服务和关键操作通知。

1.2.11 步骤十：资源合规检查（操作主体：admin 组成员）

使用一个admin组的成员登录华为云，进入配置审计控制台，**添加资源合规规则**，可以直接选用**系统内置预设策略**快速添加一组合规规则，用于评估资源是否满足合规要求。添加资源合规规则时可以指定评估的资源范围，还可以通过资源ID或标签指定资源类型下的某个具体资源参与规则评估。通过资源合规检查可以满足企业的安全合规要求。

在安全合规方面，启用华为云安全服务，如企业主机安全、Web应用防火墙、云堡垒机、数据库安全审计、加密服务、态势感知和MDR安全专业服务等，确保应用系统的安全合规和稳定运行。