ALIBABA CLOUD

Alibaba Cloud

资源管理

最佳实践

文档版本：20220531

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.资源目录

1.1. 使用管控策略实现企业可用云产品白名单

使用管控策略的允许（Allow）效果，可以简单方便地实现企业可用云产品白名单，规范企业内部用户订购和使用云产品的行为。

应用场景

企业上云过程中，一般会根据企业自身情况，通过调研和挑选，圈定需要订购的云产品列表，并与云厂商签订批量订购协议，从而使企业利益最大化。企业内部会要求各用户从圈定的云产品列表中进行订购，避免企业利益受损。这就是常见的企业需要启用可用云产品白名单的场景。

另外，基于安全合规考虑，企业需要启用可用云产品白名单，用来规范用户的使用行为，避免有意或无意的违规。

方案对比

老方案：通过访问控制（RAM）授予用户指定云产品的权限

该方案是授权到每个用户，适用业务场景比较单一的情况。当授权的数量、授权维度增加时，通过该方式满足企业可用云产品白名单的要求就会比较难，且管理成本会比较高。具体体现在以下几个方面：

- 针对用户的点对点授权，复杂度与您所管理的用户和资源数量成正比。

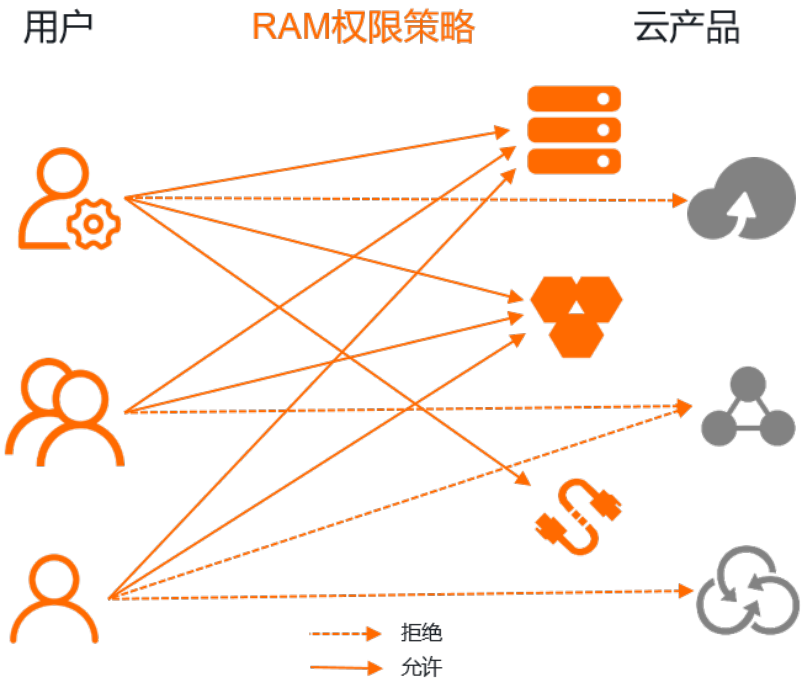
  您要为每个用户在对应环境内配置访问不同资源的所需权限。当某个用户不再需要某个权限，或者需要修改其权限时，您需要找到这个用户进行权限更新。在新增用户和减少用户时，您需要设置和回收权限。当可用云产品白名单需要更新时，您不得不再次对所有已生效用户同步这个更新，策略的维护成本不可避免。

- 授权策略复杂，需要满足赋权和规避策略的双重要求。

  当授权的因素涉及到更多维度时（例如：需要考虑资源所在位置、所在业务环境等因素），需要根据不同维度授予不同权限。例如：某地域的资源不允许用户订购、某项目订购云产品的特定限制、某些用户或角色可以无限制操作等。这些情况会进一步增加授权管理的复杂性。

- 授权和管控耦合，带来合规风险。

  权限管理员根据业务需要调整用户的授权以达到业务要求，这些操作需要避开对合规类权限的影响，他（她）需要了解权限设计的所有细节，必要时可能需要合规管理员的协助才能完成。合规管理员也面临同样的问题。很明显，两种角色职能的操作耦合状况，无论对权限管理还是合规管控，都会存在极大的安全隐患。用户身份和被访问的资源间存在诸多特定限制，从而形成复杂的权限配置要求，给管理带来麻烦。



新方案（推荐）：通过管控策略的允许（Allow）策略进行顶层管控

资源目录的管控策略支持了 `"Effect": "Allow"` ，企业可以使用它，简单高效地解决上述问题。管控策略示例如下：

```
{
  "Statement":[
    {
      "Effect": "Allow",
      "Action":[
                "ecs:*",
                "rds:*"
      ],
      "Resource": [
                "acs:*:*cn-beijing*:*:*",
                "acs:*:*cn-shanghai*:*:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
          "StringLike": {
                    "acs:PrincipalARN": [
                    "acs:ram:*:*:role/a-project-admin-*"
                       ]
                  }
            }
      }
  ],
  "Version": "1"
}
```

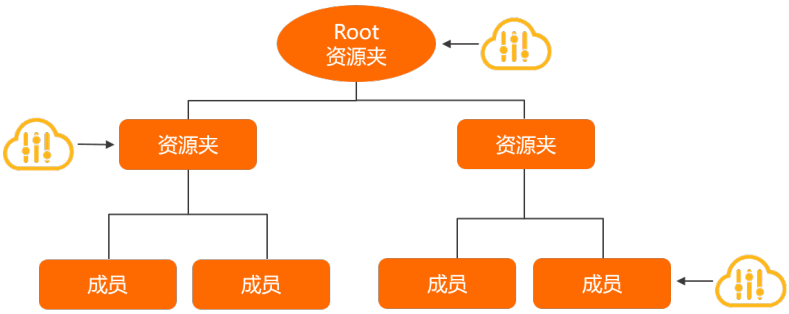
上述管控策略示例中包含以下两个内容：

- 仅允许对华北2（北京）和华东2（上海）地域的ECS和RDS进行操作（即允许订购和使用），禁止对其他不符合条件的云产品进行操作。
- 名为 `a-project-admin-*` 的RAM角色可以无限制地操作。

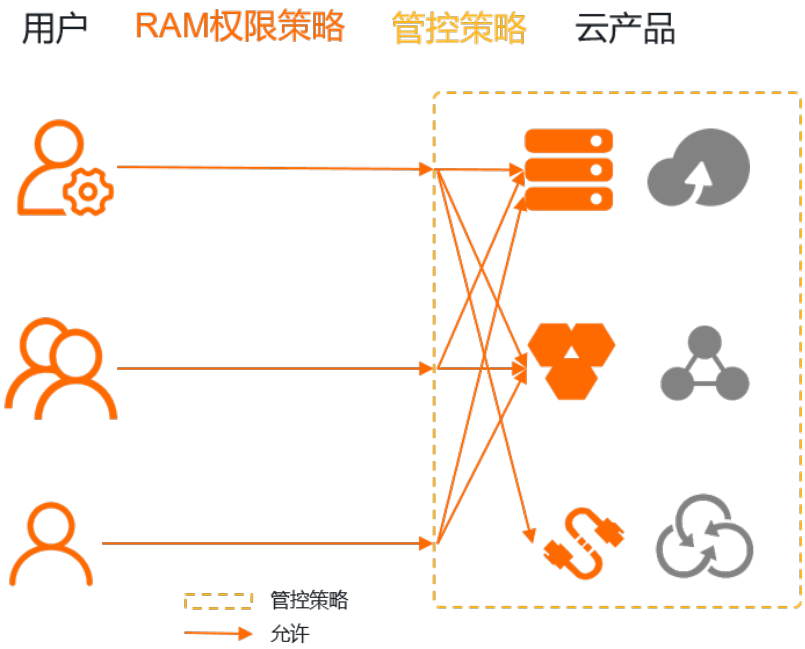
使用管控策略的优势如下：

- 管控策略具备基于资源目录树形结构从上向下继承的特点。

  您只需要将管控策略绑定到需要管控的节点（资源夹或成员）上，它将沿着资源目录树向下（当前节点及其下所有节点）影响所有账号。无论用户以何种方式访问这些账号中的资源，都将受到管控策略的管控，实现预期管控的结果。在需要更新可用云产品白名单时，您只需要维护这条管控策略即可。



- 管控策略不进行授权，它只定义权限的边界，可以在不改变用户原有授权的基础上叠加影响。



假设某用户具有访问ECS和EIP的权限，当该用户被上述示例中的管控策略影响后：

- 该用户可以访问华北2（北京）和华东2（上海）地域的ECS。

  该用户本身具有访问ECS的权限，且管控策略也允许访问华北2（北京）和华东2（上海）地域的ECS，所以该用户可以访问华北2（北京）和华东2（上海）地域的ECS。

- 该用户不能访问EIP。

  虽然该用户具有访问EIP的权限，但管控策略中未包含EIP的允许语句，所以该用户不能访问EIP。

- 该用户不能访问RDS。

  虽然管控策略允许访问华北2（北京）和华东2（上海）地域的RDS，但该用户本身没有被授予访问RDS的权限，且管控策略不会对用户授权，所以该用户不能访问RDS。

- 管控策略与RAM授权策略分开管理，共同生效。

  使用管控策略进行合规管理，使用RAM进行授权管理，使合规管理与授权管理职能分开，从而保护企业合规安全。管控策略属于顶层管控决策，高于授权策略，是企业的基本原则，所有业务规范都必须在企业基本原则之下进行制定。

方案实施

当您充分了解了管控策略新方案后，您可以开启管控策略功能、然后创建自定义管控策略，并将其绑定到资源目录的目标节点上。具体操作，请参见开启管控策略功能、创建自定义管控策略和绑定自定义管控策略。

另外，在实施过程中还需要完成以下任务：

- 在自定义管控策略中，增加允许 `sts:AssumeRole` 策略。

  在资源目录中，推荐您使用RAM用户通过STS方式登录到成员进行管理操作。此时，您需要在管控策略内增加对 `sts:AssumeRole` 的允许语句，确保管理用户的登录权限可用。修改后的管控策略示例如下：

```
{
  "Statement":[
    {
      "Effect": "Allow",
      "Action":[
                "ecs:*",
                "rds:*"
      ],
      "Resource": [
                "acs:*:*cn-beijing*:*:*",
                "acs:*:*cn-shanghai*:*:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*",
      "Condition": {
          "StringLike": {
                    "acs:PrincipalARN": [
                    "acs:ram:*:*:role/a-project-admin-*"
                       ]
                  }
            }
      },
    {
      "Effect": "Allow",
      "Action":[
                "sts:AssumeRole"
      ],
      "Resource": "*"
    }
  ],
  "Version": "1"
}
```

- 在绑定了管控策略的目标节点上，解绑系统管控策略 `FullAliyunAccess` 。

  为了避免启用自定义管控策略后因为没有显式允许（Allow）而直接导致隐式拒绝（Implicit Deny）所有操作，资源目录会默认为每个节点绑定系统管控策略 `FullAliyunAccess` ，该策略允许所有访问。在您使用了自定义Allow管控策略后，则需要解绑系统管控策略 `FullAliyunAccess` ，避免您自定义的Allow管控策略无效。关于管控策略的工作原理，请参见工作原理。

了解更多

在上述示例中，企业需要对ECS、RDS之外的所有云产品实施禁用，如果使用拒绝（Deny）语句，企业不得不列出ECS、RDS之外的所有云产品，这个操作非常繁琐，且容易遗漏。在使用Allow语句后，实现过程就变得简单可靠。

如果您有明确的禁用操作项，且数量不多时，您可以使用Deny语句显式拒绝这类操作。例如：明确不允许订购中国（香港）和华南3（广州）地域的云产品，您可以使用Deny语句，策略示例如下。如果使用Allow语句，反而复杂了。

```
{
      "Effect": "Deny",
      "Action":[
                "*"
      ],
      "Resource": [
                "acs:*:*cn-hongkong*:*:*",
                "acs:*:*cn-guangzhou*:*:*"
      ]
}
```

因此，您需要根据实际业务场景，灵活使用管控策略的Allow和Deny语句，简化策略的编写。

在一个管控策略中可以包含多组Allow和Deny语句，您需要评估其合并后产生的最终结果，在设计时避免它们之间产生冲突。一旦冲突，会遵照Deny优先原则。同一节点上绑定的所有管控策略，也会被合并在一起进行鉴权，只要命中Deny语句，系统会直接判定结果为显式拒绝（Explicit Deny），结束整个鉴权流程。

2.资源共享

2.1. 使用资源目录和共享VPC实现多账号网络互通

2.1.1. 方案概述

企业可以使用资源目录RD（Resource Directory）将多账号有序组织和管理，然后通过共享VPC快速实现多账号间的网络互通。

背景信息

随着云计算的普及，越来越多的企业将业务放在了云端，企业采购的云资源也越来越多，随之而来的问题是：企业如何高效地管控云资源。按组织结构划分业务、业务之间强隔离及多种结算模式等需求之下，单账号模式已无法支撑企业的持续发展。如果企业只是简单的使用多账号模式来适应业务发展需要，就会面临以下问题：

- **多账号管理问题**

  无序、散落的多个阿里云账号不便于集中管理，企业需要进一步做精细化管控。

- **多账号网络互通问题**

  企业可以采用云企业网CEN（Cloud Enterprise Network）将多个账号间的专有网络VPC（Virtual Private Cloud）进行连接，以实现多账号间的网络互通。但随着业务复杂度的增加，会面临如下的新问题：

  - 分散配置导致无法进行网络集中运维

    企业网络架构是一张经过规划的大网，当网络设施分散在每个业务账号之下时，企业网络运维人员很难做到网络的集中控制。

  - 重复网络资源配置导致成本增加

    在每个账号内进行VPC的配置，使得企业的配置维护成本和实例费用成本都在增加。

  - VPC数量增多导致网络复杂度提升

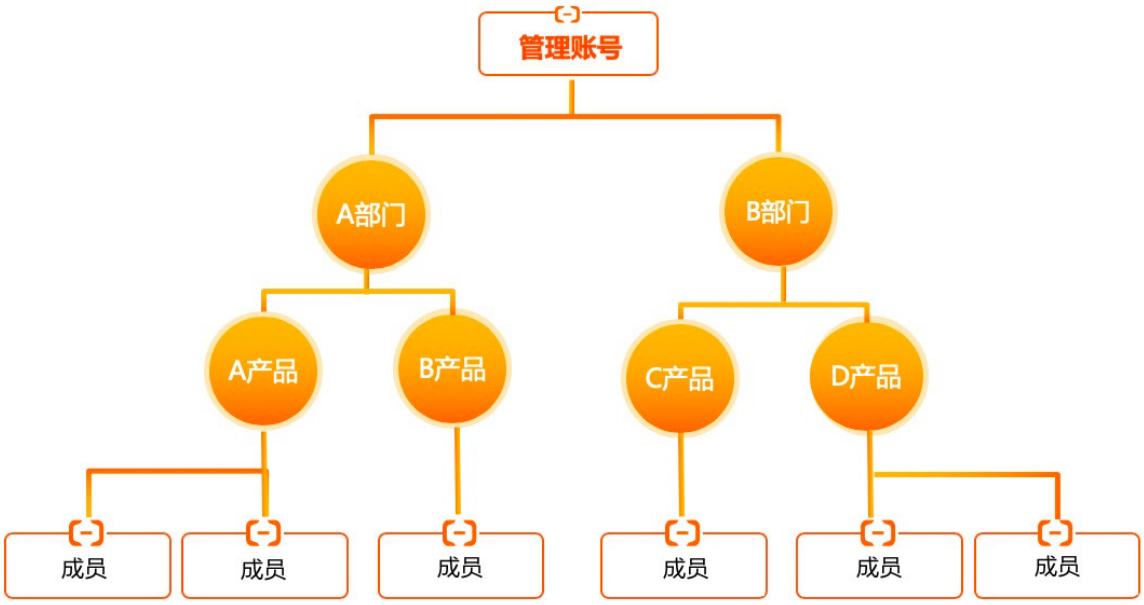
    为了满足企业的业务需要，VPC数量会不断攀升，随之而来的是网络复杂度、管理难度和配额（例如：CEN可挂载的VPC数量限制）等问题。

解决方案

阿里云提供了资源目录解决多账号管理问题，提供了资源共享RS（Resource Sharing）和共享VPC解决多账号网络互通问题。具体如下：

- **使用资源目录构建多账号管理体系**

  阿里云资源目录是面向企业提供的一套多级资源和账号关系管理服务。企业可以基于自身的组织结构或业务形态，在资源目录中构建目录结构，将企业的多个账号分布到这个目录结构中的相应位置，从而形成资源间的多层级关系。企业可依赖设定的组织关系进行资源的集中管理，满足企业资源在财资、安全、审计及合规方面的管控需要。更多信息，请参见资源目录。



- **使用资源共享构建成员间的共享关系**

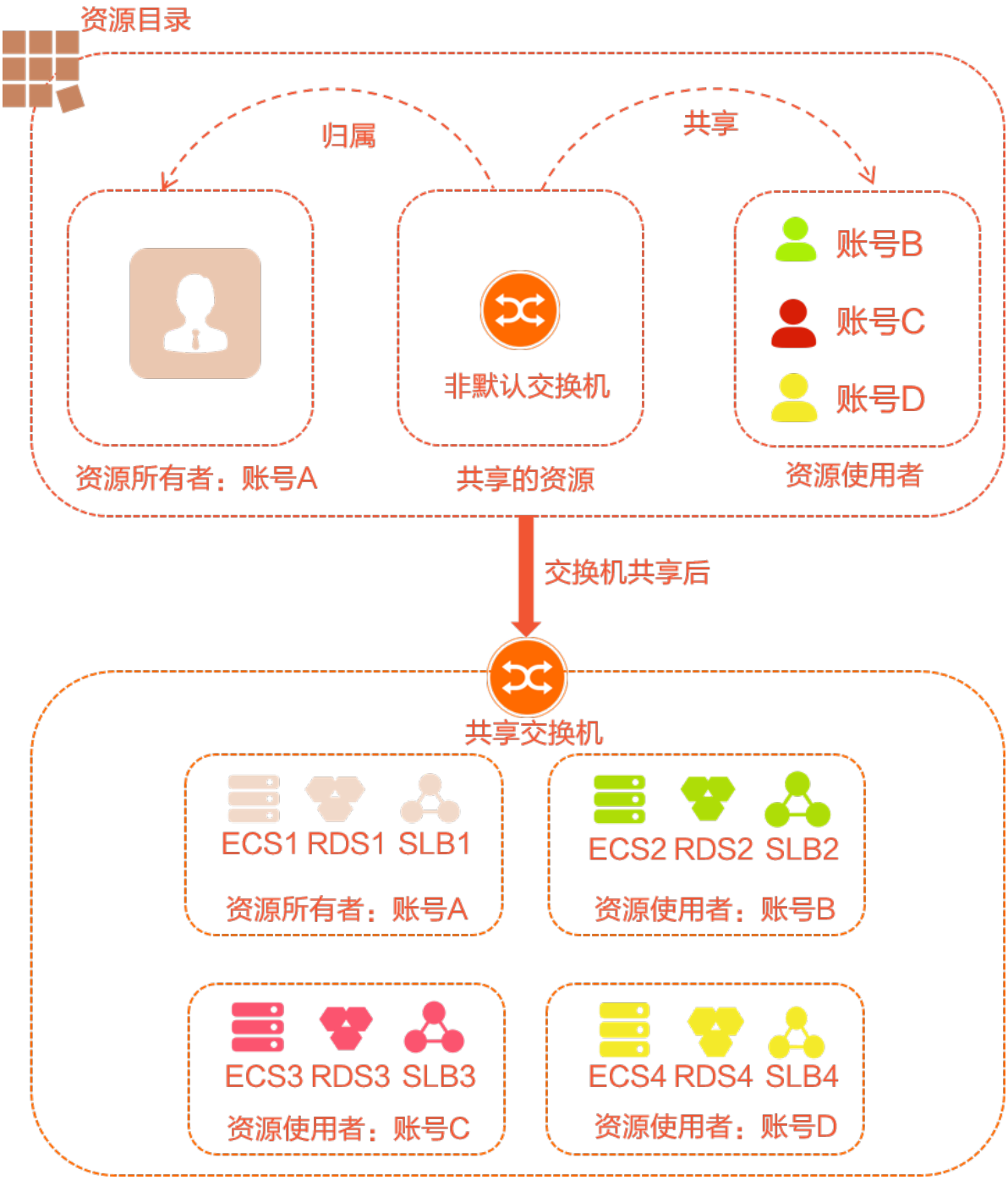
  在资源目录内，企业可以使用阿里云提供的资源共享服务，将一个账号下的指定资源共享给一个或多个目标账号使用，通过共享单元建立成员间的共享关系。更多信息，请参见资源共享概述。

概念	说明
共享单元	共享单元是资源共享的实例。共享单元本身也是一种云资源，拥有独立的ID和ARN（Aliyun Resource Name）。共享单元包括：资源所有者、资源使用者和共享的资源。
资源所有者	资源所有者是资源共享的发起方，也是共享资源的拥有者，通常为资源目录的管理账号或成员。
资源使用者	资源使用者是资源共享的受益方，对共享的资源具有特定的操作权限，通常为资源目录内的一个或多个成员。 **说明** 资源使用者对共享资源的具体操作权限，由资源所属的云服务定义。例如：共享专有网络（VPC）的交换机（vSwitch）资源后，资源使用者的操作权限请参见共享VPC权限说明。

概念	说明
共享的资源	共享的资源通常为某个云服务的某类资源。
资源目录组织共享	资源目录组织共享是指将资源共享给整个资源目录（Root资源夹）、资源夹或成员。具体操作，请参见启用资源目录组织共享。

- **共享VPC**

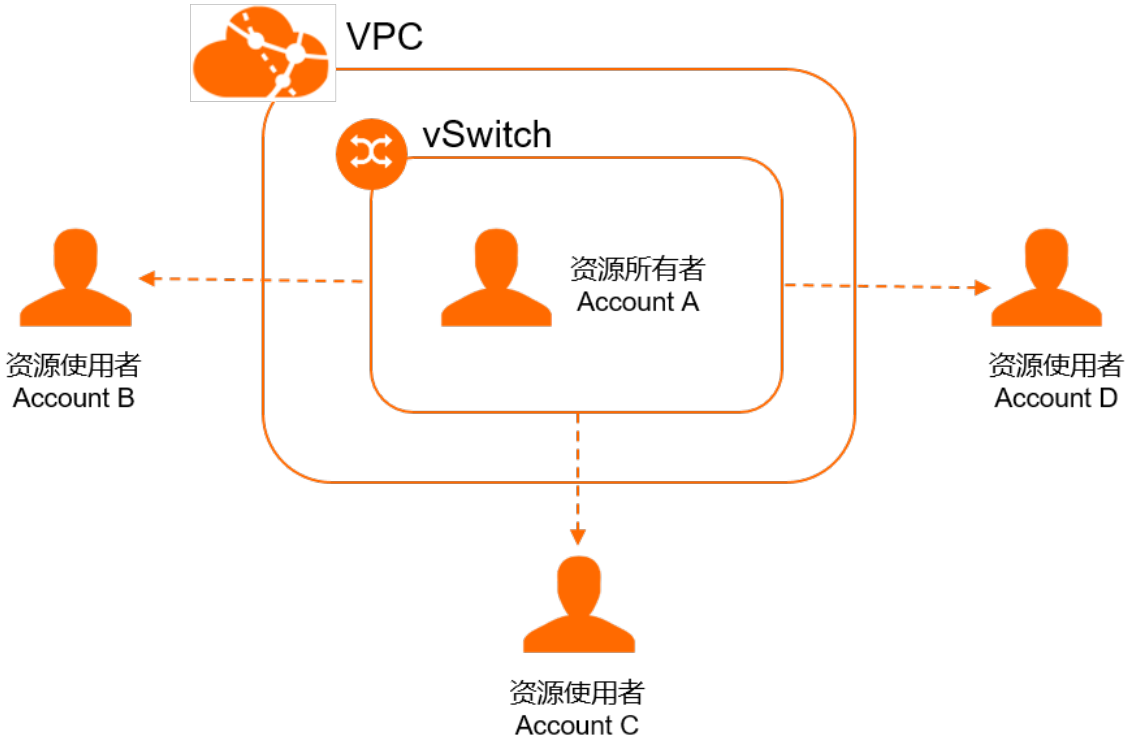
  企业可以基于资源共享机制，在资源目录内，将一个成员的VPC交换机（vSwitch）共享给其他成员使用，使多个成员在一个集中管理、共享的VPC内创建云资源，例如：云服务器ECS、负载均衡SLB、云数据库RDS等。共享交换机后，资源使用者无需确认，默认直接接受共享。资源所有者和资源使用者在同一VPC内创建的云资源默认私网互通。更多信息，请参见共享VPC概述。



共享VPC的具体实现细节如下：

- **多账号共享同一个交换机**

  企业可将VPC的交换机在多账号间进行共享，不用为每个账号单独配置VPC，极大减少了VPC的使用数量。



- **资源所有者与资源使用者的权限**

  资源所有者将交换机共享给资源使用者后，资源所有者与资源使用者对共享交换机及共享交换机内云资源的操作权限如下表所示。

角色	支持的操作	不支持的操作

资源所有者	■ 支持创建、查看、修改、删除共享交换机中的由自身创建的资源。
	■ 支持查看资源使用者在共享交换机中所创建的资源的属性，允许查看的资源属性仅限：
	  ■ 实例ID。
	  ■ 私网IP地址。
	  ■ 资源所属账号。
		不支持修改、删除资源使用者在共享交换机中创建的任何资源。

资源使用者	当交换机处于共享状态时，资源使用者支持在共享交换机中创建、修改、删除云资源。	当交换机处于共享状态时，资源使用者不支持查看、修改、删除共享交换机中其他账号（包含资源所有者和资源使用者）的任何资源。
	当交换机处于取消共享状态时，资源使用者支持继续使用共享交换机中由自身创建的已有资源，也支持查看、修改、删除共享交换机中由自身创建的已有资源。	当交换机处于取消共享状态时，资源使用者不支持查看与共享交换机相关联的资源（例如VPC、路由表、私网网段、网络ACL），也不支持在已经取消共享的交换机中创建资源。

资源所有者与资源使用者对其它网络资源的操作权限如下表所示。

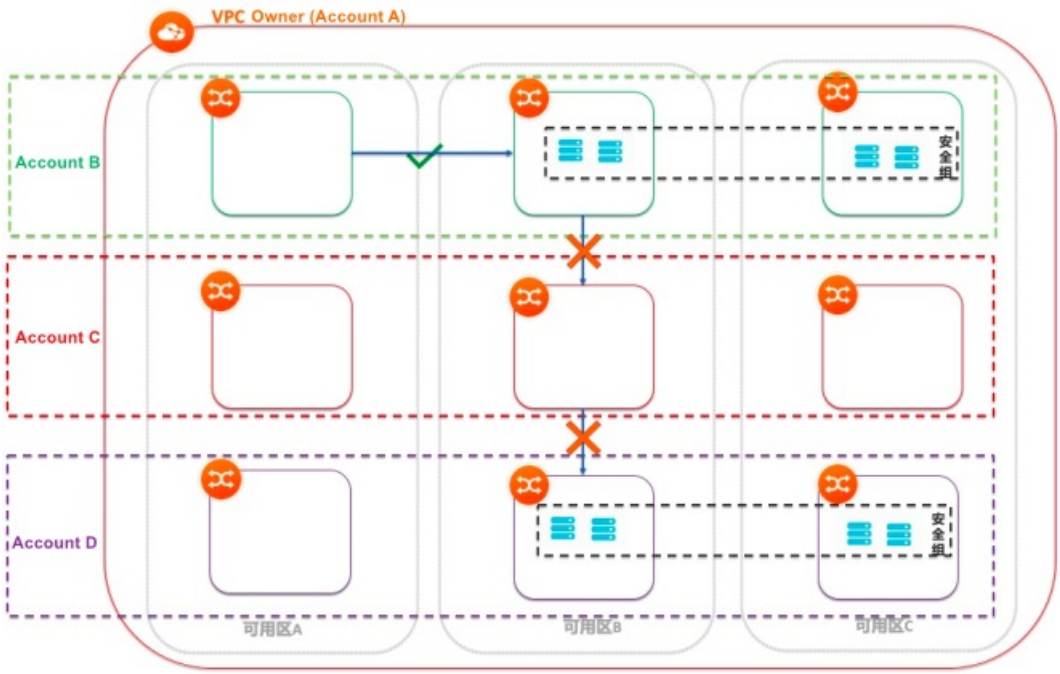
网络资源	资源所有者可执行的操作	资源使用者可执行的操作
VPC	全部操作权限。	仅支持查看共享给自己的交换机所属的VPC。
交换机	全部操作权限。 **说明** 如果要删除交换机，请确保交换机已取消共享，且该交换机中的资源（包括资源所有者和资源使用者创建的资源）已全部删除。	■ 查看共享的交换机。 ■ 在共享的交换机内创建、修改、删除云资源。
路由表	全部操作权限。	仅支持查看共享给自己的交换机绑定的路由表以及路由条目。
网络ACL	全部操作权限。	仅支持查看共享给自己的交换机绑定的网络ACL。
私网网段	查看VPC及VPC内所有交换机的私网网段。	仅支持查看共享给自己的交换机的私网网段。
流日志	■ 支持创建VPC或交换机粒度的流日志，对资源使用者的交换机下的弹性网卡生效。 ■ 支持创建弹性网卡粒度的流日志，仅对资源所有者的弹性网卡生效。	无操作权限。
NAT网关	公网NAT网关和VPC NAT网关的全部操作权限。 **说明** ■ 交换机中的资源（包括资源所有者和资源使用者创建的资源）可以通过公网NAT网关与互联网通信。 ■ 公网NAT网关仅支持绑定资源所有者的弹性公网IP。	无操作权限。
VPN网关	全部操作权限。 **说明** 交换机中的资源（包括资源所有者和资源使用者创建的资源）可以通过VPN网关与VPC外部网络互通。	无操作权限。

网络资源	资源所有者可执行的操作	资源使用者可执行的操作
云企业网	全部操作权限。 **说明** 交换机中的资源（包括资源所有者和资源使用者创建的资源）可以通过云企业网与VPC外部网络互通。	无操作权限。
VPC对等连接	全部操作权限。 **说明** 交换机中的资源（包括资源所有者和资源使用者创建的资源）可以通过VPC对等连接与VPC外部网络互通。	无操作权限。
标签	共享行为不影响资源所有者为资源配置的标签。 资源所有者将交换机共享给资源使用者后，资源所有者与资源使用者都可以为各自的资源配置标签，且标签互不可见也互不影响。当共享交换机取消共享后，系统会删除资源使用者在该共享交换机上配置的标签。	

- **安全隔离**

  企业将单个VPC中的不同交换机共享给不同账号后，网络是默认连通的。在某些场景下，企业希望将不同的交换机进行隔离。企业可通过以下两种方式进行隔离：

  - 网络ACL：实现跨交换机级别的访问控制。
  - 安全组：实现实例级别的访问控制，并且支持跨账号安全组的互相引用。

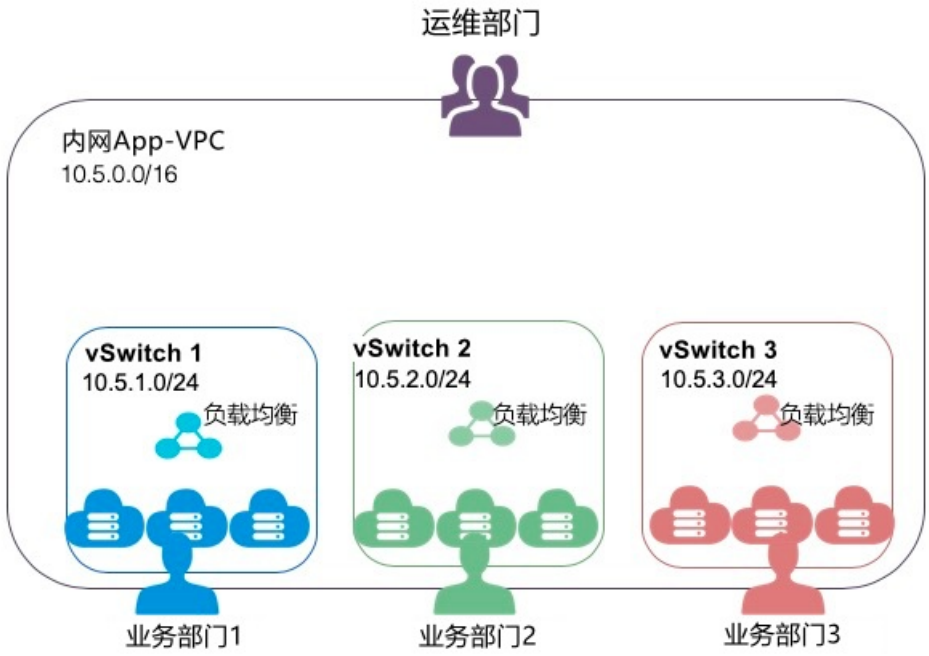


> **说明** 使用安全组设置两个实例间禁止访问规则实现网络隔离，该方法主要用以弥补在相同交换机内的实例之间无法采用网络ACL进行网络隔离的缺失。当然，企业仍然可以使用安全组跨账号引用能力，在安全组内配置源IP地址和目标IP地址，实现不同交换机、不同账号间的网络隔离。

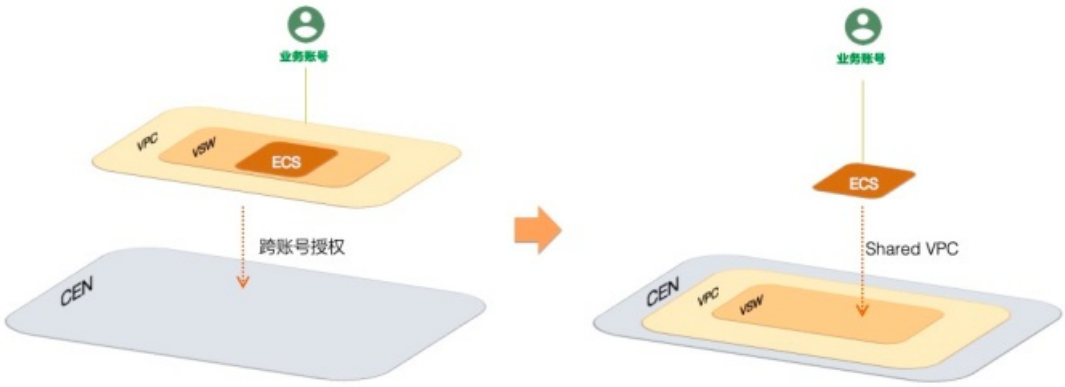
方案优势

该方案具备以下优势：

- 运维部门集中规划、配置和管理VPC，并将VPC的交换机共享给业务部门。



- 业务部门只能查看和管理自己交换机中的资源，可以根据业务需求添加或删除交换机中的云服务器、数据库等资源。



- 企业采用统一的网络架构和安全策略，业务部门可以聚焦自身业务需求。
- 企业可以将网络和安全能力作为一个服务供业务部门使用，将运维体系标准化和流程化，并提升整个组织的IT效率。

2.1.2. 操作指南

在资源目录内，一个成员（资源所有者）可以将自己专有网络（VPC）内的交换机（vSwitch）共享给另外一个成员（资源使用者）使用。本文将提供一个示例，为您介绍具体的操作。

使用限制

操作前，您需要了解共享VPC的使用限制，请参见使用限制。

步骤一：使用资源目录管理多账号

阿里云资源目录支持企业通过创建成员和邀请成员两种方式将企业所有账号集中在一个资源目录内进行管理。请使用资源目录的管理账号完成以下操作。

1. 开通资源目录。

   具体操作，请参见开通资源目录。

2. 根据企业组织结构创建资源夹。

   具体操作，请参见创建资源夹。

3. 创建成员或邀请成员。

   具体操作，请参见创建成员或邀请阿里云账号加入资源目录。

步骤二：启用资源目录组织共享

1. 使用资源目录的管理账号登录资源共享控制台。
2. 在左侧导航栏，选择**资源共享 > 设置**。
3. 单击**启用**。
4. 在**资源共享服务关联角色**对话框，单击**确定**。

   系统会自动创建一个名为AliyunServiceRoleForResourceSharing的服务关联角色，用于获取资源目录的组织信息。更多信息，请参见资源共享服务关联角色。

步骤三：资源所有者创建共享单元

资源所有者在资源共享控制台创建共享单元，然后添加需要共享的VPC资源和资源使用者。

1. 创建共享单元，并添加需要共享的VPC资源和资源使用者。
   i. 登录资源共享控制台。
   ii. 在左侧导航栏，选择**资源共享 > 我的共享**。
   iii. 在顶部状态栏，选择要共享的VPC的所属地域。
   iv. 单击**创建共享单元**。
   v. 在**创建共享单元**页面，输入**共享单元名称**（例如：Finance_VPC）。
   vi. 在**选择共享的资源**区域，先选择资源类型，然后选中需要共享的资源（例如：交换机vsw-bp183p93qs667muql****），最后单击**添加**。

vii. 在**添加资源使用者**区域，先选择添加方式，然后添加资源使用者（例如：177242285274****）。

- 通过资源目录添加

  > **说明** 该方式仅限资源目录的管理账号使用。

  从资源目录中直接选择资源使用者。具体如下：

  - Root资源夹：选择Root资源夹，将资源共享给该资源目录下的所有成员。
  - 资源夹：选择资源夹，将资源共享给该资源夹下的所有成员。
  - 成员：选择成员，将资源共享给该成员。

- 手动添加

  先选择使用者类型，然后输入资源夹ID或成员UID，最后单击**添加**。具体如下：

  - **资源目录组织**：自动获取资源目录ID，将资源共享给该资源目录下的所有成员。
  - **资源夹（组织单元）**：输入资源夹ID，将资源共享给该资源夹下的所有成员。
  - **阿里云账号**：输入成员UID，将资源共享给该成员。

viii. 单击**确定**。

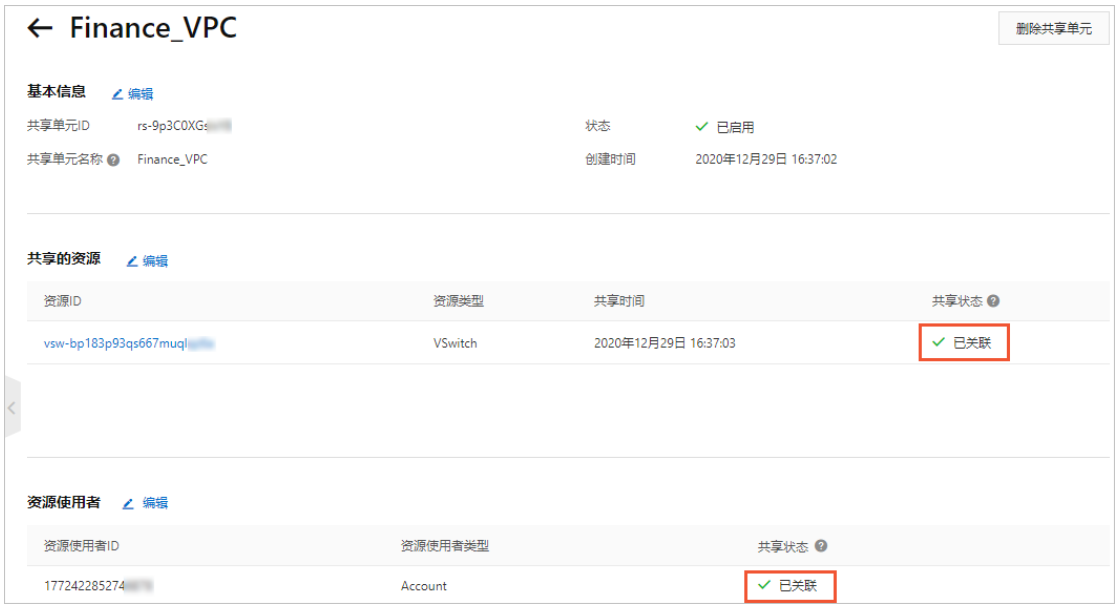
2. 查看共享单元详情。

i. 在共享单元列表中，查看**共享单元ID/名称**、**状态**和**创建时间**。

如果共享单元状态显示为**已启用**，表示共享单元创建成功。

ii. 单击共享单元ID链接，查看共享单元详情。

如果**共享的资源**和**资源使用者**的状态显示为**已关联**，表示共享的资源和资源使用者添加成功。



3. （可选）修改共享单元信息。

在共享单元详情页面，单击各个区域的**编辑**可以修改共享单元名称、添加或移除共享的资源、添加或移除资源使用者。具体操作，请参见资源所有者修改共享单元名称、资源所有者添加或移除共享资源或资源所有者添加或移除资源使用者。

步骤四：资源使用者查看和使用共享的交换机

资源所有者共享交换机后，资源使用者无需确认，默认直接接受共享的交换机。资源使用者可以查看共享给自己的交换机，并在共享的交换机中创建云资源，例如：云服务器ECS、负载均衡SLB、云数据库RDS等。

1. 使用资源使用者账号（例如：成员177242285274****）登录控制台，查看共享的交换机（vsw-bp183p93qs667muql****）。

> **说明** 资源使用者可以在资源管理控制台或者VPC控制台查看共享的交换机。具体操作，请参见查看共享交换机。

> **说明** 虽然资源所有者共享的是交换机，但因网络需要，在专有网络控制台会产生专有网络、路由表和交换机三条共享记录。

2. 在VPC控制台，资源使用者可以修改共享的专有网络、路由表及交换机的名称和描述信息。

> **说明** 该信息为资源使用者私有，资源所有者不能查看或修改该信息。

3. 资源使用者在共享交换机内创建云资源。
   i. 在**交换机**页面，找到目标共享交换机，单击**操作**列的**创建**，然后选择并创建云资源。

> **说明** 资源使用者也可以在各云产品控制台创建对应的云资源。其中，配置网络时，请选择共享的交换机。

ii. 查看交换机内创建的云资源。

资源使用者可以在VPC控制台或云产品控制台查看创建成功的云资源。下图为在VPC控制台查看的结果：

3.资源组

3.1. RAM资源分组与授权

若您的公司购买了多种阿里云资源，您可以通过创建资源组进行云资源分组，从而实现独立管理资源组内成员、权限和资源。

背景信息

游戏公司A正在开发3个游戏项目，每个游戏项目都会用到多种云资源。公司A只有1个阿里云账号，该阿里云账号下有超过100个ECS实例。

公司A有如下要求：

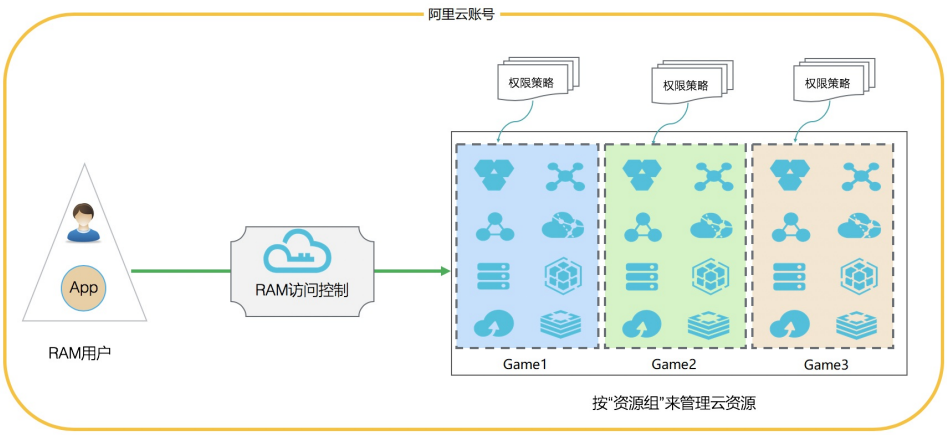
- 项目独立管理：每个管理员各自能够独立管理项目人员及其访问权限。
- 按项目分账：财务部门希望能够根据项目进行出账，以解决财务成本分摊的问题。
- 共享底层网络：客户希望云资源的底层网络默认共享。

公司A有如下解决方案：

- 多账号方案
  - 可以满足项目独立管理：公司A注册3个阿里云账号（对应3个项目），每个阿里云账号有对应项目管理员可以独立管理成员及其访问权限。
  - 可以满足按项目分账：每个阿里云账号有默认账单，可以利用阿里云提供的多账号合并记账能力来解决统一账单和发票问题。
  - 无法满足共享底层网络：阿里云账号之间是有安全边界的，不同阿里云账号之间的资源是100%隔离的，网络之间默认不通。虽然可以通过VPC-Peering来打通跨账号的VPC网络，但会带来较高的管理成本。
- 单账号给资源打标签方案
  - 无法满足项目独立管理：给资源打标签可以模拟项目分组，但无法解决项目管理员独立管理项目成员及其访问权限的问题。
  - 可以满足按项目分账：按照项目组给资源打上对应标签，根据标签实现分账。
  - 可以满足共享底层网络：公司A只用1个阿里云账号，根据项目打不同的项目标签，结合RAM提供的基于标签的条件授权能力，可以将一组资源授权给某些RAM用户，不存在打通网络所需的额外管理成本。
- 资源组管理方案
  - 可以满足项目独立管理：每个资源组有对应的管理员，资源组管理员可以独立管理成员及其访问权限。
  - 可以满足按项目分账：账单管理功能支持按资源组进行分账，解决财务成本分摊的问题。
  - 可以满足共享底层网络：资源组属于账号内部的分组功能，同一阿里云账号下的不同资源组可以共享同一个VPC网络，节约管理成本。

解决方案

资源组是在阿里云账号下进行资源分组管理的一种机制，公司A只需使用1个阿里云账号，创建3个资源组（对应3个项目）。



1. 创建3个RAM用户：`Alice@secloud.onaliyun.com`、`Bob@secloud.onaliyun.com`和`Charlie@secloud.onaliyun.com`。

   具体操作，请参见创建RAM用户。

   > **说明** 下面的操作均以RAM用户Alice为例，介绍如何将其设为项目的管理员。

2. 登录资源管理控制台。
3. 在**资源组**页面，单击**创建资源组**。
4. 在**创建资源组**面板，输入**资源组标识**和**资源组名称**，然后单击**确定**。

   > **说明** 创建3个资源组，分别命名为：Game1、Game2、Game3。

5. 单击目标资源组**操作**列的**权限管理**。
6. 在**权限管理**页签，单击**新增授权**。
7. 在**新增授权**面板的**被授权主体**区域，输入`Alice@secloud.onaliyun.com`。
8. 选择系统策略`AdministratorAccess`。
9. 单击**确定**。
10. 单击**完成**。

    > **说明** 如何将Bob或Charlie设置为资源组管理员，请参考上述步骤。

执行结果

由于Alice、Bob和Charlie分别是Game1、Game2、Game3的资源组管理员，将有以下权限：

- 登录ECS控制台，可以查看相应资源组，并可以创建和管理ECS实例。
- 登录资源管理控制台，可以管理资源组内已经授权的RAM用户、RAM用户组和RAM角色。

3.2. 资源组分账

资源分组管理之后，通过创建对应的财务单元，将资源组对应到财务单元，实现按资源组分账。

背景信息

某游戏公司A正在开发3款游戏项目，每个游戏项目都会用到多种资源。目前公司A只有1个账号，该账号下有超过100个ECS实例。

财务部门希望能够根据项目进行出账，以解决财务成本分摊的问题。

操作步骤

1. 创建资源组。
   i. 登录 资源管理控制台。
   ii. 创建各项目的资源组。
   详情请参见：创建资源组。
   iii. 将资源移动到对应的资源组内，确保分组正确。
   详情请参见：跨资源组转移资源。
2. 创建财务单元。
   i. 在控制台右上角的顶部菜单，选择**费用 > 用户中心**。
   ii. 在左侧导航栏，选择**企业财务 > 财务单元**。
   iii. 在左侧财务单元树中，单击**新增**，创建资源组对应的财务单元。

   > **说明** 创建的财务单元可与资源组名称保持一致，便于管理。

3. 将资源组对应到财务单元。
   i. 在左侧财务单元树底部，单击**未分配**分类后，右侧将列出所有未分配财务单元的资源。
   ii. 通过**资源组**筛选，列出一个资源组下的所有资源。全选后，单击**分配**。

   > **注意** 资源组的信息不会实时同步到财务单元。如果资源首次加入资源组，或修改了资源归属的资源组，大约2天后才能在财务单元查看到对应的资源组信息。

   iii. 选择资源组对应的财务单元，将资源分配到财务单元中。
   iv. 在左侧财务单元树中，单击财务单元名称，查看归属该财务单元的全部资源。
4. 按资源组对应的财务单元查看账单。
   i. 在**费用中心**控制台的左侧导航栏，选择**消费总览 > 消费总览**。
   ii. 在**账单明细**页签，根据需要通过筛选功能选择财务单元，查看对应资源组的账单汇总。

相关文档

-
- 财务单元

3.3. 使用操作审计记录资源组操作

操作审计可以记录主账号或RAM用户进行的操作，通过操作审计可以查看所有用户对资源组进行操作的记录。

操作步骤

1. 登录操作审计控制台。
2. 在**历史事件查询**页签下，通过**事件类型**和**时间**筛选事件。

> 说明 您也可以使用高级搜索功能，通过用户名、事件名称、资源名称、资源类型、产品类型及Access Key进行精准搜索。

3. 在事件列表中，单击目标事件前面的+，展开事件基本信息。
4. 单击**查看事件**查看事件详情。

执行结果


```
{
  "eventId": "B1CFCA37-83FA-4288-B623-01994CF8****",
  "eventVersion": "1",
  "requestParameters": {
  "RequestId": "B1CFCA37-83FA-4288-B623-01994CF8BDD2",
  "DisplayName": "actiontrail",
  "HostId": "resourcemanager-share.aliyuncs.com",
  "Name": "action"
},
  "eventSource": "resourcemanager-share.aliyuncs.com",
  "sourceIpAddress": "42.120.XX.XX",
  "userIdentity": {
  "sessionContext": {
  "attributes": {
  "mfaAuthenticated": "false",
  "creationDate": "2019-03-08T07:00:04Z"
}
},
  "accountId": "123456789012****",
  "principalId": "111749508818****",
  "userName": "root",
  "type": "root-account"
},
  "eventType": "ApiCall",
  "serviceName": "ResourceManager",
  "apiVersion": "2016-11-11",
  "requestId": "B1CFCA37-83FA-4288-B623-01994CF8BDD2",
  "eventTime": "2019-03-08T07:00:04Z",
  "acsRegion": "cn-hangzhou",
  "eventName": "CreateResourceGroup"
}
```


3.4. 使用资源组管理指定的ECS实例

本文介绍了如何使用资源组对ECS实例进行分组并授权，满足RAM用户只能查看和管理被授权ECS实例的需求。

操作步骤

以下将提供一个示例，仅允许RAM用户（Alice）查看和管理ECS实例（i-001），无权查看和管理其他ECS实例。您可以将ECS实例加入到资源组，利用资源组进行分组授权。

1. 在RAM控制台，创建RAM用户（Alice）。

具体操作，请参见创建RAM用户。

2. 在资源管理控制台，创建资源组（ECS-Admin）。

   具体操作，请参见创建资源组。

3. 在资源管理控制台，将ECS实例（i-001）加入资源组（ECS-Admin）。

   ECS实例加入资源组有以下两种方式，请您根据实际情况选择合适的方式：

   - 对于新创建的ECS实例，您可以在创建的同时加入资源组（ECS-Admin）。具体操作，请参见使用向导创建实例。
   - 对于已有的ECS实例，您可以将其转入到对应的资源组（ECS-Admin）。具体操作，请参见跨资源组转移资源。

4. 在RAM控制台，为RAM用户（Alice）授权。

   其中，授权范围选择资源组（ECS-Admin），授权主体选择RAM用户（Alice），权限策略选择系统策略（AliyunECSFullAccess）。具体操作，请参见为RAM用户授权。

   > **说明** 如果您仅允许RAM用户查看ECS实例，该处选择系统策略（AliyunECSReadOnlyAccess）。

5. 在ECS管理控制台，验证结果。

   i. 在左侧导航栏，选择**实例与镜像 > 实例**。

   ii. 在顶部菜单栏左上角处的资源组下拉列表，选择资源组（ECS-Admin）。

   iii. 在实例列表中，查看和管理对应的ECS实例（i-001）。

3.5. 资源组的RAM权限策略示例

本文为您提供资源组的RAM权限策略示例。

以下策略表示：您可以在资源管理中创建资源组、删除资源组、查看和修改资源组基本信息。

```
{
    "Statement": [{
        "Action": "ram:*ResourceGroup*",
        "Effect": "Allow",
        "Resource": "*"
    }],
    "Version": "1"
}
```

> **说明** 如果您想在资源组中进行更多的操作，例如：管理资源组中的资源、为资源组授权和跨资源组转移资源等，您需要添加其他的权限策略。更多信息，请参见资源组鉴权列表。

4.标签

4.1. 设计和管理标签

4.1.1. 标签设计最佳实践

本文为您介绍标签设计的背景、原则、最佳实践以及相关示例。

标签设计的背景

当企业云上资源只有几个或十几个的时候，通过人脑记忆或人工记录即可完成资源的分类。但是，随着企业云上资源不断增加（大型企业资源数量甚至成千上万），单纯依靠人工进行资源的分类变得越来越不可靠。此时，需要借助平台化能力来解决这个问题。

在阿里云，我们推荐您使用标签对资源进行标记，从而实现资源的分类。每个用户在创建资源时都要对资源的业务归属、财务归属等资源属性进行标记，例如：按创建者、地域或项目等。否则，后续再去梳理每个资源的资源属性往往变得事倍功半。

标签设计的原则

- **互斥原则**

  互斥原则是指避免对同一个资源使用两个或以上的标签键。例如：如果已经使用了标签键owner来标识资源的所有者，就不要再使用own、belonger或**所有者**等类似的标签键。

- **集体详尽原则**

  集体详尽原则是指所有资源都必须绑定已规划的标签键及其对应的标签值。例如：某公司有3个游戏项目部，标签键是project，则应至少有3个标签值分别代表这 3个项目部。

  集体详尽原则是后续基于标签维度进行资源检索、分账、自动化运维和访问控制的必要条件。

- **有限值原则**

  有限值原则是指为资源只保留核心标签值，删除多余的标签值。例如：某公司共有5个部门，那么应该有且仅有这5个部门的标签，方便管理。

  有限值原则简化了资源检索、分账、自动化运维和访问控制的流程。

- **考虑未来变化原则**

  考虑未来变化原则是指在设计标签时要考虑后续工作中增加或者减少标签值的影响，尽可能将业务边界划分得更加清晰一点，提高标签修改的灵活性。例如：企业在上云初期业务比较集中，就采用部门标签department来管理部门相关的资源归属、财务归属和自动化运维。随着企业的发展，这一个标签已经承载了一些日常业务，想要区分开就需要耗费一定成本。因此，我们建议，企业在上云初期需要先评估标签的业务诉求，如在上述例子中则需规划同时采用department、costcenter和ops标签。

  当您修改标签时，可能会引起基于标签的访问控制、自动化运维或相关账单报表的变化。无论是公司或个人层面的业务，推荐您创建与业务相关的标签，以便从技术、业务和安全维度管理资源。使用自动化运维来管理资源及服务时，还需要设计额外的自动化运维专用标签，帮助您完成自动化运维工作。

- **简化设计原则**

  简化设计原则是指在设计标签时使用固定的标签，简化标签的使用。标签的设计尽量简化key和value的值，满足业务诉求即可。例如：在设计项目环境维度的标签时，测试环境相关的标签键尽量统一成**测试环境**，不要同时保有多个，如**预测试环境**、**正式测试环境**等。

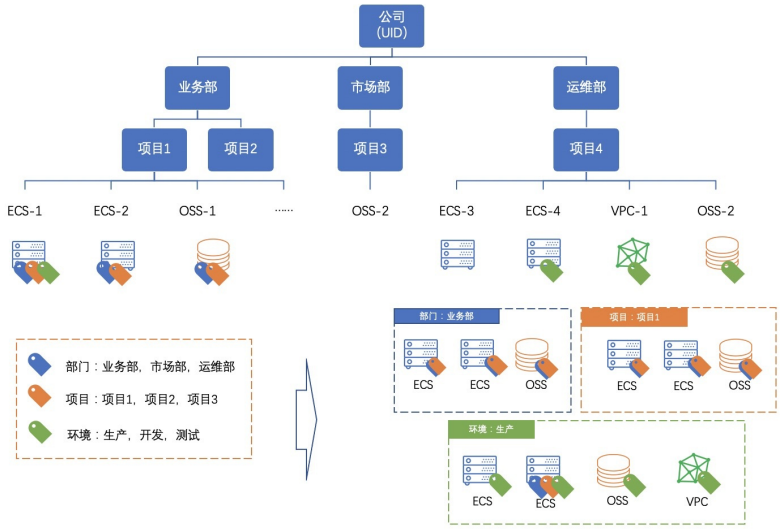
  简化设计原则可以减少由于过多的标签键导致的操作报错。

- **命名标准化原则**

  命名标准化原则是指标签采用标准化命名格式，尽量兼容不同开源工具，使后续的API集成更加便捷。例如：标签命名涉及英文时，建议使用小写英文字母。

标签设计的最佳实践

某互联网公司有3个部门：业务部、市场部和运维部。每个部门管理一个或多个项目，每个项目在不同生命周期有不同环境：生产环境、开发环境、测试环境。公司运维团队需要实时关注整个企业的资源情况，定期对每个项目的资源费用进行分账，实时控制资源的访问，并最终实现自动化运维。



为了满足上述需求，该公司从以下几个方面进行了标签设计。

需求	标签设计	说明
检索和管理资源	为所有资源创建并绑定以下3个层级的标签： • department：资源的部门归属信息 • project：资源的项目归属信息 • environment：资源环境信息	如果企业的组织架构层级比较深，可以考虑更高层级的标签，例如：分公司（company）等。
管理成本和分账	为所有资源创建并绑定成本中心标签： • 标签键：costcenter • 标签值：proj-1、proj-2、proj-3或proj-4	无
资源访问控制	限制非项目组成员对项目内ECS等资源的访问。	具体操作，请参见使用标签控制ECS资源的访问。
自动化运维	创建用途标签键purpose来进行日常资源巡检，标签值为autocheck-8am，即每日早8点自动巡检。如果巡检发现异常，通过资源持有者标签owner来通知具体责任人进行处理。	无

标签设计示例

下表列举了常见维度的标签设计示例。

划分维度	标签键（key）	标签值（value）
组织架构	• company • department • organization • team • group	相关名称
业务架构	• product • business • module • service	相关名称
角色架构	• role • user	• 网络管理员 • 应用管理员 • 系统管理员 • 运维管理员 • 研发 • 测试
用途	• purpose • use	用途值

项目	• 项目维度：
	  ◦ project
	  ◦ risk
	  ◦ schedule
	  ◦ subtask
	  ◦ environment
	• 人员维度：
	  ◦ sponsor
	  ◦ member
	  ◦ owner
	  ◦ creator
		据实填写

业务部门（实现成本分配和业务跟踪）	• costcenter • businessunit • biz • financecontact	据实填写

划分维度	标签键（key）	标签值（value）
财务维度责任人（确定资源负责人）	owner	人名或邮箱等
财务维度客户（识别资源服务的客户）	自定义或真实值	客户名称
财务维度项目（确定资源支持的项目）	project	项目名称
财务维度订单	order	订单分类ID

4.1.2. 标签管理最佳实践

在开通云服务时即使用标签对资源进行标记，可以有效预防因资源标签覆盖度不足导致的标签管理困难。本文列举了不同场景下可以采用的标签管理方式，供您参考。

场景	控制台建议	API建议
通过多云管理平台或自研管理平台管理云资源	不涉及	• 单独调用各云服务API。关于支持标签的云服务API信息，请参见支持标签的云服务。 • 调用统一的标签API TagResources。
通过阿里云管理云资源	• 在开通云服务时对资源进行标记。具体操作，请参见支持标签的云服务表格的**相关文档**列。 • 通过阿里云标签控制台对资源进行统一标记和管理。	

4.2. 使用标签分账

4.2.1. 区分存量资源归属

很多企业在上云初期并没有对资源进行有效管理，在发展一定阶段后，才开始意识到大量的云资源需要进行规范化管理，以匹配高速发展的业务诉求。随之而来的问题是，如何区分存量资源的归属。本文推荐了几种方法供您参考。

区分方法	说明
通过资源名称	如果您在创建资源时习惯对资源进行重命名，那么这些资源往往可以通过名称轻易判断归属，如**业务A-DEV-2020**。
通过创建者信息	如果运维团队的不同人员采用不同账号进行操作，那么您可以通过创建者信息判断资源归属。例如，您可以通过操作审计查询资源的创建者。具体操作，请参见通过操作审计控制台查询事件或LookupEvents。
通过地域信息	如果不同业务或分公司的购买地域不同，那么您可以通过地域信息来判断资源归属。例如，您可以通过操作审计查询地域。具体操作，请参见通过操作审计控制台查询事件或LookupEvents。

区分方法	说明
通过IP地址信息	如果不同业务使用的网段不同，那么您可以通过IP地址的归属网段判断资源归属。例如，您可以通过操作审计查询IP地址的归属网段。具体操作，请参见通过操作审计控制台查询事件或LookupEvents。
通过问询	如果上述方法都无法判断资源归属，那么您可以通过内部邮件发送资源认领通知或者与业务方一起进行资源归属梳理。

4.3. 使用标签进行自动化运维

4.3.1. 使用运维编排服务批量修改标签值

通过创建运维编排服务（OOS）自定义模板，您可以批量修改同一地域下的数百个资源的同一标签的标签值。

前提条件

已为ECS实例绑定一个标签，详情请参见创建并绑定自定义标签。

背景信息

本文以ECS实例为例，创建一个OOS自定义模板，该模板支持一次性修改数百台ECS实例的同一标签值。ECS实例绑定的源标签键值对为 `TagKey:OldTagValue` ，修改后将变为 `TagKey:NewTagValue` 。

> 说明
>
> - 批量修改资源的数量上限为1000，资源数量大于1000时需要多次执行自定义模板。
> - OOS自定义模板可以修改同一地域下任何支持绑定标签的资源，您只需要根据您的业务需求修改相应接口，支持绑定标签的资源，详情请参见支持标签的云服务。OOS支持的资源，详情请参见OOS支持的云产品列表。

步骤一：创建模板

您可以参考以下步骤，创建批量修改标签值的OOS自定义模板。

1. 登录OOS控制台。
2. 在左侧导航栏，单击**我的模板**。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击**创建模板**。
5. 在**基本信息**区域，输入模板名称。
6. 单击**JSON**页签，编写模板代码。

   模板代码示例：

```
{
    "Description": "批量修改资源的标签值",
    "FormatVersion": "OOS-2019-06-01",
    "Parameters": {
        "operateId": {
            "Description": "自定义您的操作ID",
```

```
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        },
        "tagKey": {
            "Description": "当前标签键",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        },
        "tagValue": {
            "Description": "当前标签值",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        },
        "newTagValue": {
            "Description": "修改后的标签值",
            "Type": "String",
            "MinLength": 1,
            "MaxLength": 64
        }
    },
    "Tasks": [
        {
            "Name": "DescribeInstances_ECS",
            "Action": "ACS::ExecuteAPI",
            "Description": {
                "zh-cn": "通过标签过滤ECS实例",
                "en": "filter ecs instances by tags"
            },
            "Properties": {
                "Service": "ECS",
                "API": "DescribeInstances",
                "AutoPaging": true,
                "Parameters": {
                    "Tags": [
                        {
                            "Key": "{{ tagKey }}",
                            "Value": "{{ tagValue }}"
                        }
                    ]
                }
            },
            "Outputs": {
                "Instances": {
                    "Type": "List",
                    "ValueSelector": "Instances.Instance[].InstanceId"
                }
            }
        },
        {
            "Name": "TagResources_ECS_Instances",
            "Action": "ACS::ExecuteAPI",
```

```
            "Description": {
                "zh-cn": "更新ECS实例标签",
                "en": "tag ecs instances"
            },
            "Properties": {
                "Service": "ECS",
                "API": "TagResources",
                "Parameters": {
                    "Tags": [
                        {
                            "Key": "{{ tagKey }}",
                            "Value": "{{ newTagValue }}"
                        }
                    ],
                    "ResourceType": "Instance",
                    "ResourceIds": [
                        "{{ACS::TaskLoopItem}}"
                    ]
                }
            },
            "Loop": {
                "MaxErrors": "100%",
                "Concurrency": 20,
                "Items": "{{DescribeInstances_ECS.Instances}}"
            }
        }
    ],
    "Outputs": {}
}
```

7. 单击**创建模板**。

步骤二：执行模板

您可以参考以下步骤，执行步骤一：创建模板创建的模板，批量修改标签值。

1. 在左侧导航栏，单击**我的模板**。
2. 找到步骤一：创建模板创建的模板，单击**操作**列的**创建执行**。
3. 填写**执行描述**，并选择**执行模式**，然后单击**下一步：设置参数**。
4. 输入各项参数，然后单击**下一步：确定**。

   参数说明如下：

   - operateId：操作ID，用于区分每次操作，可自定义输入。
   - tagKey：当前标签键，本示例为 `TagKey` 。
   - tagValue：当前标签值，即修改前的标签值，本示例为 `OldTagValue` 。
   - newTagValue：新标签值，即修改后的标签值，本示例为 `NewTagValue` 。
5. 单击**创建**。

   执行完成后将自动跳转到执行详情页面，可查看执行结果。

> **说明** 如果执行失败，您可以通过查看执行日志来定位失败原因。

4.3.2. 使用运维编排服务批量绑定标签

如果您希望使用特定标签控制资源的权限，可以通过运维编排服务（OOS）的自定义模板，批量为同一地域下需要控制权限的资源绑定特定标签。

背景信息

云服务器ECS和其他云服务的诸多资源支持绑定标签。如需了解哪些云服务支持绑定标签，请参见支持标签的云服务。

本文以ECS实例为例，创建一个OOS自定义模板，该模板可以为同一地域下的ECS实例批量绑定标签 `owner:zhangsan` 。

> **说明** 需要批量绑定标签的资源必须在同一地域下。

步骤一：创建RAM角色并授权

为OOS创建RAM角色OOSServiceRole，并为RAM角色授权。

1. 使用阿里云账号登录RAM控制台。
2. 创建自定义策略OOSAutoBindTag。

   具体操作，请参见创建自定义权限策略。

   > **说明** 自定义策略OOSAutoBindTag以ECS实例为例，权限设置为 `ecs:DescribeInstances` ，您可以根据业务需求设置您需要的权限。例如：如果您需要为安全组批量绑定标签，将 `ecs:DescribeInstances` 替换为 `ecs:DescribeSecurityGroups` 。

   本步骤使用的策略如下所示：

   ```
   {
       "Version": "1",
       "Statement": [
           {
               "Action": [
                   "ecs:DescribeInstances",
                   "ecs:TagResources"
               ],
               "Resource": "*",
               "Effect": "Allow"
           }
       ]
   }
   ```

3. 创建RAM角色OOSServiceRole。

   具体操作，请参见创建普通服务角色。
4. 为RAM角色OOSServiceRole授权自定义策略OOSAutoBindTag。

   具体操作，请参见为RAM角色授权。
5. 为RAM角色OOSServiceRole授权系统策略AliyunOOSFullAccess。

   具体操作，请参见为RAM角色授权。

步骤二：为资源批量绑定标签

1. 登录OOS控制台。
2. 在左侧导航栏，单击**我的模板**。
3. 在顶部菜单栏左上角处，选择地域。
4. 创建自定义模板。
   i. 单击**创建模板**。
   ii. 在**基本信息**区域，输入模板名称（例如：OOSAutoBindTag）。
   iii. 单击**YAML**页签，编写模板代码，然后单击**创建模板**。

   模板代码示例：

```
FormatVersion: OOS-2019-06-01
Description: Tag Resources Without The Specified Tags
Parameters:
  tags:
    Type: Json
    Description:
      en: The tags to select ECS instances.
      zh-cn: 已绑定ECS实例的标签。
    AssociationProperty: Tags
  regionId:
    Type: String
    Description:
      en: The region to select ECS instances.
      zh-cn: 批量绑定标签的ECS实例所在地域。
  OOSAssumeRole:
    Description:
      en: The RAM role to be assumed by OOS.
      zh-cn: OOS使用的RAM角色。
    Type: String
    Default: OOSServiceRole
RamRole: OOSServiceRole
Tasks:
  - Name: getInstancesByTags
    Action: 'ACS::ExecuteAPI'
    Description: ''
    Properties:
      Service: ECS
      API: DescribeInstances
      Parameters:
        Tags: '{{ tags }}'
        RegionId: '{{ regionId }}'
    Outputs:
      InstanceIds:
        Type: List
        ValueSelector: 'Instances.Instance[].InstanceId'
  - Name: getAllInstances
    Action: 'ACS::ExecuteAPI'
    Description: ''
    Properties:
      Service: ECS
```

```
      API: DescribeInstances
      Parameters:
        RegionId: '{{regionId}}'
    Outputs:
      InstanceIds:
        Type: List
        ValueSelector: 'Instances.Instance[].InstanceId'
  - Name: TagResources_ECS_Instances
    Action: 'ACS::ExecuteAPI'
    Description:
      zh-cn: 为未绑定指定标签的ECS实例绑定标签。
      en: 'tag ecs instances, which are without the specified tags.'
    Properties:
      Service: ECS
      API: TagResources
      Parameters:
        Tags: '{{ tags }}'
        RegionId: '{{regionId}}'
        ResourceType: Instance
        ResourceIds:
          - '{{ACS::TaskLoopItem}}'
    Loop:
      MaxErrors: 100%
      Concurrency: 20
      Items:
        'Fn::Difference':
          - '{{ getAllInstances.InstanceIds }}'
          - '{{ getInstancesByTags.InstanceIds }}'
Outputs:
  InstanceIds:
    Type: List
    Value:
      'Fn::Difference':
        - '{{ getAllInstances.InstanceIds }}'
        - '{{ getInstancesByTags.InstanceIds }}'
```

参数说明：

- tags：已绑定ECS实例的标签。
- regionId：批量绑定标签的ECS实例所在地域。
- OOSAssumeRole：OOS使用的RAM角色。

权限说明：

- DescribeInstances：根据标签过滤资源。
- TagResources：为指定的资源创建并绑定标签。

5. 执行自定义模板。
   i. 在左侧导航栏，单击**我的模板**，找到自定义模板OOSAutoBindTag，在**操作**列，单击**创建执行**。
   ii. 保持默认设置或重新选择执行模式，然后单击**下一步：设置参数**。

iii. 填写参数，并单击**下一步：确定**。

本示例中填写的参数：

- tags：选择标签 `owner:zhangsan` 。
- reginId：输入实例所在的地域ID，例如： `cn-shanghai` 。
- oosAssumeRole：使用RAM角色OOSServiceRole。

iv. 单击**创建**。

v. 在基本详情页顶部，单击**高级视图**页签。

vi. 在高级视图页面右侧，单击**执行结果**。

vii. 查看执行结果。

- 如果执行成功，界面将显示如下信息：

- 如果执行失败，您可以通过查看执行日志来定位失败原因。

4.3.3. 使用运维编排服务批量启动带指定标签的ECS实例

企业在自动化运维中非常关键的一个环节就是如何快速找到批量运维的资源集合。资源标签与运维编排服务（OOS）的组合将此问题圆满解决。本文为您介绍如何在OOS中批量启动带指定标签的多台ECS实例。

步骤一：为ECS实例创建并绑定标签

在ECS控制台或标签控制台为ECS实例创建并绑定标签 `business:bigdata` 。如下以在标签控制台的操作为例：

1. 登录标签控制台。
2. 在左侧导航栏，选择**标签 > 标签**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义标签**页签，单击**创建自定义标签**。
5. 在**创建自定义标签**对话框，创建 `business:bigdata` 标签，并绑定已有ECS实例。

   具体操作，请参见创建并绑定自定义标签。

步骤二：在OOS批量启动带标签的ECS实例

在OOS控制台执行公共模板中的批量启动ECS实例（ACS-ECS-BulkyStartInstances），将执行目标设置为绑定了标签 `business:bigdata` 的ECS实例。

1. 登录OOS控制台。
2. 在左侧导航栏，单击**公共模板**。

3. 在顶部菜单栏左上角，选择地域。

> **说明** 默认情况下，某地域的OOS负责管理本地域的资源。例如，华东1（杭州）的OOS默认管理华东1（杭州）的ECS。但是，作为例外，用户可以在模板ExecuteAPI里指定RegionId的值，来调用其他地域的API（不建议这样做）。因此，此处OOS的地域请与步骤一：为ECS实例创建并绑定标签的ECS地域保持一致。关于OOS的使用限制，详情请参见使用限制。

4. 在**公共模板**页面，查找**ACS-ECS-BulkyStartInstances**，并单击**创建执行**。
5. 在**创建**页面，完成以下操作：
   i. **基本信息**保持默认设置，单击**下一步：设置参数**。

      其中**自动执行**模式，表示模板中的所有任务都会被自行执行，而不是单个拆分地执行。

   ii. 将**targets**设置为**指定实例的标签**，选择标签键和标签值为`business`和`bigdata`，将**执行使用到的权限的来源**设置为**当前账号的已有权限**。其余参数保持默认设置。

   iii. 单击**下一步：确定**。

   iv. 确认信息无误后，单击**创建**。
6. 在**实例列表**页签，查看执行结果。

   所有带有指定标签`business:bigdata`的ECS实例已完成批量启动。

4.3.4. 使用运维编排服务自动为ECS实例的相关资源绑定标签

ECS实例一般会配置云盘、弹性网卡、弹性公网IP等相关资源。当您为ECS实例绑定标签的时候，可以使用运维编排服务（OOS）为这些相关资源自动绑定标签，保证ECS实例与相关资源标签的一致性，方便后续维护。

背景信息

本示例中，将通过OOS自定义模板为ECS实例的相关资源（云盘、弹性网卡、弹性公网IP）自动绑定标签`owner:alice`。

> **说明** OOS模板、ECS实例、云盘、弹性网卡、弹性公网IP必须在同一地域下。

步骤一：创建RAM角色并授权

1. 使用阿里云账号登录RAM控制台。
2. 创建自定义权限策略OOSAutoTag，详情请参见创建自定义权限策略。

自定义权限策略OOSAutoTag内容如下所示：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "ecs:DescribeDisks",
                "ecs:DescribeInstances",
                "ecs:TagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:TagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

权限策略说明如下表所示：

权限策略	相关参数
允许查询ECS实例、弹性网卡、弹性公网IP的信息。	`ecs:DescribeInstances`
允许查询云盘的信息。	`ecs:DescribeDisks`
允许为ECS实例、云盘、弹性网卡创建并绑定标签。	`ecs:TagResources`
允许为弹性公网IP创建并绑定标签。	`vpc:TagResources`

3. 创建RAM角色OOSServiceRole。

   详情请参见创建普通服务角色。

4. 为RAM角色OOSServiceRole授权自定义策略OOSAutoTag。

   详情请参见为RAM角色授权。

5. 为RAM角色OOSServiceRole授权系统策略AliyunOOSFullAccess。

   详情请参见为RAM角色授权。

步骤二：创建并执行OOS模板

1. 登录OOS控制台。
2. 在左侧导航栏，单击**我的模板**。
3. 在顶部菜单栏左上角处，选择地域。
4. 创建自定义模板。
   i. 单击**创建模板**。

ii. 在**基本信息**区域，输入模板名称（例如：AutoTag）。

iii. 单击**JSON**页签，编写模板代码，然后单击**创建模板**。

模板代码示例：

```
{
  "FormatVersion": "OOS-2019-06-01",
  "Description": {
    "en": "When instance is labeled with the specified tag, Tags will be propagated
to the related resources.",
    "zh-cn": "当实例绑定特定标签时，传播标签到与实例相关的云盘、弹性网卡、弹性公网IP资源",
    "name-zh-cn": "当实例绑定特定标签时，传播标签到与实例相关的云盘、弹性网卡、弹性公网IP资
源",
    "categories": [
      "event-trigger"
    ]
  },
  "Parameters": {
    "TagKey": {
      "Type": "String",
      "Description": "Tag key for tag instance"
    },
    "TagValue": {
      "Type": "String",
      "Description": "Tag value for tag instance"
    },
    "OOSAssumeRole": {
      "Description": {
        "en": "The RAM role to be assumed by OOS.",
        "zh-cn": "OOS扮演的RAM角色"
      },
      "Type": "String",
      "Default": "OOSServiceRole"
    }
  },
  "RamRole": "{{ OOSAssumeRole }}",
  "Tasks": [
    {
      "Name": "eventTrigger",
      "Description": {
        "en": "Monitor the ECS instance TAG event.",
        "zh-cn": "监控实例标签变化"
      },
      "Action": "ACS::EventTrigger",
      "Properties": {
        "Product": "tag",
        "Name": [
          "Tag:ChangeOnResource"
        ],
        "Level": [
          "INFO"
        ],
        "Content": {
          "product": [
```

```
            "ecs"
          ],
          "resourceType": [
            "instance"
          ]
        }
      },
      "Outputs": {
        "instanceId": {
          "ValueSelector": ".content.resourceId",
          "Type": "String"
        },
        "isTag": {
          "ValueSelector": ".content.addedTags|select(.{{TagKey}}==\"{{TagValue}}\"
) |[.] |all|tostring",
          "Type": "String"
        }
      }
    },
    {
      "Name": "whetherNeedTag",
      "Action": "ACS::Choice",
      "Description": {
        "zh-cn": "判断是否需要传播的标签",
        "en": "Determine whether the tag needs to be propagated"
      },
      "Properties": {
        "DefaultTask": "describeInstancesFinally",
        "Choices": [
          {
            "When": {
              "Fn::Equals": [
                "true",
                "{{ eventTrigger.isTag }}"
              ]
            },
            "NextTask": "describeInstances"
          }
        ]
      }
    },
    {
      "Name": "describeInstances",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "zh-cn": "查询实例，获取与实例相关的弹性网卡、弹性公网IP资源",
        "en": "Query the instance to obtain the network interface and elastic publi
c network IP resources related to the instance."
      },
      "Properties": {
        "Service": "ECS",
        "API": "DescribeInstances",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "InstanceIds": [
```

```
            "{{ eventTrigger.instanceId }}"
          ]
        }
      },
      "Outputs": {
        "eips": {
          "Type": "List",
          "ValueSelector": "Instances.Instance[].EipAddress.AllocationId"
        },
        "enis": {
          "Type": "List",
          "ValueSelector": "Instances.Instance[].NetworkInterfaces.NetworkInterface
[].NetworkInterfaceId"
        }
      }
    },
    {
      "Name": "describeDisks",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "zh-cn": "根据实例ID获取云盘信息",
        "en": "Obtain disk ids based on instance id."
      },
      "Properties": {
        "Service": "ECS",
        "API": "DescribeDisks",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "InstanceId": "{{ eventTrigger.instanceId }}"
        }
      },
      "Outputs": {
        "diskIds": {
          "Type": "List",
          "ValueSelector": "Disks.Disk[].DiskId"
        }
      }
    },
    {
      "Name": "tagResourcesDisks",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "zh-cn": "标记云盘",
        "en": "Tag disks"
      },
      "Properties": {
        "Service": "ECS",
        "API": "TagResources",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "ResourceIds": [
            "{{ ACS::TaskLoopItem }}"
          ],
          "ResourceType": "disk",
```

```
        "Tags": [
          {
            "Key": "{{TagKey}}",
            "Value": "{{TagValue}}"
          }
        ]
      }
    },
    "Loop": {
      "RateControl": {
        "Mode": "Batch",
        "MaxErrors": 0,
        "Batch": [
          50
        ],
        "BatchPauseOption": "Automatic",
        "ConcurrencyInBatches": [
          1
        ]
      },
      "Items": "{{ describeDisks.diskIds }}"
    }
  },
  {
    "Name": "tagResourcesEnis",
    "Action": "ACS::ExecuteAPI",
    "Description": {
      "zh-cn": "标记弹性网卡",
      "en": "Tag network interface."
    },
    "Properties": {
      "Service": "ECS",
      "API": "TagResources",
      "Parameters": {
        "RegionId": "{{ ACS::RegionId }}",
        "ResourceIds": [
          "{{ ACS::TaskLoopItem }}"
        ],
        "ResourceType": "eni",
        "Tags": [
          {
            "Key": "{{TagKey}}",
            "Value": "{{TagValue}}"
          }
        ]
      }
    },
    "Loop": {
      "RateControl": {
        "Mode": "Batch",
        "MaxErrors": 0,
        "Batch": [
          50
        ],
```

```
          "BatchPauseOption": "Automatic",
          "ConcurrencyInBatches": [
            1
          ]
        },
        "Items": "{{ describeInstances.enis }}"
      }
    },
    {
      "Name": "tagResourcesEips",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "zh-cn": "标记弹性公网IP",
        "en": "Tag eips"
      },
      "Properties": {
        "Service": "VPC",
        "API": "TagResources",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "ResourceIds": [
            "{{ ACS::TaskLoopItem }}"
          ],
          "ResourceType": "eip",
          "Tags": [
            {
              "Key": "{{TagKey}}",
              "Value": "{{TagValue}}"
            }
          ]
        }
      },
      "Loop": {
        "RateControl": {
          "Mode": "Batch",
          "MaxErrors": 1,
          "Batch": [
            50
          ],
          "BatchPauseOption": "Automatic",
          "ConcurrencyInBatches": [
            1
          ]
        },
        "Items": "{{ describeInstances.eips }}"
      }
    },
    {
      "Name": "describeInstancesFinally",
      "Action": "ACS::ExecuteAPI",
      "Description": {
        "zh-cn": "查询实例状态",
        "en": "Views the ECS instances Status."
      },
```

```
      "Properties": {
        "Service": "ECS",
        "API": "DescribeInstances",
        "Parameters": {
          "RegionId": "{{ ACS::RegionId }}",
          "InstanceIds": [
            "{{ eventTrigger.instanceId }}"
          ]
        }
      },
      "Outputs": {
        "status": {
          "Type": "String",
          "ValueSelector": "Instances.Instance[].Status"
        }
      }
    }
  ],
  "Outputs": {
    "instanceId": {
      "Value": "{{ eventTrigger.instanceId}}",
      "Type": "String"
    },
    "diskIds": {
      "Value": "{{ describeDisks.diskIds }}",
      "Type": "String"
    },
    "eips": {
      "Value": "{{ describeInstances.eips  }}",
      "Type": "String"
    },
    "enis": {
      "Value": "{{ describeInstances.enis  }}",
      "Type": "String"
    }
  }
}
```

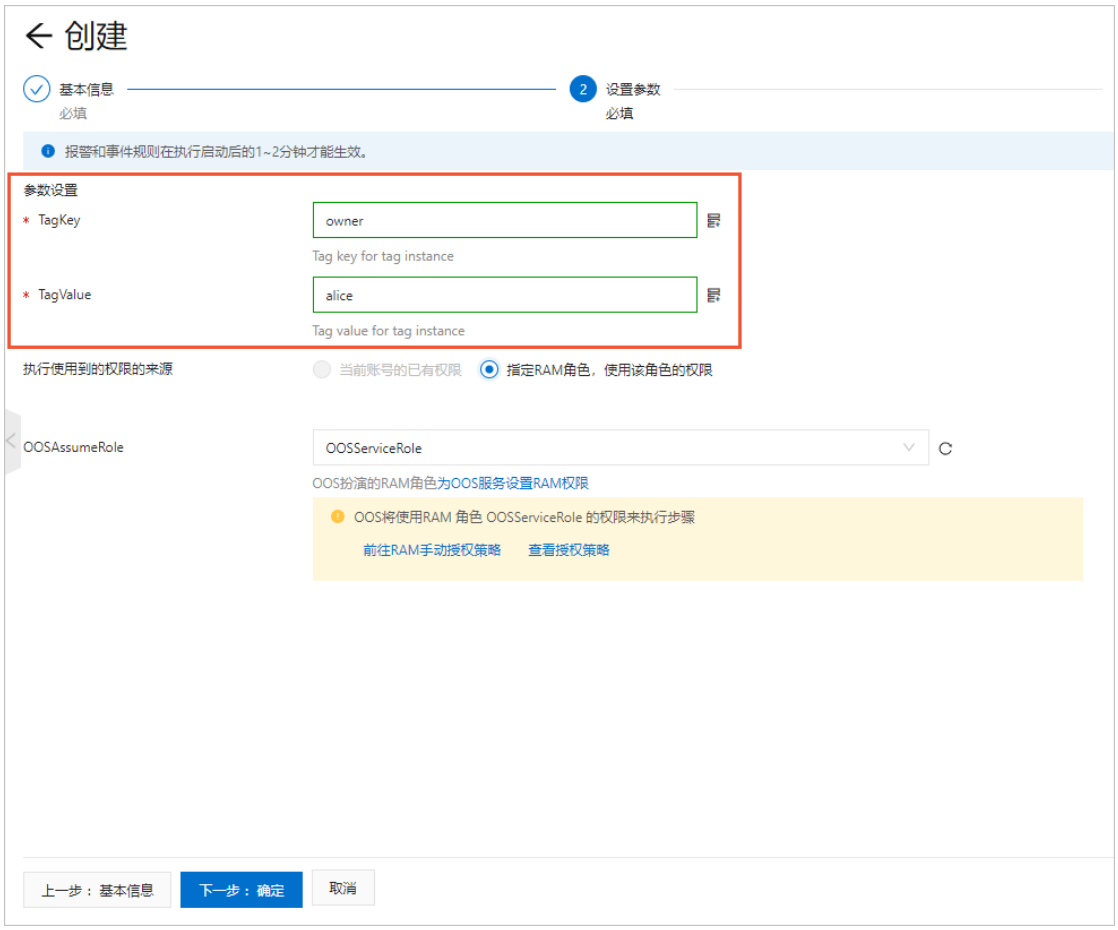
5. 执行自定义模板。

   i. 在左侧导航栏，单击**我的模板**，找到自定义模板AutoTag，在**操作**列，单击**创建执行**。

   ii. 保持默认设置，单击**下一步：设置参数**。

iii. 填写参数，并单击**下一步：确定**。

本示例中填写的参数如下：



- TagKey：输入标签键 `owner` 。
- TagValue：输入标签值 `alice` 。
- OOSAssumeRole：选择RAM角色OOSServiceRole。

iv. 单击**创建**。

步骤三：为ECS实例绑定标签

1. 登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在实例列表中，找到目标ECS实例，在**标签**列单击标签图标，为其绑定标签 `owner:alice` 。

执行结果

为ECS绑定标签的事件会自动触发OOS模板AutoTag的执行，该ECS实例下的云盘、弹性网卡、弹性公网IP会自动绑定标签 `owner:alice` 。

4.3.5. 使用运维编排服务批量继承ECS实例的标签

您可以使用运维编排服务（OOS）提供的公共模板创建执行，为ECS实例下的云盘、弹性网卡、弹性公网IP或快照批量继承ECS实例的标签，提高运维效率。

背景信息

本示例中，假设已为多个ECS实例绑定标签 `team:dev` ，且要求ECS实例下的云盘也继承绑定同样的标签。但实际情况可能是部分云盘漏绑定该标签，不符合要求。此时，您可以通过OOS的公共模板**ACS-TAG-ExtendEcsInstanceTagsByInputParams**，自动查找不符合要求的云盘并批量绑定该标签。

操作步骤

1. 登录OOS控制台。
2. 在左侧导航栏，单击**公共模板**。
3. 在顶部菜单栏左上角，选择地域。

> **说明** 默认情况下，某地域的OOS负责管理本地域的资源。例如，华东1（杭州）的OOS默认管理华东1（杭州）的ECS实例。但是，作为例外，用户可以在模板ExecuteAPI里指定RegionId的值，来调用其他地域的OpenAPI（不建议这样做）。因此，此处OOS的地域需要与ECS实例地域保持一致。关于OOS的使用限制，请参见使用限制。

4. 在**公共模板**中，查找ACS-TAG-ExtendEcsInstanceTagsByInputParams，并单击**创建执行**。
5. 在**基本信息**页面，填写执行的基本信息，然后单击**下一步：设置参数**。

   本示例中，**基本信息**采用默认值。

   > **说明** **执行模式**选择**自动执行**，表示模板中的所有任务都会被自行执行，而不是单个拆分地执行。

6. 在**设置参数**页面，设置执行的参数，然后单击**下一步：确定**。
   i. 在**地域ID**区域，选择ECS实例所在的地域。
   ii. 在**目标实例**区域，选择目标ECS实例。

   选择目标实例的方式有多种，您可以根据实际需要进行选择。本示例中，将通过**指定实例标签**的方式筛选绑定了标签 `team:dev` 的ECS实例。

   iii. 在**所需继承的标签键**区域，设置要继承的ECS实例标签键。

   本示例中，填写标签键 `team` 。此处支持填写多个标签键。

   iv. 在**继承标签的资源类型**区域，选择ECS实例下的资源类型。

   支持的资源类型：disk（云盘）、snapshot（快照）、eni（弹性网卡）和eip（弹性公网IP）。本示例中，选择disk（云盘）。

   v. 选择是否打开**如果标签键相同，是否覆盖标签值**开关。

   本示例中，选择打开开关。即当标签键相同，但标签值不同时，使用新的标签值覆盖原来的。

   vi. **OOS扮演的RAM角色**保持默认值。
7. 确认信息无误后，单击**创建**。

执行结果

如果执行状态显示成功，则表示已为ECS实例下的云盘批量继承了ECS实例的标签 `team:dev` 。您可以在ECS控制台的实例列表中，查看对应ECS实例下的云盘是否已成功绑定该标签。

4.3.6. 使用运维编排服务为ECS实例自动绑定操作系统类型标签

您可以使用运维编排服务（OOS）提供的公共模板创建执行，自动获取指定ECS实例的操作系统类型（例如：Windows、Linux），为该ECS实例自动绑定操作系统类型标签，方便运维。

操作步骤

1. 登录OOS控制台。
2. 在左侧导航栏，单击**公共模板**。
3. 在顶部菜单栏左上角，选择地域。

   > **说明** 默认情况下，某地域的OOS负责管理本地域的资源。例如，华东1（杭州）的OOS默认管理华东1（杭州）的ECS。但是，作为例外，用户可以在模板ExecuteAPI里指定RegionId的值，来调用其他地域的OpenAPI（不建议这样做）。因此，此处OOS的地域需要与ECS地域保持一致。关于OOS的使用限制，请参见使用限制。

4. 在**公共模板**中，查找**ACS-ECS-BulkyTagInstanceByOSType**，并单击**创建执行**。
5. 在**创建**页面，完成以下操作：
   i. **基本信息**保持默认设置，单击**下一步：设置参数**。

   > **说明** **执行模式**选择**自动执行**，表示模板中的所有任务都会被自行执行，而不是单个拆分地执行。

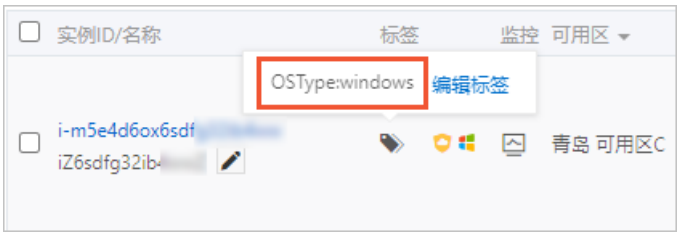
   ii. 将**targets**设置为**手动选择实例**，然后选择需要绑定标签的ECS实例。

> **说明** 支持批量选择多台ECS实例。

   iii. 将**tagKey**设置为**OSType**。
   iv. 单击**下一步：确定**。
   v. 确认信息无误后，单击**创建**。

执行结果

在ECS控制台的实例列表中，查看对应ECS实例是否已经成功绑定操作系统类型标签。例如：Windows操作系统的ECS实例会自动绑定 `OSType:windows` 标签，如下图所示。



4.3.7. 使用运维编排服务为ECS实例自动绑定Linux内核版本标签

您可以使用运维编排服务（OOS）提供的公共模板创建执行，自动获取指定ECS实例的Linux内核版本信息，为该ECS实例自动绑定Linux内核版本标签，方便运维。

操作步骤

1. 登录OOS控制台。
2. 在左侧导航栏，单击**公共模板**。
3. 在顶部菜单栏左上角，选择地域。

   > **说明** 默认情况下，某地域的OOS负责管理本地域的资源。例如，华东1（杭州）的OOS默认管理华东1（杭州）的ECS。但是，作为例外，用户可以在模板ExecuteAPI里指定RegionId的值，来调用其他地域的OpenAPI（不建议这样做）。因此，此处OOS的地域需要与ECS地域保持一致。关于OOS的使用限制，请参见使用限制。

4. 在**公共模板**中，查找**ACS-ECS-BulkyTagInstanceByLinuxKernelVersion**，并单击**创建执行**。
5. 在**创建**页面，完成以下操作：
   i. **基本信息**保持默认设置，单击**下一步：设置参数**。

      > **说明** **执行模式**选择**自动执行**，表示模板中的所有任务都会被自行执行，而不是单个拆分地执行。

ii. 将targets设置为**手动选择实例**，然后选择需要绑定标签的ECS实例。

> **说明**
>
> - 支持批量选择多台ECS实例。
> - 您只能选择Linux操作系统的ECS实例，不能选择Windows操作系统的ECS实例。否则，会执行失败。

iii. 将tagKey设置为KernelVersion。

iv. 单击**下一步：确定**。

v. 确认信息无误后，单击**创建**。

执行结果

在ECS控制台的实例列表中，查看对应ECS实例是否已经成功绑定Linux内核版本标签。

4.3.8. 使用配置审计查找未绑定指定标签的资源

本文为您介绍如何使用配置审计（Config）查找未绑定指定标签的资源，让资源管理变得更加轻松。

前提条件

请确保您的资源标签符合设计原则。详情请参见标签设计最佳实践。

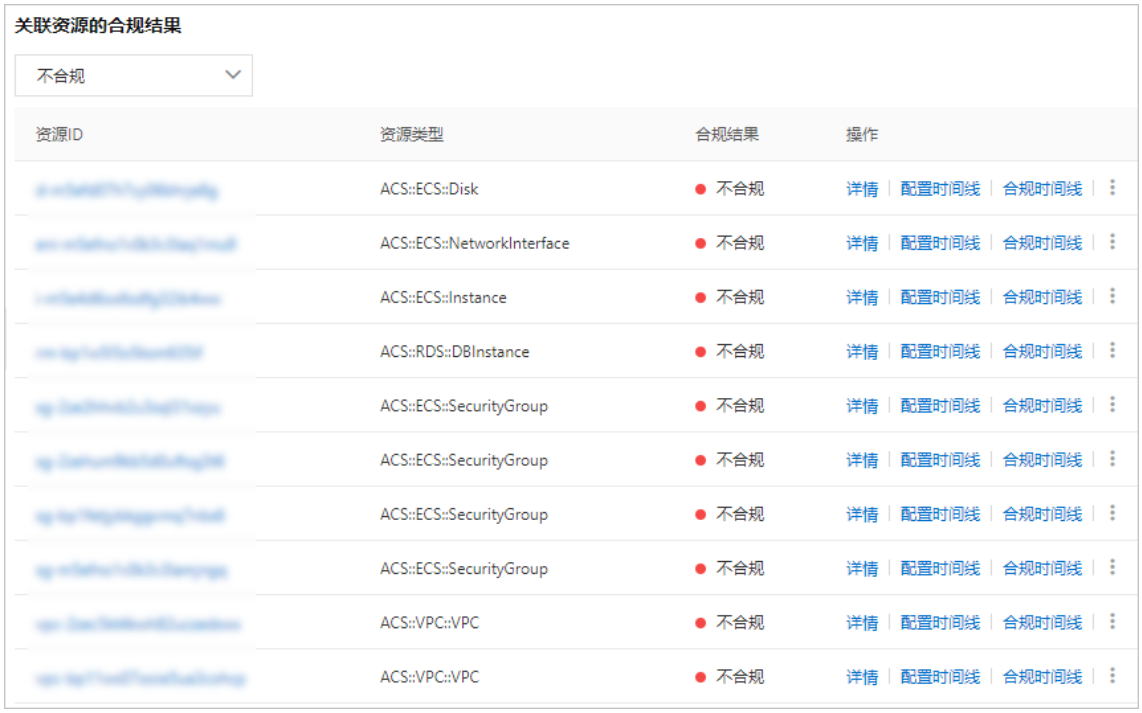
操作步骤

1. 登录配置审计控制台。
2. 在左侧导航栏，单击**规则**。
3. 在**规则**页面，单击**新建规则**。
4. 在**新建规则**页面，查找托管规则required-tags，然后单击**应用规则**。
5. 在**基本属性**页面，设置规则名称、风险等级和备注，然后单击**下一步**。
6. 在**评估资源范围**页面，选中资源类型，然后单击**下一步**。

   本示例中，需要查找ECS、EIP、OSS和RDS中未绑定指定标签的资源，所以此处选中ECS、EIP、OSS和RDS。
7. 在**参数设置**页面，设置指定的标签键和标签值，然后单击**下一步**。
8. 在**修正设置**页面，选中**修正设置**复选框，设置修正执行方式，然后单击**下一步**。

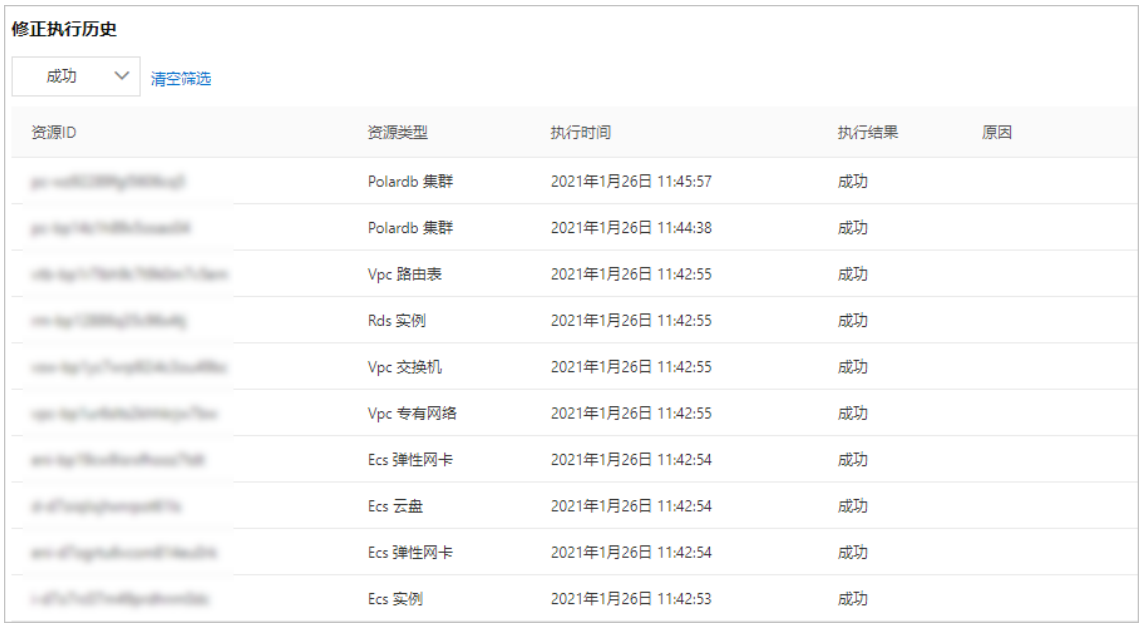
   修正执行方式有以下几种：
   - **自动执行**：当检测到不合规资源时，将自动执行修正。
   - **手动执行**：当检测到不合规资源时，您需要手动执行修正。
9. 在**预览并保存**页面，单击**提交**。
10. 单击**查看规则详情**，查看规则详情。
    - 在**规则详情**页签，查看资源的合规结果。

      配置审计为您找到了未绑定指定标签的资源，如下图所示。



- 在**修正详情**页签，查看修正执行历史。

  如果执行了修正设置，配置审计就会为未绑定指定标签的资源自动绑定标签，如下图所示。



后续操作

您可以设置发送资源不合规事件到消息服务（MNS）。具体操作，请参见设置投递数据到消息服务MNS。

4.3.9. 使用操作审计为资源自动绑定标签

本文为您提供了一个自动化绑定标签程序，用于为新创建的资源自动绑定创建者标签，标识该资源的创建者，以此提升分账效率。您可以借助操作审计（ActionTrail）的跟踪功能，实现该任务。

前提条件

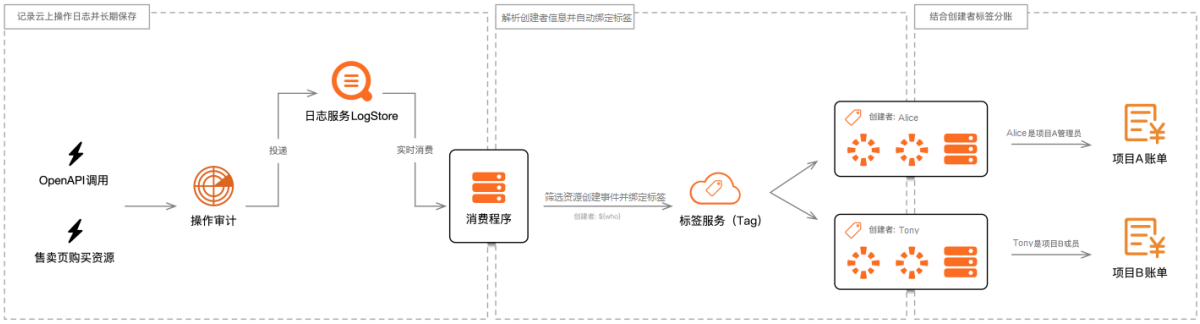
运行程序前，请确保您已开通以下云服务：

- 访问控制（RAM）
- 操作审计（ActionTrail）
- 函数计算（FC）
- 日志服务（SLS）

> **说明** 访问控制和操作审计目前免费。但您使用操作审计时用到的日志服务、函数计算这两个云服务，在超出免费额度后，会产生少量费用。更多信息，请参见日志服务计费说明、函数计算计费说明。

方案介绍

操作审计会记录阿里云账号内的操作日志，这份操作日志可以被实时消费。因此我们可以部署一个消费程序，在处理到资源创建对应的操作事件时，调用标签服务的API，为资源绑定创建者标签。最后，在用户中心通过标签进行分账。工作流程如下图所示：



1. 在操作审计中创建跟踪。

   使用操作审计的跟踪功能，记录云上操作日志，并投递到日志服务中。

2. 在日志服务中消费日志数据。

   消费方式可以选择函数计算、Flink或是自行开发的程序。本程序采用的是函数计算。

   在完成消费后，调用标签服务的API，为资源绑定标签。

3. 在用户中心查看分账账单。

   您可以基于资源的创建者标签，通过用户中心的分账账单、费用分析或财务单元等功能，查看费用分摊账单。

部署程序

以下步骤以VPC为例。在程序部署完成后，当您创建了VPC，系统会自动为该VPC绑定创建者标签。

1. 访问实时消费操作审计日志并自动绑定资源标签。
2. 在弹出的对话框中，单击**确认**，克隆代码到CloudShell。
3. 输入以下命令，一键创建跟踪并部署自动绑定标签程序。

   ```
   ./install.sh
   ```

4. 在程序部署完成后，请等待至少1分钟，然后输入以下命令，创建1个VPC，用来验证自动绑定标签程序是否已经生效。

   ```
   sleep 60
   CREATED_VPC_ID=`aliyun vpc CreateVpc --RegionId cn-huhehaote | jq ".VpcId"`
   ```

5. 请等待1~5分钟，然后输入以下命令，查看刚创建的VPC是否绑定了创建者标签。

```
aliyun vpc DescribeVpcs --RegionId cn-huhehaote --VpcId $CREATED_VPC_ID | jq ".Vpcs.Vpc
[0].Tags"
```

如果返回如下信息，说明该VPC已成功绑定创建者标签。

```
{
  "Tag": [
    {
      "Key": "created_by",
      "Value": "ram-user:221357305020244****"
    }
  ]
}
```

（可选）删除资源

输入以下命令，删除程序中创建的所有资源。删除后，自动绑定标签程序将失效。

```
./uninstall.sh
```

（可选）修改资源类型

上述程序支持为以下资源类型自动绑定创建者标签：

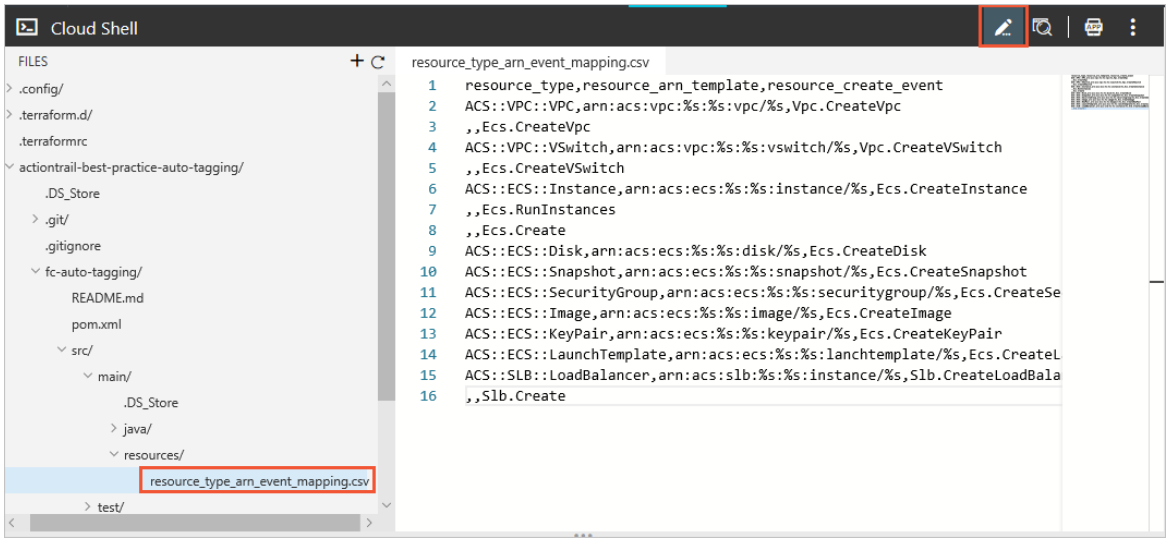
- 云服务器ECS：ECS实例、云盘、快照、安全组、镜像、密钥对和启动模板。
- 云数据库RDS实例。
- 负载均衡SLB实例。
- 专有网络VPC：专有网络、交换机。

您也可以尝试修改程序的配置文件，为其他资源类型自动绑定创建者标签。资源类型必须支持操作审计和标签，详情请参见支持操作审计的资源类型、支持标签的云服务。

1. 在CloudShell右上角，单击编辑器图标，找到并复制resource_type_arn_event_mapping.csv文件里的内容，然后保存CSV格式的文件到本地。

   resource_type_arn_event_mapping.csv文件访问路径如下：

   actiontrail-best-practice-auto-tagging/fc-auto-tagging/src/main/resources/resource_type_arn_event_mapping.csv



2. 在本地修改resource_type_arn_event_mapping.csv文件中的资源类型。
3. 将新修改的内容复制到CloudShell的resource_type_arn_event_mapping.csv文件中。
4. 输入以下命令，重新部署程序。

```
./reinstall.sh
```

4.3.10. 使用标签将ECS实例自动加入云监控应用分组

在弹性伸缩（Auto Scaling）中通过伸缩组自动创建绑定特定标签的实例，然后在云监控（CloudMonitor）中配置基于标签的应用分组规则，将实例自动进行分组，方便进行集中的运维管理。该方案具备服务自发现、应用高可用和运维自动化等特点。

背景信息

- 云监控支持自动化分组的云产品：云服务器ECS（只支持ECS实例，不支持网卡、磁盘等）、云数据库RDS和负载均衡SLB。
- 本文以弹性伸缩组内自动创建的ECS实例为例，该ECS实例需要绑定的标签为 `team:dev` 。

步骤一：在弹性伸缩中创建绑定标签的ECS实例

1. 登录弹性伸缩控制台。
2. 创建伸缩组。具体操作，请参见创建伸缩组。

   请根据业务需求选择**均衡分布策略**，从而实现高可用的自动扩缩容。
3. 创建伸缩配置，创建ECS实例，并为ECS实例绑定标签 `team:dev` 。具体操作，请参见创建伸缩配置（ECS实例）。

4. 在伸缩组列表中，单击伸缩组名称，然后在**实例列表**页签，查看伸缩组自动创建的ECS实例。

步骤二：在云监控中创建应用分组

1. 登录云监控控制台。
2. 创建云监控应用分组。具体操作，请参见创建应用分组。

   其中，创建方式和匹配规则如下所示：

   - 创建方式：选择**智能标签同步创建**。

   - 匹配规则：设置资源标签键`team`，标签值可根据您的需求设定范围，本示例设定范围为**包含**`dev`。

3. 在应用分组页面的搜索区域，选择**资源标签**，并通过标签键`team`搜索应用分组。

4. 单击应用分组名称，查看组内资源。
   伸缩组自动创建的ECS实例，已经自动添加至该应用分组。

   您还可以查看ECS实例的监控数据。更多信息，请参见概览。

4.3.11. 使用资源编排为云资源批量绑定或更新标签

您可以使用资源编排服务ROS（Resource Orchestration Service）创建资源栈，在资源栈中创建资源，并同时为资源绑定标签，方便日后的运维管理。支持为多个云资源批量绑定或更新标签，提升运维效率。

背景信息

本文将使用ROS Python SDK创建资源栈。更多信息，请参见Python SDK使用示例。

为多个云资源绑定相同标签

如下将提供一个示例，使用资源栈创建专有网络VPC `mytest-vpc` 和交换机vSwitch `mytest-vsw-h` ，并同时为VPC和vSwitch绑定 `app:test` 标签。

1. 编写模板。

```
{
  "ROSTemplateFormatVersion": "2015-09-01",
  "Resources": {
    "VPC": {
      "Type": "ALIYUN::ECS::VPC",
      "Properties": {
        "VpcName": "mytest-vpc"
      }
    },
    "VSwitch": {
      "Type": "ALIYUN::ECS::VSwitch",
      "Properties": {
        "VpcId": { "Ref": "VPC" },
        "ZoneId": "cn-hangzhou-h",
        "CidrBlock": "172.16.0.0/24",
        "VSwitchName": "mytest-vsw-h"
      }
    }
  }
}
```

   模板说明：创建一个VPC和一个vSwitch。

2. 创建资源栈，并为VPC和vSwitch绑定标签 `app:test` 。

```
# pip install aliyun-python-sdk-ros
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkros.request.v20190910.CreateStackRequest import CreateStackRequest
client = AcsClient(
    '<AccessKeyId>',
    '<AccessKeySecret>',
    'cn-hangzhou',
)
template = '''
<Template>
'''
req = CreateStackRequest()
req.set_StackName('vpc-vswitch-test')
req.set_TemplateBody(template)
req.set_TimeoutInMinutes(10)
req.set_Tags([{'Key': 'app', 'Value': 'test'}])
ret = client.do_action_with_exception(req)
print(ret)
```

参数说明：

- <AccessKeyId>和<AccessKeySecret>请替换为您实际的AccessKey ID 和AccessKey Secret。
- <Template>请替换为步骤1中的模板。

3. （可选）登录专有网络管理控制台，查看VPC和vSwitch绑定的标签。

   当VPC和vSwitch都绑定了标签 `app:test` ，表示操作成功。

为多个云资源绑定不同标签

如下将提供一个示例，使用资源栈创建专有网络VPC `mytest-vpc` 和交换机vSwitch `mytest-vsw-h` ，为VPC和vSwitch绑定通用标签 `app:test` ，除此之外还要为vSwitch绑定特定标签 `group:test` 。最终效果为：

- VPC `mytest-vpc` 绑定的标签： `app:test` 。
- vSwitch `mytest-vsw-h` 绑定的标签： `app:test` 和 `group:test` 。

1. 编写模板。

```
{
  "ROSTemplateFormatVersion": "2015-09-01",
  "Resources": {
    "VPC": {
      "Type": "ALIYUN::ECS::VPC",
      "Properties": {
        "VpcName": "mytest-vpc"
      }
    },
    "VSwitch": {
      "Type": "ALIYUN::ECS::VSwitch",
      "Properties": {
        "VpcId": { "Ref": "VPC" },
        "ZoneId": "cn-hangzhou-h",
        "CidrBlock": "172.16.0.0/24",
        "VSwitchName": "mytest-vsw-h",
        "Tags": [{ "Key": "group", "Value": "test" }]
      }
    }
  }
}
```

模板说明：创建一个VPC和一个vSwitch，并为vSwitch绑定特定标签 `group:test` 。

2. 创建资源栈，并为VPC和vSwitch绑定通用标签 `app:test` 。

```
# pip install aliyun-python-sdk-ros
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkros.request.v20190910.CreateStackRequest import CreateStackRequest
client = AcsClient(
    '<AccessKeyId>',
    '<AccessKeySecret>',
    'cn-hangzhou',
)
template = '''
<Template>
'''
req = CreateStackRequest()
req.set_StackName('vpc-vswitch-test')
req.set_TemplateBody(template)
req.set_TimeoutInMinutes(10)
req.set_Tags([{'Key': 'app', 'Value': 'test'}])
ret = client.do_action_with_exception(req)
print(ret)
```

参数说明：

- <AccessKeyId>和<AccessKeySecret>请替换为您实际的AccessKey ID 和AccessKey Secret。
- <Template>请替换为步骤1中的模板。

3. （可选）登录专有网络管理控制台，查询VPC和vSwitch绑定的标签。

   当VPC绑定的标签为 `app:test` ，vSwitch绑定的标签为 `app:test` 和 `group:test` 时，表示操作成功。

为多个云资源更新标签

如下将提供一个示例，在为多个云资源绑定相同标签的基础上，将VPC `mytest-vpc` 和vSwitch `mytest-vsw-h` 已绑定的标签 `app:test` 更新为 `app:normal` 。

1. 创建资源栈，并为VPC和vSwitch绑定新标签 `app:normal` 。

```
# pip install aliyun-python-sdk-ros
import json
from aliyunsdkcore.client import AcsClient
from aliyunsdkros.request.v20190910.UpdateStackRequest import UpdateStackRequest
client = AcsClient(
    '<AccessKeId>',
    '<AccessKeySecret>',
    'cn-hangzhou',
)
template = '''
<Template>
'''
req = UpdateStackRequest()
req.set_StackId('<StackId>')
req.set_TemplateBody(template)
req.set_Tags([{'Key': 'app', 'Value': 'normal'}])
ret = client.do_action_with_exception(req)
print(ret)
```

   参数说明：

   - <AccessKeyId>和<AccessKeySecret>请替换为您实际的AccessKey ID 和AccessKey Secret。
   - <Template>请替换为为多个云资源绑定相同标签中的模板。

2. （可选）登录专有网络管理控制台，查询VPC和vSwitch绑定的标签。

   当VPC和vSwitch都绑定了新标签 `app:normal` 时，表示操作成功。

4.4. 使用标签控制资源访问

4.4.1. 创建带特定标签的资源

标签与RAM的结合使用，能够让不同的RAM用户根据标签拥有不同的云资源访问和操作权限。本文介绍如何为RAM用户授权自定义策略，使该RAM用户在创建ECS资源时必须绑定特定标签，否则无法创建。

前提条件

请确保您已使用阿里云账号创建了一个RAM用户，详情请参见创建RAM用户。

步骤一：创建自定义策略并为RAM用户授权

本步骤中，将为RAM用户userTest授权自定义策略BindTagForRes，使该RAM用户在创建ECS资源时，必须选择带有标签的VPC并且必须绑定特定标签。本示例中，VPC绑定的标签为 `user:lisi` ，ECS实例必须绑定的特定标签为 `owner:zhangsan` 。

1. 使用阿里云账号登录RAM控制台。
2. 创建自定义策略BindTagForRes，详情请参见创建自定义权限策略。

自定义策略如下所示：

```
{
    "Statement": [
        {
           "Effect": "Allow",
            "Action": "ecs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:tag/owner": "zhangsan"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ecs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "vpc:tag/user": "lisi"
                }
            }
        },
        {
            "Action": [
                "ecs:DescribeTagKeys",
                "ecs:ListTagResources",
                "ecs:DescribeTags",
                "ecs:DescribeKeyPairs",
                "ecs:DescribeImages",
                "ecs:DescribeSecurityGroups",
                "ecs:DescribeLaunchTemplates",
                "ecs:DescribeDedicatedHosts",
                "ecs:DescribeDedicatedHostTypes",
                "ecs:DescribeAutoSnapshotPolicyEx",
                "vpc:DescribeVpcs",
                "vpc:DescribeVSwitches",
                "bss:PayOrder"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ecs:DeleteTags",
                "ecs:UntagResources",
                "ecs:CreateTags",
                "ecs:TagResources"
            ],
            "Resource": "*"
        }
    ],
```

```
    "Version": "1"
}
```

权限策略说明如下表所示：

权限策略	相关参数
创建或访问已绑定标签的资源的权限	`"ecs:tag/owner": "zhangsan"`
允许查询标签的接口权限	○ `ecs:DescribeTagKeys` ○ `ecs:ListTagResources` ○ `ecs:DescribeTags`
允许查询ECS资源的接口权限	○ `ecs:DescribeKeyPairs` ○ `ecs:DescribeImages` ○ `ecs:DescribeSecurityGroups` ○ `ecs:DescribeLaunchTemplates` ○ `ecs:DescribeDedicatedHosts` ○ `ecs:DescribeDedicatedHostTypes` ○ `ecs:DescribeAutoSnapshotPolicyEx`
允许查询VPC资源的接口权限	○ `vpc:DescribeVpcs` ○ `vpc:DescribeVSwitches`
允许支付订单的接口权限	`bss:PayOrder`
不允许操作标签相关的接口权限	○ `ecs:DeleteTags` ○ `ecs:UntagResources` ○ `ecs:CreateTags` ○ `ecs:TagResources`
VPC绑定标签策略	`"vpc:tag/user": "lisi"`

3. 将自定义策略BindTagForRes授权给RAM用户userTest。详情请参见为RAM用户授权。

步骤二：为专有网络VPC绑定标签

步骤一：创建自定义策略并为RAM用户授权中的自定义策略规定了创建ECS时需要选择带有`user:lisi`标签的专有网络VPC，因此需要为VPC绑定标签。如果VPC没有绑定特定标签，在创建ECS时会没有权限。

> **说明** 如果您没有VPC，请先创建VPC。详情请参见创建和管理专有网络。

1. 登录标签控制台。
2. 在左侧导航栏，选择**标签 > 标签**。

3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义标签**页签，单击**创建自定义标签**。
5. 在**创建自定义标签**对话框，创建 `user:lisi` 标签，并绑定已有VPC。

   具体操作，请参见创建并绑定自定义标签。

步骤三：创建ECS并绑定标签

通过RAM用户userTest登录ECS管理控制台，创建ECS并绑定标签。

1. 使用RAM用户登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 单击**创建实例**，创建ECS实例。

> **说明** 必须选择步骤二：为专有网络VPC绑定标签中绑定标签 `user:lisi` 的VPC，并且为ECS实例绑定特定标签 `owner:zhangsan`，才能创建成功。若未绑定特定标签，则会创建失败，提示**您没有权限进行此操作**。

相关文档

您还可以为已有的资源绑定特定标签，实现对资源的访问控制，并对带特定标签的资源进行访问。详情请参见使用标签控制资源的访问。

4.4.2. 使用标签控制ECS资源的访问

云服务器ECS资源绑定标签后，您可以使用标签为资源做分类并控制访问。本文以ECS实例为例，介绍如何为RAM用户授权特定的策略，使该RAM用户能够通过标签控制ECS实例的访问。

前提条件

已使用阿里云账号创建一个RAM用户，详情请参见创建RAM用户。

背景信息

标签是云资源的标识，可以帮助您从不同的维度对具有相同特征的云资源进行分类、搜索和聚合，使资源管理更加容易。每个云资源均支持绑定多个标签。支持标签的云服务和资源类型，详情请参见支持标签的云服务、支持标签API的资源类型。

阿里云的用户权限是基于策略为管理主体的，您可以根据不同用户的职责配置RAM策略。在策略中，您可以定义多个标签，然后将一个或多个策略授权给RAM用户或用户组。如果要控制RAM用户可以访问哪些资源，您可以创建自定义策略并使用标签来实现访问控制。

默认情况下，资源列表将展示本地域中所有的资源，如果您希望为RAM用户设置查看资源的范围，您可以通过创建自定义策略，利用标签控制RAM用户对资源的访问。

步骤一：创建自定义策略并为RAM用户授权

本步骤将使用阿里云账号创建一个自定义策略UseTagAccessRes（规定了RAM用户需要指定标签 `owner:zhangsan` 和 `environment:production` 后方可访问ECS资源），并将自定义策略UseTagAccessRes授权给RAM用户userTest。

1. 使用阿里云账号登录RAM控制台。
2. 创建自定义策略UseTagAccessRes。

   具体操作，请参见创建自定义权限策略。

   如下所示，您可以在策略中为云资源设置多个标签。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ecs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ecs:tag/owner": "zhangsan",
                    "ecs:tag/environment": "production"
                }
            }
        },
        {
            "Action": [
                "ecs:DescribeTagKeys",
                "ecs:DescribeTags"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "ecs:DeleteTags",
                "ecs:UntagResources",
                "ecs:CreateTags",
                "ecs:TagResources"
            ],
            "Resource": "*"
        }
    ],
    "Version": "1"
}
```

权限策略	内容	说明
访问带标签资源的权限	○ `"ecs:tag/owner": "zhangsan"` ○ `"ecs:tag/environment": "production"`	控制绑定该标签的资源的访问。
允许查询标签的接口权限	○ `ecs:DescribeTagKeys` ○ `ecs:DescribeTags`	ECS控制台需要支持标签查询的权限。
不允许操作标签相关的接口权限	○ `ecs:DeleteTags` ○ `ecs:UntagResources` ○ `ecs:CreateTags` ○ `ecs:TagResources`	权限中不允许出现与操作标签有关的接口，避免用户因修改标签导致没有权限。

3. 将自定义策略授权给RAM用户userTest。

   具体操作，请参见为RAM用户授权。

步骤二：为ECS实例绑定标签

本步骤将使用阿里云账号为ECS实例绑定特定标签。

> **说明** 如果您没有ECS实例，请先创建ECS实例。详情请参见创建方式导航。

1. 登录标签控制台。
2. 在左侧导航栏，选择**标签 > 标签**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**自定义标签**页签，单击**创建自定义标签**。
5. 在**创建自定义标签**对话框，创建 `owner:zhangsan` 和 `environment:production` 标签，并绑定已有ECS实例。

   具体操作，请参见创建并绑定自定义标签。

步骤三：访问带标签的ECS实例

本步骤将使用RAM用户userTest（已授权自定义策略UseTagAccessRes）登录ECS控制台，访问带标签的ECS实例。

1. 使用RAM用户登录ECS管理控制台。
2. 在左侧导航栏，选择**实例与镜像 > 实例**。
3. 在顶部菜单栏左上角处，选择地域。
4. 在**实例**页面，单击搜索栏旁边的**标签**，选择 `owner:zhangsan` 和 `environment:production` 标签。

5. 查看仅绑定了 `owner:zhangsan` 和 `environment:production` 标签的资源。