组织管理

目录

产品动态

2025年12月

时间节点	功能名称	功能描述	相关文档
2025/12/15	组织管理	组织管理功能内测转商用	组织管理

产品介绍

产品概述

组织管理为企业用户提供多账号关系的管理能力。用户可以将多个账号整合到创建的组织中，并集中管理组织下的所有账号，还可以在组织中统一治理成员账号的权限策略。

术语解释

主账号

在天翼云注册的独立账号，且完成了企业实名认证的实体账号。在该账号下申请开通的企业中心功能，主账号是企业中心管理员账号，是唯一可以访问且管理企业中心平台功能的账号。

子账号（成员账号）

在天翼云注册的独立账号，且完成了企业实名认证的实体账号。通过主账号邀请或者创建，成为了主账号下的关联账号，子账号（成员账号）无法登录企业中心，资源/权限/财务等受到主账号管理。

组织

“组织”是企业中心账号间的虚拟归属关系，将子账号划分到归属的组织，便于统一操作与管理。企业中心当前最多支持三层组织架构。

一个组织由管理账号、成员账号、组织单元组成。一个组织有且仅有一个管理账号，若干个成员账号，以及由一个根组织单元和多层级组织单元组成的树状结构。成员账号可以关联在任一层级的组织单元。

组织策略

可以为组织绑定权限策略，绑定后的策略对组织内所有成员账号中的IAM用户生效。

创建/邀请

主账号可以创建或邀请子账号，但受一定约束条件，满足条件的账号才可以进行邀请或者创建，共同组成企业中心下的组织单元。

功能介绍

组织策略管理

组织策略

“组织策略”是一种基于组织的访问控制策略。组织管理账号可以使用组织策略指定组织中成员账号的权限边界，限制账号内用户的操作。组织策略可以关联到组织、组织单元和成员账号。组织策略关联到组织或组织单元时，该组织或组织单元下所有账号受到该策略影响。

- 当组织未设置任何策略时，因系统默认在根组织中配置有“CtyunFullAccess全局权限”，该组织以及子组织下面的所有账号及IAM用户权限判定遵循CTIAM的权限返回。关于CTIAM的介绍可参考“统一身份认证CTIAM”

- 当组织添加策略后，组织策略将作用于组织以及子组织下面关联的所有账号，其判定优先级高于CTIAM。
- 按组织策略的限制，账号只能做限定允许的操作或非限定禁止的操作。
- 当前组织策略仅对成员账号下的IAM子用户生效。

策略

策略是IAM提供的细粒度权限集合，可以精确到具体资源、条件等。使用基于策略的授权是一种灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对弹性云主机服务，管理员能够控制IAM用户仅能对云主机的资源进行指定的管理操作。

策略包含系统策略和自定义策略两种，“组织策略”及为定义到企业中心组织的访问控制策略。

系统策略

云服务在IAM预置的常用权限集合，称为系统策略。管理员给用户组授权时，可以直接使用这些系统策略，系统策略只能使用，不能修改和删除。如果管理员在IAM控制台给用户组或者委托授权时，无法找到特定服务的系统策略，这是因为该服务暂时不支持IAM，管理员可通过天翼云网门户给对应云服务提交工单，申请该服务接入IAM并预置权限。如何选择对应的系统策略，可从“系统策略”中查询。

自定义策略

如果系统策略无法满足授权要求，管理员可以根据各服务支持的权限，创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制，自定义策略是对系统策略的扩展和补充。您可以通过可视化和JSON视图完成自定义策略的配置。如何创建自定义策略，可参考“创建自定义策略”。

操作实践

操作方式及指引请参考“用户指南”。

组织资源管理

查看组织资源

在企业中心，资源管理界面可查询组织内所订购的资源情况。

支持按账号维度进行资源筛选查询，支持按组织维度进行资源筛选查询，同时也支持企业内全局资源的查询与展示。

管理组织资源

若管理员账号需要对资源管理界面的资源进行操作，在获取子账号授权后（邀请或创建子账号勾选“允许资源管理”权限），管理员可通过云SSO功能，跨账号登陆访问成员账号，进行资源的管理与维护。

可信服务

什么是可信服务

可信服务是指可与组织管理服务集成，提供组织级相关能力的云服务。管理账号及主账号可以在组织中开启某个云服务为可信服务。成为可信服务后，云服务可以获取组织中的组织单元及成员账号信息，并基于此信息提供组织级的管理能力。例如，开启云防火墙为可信服务后，云防火墙可以获取组织单元及成员账号信息，统一为整个组织提供基于云防火墙的产品服务。

产品介绍

什么是委托管理员

委托管理员账号是一个组织中有特殊权限的成员账号。管理账号可指定某个成员账号为某个可信服务的委托管理员账号。成为委托管理员账号后，该成员账号下的用户可以使用对应可信服务的组织级管理能力。例如，某一个成员账号成为云防火墙的委托管理员后，可以共享云防火墙服务在组织成员账号内共同防护。

当前支持可信服务的云产品

可信服务	功能介绍	是否支持委派管理员账号	相关文档
云防火墙	云防火墙集成组织管理后，能够统一管理多账号的公网IP资产，统一配置防御策略，实现集中安全管控。	是	多账号管理

启用或禁用可信服务

登入企业组织管理员账号后，您可以在“企业中心-可信服务”界面，对支持可信服务的产品进行开启或禁用。

- 组织管理员禁用某个云服务的可信访问后，此云服务便不能给成员账号创建此服务的服务关联委托。
- 服务启用可信后才可以设置委托管理员。

设置委托管理员

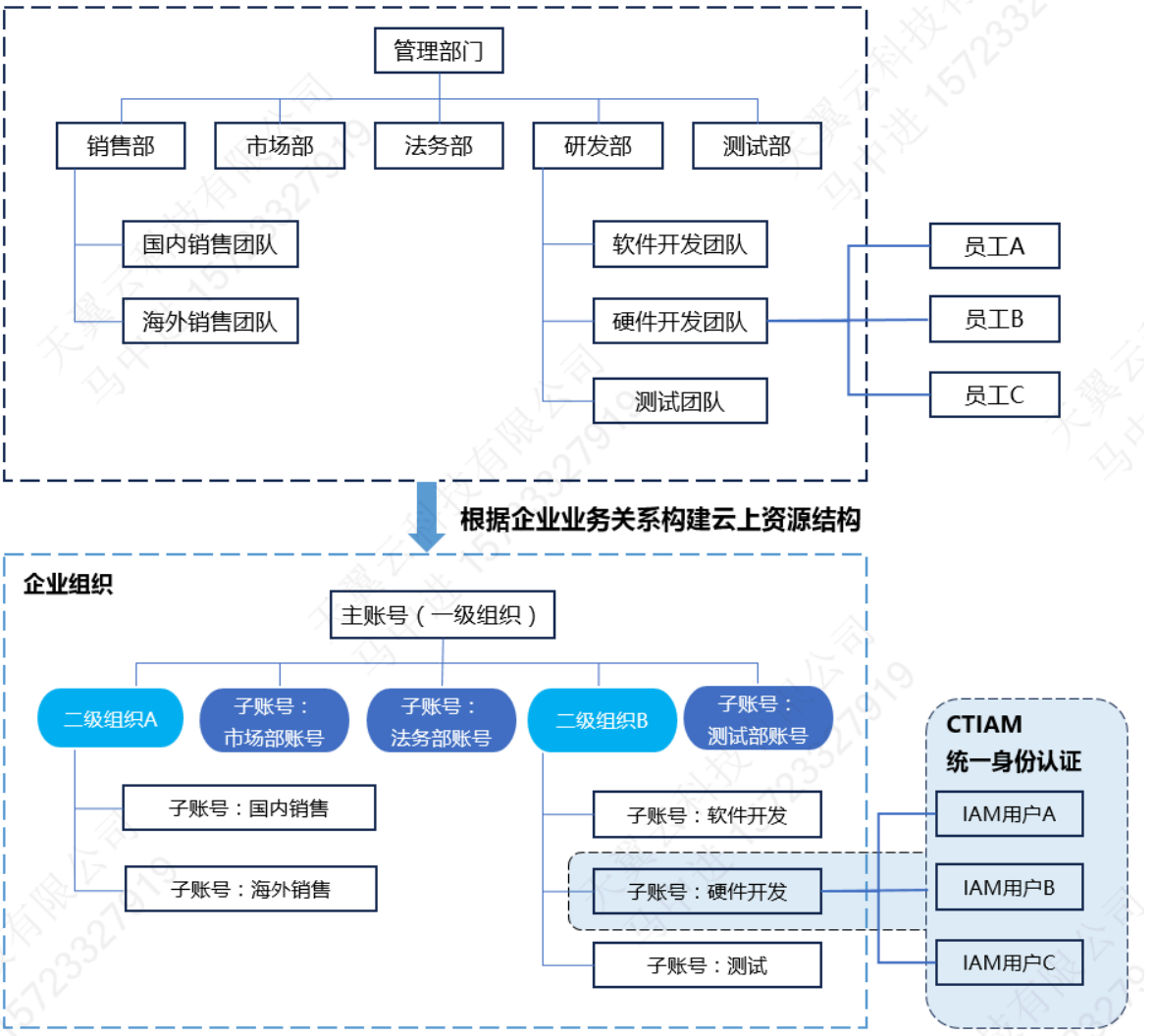
- 使用企业中心管理员账号登入“企业中心-可信服务”界面。
- 选择对应云服务，点击“启用”，开启该云服务可信功能。
- 选择对应云服务，点击“设置委托管理员”设置对应云服务的委托管理员账号。

取消委托管理员

- 使用企业中心管理员账号登入“企业中心-可信服务”界面。
- 选择对应云服务，点击“查看委托管理员”
- 点击“取消委托”

应用场景

根据企业业务关系构建云上组织架构



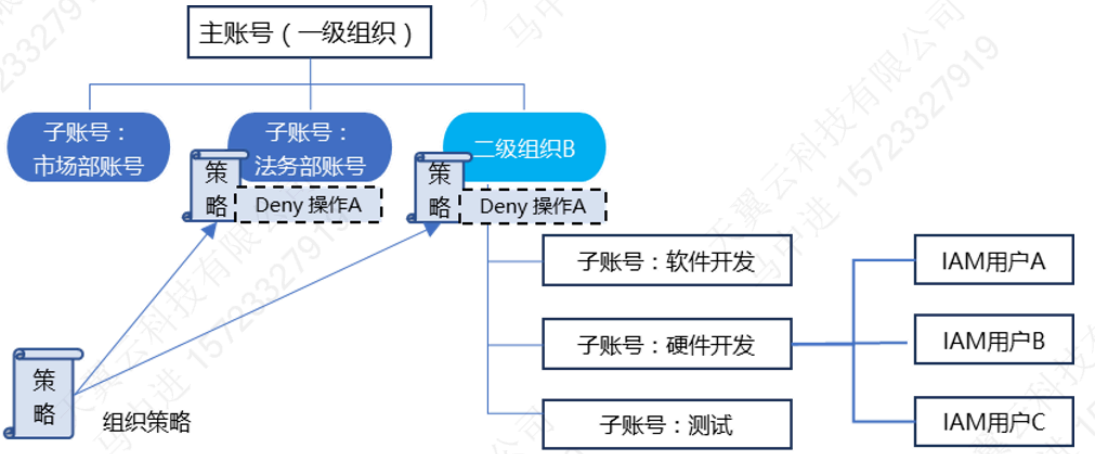
说明：子账号与IAM用户的区别：

子账号是完成实名认证的实体账号。IAM用户是某个天翼云账号下的通过IAM云服务创建出来的虚拟用户，所有IAM虚拟用户创建出的资源都归属该账号。

统一预防业务违规行为

管理部门可以根据业务规则要求，对其下组织及成员账号统一设置上云的行为边界，“组织管理”服务可以主动拦截成员账号内不符合策略要求的行为，以预防业务违规操作。

下图示例：当为“法务部子账号”以及“二级组织B”进行“拒绝操作A”的策略绑定后，法务部子账号”以及“二级组织B”下的子账号，上述子账号内的所有IAM用户将不允许执行操作A。



为其它服务提供企业级的治理框架

为企业内跨账号的上云服务提供组织成员架构，供其它云服务调取，如可信服务、财务管理、资源共享等均依赖组织管理架构。

计费说明

组织管理当前为免费试用的云服务

创建/邀请子账号

前提条件

完成企业中心的开通，开通方式参考“开通企业中心”。

只有企业中心管理员账号及主账号可以创建/邀请子账号。

子账号关联模式

子账号分“财务托管”与“财务独立”两种关联模式

财务托管：指主账号对子账号的财务纳入统一管控，包括资金代付，发票代开等。子账号无独立的商务，账单/订单由主账号支付，子账号专注于业务层面的资源使用与管理。

财务独立：指子账号具备自主处理自身财务事务的核心权限，同时主账号可按需进行辅助管理。

更多规则与介绍，请参考“ 创建子账号 ”“ 邀请子账号 ”。

附1：各渠道账号关联账号支持规则

关联模式/账号渠道		天翼云公司		天翼云省分公司		电信省公司	
		线上预付费账号	线下后付费账号	线上预付费账号	线下后付费账号	线上预付费账号	线下后付费账号
创建子账号	财务独立模式	支持	支持（需客户经理完成申请）	支持	支持（需客户经理完成申请）	不支持	不支持
	财务托管模式	支持	支持（需客户经理完成申请）	支持	支持（需客户经理完成申请）	不支持	不支持
邀请子账号（跨渠道账号之间不能邀请）	财务独立模式	支持	支持	支持	支持	支持	支持
	财务托管模式	不支持	不支持	不支持	不支持	不支持	不支持

说明

1. 后付费客户账号若要创建子账号，需要联系客户经理，由客户经理或客服人员在BCP系统完成申请后，才能创建子账号。省公司渠道账号暂时不允许创建子账号。
2. 由主账号创建出来的子账号，其实名认证以及渠道信息继承主账号信息。
3. 由主账号邀请加入的子账号，原则上要求子账号必须与主账号实名认证信息一致，或为关联母子公司。
4. 同一个实名认证主体，当前天翼云最多允许存在五个天翼云账号，若需要提高限额，需联系客户经理申请。

创建/邀请子账号方式

绑定方式

进入“企业中心-组织管理”，进入界面点击“创建/邀请”子账号，并勾选管理员账号所需权限范围。邀请子账号加入组织，需要子账号在企业中心入口，查阅授权范围并勾选“同意邀请”后才能建立绑定关系。

勾选权限

在关联关系绑定时，主账号需要选择对子账号的管理权限。邀请模式下，关联关系的绑定，需要子账号确认授权并接受邀请。

- 允许主账号查看子账号的财务信息（余额/消费/成本/订单/账单等）
- 为子账号发票开具
- 允许子账号集成主账号的商务折扣
- 允许主账号管理子账号的云资源

为组织成员分配权限

创建自定义策略

目前组织策略管理支持以下两种方式创建自定义策略：

1. 可视化视图：通过可视化视图创建自定义策略，无需了解JSON语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
2. JSON视图：通过JSON视图创建自定义策略，可以直接在编辑框内编写JSON格式的策略内容。

可视化视图配置自定义策略

1. 进入“组织策略管理>全部策略”页面。
2. 点击“创建自定义策略”按键，进入创建自定义策略页面。
3. 输入策略名称、策略描述等基本信息后，点击“下一步”。
4. 选择“可视化视图”，按页面提示进行选择。

   效果：选择“允许”或“拒绝”。

   云服务：选择需要进行权限控制的云服务。

说明

1. 此处只能选择一个云服务，如需配置多个云服务的自定义策略，请在完成此条配置后，点击“添加权限”，创建多个服务的授权语句。或使用JSON视图配置自定义策略。
2. 暂不支持一个自定义策略同时包含全局级云服务和资源池级云服务。如果需要同时设置全局级服务和资源池级服务的自定义策略，请创建两条自定义策略，便于授权时设置最小授权范围。
3. 操作：根据需求勾选产品的操作权限。
4. 资源：默认配置所有资源。若选择“特定资源”，可以根据目前权限的关联资源路径模板，通过单击“添加资源”来指定需要授权的资源。

5. （可选）选择“JSON视图”，将可视化视图配置的策略内容转换为JSON语句进行检视和编辑，您可以在JSON视图中对策略内容进行修改。

   如果您修改后的JSON语句有语法错误，将无法创建策略，可以根据提示信息自行检查并修改内容。

   此外，如果将JSON语句重新转换到可视化视图时失败，一般是由于Statement下包含多个不同云服务的Action，和可视化的映射规则不符合，这种情况不会影响策略的正常创建。
6. 点击“保存”，完成自定义策略的创建。

JSON视图配置自定义策略

1. 进入“组织策略管理>全部策略”页面。
2. 点击“创建自定义策略”按键，进入创建自定义策略页面。
3. 输入策略名称、策略描述等基本信息后，点击“下一步”。
4. 选择“JSON视图”。
5. （可选）在“策略内容”区域，点击“从已有策略复制”，例如选择“ecs admin”作为模板。

说明

此处仅可选择一个服务策略，这些策略的作用范围必须一致，即都是全局级服务或者资源池级服务。如果需要同时设置全局服务和资源池级服务的自定义策略，请创建两条自定义策略，便于授权时设置最小授权范围。

6. 修改模板中策略授权语句。您可以参考策略语法，完成策略JSON语句的编写。

作用（Effect）：允许（Allow）和拒绝（Deny）。

权限集（Action）：写入各服务API授权项列表中“授权项”中的内容，例如："ecs:cloudServers:start"，来实现细粒度授权。

说明

自定义策略版本号（Version）固定为1.1，不可修改。

7. 点击“保存”后，系统会自动校验语法，如跳转到策略列表，则自定义策略创建成功。如提示“策略内容错误”、“JSON格式有误”，请按照策略JSON语法规范进行修改。

编辑企业组织策略

约束与限制

您只能对自定义策略进行编辑，您不能编辑系统策略。

操作步骤

1. 进入“组织策略管理>全部组织策略”页面。
2. 在策略列表选择已有策略，点击右侧操作栏的“编辑”按键，进入策略编辑页面。
3. 根据需要，编辑策略名称、策略描述后，点击“下一步”。
4. 选择“可视化视图”或“JSON视图”编辑自定义策略内容，策略内容的编辑详见策略语法。点击“保存”完成编辑。

删除企业组织策略

约束与限制

您只能对自定义策略进行删除，删除自定义策略前，请解除该策略在用户组、用户上的授权关系。

操作步骤

1. 进入“组织策略管理>全部组织策略”页面。
2. 点击策略管理列表操作栏的“删除”。
3. 在弹出的二次确认提示框中，点击“确认”即可删除成功。

绑定/解绑企业组织策略

绑定企业组织策略

1. 进入“组织策略管理>组织对应策略”页面。

2. 选择组织后，点击“绑定策略”。
3. 可在弹窗页面搜索选择策略，点击“确认”后则绑定成功，该组织应用的策列列表显示该策略信息。

解绑企业组织策略

1. 进入“组织策略管理>组织对应策略”页面。
2. 选择组织后，可查看组织绑定的策略，选择待解绑的策略，点击操作列的“取消绑定”。
3. 在弹出的二次确认提示框中，点击“确认”后则解绑成功，该组织应用的策列列表清除该策略信息。

查看组织全局资源

组织名称/账号名称搜索

1. 进入“资源管理>组织资源视图”页面。
2. 左侧组织与账号层级列表，支持组织名称/账号名称搜索，点击搜索结果组织/账号，右侧展示该组织/账号的资源信息。

所属资源池筛选、搜索

1. 进入“资源管理>组织资源视图”页面。
2. 以下拉列表形式展示资源池，默认展示全部。点击可搜索选择，页面下方展示筛选后的资源信息。

资源名称/ID搜索

1. 进入“资源管理>组织资源视图”页面。
2. 筛选搜索类型“资源名称”或“资源ID”，输入资源名称/ID，可跨账号搜索资源。

说明

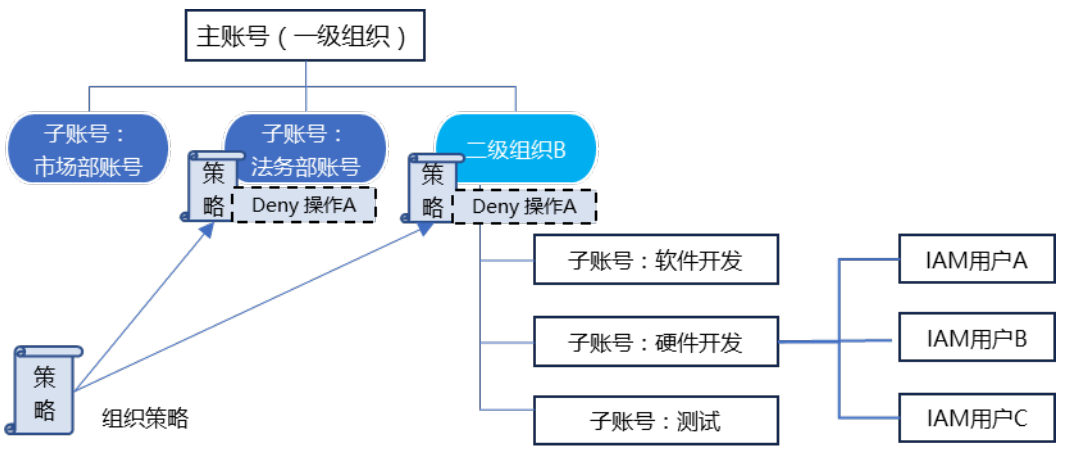
仅限已授权展示资源视图的账号，可进行按需筛选与搜索

为企业配置全局权限

统一预防业务违规行为

管理部门可以根据业务规则要求，对其下组织及成员账号统一设置上云的行为边界，“组织管理”服务可以主动拦截成员账号内不符合策略要求的行为，以预防业务违规操作。

下图示例：当为“法务部子账号”以及“二级组织B”进行“拒绝操作A”的策略绑定后，法务部子账号”以及“二级组织B”下的子账号，上述子账号内的所有IAM用户将不允许执行操作A。



策略绑定执行后，法务部门子账号与二级组织B下的所有子账号在控制台将无法执行“操作A”。

常见问题

我是主账号，为什么我不能创建子账号？

天翼云对不同渠道来源的账号做了创建子账号的限制动作。若您为电信省公司渠道账号将不允许在企业中心创建子账号，您可以通过客户经理为您创建账号，再进行邀请加入企业组织。若您为天翼云公司或天翼云省分公司后付费渠道账号，需要由客户经理在BCP完成申请动作才能在企业中心创建子账号。

邀请子账号有什么限制？

被邀请的子账号需要完成企业实名认证，且原则上要求待被邀请的子账号实名认证信息需与主账号一致，或为关联企业。

代理商渠道账号是否允许开通企业中心功能?

暂时不支持代理商渠道账号开通企业中心。

企业组织对成员账号的授权与CTIAM授权的区别？

企业组织对成员账号的授权是隐式拒绝权限，是范围权限，判定成员账号只能在其授权范围内，对账号下的用户进行权限管理。对某个IAM用户而言，企业组织权限判定优先级高于CTIAM。

财务托管与财务独立模式子账号的区别？

详细请参考“关联账号”。

使用协议

企业中心服务声明协议

企业中心服务协议

天翼云企业中心财务托管协议